Introduction à la combinatoire
Notes de cours

Professeur : François Bergeron

Hiver 2010

UQÀM **Université du Québec à Montréal**
Département de mathématiques
Case postale 8888, Succursale Centre-Ville
Montréal (Québec) H3C 3P8

Table des matières

1 Ensembles et fonctions **5**
- 1.1 Introduction . . . 5
- 1.2 Ensembles . . . 5
- 1.3 Fonctions . . . 12
- 1.4 Compter les éléments d'un ensemble . . . 22
- 1.5 Multi-sous-ensembles et monômes . . . 31
- 1.6 Suite et séries génératrices . . . 34
- 1.7 Exercices . . . 38

2 Relations et graphes **45**
- 2.1 Introduction . . . 45
- 2.2 Relations sur un ensemble . . . 45
- 2.3 Relation d'équivalence . . . 51
- 2.4 Bijections naturelles$^{(*)}$ . . . 59
- 2.5 Ordres . . . 60
- 2.6 Chemins dans un graphe orienté . . . 68
- 2.7 Arbres . . . 74
- 2.8 Endofonctions . . . 77
- 2.9 Exercices . . . 78

3 Mots, langages, automates et chemins **83**
- 3.1 Introduction. . . . 83
- 3.2 Mots . . . 84
- 3.3 Langages . . . 86
- 3.4 Automates . . . 90
- 3.5 Chemins dans le réseau $\mathbb{N} \times \mathbb{N}$ . . . 92
- 3.6 Aire de chemin . . . 94
- 3.7 Chemins de Dyck . . . 97
- 3.8 Chemins de Dyck avec poids . . . 102

3.9 Exercices . . . 102

4 Diverses structures combinatoires 105
4.1 Introduction. . . . 105
4.2 Arbres binaires . . . 105
4.3 Arbres binaires croissants . . . 107
4.4 Arbres plans . . . 109
4.5 Triangulations d'un polygone . . . 109
4.6 Configurations de Catalan . . . 110
4.7 Fonction de stationnement . . . 114
4.8 Polyominos . . . 118
4.9 Exercices . . . 121

5 Permutations et partitions 123
5.1 Introduction. . . . 123
5.2 Permutations . . . 123
5.3 Partages . . . 136
5.4 Diagrammes de Ferrers . . . 137
5.5 Énumération de partages . . . 139
5.6 Théorème pentagonal d'Euler . . . 142
5.7 Tableaux de Young . . . 146
5.8 Formule des équerres . . . 147
5.9 Correspondance RSK . . . 148
5.10 Exercices . . . 151

6 Introduction à la théorie des espèces 157
6.1 Introduction. . . . 157
6.2 Espèces de structures. . . . 157
6.3 Exemples d'espèces . . . 159
6.4 Espèces auxiliaires simples. . . . 165
6.5 Isomorphisme d'espèces (bijections naturelles). . . . 167
6.6 Somme et produit. . . . 168
6.7 Dessins de structures génériques. . . . 170
6.8 Passage aux séries. . . . 172
6.9 Exemples de calcul de séries. . . . 173
6.10 Substitution. . . . 175
6.11 Exemples de substitutions. . . . 176
6.12 L'espèce des arborescences. . . . 178
6.13 Dérivée et pointage. . . . 178
6.14 Vertébrés. . . . 180

6.15 Isomorphisme de structures et types de structures. 182
6.16 Énumération de structures non étiquetées 182
6.17 Espèces à plusieurs sortes 185
6.18 Exercices 187

Appendices **190**

A Calcul formel **191**
A.1 Introduction 191
A.2 Théorie des ensembles et calcul formel 192
A.3 Le package GFUN 196
A.4 Analogues polynomiaux 198

B Séries génératrices pour des nombres bien connus **203**

C Notations **207**

Introduction

Répondre à des questions du genre

Quelles sont les façons de ... ?
Quelles sont les diverses possibilités de ... ?
De combien de façons peut-on ... ?

est parfois assez difficile. Une première étape, essentielle à la résolution du problème, consiste à clarifier la signification des « ... ». Mathématiser le problème soulevé demande alors de décrire précisément un certain ensemble fini, dont les éléments sont les diverses possibilités dont il est question dans cette partie de la question. On cherchera alors comment énumérer (lister, classifier) les éléments de cet ensemble, ou plus simplement comment les « compter »[1]. Très souvent, ces deux objectifs ne vont pas l'un sans l'autre. En effet, on ne peut être certain d'avoir bien compté toutes les possibilités, que si l'on est certain de bien savoir quelles sont ces possibilités.

La situation est très souvent la suivante. Pour chaque entier positif n, on considère un ensemble A_n de « configurations », ou « structures d'une certaine espèce ». Ici, l'entier n mesure la « taille » des structures considérées, qui est souvent le nombre « d'atomes » à partir desquels ces structures sont construites. Le problème typique consiste alors à trouver une « formule » pour le nombre d'éléments de A_n, en fonction de la taille n. On dit alors qu'on a énuméré les éléments des ensembles A_n. Une des principales stratégies employées pour s'attaquer à ce problème d'énumération consiste à décomposer les structures étudiées en amalgames de structures plus simples. On espère ainsi se ramener à compter le nombre d'éléments d'ensembles plus simples.

Bien entendu, l'intérêt d'un problème donné dépend de l'importance d'énumérer les objets considérés, soit dans un contexte mathématique, soit pour les besoins d'une autre science comme la physique, la biologie ou l'informatique. Historiquement, la combinatoire est perçue par plusieurs comme liée au calcul de probabilités via une formule du genre :

$$\text{probabilité de gagner} = \frac{\text{nombre de configurations gagnantes}}{\text{nombre total de configurations}}.$$

1. Les guillemets sont utilisés dans ce texte pour souligner que l'on utilise informellement un terme qui aurait avantage à être défini précisément. Une partie de notre travail consistera à dégager clairement de bonnes définitions pour ces termes, ou d'autres mieux adaptés aux problèmes considérés.

Par exemple, on calcule que 1/6 est la probabilité d'obtenir un total de 7 en lançant deux dés, puisque c'est

$$\frac{1}{6} = \frac{\left|\left\{\text{⚁⚀}, \text{⚂⚁}, \text{⚃⚂}, \text{⚄⚃}, \text{⚅⚄}, \text{⚀⚅}\right\}\right|}{|\mathcal{D}|},$$

où $\mathcal{D}$ est l'ensemble des 36 résultats possible :

$$\mathcal{D} = \Big\{\text{⚀⚀}, \text{⚁⚀}, \text{⚂⚀}, \text{⚃⚀}, \text{⚄⚀}, \text{⚅⚀},$$
$$\text{⚀⚁}, \text{⚁⚁}, \text{⚂⚁}, \text{⚃⚁}, \text{⚄⚁}, \text{⚅⚁},$$
$$\text{⚀⚂}, \text{⚁⚂}, \text{⚂⚂}, \text{⚃⚂}, \text{⚄⚂}, \text{⚅⚂},$$
$$\text{⚀⚃}, \text{⚁⚃}, \text{⚂⚃}, \text{⚃⚃}, \text{⚄⚃}, \text{⚅⚃},$$
$$\text{⚀⚄}, \text{⚁⚄}, \text{⚂⚄}, \text{⚃⚄}, \text{⚄⚄}, \text{⚅⚄},$$
$$\text{⚀⚅}, \text{⚁⚅}, \text{⚂⚅}, \text{⚃⚅}, \text{⚄⚅}, \text{⚅⚅}\Big\}$$

Cependant, il y a une multitude d'autres situations intéressantes (dans de nombreuses sphères d'activité) qui soulèvent des problèmes d'énumération importants. Ainsi, pour comparer la performance de certains algorithmes informatiques, il est nécessaire de compter le nombre de structures intervenant dans les programmes qui mettent en oeuvre ces algorithmes. D'autre part, en physique statistique on ramène l'étude des changements de phase (par exemple de liquide à solide) à l'énumération de configurations d'un certain genre. De plus, en biologie, un grand nombre de concepts de la combinatoire jouent un rôle crucial dans l'étude de la structure de génomes, Enfin, pour ne citer rapidement que quelques exemples de nature mathématiques, des problèmes profonds de la théorie de la représentation des groupes, de la théorie des nombres, ou de la géométrie algébrique, soulèvent des problèmes d'énumération difficiles dont certains n'ont pas encore de solution satisfaisante.

De façon complémentaire à l'étude de la décomposition de structures complexes en structures plus simples (entre autres pour en faciliter l'énumération), il est tout à fait naturel de chercher à mieux comprendre les mécanismes qui permettent de combiner des structures simples pour en former des plus complexes. On est tenté ici de faire le parallèle avec l'étude de la construction de molécules à partir d'atomes, ou d'organismes à partir de cellules. Mais un parallèle encore plus profond peut être fait avec une des composantes essentielles de la programmation en informatique, à savoir la construction de structures de données complexes à partir des structures de données de base (dans le langage de programmation utilisé).

Tout comme pour les langages de programmation, les plus simples des mécanismes de combinaison de la combinatoire font appel aux constructions de base de la théorie des ensembles : sous-ensembles, union, intersection, produit cartésien, etc. Voilà pourquoi nous allons commencer par étudier cer-

tains aspects de la théorie (naïve [2]) des ensembles, tout en soulignant comment lier les constructions considérées à l'énumération. Nous allons ensuite répertorier les structures combinatoires les plus courantes, celles qui jouent un rôle plus important parce qu'elles interviennent plus fréquemment dans toutes sortes de situations. Notre but est de dégager une vue d'ensemble qui (à la fin du cours) culminera avec une petite introduction à la théorie de « espèces de structures », qui permet d'avoir un point de vue global pour la construction de structures complexes à partir des éléments d'un ensemble considérés comme atomes de base.

L'approche de ce texte consiste à d'abord développer une description systématique des structures combinatoires dans le contexte de la théorie des ensembles. Les constructions sont décrites de façon à être facilement programmables dans un système de calcul formel tel que Sage, Maple ou Mathematica, est des exercices à cet effet sont prévus. Les sections ou les exercices plus difficiles sont marqués d'une étoile.

2. Dans notre contexte les ensembles sont essentiellement des ensembles finis, et il n'y a pas de problèmes à procéder ainsi.

Chapitre 1

Ensembles et fonctions

1.1 Introduction

On développe dans ce chapitre les constructions de base de la théorie des ensembles, en particulier celles qui concernent les fonctions, en même temps que certains outils de base pour l'énumération des éléments des ensembles considérés.

1.2 Ensembles

Tout au cours de ce texte, on vise à construire explicitement des « structures combinatoires » à partir des éléments d'ensembles finis donnés, comme l'ensemble

$$[n] := \{i \in \mathbb{N} \mid 1 \leq i \leq n\},$$

ou l'ensemble des lettres de l'alphabet

$$\mathcal{A} := \{a, b, c, d, \ \ldots \ , z\},$$

ou encore les ensembles

$$\{\bullet, \bullet, \bullet\}, \qquad \text{ou} \qquad \{\clubsuit, \ \diamondsuit, \ \heartsuit, \ \spadesuit\}.$$

Informellement, on peut penser que les éléments de ces « ensembles de base » sont des atomes avec lesquels on entend construire les structures considérées.

Georg Cantor
(1845–1918)

La théorie des ensembles a été introduite par Georg Cantor. Bien qu'il soit nécessaire d'en donner une axiomatique rigoureuse pour éviter les paradoxes, nous n'aurons pas trop besoin d'insister là-dessus, étant donné que les ensembles considérés sont soit finis, soit des ensembles classiques comme $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, l'ensemble $\mathbb{Q}$ des nombres rationnels, ou l'ensemble $\mathbb{R}$ des nombres réels. Rappelons que deux ensembles sont égaux si et seulement si ils ont les mêmes éléments. Ainsi, on a les présentations équivalentes

$$\{a, b, c\} = \{c, a, b\} = \{a, b, a, b, c, a, b, a\},$$

d'un même ensemble qui contient trois éléments : a, b et c. Pour des ensembles décrits sous la forme

$$A = \{x \in S \mid P(x)\}, \qquad \text{et} \qquad B = \{x \in S \mid Q(x)\}, \tag{1.1}$$

avec $P(x)$ et $Q(x)$ des propriétés formulées en terme d'énoncés logiques, on a l'égalité $A = B$ si et seulement si $P(x)$ et $Q(x)$ sont logiquement équivalent. On dénote $\emptyset$, l'**ensemble vide**, qui ne contient aucun élément.

Le nombre d'éléments (distincts) d'un ensemble A (ou **cardinal**), est dénoté $|A|$.

Opérations de base sur les ensembles. Une première opération de base sur les ensembles est celle d'**intersection**, $A \cap B$, de deux ensembles A et B. C'est l'ensemble des éléments qui sont communs à ces deux ensembles. Plus précisément on a

$$A \cap B := \{x \mid x \in A, \quad \text{et} \quad x \in B\}. \tag{1.2}$$

Par exemple, on a

$$\{a, b, c, d\} \cap \{1, b, 3, d\} = \{b, d\}.$$

D'autre part, l'**union** de A et B est l'ensemble

$$A \cup B := \{x \mid x \in A, \quad \text{ou} \quad x \in B\}. \tag{1.3}$$

Par exemple

$$\{a, b, c, d\} \cup \{1, b, 3, d\} = \{a, b, c, d, 1, 3\}.$$

On vérifie facilement que les égalités suivantes sont valables en général, quel que soient les ensembles A, B, et C :

$$\begin{array}{ll} \text{(i)} \ A \cap \emptyset = \emptyset, & \text{(i)}' \ A \cup \emptyset = A, \\ \text{(ii)} \ A \cap B = B \cap A, & \text{(ii)}' \ A \cup B = B \cup A, \\ \text{(iii)} \ A \cap (B \cap C) = (A \cap B) \cap C, & \text{(iii)}' \ A \cup (B \cup C) = (A \cup B) \cup C, \\ \text{(iv)} \ A \cap (B \cup C) = (A \cap B) \cup (A \cap C), & \text{(iv)}' \ A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \end{array} \tag{1.4}$$

Lorsque $A \cap B = \emptyset$, on dit que $A \cup B$ est une **union disjointe**, et on écrit alors $A + B$ pour désigner cette union. Voir l'exercice 1.2 pour ce qui concerne les propriétés de l'union disjointe [1].

La **différence**, $A \setminus B$, de deux ensembles A et B, est l'ensemble des éléments de A qui ne sont pas dans B, c.-à-d. :

$$A \setminus B := \{x \in A \mid x \notin B\}. \tag{1.5}$$

Sous-ensembles. Si tous les éléments de B sont aussi des éléments de A, on dit que B est un **sous-ensemble** de A, et on écrit $B \subseteq A$. On dit aussi parfois que B est une **partie** de A. Se donner un sous-ensemble B, de k éléments d'un ensemble A de cardinal n, correspond donc à

$$\ll \textit{ choisir } k \textit{ éléments parmi } n \gg.$$

L'inclusion d'ensembles possède les propriétés suivantes. Pour tout A, B et C, on a

$$\begin{aligned} &\text{a) } \emptyset \subseteq A, \\ &\text{b) } A \subseteq A, \\ &\text{c) si } A \subseteq B \quad \text{et} \quad B \subseteq A, \text{ alors } A = B, \\ &\text{d) si } A \subseteq B \quad \text{et} \quad B \subseteq C, \text{ alors } A \subseteq C. \end{aligned} \tag{1.6}$$

Lorsque A et B sont décrit comme en (1.1), on a $B \subseteq A$ si et seulement si l'énoncé logique $Q(x) \Longrightarrow P(x)$ est vrai. D'autre part, quel que soient les ensembles A et B, on a toujours

$$A \cap B \subseteq A, \quad \text{et} \quad A \subseteq A \cup B. \tag{1.7}$$

De plus, Si B est un sous-ensemble de A, alors on a

$$A \cap B = B \quad \text{et} \quad A \cup B = A. \tag{1.8}$$

On dénote $\mathcal{P}[S]$ l'ensemble de tous les sous-ensembles de S :

$$\mathcal{P}[S] := \{A \mid A \subseteq S\}. \tag{1.9}$$

On dit aussi que $\mathcal{P}[S]$ est l'**ensemble des parties** de S. Par exemple,

$$\mathcal{P}[\{a, b, c\}] = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

1. Lorsque A et B ne sont pas disjoints ($A \cap B \neq \emptyset$), on peut tout de même considérer leur union disjointe en « forçant » A et B à être disjoints. Plus précisément, on pose

$$A + B = (\{0\} \times A) \cup (\{1\} \times B).$$

On donne ainsi des « couleurs » distinctes aux éléments de A et de B.

Pour un ensemble S fixé, le **complément** de A dans S, dénoté $\overline{A}$, est l'ensemble

$$\overline{A} := \{x \in S \mid x \notin A\},$$

des éléments de S qui ne sont pas éléments de A (on écrit $x \notin A$). Ainsi, pour $S = \{a, b, c, d, e, f\}$ et $A = \{b, c, e\}$, on a $\overline{A} = \{a, d, f\}$. Si $A = \{x \in S \mid P(x)\}$, alors on a $\overline{A} = \{x \in S \mid \neg P(x)\}$.

Quel que soient A et B des sous-ensembles de S (donc des éléments de $\mathcal{P}[S]$), les identités suivantes sont valables

$$\begin{array}{lll} \text{(i)}\ \overline{\overline{A}} = A, & & \\ \text{(ii)}\ A \cap \overline{A} = \emptyset, & \text{(ii)}'\ A \cup \overline{A} = S, & \\ \text{(iii)}\ \overline{A} \cap \overline{B} = \overline{A \cup B}, & \text{(iii)}'\ \overline{A} \cup \overline{B} = \overline{A \cap B}. & \end{array} \tag{1.10}$$

Supposons que pour chaque élément i d'un ensemble I, on choisisse un sous-ensemble A_i de S. On dit alors qu'on a une **famille** d'ensembles indexée par les éléments de I, et on dénote $\{A_i\}_{i \in I}$ cette famille d'ensembles (c'est simplement un ensemble d'ensembles). On a souvent la situation $I = [n]$, et alors la famille est l'ensemble

$$\{A_1, A_2, A_3, \ldots, A_n\}.$$

Grâce aux associativités (1.4, (iii) et (iii)'), on peut étendre sans problème les notions d'union et d'intersection à de telles familles, en posant

$$\bigcap_{i \in I} A_i := \{x \mid \text{pour tout } i \in I,\ x \in A_i\}, \qquad \text{et} \tag{1.11}$$

$$\bigcup_{i \in I} A_i := \{x \mid \text{il existe } i \in I,\ x \in A_i\}. \tag{1.12}$$

Ainsi, pour $I = [n]$, on écrit aussi

$$\bigcap_{i \in [n]} A_i = \bigcap_{i=1}^{n} A_i, \quad \text{et} \quad \bigcup_{i \in [n]} A_i = \bigcup_{i=1}^{n} A_i,$$

et pour $n = 3$ on a

$$\bigcap_{i=1}^{3} A_i = A_1 \cap A_2 \cap A_3, \quad \text{et} \quad \bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3.$$

On a les identités

$$\bigcap_{k \in I \cup J} A_k = \left(\bigcap_{i \in I} A_i\right) \cap \left(\bigcap_{j \in J} A_j\right), \qquad \text{et} \tag{1.13}$$

$$\bigcup_{k \in I \cup J} A_k = \left(\bigcup_{i \in I} A_i\right) \cup \left(\bigcup_{j \in J} A_j\right). \tag{1.14}$$

On doit cependant prendre la précaution d'avoir posé par convention [2] que

$$\bigcap_{i\in\emptyset} A_i := S, \quad \text{et} \quad \bigcup_{i\in\emptyset} A_i := \emptyset.$$

De façon tout à fait similaire, on étend la notion d'union disjointe aux familles d'ensembles deux à deux disjoints. On utilise alors le symbole de « $\sum$ », et on écrit donc

$$\sum_{i\in I} A_i := \bigcup_{i\in I} A_i, \tag{1.15}$$

pour l'union en question. En particulier, on a les deux écritures équivalentes

$$\sum_{i=1}^{n} A_i = A_1 + A_2 + \ldots + A_n,$$

tout comme d'habitude.

Pour chaque $0 \leq k$, on considère aussi l'ensemble des **parties à k-éléments** de S :

$$\mathcal{P}_k[S] := \{A \mid A \subseteq S, \quad |A| = k\}.$$

C'est donc

« l'ensemble des possibilités de choix de k éléments parmi n ».

Ainsi, on a $\mathcal{P}_0[S] = \{\emptyset\}$, puis

$$\mathcal{P}_1[S] = \{\{x\} \mid x \in S\},$$

et encore

$$\mathcal{P}_2[S] = \{\{x, y\} \mid x, y \in S, \quad \text{et} \quad x \neq y\},$$

et ainsi de suite jusqu'à $\mathcal{P}_n[S] = \{S\}$, pour n égal au cardinal de S. Ainsi, si $S = \{a, b, c\}$, alors on a

$$\mathcal{P}_0[S] = \{\emptyset\}, \quad \mathcal{P}_1[S] = \{\{a\}, \{b\}, \{c\}\}, \quad \mathcal{P}_2[S] = \{\{a, b\}, \{a, c\}, \{b, c\}\}, \quad \mathcal{P}_3[S] = \{\{a, b, c\}\}.$$

Ces ensembles contiennent donc respectivement 1, 3, 3, et 1 éléments, et leur union disjointe donne l'ensemble à 8 éléments $\mathcal{P}[S]$ vus plus haut. En fait, $\mathcal{P}[S]$ est toujours l'union disjointe des ensembles $\mathcal{P}_k[S]$, c.-à-d. :

$$\mathcal{P}[S] = \sum_{k=0}^{\infty} \mathcal{P}_k[S]. \tag{1.16}$$

2. On voit ici la nécessité d'avoir choisit les A_i comme étant tous sous-ensemble d'un même « univers » S.

Comme $\mathcal{P}_k[S] = \emptyset$, si k est plus grand que le cardinal de S, cette sommation est en fait finie. On a donc ici deux descriptions du même ensemble, et nous allons voir plus loin qu'il en résulte une identité intéressante (voir (1.72)).

On peut « calculer » récursivement (voir les exercices 1.10 et 1.20) l'ensemble des parties à k éléments d'un ensemble via la formule

$$\mathcal{P}_k[S + \{y\}] \;=\; \mathcal{P}_k[S] \;+\; \Big\{B + \{y\} \mid B \in \mathcal{P}_{k-1}[S]\Big\}, \tag{1.17}$$

où y n'est pas élément de S. On a évidemment les conditions initiales :

$$\mathcal{P}_k[S] = \begin{cases} \emptyset & \text{si, } k > |S|\,, \\ \{S\} & \text{si, } k = |S|\,. \end{cases} \tag{1.18}$$

Pour illustrer comment l'identité (1.18) permet de calculer effectivement, considérons le cas $\mathcal{P}_2[\{a,b,c\}]$. On débute avec $S = \{a,b\}$ et $y = c$, et le calcul se déroule comme suit

$$\begin{aligned} \mathcal{P}_2[\{a,b,c\}] &= \mathcal{P}_2[\{a,b\}] + \Big\{B + \{c\} \mid B \in \mathcal{P}_1[\{a,b\}]\Big\} \\ &= \{\{a,b\}\} + \Big\{B + \{c\} \mid B \in \{\{a\},\{b\}\}]\Big\} \\ &= \{\{a,b\}\} + \{\{a,c\},\{b,c\}\} \\ &= \{\{a,b\},\{\{a,c\},\{b,c\}\}]\} \end{aligned}$$

Pour des ensembles disjoints A (de cardinal n) et B (de cardinal k), on a aussi la bijection

$$\mathcal{P}_k[A+B] \xrightarrow{\sim} \sum_{i=0}^{k} \mathcal{P}_i[A] \times \mathcal{P}_{k-i}[B], \tag{1.19}$$

qui envoie une partie C de $A + B$ sur le couple $(C \cap A, C \cap B)$, pour lequel on a clairement $C = (C \cap A) + (C \cap B)$. On en déduit l'identité de l'exercice 1.10, c)

Produit cartésien. Avant de décrire la prochaine construction, rappelons que deux couples (a,b) et (c,d) sont égaux, si et seulement si on a les deux égalités $a = c$ et $b = d$. Le **produit cartésien** de A et B est l'ensemble de tous les couples (x,y), avec x élément de A et y élément de B. Autrement formulé, on a

$$A \times B = \{(x,y) \mid x \in A \quad \text{et} \quad y \in B\}.$$

Si l'un des ensembles A ou B est vide, alors le produit cartésien $A \times B$ est vide, c.-à-d. :

$$A \times \emptyset = \emptyset \times B = \emptyset. \tag{1.20}$$

Une illustration du produit cartésien est

$$\begin{aligned}\{a,b,c,d\} \times \{1,2,3\} = \; & \{(a,1), \quad (b,1), \quad (c,1), \quad (d,1),\\ & \;\;(a,2), \quad (b,2), \quad (c,2), \quad (d,2),\\ & \;\;(a,3), \quad (b,3), \quad (c,3), \quad (d,3)\}.\end{aligned}$$

Il est facile de vérifier que, pour tout ensemble A, B et C (avec B et C disjoints), on a

$$A \times (B + C) \;=\; (A \times B) + (A \times C), \tag{1.21}$$

$$(A + B) \times C \;=\; (A \times C) + (B \times C), \tag{1.22}$$

Pour un ensemble fini d'indices I, dénotons par $(a_i)_{i\in I}$ les suites indexées par les éléments de I. Rappelons que l'on a l'égalité

$$(a_i)_{i\in I} = (b_i)_{i\in I},$$

si et seulement $a_i = b_i$ pour tout i dans I. Si $(A_i)_{i\in I}$ est une suite d'ensembles indexés par I. On dit de a_i que c'est la i-ième **coordonnée** de la suite. Le produit cartésien généralisé est l'ensemble

$$\prod_{i\in I} A_i := \{(a_i)_{i\in I} \mid (\forall i \in I)\, a_i \in A_i \,\}. \tag{1.23}$$

Par convention, le produit vide $\prod_{k\in\emptyset} A_k$ est un ensemble à un élément : $\{*\}$ (un **singleton**). On vérifie alors que [3]

$$\prod_{k\in I+J} A_k \xrightarrow{\sim} \left(\prod_{i\in I} A_i\right) \times \left(\prod_{j\in J} A_J\right). \tag{1.24}$$

Le cas particulier qui correspond à choisir $I = [n]$ donne la construction du produit cartésien

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ 1 \le i \le n\},$$

et lorsque $A_i = B$, pour tous les i, on obtient la **puissance cartésienne** n-ième,

$$B^n := \underbrace{B \times B \times \cdot \times B}_{n \text{ copies}},$$

de l'ensemble B, avec $B^0 := \{*\}$. On a alors les identités suivantes (modulo les bijections naturelles nécessaires)

$$\text{(i) } B^n \times B^k \xrightarrow{\sim} B^{n+k}, \quad \text{et} \quad \text{(iii) } (B^n)^k \xrightarrow{\sim} B^{n\,k}. \tag{1.25}$$

3. À strictement parler, les éléments des ensembles comparés ici ne sont pas égaux. Plutôt qu'une égalité, on a une bijection naturelle entre les deux ensembles, ce qui signifie qu'on doit transformer légèrement les éléments pour pouvoir les comparer (voir Exercice 1.3).

Relations. Une **relation** R, allant d'un ensemble A vers un ensemble B, est simplement un sous-ensemble du produit cartésien $A \times B$, c.-à-d. : $R \subseteq A \times B$. La **relation transposée** de B vers A, dénotée R^{T}, est donnée par le sous-ensemble

$$R^{\mathrm{T}} := \{(y, x) \mid (x, y) \in R\}$$

de $B \times A$. Par exemple, pour $A = \{a, b, c, d\}$ et $B = \{1, 2, 3\}$, on a la relation

$$R = \{(a, 1), (a, 2), (b, 3), (c, 2), (d, 1)\},$$

dont la transposée est la relation

$$R^{\mathrm{T}} = \{(1, a), (1, d), (2, c), (2, a), (3, b)\}.$$

On désigne par $\mathsf{Rel}[A, B]$ l'ensemble des relations de A vers B. Observons que, par définition, on a

$$\mathsf{Rel}[A, B] = \mathcal{P}[A \times B]. \tag{1.26}$$

Si $A = \{a, b\}$, et $B = \{1, 2\}$, l'ensemble $\mathsf{Rel}[A, B]$ contient les 16 éléments :

$$\begin{aligned}
\mathsf{Rel}[A, B] = \{\ & \emptyset, \\
& \{(a,1)\}, && \{(a,2)\}, && \{(b,1)\}, && \{(b,2)\}, \\
& \{(a,1),(a,2)\}, && \{(a,1),(b,1)\}, && \{(a,1),(b,2)\}, \\
& \{(a,2),(b,1)\}, && \{(a,2),(b,2)\}, && \{(b,1),(b,2)\}, \\
& \{(a,1),(a,2),(b,1)\}, && \{(a,1),(a,2),(b,2)\}, \\
& \{(a,1),(b,1),(b,2)\}, && \{(a,2),(b,1),(b,2)\}, \\
& \{(a,1),(a,2),(b,1),(b,2)\}\ \}.
\end{aligned}$$

On dénote $\mathsf{Rel}_k[A, B]$ l'ensemble des relations de A vers$B$ contenant k couples. Clairement, on a

$$\mathsf{Rel}[A, B] = \sum_{k \geq 0} \mathsf{Rel}_k[A, B]. \tag{1.27}$$

1.3 Fonctions

Bien que la notion de fonction soit l'une des plus importantes en mathématiques, ce n'est qu'à la fin du dix-neuvième siècle qu'elle a pris la forme moderne [4] qu'on lui connaît. Une **relation**

4. On ne sait trop qui doit être crédité pour cela.

fonctionnelle f, de l'ensemble A vers l'ensemble B, est une relation $f \subseteq A \times B$, qui possède la propriété que :

$$\ll \text{ pour tout } x \in A, \text{ il y a un et un seul } y \in B \text{ tel que } (x, y) \in f \gg. \tag{1.28}$$

Autrement dit, l'élément x dans A caractérise uniquement l'élément correspondant y dans B. Il est habituel de désigner par $f(x)$ cet élément, et on a donc

$$f(x) = y \quad \text{ssi} \quad (x, y) \in f. \tag{1.29}$$

Formellement parlant, une **fonction** de A vers B est un triple (f, A, B), avec f un relation fonctionnelle de A vers B. Il est habituel d'écrire $f : A \to B$ pour ce triple. Ainsi, on a la fonction $f : \{a, b, c, d\} \to \{1, 2, 3\}$, telle que

$$f = \{(a, 1), (b, 3), (c, 2), (d, 1)\}. \tag{1.30}$$

Elle peut aussi se décrire en écrivant que :

$$f(a) = 1, \quad f(b) = 3, \quad f(c) = 2, \quad \text{et} \quad f(d) = 1.$$

On écrit aussi parfois

$$x \mapsto f(x),$$

pour signifier que le couple $(x, f(x))$ fait partie de la relation fonctionnelle f. Ceci est particulièrement utile lorsque f est décrite par une formule. On peut penser à une fonction comme étant un processus f qui

$$\ll \text{ choisit un élément } f(x) \text{ de } B \text{ pour chaque élément } x \text{ de } A \gg.$$

Pour une fonction $f : A \to B$, on dit que l'ensemble A est la **source** de F, et que l'ensemble B en est le **but**. Cette définition très abstraite de fonction rend possible la définition de l'ensemble $\mathsf{Fonct}[A, B]$ dont les éléments sont les relations fonctionnelles de A vers B :

$$\mathsf{Fonct}[A, B] := \{f \mid f : A \to B\}. \tag{1.31}$$

Ainsi, à chaque élément f de $\mathsf{Fonct}[A, B]$, il correspond une fonction $f : A \to B$ de source A et de but B. Il nous arrivera souvent de parler de la fonction f, si la source et le but associés sont clairs dans le contexte. Pour $A = \{a, b, c\}$ et $B = \{0, 1\}$, on a

$$\begin{aligned} \mathsf{Fonct}[A, B] = \{ \quad & \{(a,0),(b,0),(c,0)\}, \quad \{(a,0),(b,0),(c,1)\}, \\ & \{(a,0),(b,1),(c,0)\}, \quad \{(a,0),(b,1),(c,1)\}, \\ & \{(a,1),(b,0),(c,0)\}, \quad \{(a,1),(b,0),(c,1)\}, \\ & \{(a,1),(b,1),(c,0)\}, \quad \{(a,1),(b,1),(c,1)\} \quad \}. \end{aligned}$$

Il y a donc 8 fonctions de A vers B. Observons que l'ensemble $\mathsf{Fonct}[\emptyset, B]$ contient exactement un élément, quel que soit l'ensemble B. C'est la relation vide (qui est fonctionnelle par défaut), et on a explicitement

$$\mathsf{Fonct}[\emptyset, B] = \{\emptyset\}. \tag{1.32}$$

En utilisant ceci comme condition initiale, on peut calculer récursivement l'ensemble des fonctions entre deux ensembles en exploitant la formule

$$\mathsf{Fonct}[A + \{x\}, B] = \sum_{y \in B} \{f + \{(x, y)\} \mid f \in \mathsf{Fonct}[A, B]\}. \tag{1.33}$$

Il est facile de vérifier que

$$\mathsf{Fonct}[A, B \cap C] = \mathsf{Fonct}[A, B] \cap \mathsf{Fonct}[A, C]. \tag{1.34}$$

On peut agréablement présenter les fonctions $f : [n] \to B$ (lorsque les éléments de B s'y prêtent), en exploitant l'ordre de présentation usuel des éléments de $[n] = \{1, 2, 3, \ldots, n\}$. Ainsi, on simplifie

$$f = \{(1, f(1)), (2, f(2)), (3, f(3)), \ldots, (n, f(n))\},$$

en écrivant plutôt

$$f = f(1)f(2)f(3)\cdots f(n), \qquad \text{ou même} \qquad f = f_1 f_2 f_3 \cdots f_n,$$

avec la convention que $f_i = f(i)$. Par exemple, $f = \{(1, b), (2, a), (3, b), (4, a)\}$ s'écrit encore comme $f = baba$. On dit alors qu'on a présenté f **sous forme de mot**. Toujours avec cette convention, l'ensemble des 64 fonctions $f : \{1, 2, 3\} \to \{1, 2, 3, 4\}$ peut donc s'écrire

$$\begin{array}{cccccccc}
\{111, & 112, & 113, & 114, & 121, & 122, & 123, & 124, \\
131, & 132, & 133, & 134, & 141, & 142, & 143, & 144, \\
211, & 212, & 213, & 214, & 221, & 222, & 223, & 224, \\
231, & 232, & 233, & 234, & 241, & 242, & 243, & 244, \\
311, & 312, & 313, & 314, & 321, & 322, & 323, & 324, \\
331, & 332, & 333, & 334, & 341, & 342, & 343, & 344, \\
411, & 412, & 413, & 414, & 421, & 422, & 423, & 424, \\
431, & 432, & 433, & 434, & 441, & 442, & 443, & 444\}
\end{array}$$

Pour $f : A \to B$, et C un sous-ensemble de A, on a une relation fonctionnelle, dénotée $f\big|_C$, appelée la **restriction** de f à C, définie en posant

$$f\big|_C := \{(x, f(x)) \mid x \in C\}. \tag{1.35}$$

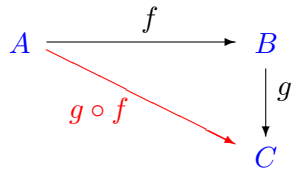
Il en résulte une fonction $f\big|_C : C \to B$ qui est injective si f l'est. L'opération de restriction donne une surjection

$$\mathsf{Fonct}[A, B] \twoheadrightarrow \mathsf{Fonct}[C, B], \qquad f \mapsto f\big|_C, \tag{1.36}$$

Pour deux fonctions $f : A \to B$ et $g : B \to C$, avec le but de f égal à la source de g, on définit une nouvelle fonction $g \circ f : A \to C$, en posant, pour x dans A :

$$(g \circ f)(x) := g(f(x)). \tag{1.37}$$

On dit alors que $g \circ f$ est le **composé** de f et de g. La source de $g \circ f$ est la source de f, et son but est le but de g. On a donc la situation suivante



La composition de fonction est associative. C'est donc dire que, pour trois fonctions $f : A \to B$, $g : B \to C$, et $h : C \to D$, on a toujours

$$(h \circ g) \circ f = h \circ (g \circ f).$$

De plus, pour chaque ensemble A, on a une fonction appelée **identité**, $\mathrm{Id}_A : A \to A$, simplement définie en posant $\mathrm{Id}_A(x) = x$, pour tout x dans A. Pour toute fonction $f : A \to B$, on a alors

$$f \circ \mathrm{Id}_A = f = \mathrm{Id}_B \circ f.$$

Quel que soit B, sous-ensemble de A, on peut définir la **fonction caractéristique**, $\chi_B : A \to \{0, 1\}$, de B dans A. On pose, pour x dans A, que

$$\chi_B(x) := \begin{cases} 1 & \text{si, } x \in B, \\ 0 & \text{sinon.} \end{cases} \tag{1.38}$$

Comme son nom le dit, cette fonction caractérise le sous-ensemble B, ainsi que son complément $\overline{B}$, puisque

$$B = \{x \in A \mid \chi_B(x) = 1\}, \quad \text{et} \quad \overline{B} = \{x \in A \mid \chi_B(x) = 0\}. \tag{1.39}$$

En particulier, considérons le cas où R est une relation de $[n]$ vers $[k]$. On peut penser à la fonction caractéristique $\chi_R : [n] \times [k] \to \{0, 1\}$ correspondante :

$$\chi_R(i, j) := \begin{cases} 1 & \text{si, } (i, j) \in R, \\ 0 & \text{si, } (i, j) \notin R, \end{cases} \tag{1.40}$$

comme étant la donné d'une matrice $n \times k$, aussi dénotée χ_R, dont les entrées sont des 1 ou des 0. On dit que χ_R est la **matrice** de la relation R. Par exemple, avec $n = 3$ et $k = 4$, la relation

$$R = \{(1, 1), (1, 3), (1, 4), (2, 2), (2, 3), (3, 1), (3, 4)\}$$

correspond ainsi à la matrice

$$\chi_R = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Dans le cas d'une relation fonctionnelle f, la matrice obtenue contient un et un seul un 1 sur chacune de ses lignes. La matrice de la relation transposée R^{T}, est la matrice transposée de χ_R, c.-à-d. :

$$\chi_{R^{\mathrm{T}}} = (\chi_R)^{\mathrm{T}}. \tag{1.41}$$

Toute fonction $f : A \to B$ établie une correspondance entre les sous-ensembles de A et ceux de B de la façon suivante. On introduit une fonction $\mathcal{P}[f] : \mathcal{P}[A] \to \mathcal{P}[B]$ définie, pour un sous-ensemble C de A, en posant

$$\begin{aligned} \mathcal{P}[f](C) &:= \{f(x) \mid x \in C\} \\ &= \{y \mid x \in C \text{ et } (x,y) \in f\}. \end{aligned} \tag{1.42}$$

Observons qu'on exploite ici le fait que la répétition d'éléments ne change rien à la description d'un ensemble. Donc, même s'il est fort possible que plusieurs éléments de C donne une même valeur $f(x)$ dans B, cette valeur n'apparaît qu'une seule fois dans $\mathcal{P}[f](C)$.

On écrit aussi plus simplement $f^+(C)$, pour $\mathcal{P}[f](C)$, et on dit que $f^+(C)$ est l'**image de C par f**. Dans le cas où on choisit $C = A$, l'ensemble source de f, on dit plus simplement que $f^+(A)$ est l'**image de f**, et on dénote cet ensemble $\mathrm{Im}(f)$. On a donc

$$\mathrm{Im}(f) := \{\ y \mid (x,y) \in f\}. \tag{1.43}$$

Pour la fonction en (1.30), on a

$$f^+(\{a,b,c\}) = \{1,2,3\}, \quad \text{et} \quad f^+(\{b,d\}) = \{1,3\}.$$

Il est aussi possible de considérer l'**image inverse** de sous-ensembles de B le long de la fonction f. Ainsi, pour un sous-ensemble D de B, on pose

$$f^-(D) := \{x|\ (x,y) \in f \text{ et } y \in D\}. \tag{1.44}$$

C'est donc une fonction $f^- : \mathcal{P}[B] \to \mathcal{P}[A]$. Toujours avec l'exemple en (1.30), on a

$$f^-(\{1\}) = \{a,d\}, \quad \text{et} \quad f^-(\{2,3\}) = \{b,c\}.$$

Les notions d'image, et d'image inverse de sous-ensembles, sont illustrées à la Figure 1.1, avec la convention qu'une flèche va de x dans A vers $f(x)$ dans B.

Il est intéressant de remarquer que la définition de fonction assure que

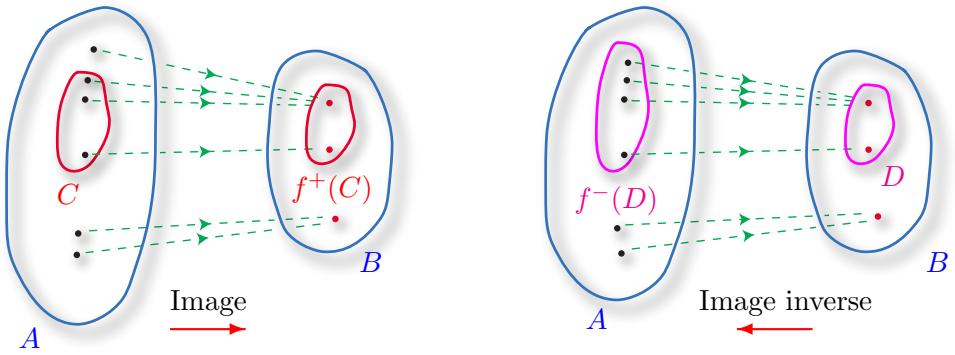


FIGURE 1.1 – Image et image inverse de sous-ensembles.

Proposition 1.1. *Pour toute fonction $f : A \to B$, si $\{C_i\}_{i\in I}$ est une famille de sous-ensembles disjoints de B, alors la famille $\{f^-(C_i)\}_{i\in I}$ est une famille de sous-ensembles disjoints de A. En particulier, la famille $\{f^-(\{y\})\}_{y\in \mathrm{Im}(f)}$ est une famille de sous-ensembles non vides disjoints de A, et on a*

$$A = \sum_{y\in \mathrm{Im}(f)} f^-(\{y\}). \tag{1.45}$$

Les sous-ensembles $f^-(\{y\})$, pour y dans B, sont appelés les **fibres** de la fonction f. On dit alors que $f^-(\{y\})$ est la fibre de f en y. Ces notions, et la Proposition 1.1, sont illustrées à la Figure 1.2.

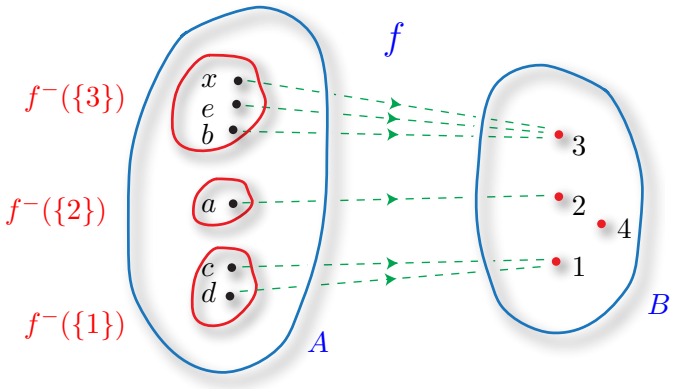


FIGURE 1.2 – Fibres d'une fonction.

Bijections. Dans une première introduction à la théorie des ensembles, la correspondance établie par une bijection $f : A \to B$, entre les éléments de A et ceux de B, est souvent introduite par une Figure naïve comme celle de la Figure 1.3. De façon plus précise, on a la définition suivante.

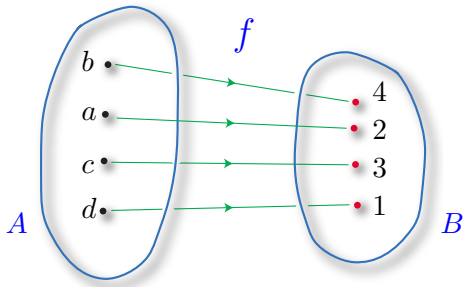


FIGURE 1.3 – Représentation naïve d'une bijection.

Pour une fonction f de A vers B, si la relation transposée f^{T} est aussi une relation fonctionnelle, alors on dit que f est une **bijection**. On obtient une fonction $f^{-1} : B \to A$, c.-à-d. : la source de f^{-1} est l'ensemble B, et son but est l'ensemble A. La fonction $f^{-1} : B \to A$ est la **fonction inverse** de la fonction $f : A \to B$ pour la composition, c.-à-d. :

$$f^{-1} \circ f = \mathrm{Id}_A, \quad \text{et} \quad f \circ f^{-1} = \mathrm{Id}_B. \tag{1.46}$$

Il est très facile de vérifier qu'il ne peut y avoir qu'un inverse pour la composition, c.-à-d. :

Proposition 1.2. *Pour toute fonction $f : A \to B$, si $g : B \to A$ est telle que*

$$g \circ f = \mathrm{Id}_A, \quad \text{et} \quad f \circ g = \mathrm{Id}_B, \tag{1.47}$$

alors $g = f^{-1}$.

Donc, pour montrer que $f : A \to B$ est une bijection, il suffit de montrer qu'on peut construire une fonction qui satisfait (1.47).

La relation de l'exemple (1.30) est une fonction qui n'est pas bijective, puisque la relation transposée : $\{(1, a), (1, d), (2, c), (3, b)\}$ ne satisfait pas la propriété (1.28). En effet, il y deux couples commençant par l'élément 1 : qui sont $(1, a)$ et $(1, d)$. Le symbole « $\xrightarrow{\sim}$ » dénote le fait qu'on ai une bijection, et on écrit $f : A \xrightarrow{\sim} B$ pour dire que f est bijective.

Un des principes de base de la théorie des ensembles affirme que :

$$\begin{array}{c} \textit{Il existe une bijection entre deux ensembles finis } A \textit{ et } B, \\ \textit{si et seulement si } A \textit{ et } B \textit{ ont même cardinal, i.e. : } |A| = |B|. \end{array} \tag{1.48}$$

Dans la suite de ce texte, nous allons illustrer plusieurs fois comment on peut utiliser ce principe pour dégager des identités intéressantes. Observons par exemple que lorsque B n'a qu'un seul élément (par exemple $B = \{*\}$), alors les ensembles A et $A \times B$ doivent avoir le même nombre d'éléments. Il y a donc une bijection entre A et $A \times B$. Voir l'exercice 1.4 à ce propos.

On désigne par $\mathsf{Bij}[A, B]$ l'ensemble (fini) des relations bijectives entre A et B, c.-à-d. :

$$\mathsf{Bij}[A, B] := \{f \in \mathsf{Fonct}[A, B] \mid f : A \xrightarrow{\sim} B\}. \tag{1.49}$$

Il découle directement du principe ci-haut qu'on a $\mathsf{Bij}[A, B] = \emptyset$, lorsque $|A| \neq |B|$. Observons que $\mathsf{Bij}[\emptyset, \emptyset] = \{\emptyset\}$ est de cardinal 1. La formule suivante permet de calculer récursivement l'ensemble des bijections entre deux ensembles de même cardinal :

$$\mathsf{Bij}[A + \{x\}, B] = \sum_{y \in B} \{f + \{(x, y)\} \mid f \in \mathsf{Bij}[A, B \setminus \{y\}]\}, \tag{1.50}$$

où $|B| = |A| + 1$. Ainsi, pour $A = \{a, b, c\}$ et $B = \{1, 2, 3\}$, on trouve

$$\begin{aligned} \mathsf{Bij}[A, B] = \{ \quad & \{(a,1),(b,2),(c,3)\}, \quad \{(a,1),(b,3),(c,2)\}, \\ & \{(a,2),(b,1),(c,3)\}, \quad \{(a,2),(b,3),(c,1)\}, \\ & \{(a,3),(b,1),(c,2)\}, \quad \{(a,3),(b,2),(c,1)\} \quad \}. \end{aligned}$$

Il y a donc exactement 6 bijections entre les deux ensembles à trois éléments A et B.

Le composé de fonctions bijectives est une fonction bijective, et l'inverse d'une fonction bijective est une fonction bijective. Pour tout ensemble fini A, l'ensemble $\mathsf{Bij}[A, A]$, des bijections de A vers A, forme un groupe pour la composition de fonctions, avec Id_A comme identité. On dit habituellement d'une bijection de A vers A que c'est une **permutation** de A, et on désigne souvent par $\mathbb{S}[A]$ l'ensemble des permutations de A. Lorsque $A = [n]$, on écrit simplement $\mathbb{S}[n]$ plutôt que $\mathbb{S}[[n]]$ [5]. Les permutations sont souvent dénotées par des lettres grecques minuscules : σ, τ, θ, etc.

La matrice χ_σ associée à une permutation σ de $[n]$, est une matrice carrée $n \times n$ de 0 et de 1, ayant un 1 dans chaque ligne, et un 1 dans chaque colonne. On dit que c'est une **matrice de permutation**, et on a les identités

$$\chi_{\mathrm{Id}_A} = \mathrm{Id}_n, \tag{1.51}$$

$$\chi_{\sigma\circ\tau} = \chi_\sigma \, \chi_\tau, \tag{1.52}$$

pour tout σ et τ dans $\mathbb{S}_n$. Ici, Id_n désigne la matrice identité, et le produit dans le membre de droite de (1.52) est le produit matriciel usuel, c.-à-d. :

$$(\chi_\sigma \chi_\tau)(i, j) = \sum_{k=0}^{n} \chi_\sigma(i, k) \chi_\tau(k, j).$$

5. Cette convention d'éliminer les doubles crochets sera souvent employée dans la suite.

Injections. Parmi les propriétés particulières des fonctions, l'injectivité et la surjectivité sont très certainement des notions importantes. Une fonction $f : A \to B$ est dite **injective** si et seulement si

« *Pour chaque élément y de B, il existe au plus un élément x de A tel que $f(x) = y$.* »

Autrement dit, la fonction f et un processus qui

« *choisit des éléments $f(x)$ de B, un pour chaque x dans A, tous distincts,* »

c'est-à-dire qu'un élément ne peut-être choisit qu'une seule fois. Une formulation un peu plus technique (mais plus facile à manipuler) de cette définition prend la forme suivante. Une fonction $f : A \to B$ est injective si et seulement si, pour tout x_1 et tout x_2 dans A

$$x_1 \neq x_2 \quad \text{implique} \quad f(x_1) \neq f(x_2), \tag{1.53}$$

ce qui équivaut (logiquement) à dire aussi que

$$f(x_1) = f(x_2) \quad \text{entraine forcément} \quad x_1 = x_2. \tag{1.54}$$

Il en découle (voir Exercice 1.6) que f est injective si et seulement si f admet un **inverse à gauche**, c.-à-d. : il existe $g : B \to A$ tel que $g \circ f = \mathrm{Id}_A$. En général, un tel inverse à gauche n'est pas unique, et il n'est pas un inverse à droite.

On dénote souvent par le symbole « $\hookrightarrow$ » le fait qu'une fonction soit injective. On écrit donc $f : A \hookrightarrow B$, pour dire que f est une injective. On désigne par $\mathsf{Inj}[A, B]$ l'ensemble des relations fonctionnelles f telles que $f : A \hookrightarrow B$ soit une fonction injective de A vers B, c.-à-d. :

$$\mathsf{Inj}[A, B] := \{f \in \mathsf{Fonct}[A, B] \mid f : A \hookrightarrow B\}. \tag{1.55}$$

On calcule récursivement cet ensemble comme suit :

$$\mathsf{Inj}[A + \{x\}, B] = \sum_{y \in B} \{f + \{(x, y)\} \mid f \in \mathsf{Inj}[A, B \setminus \{y\}]\}, \tag{1.56}$$

La ressemblance entre la formule (1.56) et la formule (1.50) n'est pas fortuite. Elle s'ensuit du fait qu'une injection entre deux ensembles de même cardinal est forcément une bijection (voir Proposition 1.3). Pour $A = \{a, b\}$ et $B = \{1, 2, 3\}$, on a

$$\begin{aligned} \mathsf{Inj}[A, B] = \{ \quad & \{(a,1),(b,2)\}, \quad \{(a,2),(b,1)\}, \\ & \{(a,1),(b,3)\}, \quad \{(a,3),(b,1)\}, \\ & \{(a,2),(b,3)\}, \quad \{(a,3),(b,2)\} \quad \}. \end{aligned}$$

Pour qu'il existe un injection $f : A \hookrightarrow B$, le nombre d'éléments de A doit nécessairement être plus petit ou égal à celui de B, c.-à-d. : $|A| \leq |B|$. On a donc $\mathsf{Inj}[A, B] = \emptyset$, lorsque $|A| > |B|$.

Le composé de deux fonctions injectives est toujours une fonction injective. De plus, si on a deux fonctions telles que le composé $g \circ f$ soit une fonction injective, alors f est forcément injective (mais pas nécessairement g).

Surjections. Une fonction $f : A \to B$ est dite **surjective** si et seulement si

« *Pour chaque élément y de B, il existe au moins un élément x de A tel que $f(x) = y$.* »

Autrement dit, f est un processus qui

« *choisit chaque élément y de B au moins une fois.* »

Pour chaque y dans B, la fibre de f en y est donc non vide, et on a

$$A = \sum_{y \in B} f^{-}(\{y\}). \tag{1.57}$$

Une fonction $f : A \to B$ est surjective si et seulement si elle admet un **inverse à droite**, c.-à-d. : il existe $g : B \to A$ tel que $f \circ g = \mathrm{Id}_B$. En général, un tel inverse à droite n'est pas unique, et il n'est pas un inverse à gauche. On dénote souvent par le symbole « $\twoheadrightarrow$ » le fait qu'une fonction est surjective. On écrit alors $f : A \twoheadrightarrow B$, pour dire que f est une surjective. On désigne par $\mathsf{Surj}[A, B]$ l'ensemble des relations fonctionnelles surjectives de A vers B, c.-à-d. :

$$\mathsf{Surj}[A, B] := \{f \in \mathsf{Fonct}[A, B] \mid f : A \twoheadrightarrow B\}. \tag{1.58}$$

Pour qu'il existe une surjection $f : A \twoheadrightarrow B$, le nombre d'éléments de A doit nécessairement être plus grand ou égal à celui de B, c.-à-d. : $|A| \geq |B|$. On a donc $\mathsf{Surj}[A, B] = \emptyset$, lorsque $|A| < |B|$. On peut calculer récursivement l'ensemble des fonctions surjectives entre deux ensembles par la récurrence

$$\mathsf{Surj}[A, B + \{y\}] = \sum_{C \subset A} \{f + g \mid f \in \mathsf{Surj}[A \setminus C, B] \quad \text{et} \quad g \in \mathsf{Fonct}[C, \{y\}]\} \tag{1.59}$$

Le composé de deux fonctions surjectives est toujours une fonction surjective. De plus, si on a deux fonctions telles que le composé $g \circ f$ soit une fonction surjective, alors g est forcément surjective (mais pas nécessairement f).

On montre facilement que

Proposition 1.3. *Une fonction qui est à la fois surjective et injective est une fonction bijective. Autrement dit,*

$$\mathsf{Bij}[A,B] = \mathsf{Inj}[A,B] \cap \mathsf{Surj}[A,B]. \tag{1.60}$$

Lorsque $|A| = |B|$, on a en fait

$$\mathsf{Bij}[A,B] = \mathsf{Inj}[A,B] = \mathsf{Surj}[A,B]. \tag{1.61}$$

On montre que (voir Exercice 1.7).

Proposition 1.4. *Pour toute fonction $f : A \to B$,*

a) *f^+ est une injection si f est une injection,*

b) *f^+ est une surjection si f est une surjection,*

c) *f^+ est une bijection si f est une bijection.*

De plus, on a

Proposition 1.5. *Pour toute fonction $f : A \to B$,*

a) *f^- est une surjection si f est une injection,*

b) *f^- est une injection si f est une surjection,*

c) *f^- est une bijection si f est une bijection (en fait, dans cette situation c'est l'inverse de f^+).*

Il nous reste beaucoup d'autres observations à faire sur les relations et les fonctions, mais nous y reviendrons. Pour l'instant, considérons plus en détail le problème de l'énumération des éléments d'un ensemble.

1.4 Compter les éléments d'un ensemble

Lorsqu'on cherche à calculer la dérivée d'une fonction, le problème se décompose en un ou des problèmes plus simples, selon que la fonction à dériver est la somme, le produit, ou encore le composé de deux fonctions plus simples. Il en est souvent de même pour l'énumération des éléments d'un ensemble A. Le problème donné se décompose souvent en un (ou des) problème(s) plus simple(s), selon que l'ensemble à énumérer peut se décrire en terme des constructions de base sur les ensembles.

On démarre les choses en montrant (par récurrence) que

Théorème 1.6. *Si A et B sont des ensembles finis, respectivement de cardinal n et k, alors on a les égalités suivantes :*

$$\text{(i) } |A + B| = n + k, \quad \text{(ii) } |A \times B| = n\,k. \tag{1.62}$$

Nous allons maintenant illustrer en détail le type de démarche que nous allons souvent utiliser par la suite. On cherche à compter les éléments de l'ensemble $\mathcal{P}[A]$, pour un ensemble A de cardinal n. Prenons d'abord le soin de souligner que $\mathcal{P}[A]$ et $\mathcal{P}[A']$ ont le même nombre d'éléments, si A et A' sont de même cardinal. En effet, par le Principe (1.48), il existe une bijection $f : A \to A'$, et donc, par la Proposition 1.4, f^+ est une bijection entre $\mathcal{P}[A]$ et $\mathcal{P}[A']$. Ainsi, le cardinal de $\mathcal{P}[A]$ est une fonction de n, et on dénote $p(n)$ ce nombre d'éléments. Notre objectif est donc de trouver (si possible) une formule pour $p(n)$.

Observons que, quelque soit les ensembles disjoints A_1 et A_2, il y a une bijection

$$\alpha : \mathcal{P}[A_1 + A_2] \xrightarrow{\sim} \mathcal{P}[A_1] \times \mathcal{P}[A_2], \tag{1.63}$$

qui est tout simplement définie en posant, pour B un sous-ensemble de $A_1 + A_2$,

$$\alpha(B) := (B \cap A_1, B \cap A_2).$$

C'est bien une bijection, puisqu'on a la fonction inverse β, définie en posant $\beta((B_1, B_2)) := B_1 + B_2$, pour $B_1 \subseteq A_1$ et $B_2 \subseteq A_2$. En passant au cardinal de chaque membre, avec $n_1 = |A_1|$ et $n_2 = |A_2|$, on obtient alors l'identité

$$p(n_1 + n_2) = p(n_1)\, p(n_2). \tag{1.64}$$

En particulier, on a $p(n+1) = 2\, p(n)$, puisqu'on peut calculer directement que $p(1) = 2$. Observons aussi qu'on a déjà vu que $p(0) = 1$. Tout ceci donne une récurrence pour les nombres $p(n)$, qu'on résout facilement puisque

$$p(n) = 2\, p(n-1) = 4\, p(n-2) = \ \ldots \ = 2^n. \tag{1.65}$$

On a donc trouvé la formule cherchée. Plus généralement, l'énumération des éléments d'ensembles est en partie basée sur les autres égalités du théorème suivant.

Théorème 1.7. *Si A et B sont des ensembles finis, respectivement de cardinal n et k, alors on a les égalités suivantes :*

$$\begin{aligned} &\text{(iii)}\ |\mathcal{P}[A]| = 2^n, \quad \text{(iv)}\ |\mathcal{P}_k[A]| = \binom{n}{k}, \\ &\text{(v)}\ |B^n| = k^n, \qquad \text{(vi)}\ |\mathsf{Fonct}[A, B]| = k^n, \\ &\text{(vii)}\ |\mathbb{S}[A]| = n!, \quad \text{(viii)}\ |\mathsf{Inj}[A, B]| = k_{(n)}. \end{aligned} \tag{1.66}$$

Rappelons que pour des entiers positifs n et k, on a les notions de

– **factoriel** :

$$n! := n \cdot (n-1) \cdots 2 \cdot 1, \tag{1.67}$$

avec $0! := 1$, et

– **factorielle décroissante** :

$$t_{(k)} := t \cdot (t-1) \cdots (t-k+1), \tag{1.68}$$

pour t une variable quelconque.

– **factorielle croissante** :

$$t^{(k)} := t \cdot (t+1) \cdots (t+k-1), \tag{1.69}$$

pour t une variable quelconque.

– **coefficient binomial**[6] :

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}. \tag{1.70}$$

On a les valeurs de la Table 1.1 pour les coefficients binomiaux :

$n \setminus k$	0	1	2	3	4	5	6	7	8	9
0	1									
1	1	1								
2	1	2	1							
3	1	3	3	1						
4	1	4	6	4	1					
5	1	5	10	10	5	1				
6	1	6	15	20	15	6	1			
7	1	7	21	35	35	21	7	1		
8	1	8	28	56	70	56	28	8	1	
9	1	9	36	84	126	126	84	36	9	1

TABLE 1.1 – Le triangle de Pascal (coefficients binomiaux $\binom{n}{k}$).

Plus généralement, on a aussi que

Théorème 1.8. *Si $\{A_i\}_{i\in I}$ est une famille d'ensembles finis, respectivement de cardinal n_i, alors on a les égalités suivantes :*

$$\text{(i)} \left|\sum_{i\in I} A_i\right| = \sum_{i\in I} n_i, \qquad \text{(ii)} \left|\prod_{i\in I} A_i\right| = \prod_{i\in I} n_i. \tag{1.71}$$

Par exemple, il résulte de (1.16) et de (1.71, i) que

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n. \tag{1.72}$$

6. Voir l'exercice 1.10 pour plus de détails sur ces coefficients.

Preuves des Théorèmes 1.7 et 1.8. Les identités (i) et (ii) de (1.71) se montre facilement par récurrence. Pour terminer la preuve du Théorème 1.7, on commence par observer que (v) se déduit directement de (1.71, ii).

On déduit (vi) de (v) en procédant comme suit. Comme le cardinal de A est égal à n, il existe une bijection allant de A vers $[n]$. Soit $\varphi : A \to [n]$ une telle bijection. Observons maintenant qu'on peut identifier les suites $s = (b_i)_{1\leq i\leq n}$ dans B^n à des fonctions $\hat{s} : [n] \to B$, simplement par la correspondance

$$s = (b_i)_{1\leq i\leq n} \qquad \longleftrightarrow \qquad \hat{s} = \{(i, b_i) \mid 1 \leq i \leq n\}.$$

Autrement dit, la fonction $\hat{s}$ est telle que $\hat{s}(i) = b_i$. Nous avons donc une bijection entre les ensembles B^n et $\mathsf{Fonct}[n, B]$. Pour conclure que (vi) est valable, il ne nous reste plus qu'à voir qu'il y a une bijection $\Phi : \mathsf{Fonct}[n, B] \to \mathsf{Fonct}[A, B]$. On obtient facilement cette bijection en posant $\Phi(f) := \varphi \circ f$, pour φ la bijection choisie allant de A vers $[n]$. On rappelle à ce propos que le composé de deux fonctions bijectives est bijectif. Pour voir que Φ est bien une bijection, il suffit de constater (par calcul direct) que son inverse est donné par $\Phi^{-1}(g) := \varphi^{-1} \circ g$.

On a déjà montré (iii). Observons que (iii) découle aussi de (vi) via la bijection entre $\mathcal{P}[A]$ et l'ensemble $\mathsf{Fonct}[A, \{0, 1\}]$ qui correspond à associer à $C \subseteq A$ sa fonction caractéristique χ_C définie en (1.38). Bien entendu, il faut vérifier que c'est bien là une bijection. Cette vérification est laissée au lecteur (voir Exercice 1.8).

Pour voir (viii), on procède de façon analogue en montrant d'abord que la formule est valable pour $A = [n]$. Le même type d'argument que ci-dessus montre alors que le nombre d'éléments de $\mathsf{Inj}[n, B]$ est égal au nombre d'éléments de $\mathsf{Inj}[A, B]$. Il faut utiliser le fait que $\Phi(f) := \varphi \circ f$ est injectif si f l'est (puisque φ est une bijection, c'est aussi une injection). Pour voir que la formule (viii) donne bien le nombre de fonctions injectives de $[n]$ vers B, on constate d'abord que ces injections correspondent au choix de suites : $(b_1, b_2, \ldots, b_n)$ d'éléments de B, qui sont tous distincts. Pour construire toutes les suites possibles, on commence par choisir librement b_1 dans B (il y a k choix possibles). Il ne reste alors que $k - 1$ éléments distincts de ce premier choix, on choisit b_2 parmi ces $k - 1$ éléments de $B \setminus \{b_1\}$. On procède, ainsi de suite jusqu'au choix de b_n parmi les $k - (n - 1)$ éléments de $B \setminus \{b_1, \ldots, b_{n-1}\}$. Il s'ensuit qu'on a bien $k_{(n)}$ façon de réaliser tous ces choix.

La formule (vii) découle directement de (viii), en vertu de (1.3).

Ne nous reste plus qu'à montrer (iv). Pour ce faire, on considère l'ensemble $\mathsf{Inj}[k, A]$ des injections de $[k]$ dans A. Chacune de ces injections f possède une image $\mathrm{Im}(f)$ qui est un sous-ensemble de A ayant k éléments. De plus, il est clair que chaque sous-ensemble à k éléments de A est l'image d'une certaine injection. On a donc

$$\mathcal{P}_k[A] = \{\ \mathrm{Im}(f) \mid f : [k] \hookrightarrow A\}.$$

Cependant, plusieurs injections ont la même image. En fait, il y a exactement $k!$ injections ayant un sous-ensemble C fixé (dans $\mathcal{P}[A]$) comme image. En effet, la relation fonctionnelle sous-jacente à

une injection $f : [k] \hookrightarrow A$ donne une relation bijective entre $[k]$ et B. Il est facile (voir Exercice 1.9) de déduire de (vii) que $k!$ est le nombre de relations bijectives entre deux ensembles de cardinal k. On peut donc conclure qu'il y a bijection (voir Exercice 1.15)

$$\mathsf{Inj}[k, A] \xrightarrow{\sim} \sum_{B \in \mathcal{P}_k[A]} \mathsf{Bij}[k, B]. \tag{1.73}$$

Comme chaque terme de cette somme contient $k!$ éléments, on a donc $n_{(k)} = (\mathcal{P}_k[A])\, k!$, d'où

$$\mathcal{P}_k[A] = \frac{n_{(k)}}{k!} = \binom{n}{k},$$

ce qui achève notre démonstration. ■

On déduit facilement le corollaire suivant :

Corollaire 1.9. *Si $|A| = n$ et $|B| = k$, alors le nombre de relations de A vers B est égal à $2^{n\,k}$.*

Preuve. Selon (1.26), les relations de A vers B sont les éléments de l'ensemble $\mathcal{P}[A \times B]$. En passant par les fonctions caractéristiques (tout comme ci-haut), on voit que cet ensemble est en bijection avec l'ensemble $\mathsf{Fonct}[A \times B, \{0, 1\}]$, des fonctions de $A \times B$ vers $\{0, 1\}$. On conclut donc au moyen des identités (ii) et (iii) du Théorème 1.7. ■

Proposition 1.10. *Les identités suivantes se démontrent bijectivement.*

a) $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0, \qquad n \geq 1.$

b) $\displaystyle n\, 2^{n-1} = \sum_{k=1}^{n} k \binom{n}{k}.$

Preuve de (a). La démonstration de a) est équivalente à la démonstration de l'identité

$$\sum_{0 \leq 2\,k \leq n} \binom{n}{2\,k} = \sum_{0 \leq 2\,k+1 \leq n} \binom{n}{2\,k+1}, \tag{1.74}$$

obtenue en transférant tous les termes négatifs du côté droit de l'égalité. Désignons par $\mathcal{P}_+[A]$ (resp. $\mathcal{P}_-[A]$) l'ensemble des sous-ensembles de A ayant un nombre pair (resp. impair) d'éléments. L'identité en (1.74) est équivalente l'existence d'une bijection entre les ensembles $\mathcal{P}_+[A]$ et $\mathcal{P}_-[A]$. Pour construire une telle bijection (qui ne sera pas naturelle), fixons arbitrairement un élément x dans A. La bijection φ (qui dépend du choix de x) associe à B dans $\mathcal{P}_+[A]$ l'ensemble

$$\varphi(B) := \begin{cases} B \setminus \{x\} & \text{si } x \in B, \\ B + \{x\}, & \text{si } x \notin B, \end{cases}$$

qu'on obtient de B, soit en enlevant x, soit en ajoutant x, selon qu'il appartienne ou non à B. Le résultat est bien dans $\mathcal{P}_-[A]$, puisqu'on a changé le nombre d'éléments par ± 1. On conclut que $|\mathcal{P}_+(A)| = |\mathcal{P}_-(A)| = 2^{n-1}$, $n \geq 1$. ■

Comme exemple d'une telle bijection, appliquée dans le cas $A = \{a, b, c\}$, avec c comme élément choisi. La bijection résultante entre

$$\mathcal{P}_+[A] = \{\emptyset, \{b, c\}, \{a, c\}, \{a, b\}\}$$

et

$$\mathcal{P}_-[A] = \{\{a\}, \{b\}, \{c\}, \{a, b, c\}\}$$

est obtenue comme

$$\emptyset \mapsto \{c\}, \qquad \{b, c\} \mapsto \{b\}, \qquad \{a, c\} \mapsto \{a\}, \qquad \{a, b\} \mapsto \{a, b, c\}.$$

Peuve de b). Nous allons vérifier que les deux membres comptent le nombre de couples (x, B), avec x dans B, et B un sous-ensemble quelconque d'un ensemble A à n éléments, c.-à-d. : le cardinal de l'ensemble

$$\mathcal{A} = \{(x, B) \mid x \in B, \quad \text{et} \quad B \subseteq A\}.$$

Cet ensemble peut s'envisager de deux façons distinctes. Soit directement comme la somme

$$\mathcal{A} = \sum_{x \in A} \Big\{ (x, B + \{x\}) \;\Big|\; B \in \mathcal{P}[A \setminus \{x\}] \Big\},$$

soit en décomposant selon le cardinal de B, c.-à-d. :

$$\mathcal{A} = \sum_{k=0}^{n} \sum_{B \in \mathcal{P}_k[A]} B \times \{B\}.$$

Le nombre d'éléments de la première expression est $n\, 2^{n-1}$, puisque chaque terme de la somme contient 2^{n-1} éléments, un pour chaque élément de $\mathcal{P}[A \setminus \{x\}]$. On obtient donc le membre de gauche de b).

Pour la deuxième expression, on a $k \binom{n}{k}$ éléments dans la terme $\sum_{B \in \mathcal{P}_k[A]} B \times \{B\}$. En sommant pour k, on trouve le terme de droite de b). ■

Principe des tiroirs. Le **principe des tiroirs** (ou **principe des pigeons** ou **principe de Dirichlet**) facilite souvent l'analyse d'une situation complexe. Dans sa version la plus simple, il est formulé en disant que

Si n « objets » sont « placés » dans k « boîtes », avec $n > k$, alors il y a au moins une boîte contenant plus d'un objet.

Ceci est assez imprécis, et on gagne à tout reformuler dans le langage de la théorie des ensembles. Les n objets dont il est question sont les n éléments d'un ensemble A. Les k « boîtes » sont les k éléments d'un ensemble B, et « placer » ces objets dans les boîtes, consiste simplement à choisir une fonction $f : A \to B$. On interprète donc $f(x) = y$ comme signifiant que l'objet x a été placé dans la boîte y. Le contenu d'une boîte y est la fibre de f en y. Le principe des tiroirs devient donc

Si $|A|$ est plus grand que $|B|$, alors pour toute fonction $f : A \to B$, on a au moins un élément y de B pour lequel $|f^-(\{y\})| > 1$.

Principe d'inclusion-exclusion. Le principe d'inclusion-exclusion permet de calculer indirectement le cardinal de certains ensembles. En particulier, il va nous permettre de calculer le cardinal de l'ensemble $\mathsf{Surj}[A, B]$ des surjections de A dans B.

Dans sa version la plus simple, le principe d'inclusion-exclusion prend la forme suivante. Soit A un sous-ensemble d'un ensemble S fixé. On observe que

$$\left|\overline{A}\right| = |S| - |A|. \tag{1.75}$$

On obtient donc indirectement le cardinal de $\overline{A}$ via le calcul du nombre d'éléments de A. L'idée du principe d'inclusion-exclusion est de généraliser cette observation. En guise de préparation au cas général, considérons le cas de deux sous-ensembles A et B de S. On peut verifier que

$$\left|\overline{A} \cap \overline{B}\right| = |S| - |A| - |B| + |A \cap B|$$

Pour des sous-ensembles quelconques A, B, et C de S, on a aussi toujours

$$\left|\overline{A} \cap \overline{B} \cap \overline{C}\right| = |S| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|\,.$$

En général, soit $\{A_i\}_{1 \le i \le m}$,une famille de sous-ensembles de S, on a toujours

$$\begin{aligned}\left|\overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_m\right| \;=\; |S| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \;\cdots \\ +(-1)^m\, |A_1 \cap A_2 \cap \cdots \cap A_m|.\end{aligned}$$

C'est ce qu'on appelle le **principe d'inclusion-exclusion**. On peut le formuler de façon plus condensée comme suit.

Soit $\{A_i\}_{i\in I}$, une famille de sous-ensembles de S, alors on a toujours

$$\left|\bigcap_{i\in I}\overline{A_i}\right| = \sum_{J\subseteq I}(-1)^{|J|}\left|\bigcap_{j\in J}A_j\right|. \tag{1.76}$$

Pour voir que (1.76) est valable, supposons qu'un élément x fixé appartient à exactement k des sous-ensembles A_i, pour un certain $1 \leq k \leq m$. Pour fixer les idées disons que ces sous-ensembles sont A_1, A_2, $\cdots$, A_k. C'est donc dire que

$$x \in A_1 \cap A_2 \cap \cdots \cap A_k.$$

Dans le membre de droite, il est clair que x est compté une fois dans $|S|$, puis une fois (avec le signe approprié) dans chaque intersection $\bigcap_{j\in J} A_j$, pour J variant dans l'ensemble des $\binom{k}{\ell}$ sous-ensembles à ℓ éléments de $\{1, 2, \ldots, k\}$. En tenant compte du signe, la contribution totale de x au membre de droite de la formule d'inclusion-exclusion est donc [7]

$$\sum_{\ell=0}^{k}(-1)^{\ell}\binom{k}{\ell} = 0,$$

C'est donc dire que x n'est pas compté. Par contre, si x n'est dans aucun des A_i, alors il est compté exactement une fois (par $|S|$) dans ce même membre de droite.

Par complémentation, il est clair qu'on a aussi

$$\left|\bigcup_{i\in I}A_i\right| = \sum_{\substack{J\subseteq I\\ J\neq\emptyset}}(-1)^{|J|-1}\left|\bigcap_{j\in J}A_j\right|. \tag{1.78}$$

L'une des formes typiques d'utilisation du principe d'inclusion-exclusion correspond au cas où les sous-ensembles A_i sont décrits via des propriétés P_i :

$$A_i := \{x \in S \mid P_i(x)\}.$$

Le principe d'inclusion-exclusion permet alors d'énumérer l'ensemble des éléments de S qui n'ont aucune des (ou toutes les) propriétés P_i. Pour illustrer ce type de situation, comptons le nombre d'entiers entre 1 et 1000 qui ne sont divisibles ni par 5, ni par 6, ni par 8. On remarque d'abord

7. On utilise ici la formule du binôme de Newton

$$(s+t)^k = \sum_{\ell=0}^{k}\binom{k}{\ell}s^{k-\ell}\,t^{\ell}, \tag{1.77}$$

avec $s = 1$ et $t = -1$. Nous reviendrons à la prochaine section sur cette formule.

que le nombre d'entiers $\leq n$ qui sont divisibles à la fois par k_1, k_2, ..., et k_m est $\lfloor n/m \rfloor$, où m est le plus petit commun multiple de $k_1, k_2, \ldots, k_m$. Ici $\lfloor x \rfloor$ (**plancher** de x) dénote la **partie entière** de x, c'est-à-dire le plus grand entier ne dépassant pas x. Comme on a

$$\left\lfloor \frac{1000}{5} \right\rfloor = 200, \quad \left\lfloor \frac{1000}{6} \right\rfloor = 166, \quad \left\lfloor \frac{1000}{8} \right\rfloor = 125,$$
$$\left\lfloor \frac{1000}{30} \right\rfloor = 33, \quad \left\lfloor \frac{1000}{40} \right\rfloor = 25, \quad \left\lfloor \frac{1000}{24} \right\rfloor = 41,$$
$$\left\lfloor \frac{1000}{120} \right\rfloor = 8,$$

et comme les valeurs 30, 40, 24 et 120 correspondant respectivement aux plus petits communs multiples de (5 et 6), (5 et 8), (6 et 8), et (5 et 6 et 8). Le principe d'inclusion donne qu'il y

$$600 = 1000 - 200 - 166 - 125 + 33 + 25 + 41 - 8$$

entiers qui satisfont la propriété voulue.

Nous sommes maintenant en mesure d'énumérer le nombre de surjections entre deux ensembles.

Proposition 1.11. *Pour des ensembles A et B, avec respectivement n et k éléments ($k \leq n$),*

$$|\mathsf{Surj}[A, B]| = \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n. \tag{1.79}$$

Preuve. Pour chaque sous-ensemble C de B, dénotons $\mathcal{F}_C$ les fonctions qui n'ont pas d'image dans C, c.-à-d. :

$$\mathcal{F}_C := \{f \in \mathsf{Fonct}[A, B] \mid \mathrm{Im}(f) \cap C = \emptyset\}.$$

Autrement dit,

$$\mathcal{F}_C = \mathsf{Fonct}[A, \overline{C}].$$

Bien entendu, par (1.66, iv), le cardinal de cet ensemble est égal à $(k-j)^n$, si j est le nombre d'éléments de C. Utilisant (1.34), on trouve

$$\begin{aligned} \mathcal{F}_{C_1 \cup C_2} &= \mathsf{Fonct}[A, \overline{C_1 \cup C_2}] \\ &= \mathsf{Fonct}[A, \overline{C_1} \cap \overline{C_2}] \\ &= \mathsf{Fonct}[A, \overline{C_1}] \cap \mathsf{Fonct}[A, \overline{C_2}]. \end{aligned}$$

Écrivant plus simplement $\mathcal{F}_y$ pour $\mathcal{F}_{\{y\}}$, il s'ensuit que

$$\mathcal{F}_C = \bigcap_{y \in C} \mathcal{F}_y.$$

D'autre part, l'ensemble $\overline{\mathcal{F}_y}$ étant l'ensemble des fonctions de A dans B, qui ont y dans leur image, il s'ensuit que

$$\mathsf{Surj}[A,B] = \bigcap_{y\in B} \overline{\mathcal{F}_y}. \tag{1.80}$$

On est donc maintenant bien placé pour pouvoir utiliser le principe d'inclusion-exclusion dans le calcul du cardinal de $\mathsf{Surj}[A,B]$. Le calcul se déroule comme suit :

$$\begin{aligned}
|\mathsf{Surj}[A,B]| &= \left|\bigcap_{y\in B} \overline{\mathcal{F}_y}\right| \\
&= \sum_{C\subseteq B} (-1)^{|C|} \left|\bigcap_{y\in C} \mathcal{F}_y\right| \\
&= \sum_{C\subseteq B} (-1)^{|C|} \,|\mathcal{F}_C| \\
&= \sum_{k=0}^{n} \sum_{C\in\mathcal{P}_k[B]} (-1)^k \,|\mathcal{F}_C| \\
&= \sum_{k=0}^{n} \sum_{C\in\mathcal{P}_k[B]} (-1)^k \,(k-j)^n \\
&= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (k-j)^n.
\end{aligned}$$

ce qui achève la démonstration. ■

1.5 Multi-sous-ensembles et monômes

La notion de « multi-sous-ensemble » apparaît lorsqu'on désire permettre (contrairement aux principes de la théorie des ensembles) la répétition d'éléments d'un ensemble. Pour atteindre cet objectif, on procède comme suit.

Pour chaque élément x, d'un ensemble fini A donné de cardinal k, on se donne un entier μ_x (dans $\mathbb{N}$). C'est la **multiplicité** de x. Un **multi-sous-ensemble** est donc un couple (A,ν), avec une fonction $\nu : A \to \mathbb{N}$ qui associe à chaque élément de A une multiplicité. Si la multiplicité d'un élément est 0, alors l'élément on considère qu'il ne fait pas partie du multi-sous-ensemble. Le **multi cardinal** de (A,ν) est la somme des multiplicités de ses éléments :

$$|A|_\nu := \sum_{x\in A} \nu_x, \qquad \nu_x := \nu(x). \tag{1.81}$$

On désigne par $\mathcal{M}_n[A]$ l'ensemble des multi-sous-ensembles de cardinal n de A. Pour présenter agréablement les multi-sous-ensembles de A, on se sert d'une notation sous forme de **monôme**. Pour ce faire, on considère les éléments de A comme des variables commutatives, c.-à-d. : $x\,y = y\,x$, si x et y sont dans A. On associe alors à un multi-sous-ensemble (A, ν), le monôme

$$\prod_{x\in A} x^{\nu(x)}.$$

L'exposant de x est donc sa multiplicité dans le multi-sous-ensemble, et le cardinal $|A|_\nu$ est le **degré** de monôme. Du ce point de vue monômial, les 7 multi-sous-ensembles de cardinal 6 de l'ensemble $A = \{a, b\}$ correspondent aux 7 monômes de degré 6 de l'ensemble

$$\mathcal{M}_6[A] = \{a^6, a^5b, a^4b^2, a^3b^3, a^2b^4, a\,b^5, b^6\}.$$

Dans le cas $A = [k]$, un monôme est caractérisé par un **vecteur** d'exposants $v = (\nu_1, \nu_2, \ \dots\ , \nu_k)$ dans $\mathbb{N}^k$, avec **norme**

$$|v| := \nu_1 + \nu_2 + \ldots + \nu_k = n, \qquad (\text{avec } \nu_i \geq 0). \tag{1.82}$$

Pour la suite de notre discussion, on considère aussi la notion de **composition** de n en k parts, qui est tout simplement un vecteur n'ayant aucune coordonné égale à 0. Autrement dit, c'est une solution de l'équation

$$\nu_1 + \nu_2 + \ \dots\ + \nu_k = n, \qquad (\text{avec } \nu_i > 0). \tag{1.83}$$

Observons qu'on a une bijection entre l'ensemble $\mathsf{Comp}_k[n]$ des compositions de n en k parts (non nulles), et l'ensemble des sous-ensembles à $k-1$ éléments de l'ensemble $[n-1]$:

$$\mathsf{Comp}_k[n] \xrightarrow{\sim} \mathcal{P}_{k-1}[n-1]. \tag{1.84}$$

Elle s'obtient en associant à une composition $(\nu_1, \nu_2, \ \dots\ , \nu_k)$ de n, le sous-ensemble des sommes partielles

$$\{\nu_1, \nu_1 + \nu_2, \nu_1 + \nu_2 + \nu_3, \ \dots\ , (\nu_1 + \nu_2 + \ \dots\ + \nu_{k-1})\}, \tag{1.85}$$

Inversement, pour un sous-ensemble à $k-1$ éléments

$$\{x_1, x_2, \ \dots\ , x_{k-1}\},$$

de l'ensemble $[n-1]$ (pour lequel les éléments sont placés en ordre croissant), on pose

$$\nu_i := \begin{cases} x_1 & \text{si, } i = 1, \\ x_i - x_{i-1} & \text{si } 2 \leq i \leq k-1, \\ n - x_i & \text{si } i = k. \end{cases} \tag{1.86}$$

On conclut donc que

$$|\mathsf{Comp}_k[n]| = \binom{n-1}{k-1}. \tag{1.87}$$

Avec tout ceci on peut maintenant calculer le nombre de multi-sous-ensembles de cardinal n d'un ensemble à k éléments de la façon suivante. Tout simplement, à chaque vecteur $(\nu_1, \nu_2, \ \dots \ , \nu_k)$ de norme n, on associe bijectivement la composition $(\nu_1 + 1, \nu_2 + 1, \ \dots \ , \nu_k + 1)$ de $n + k$. On a donc une bijection

$$\mathcal{M}_k[n] \xrightarrow{\sim} \mathsf{Comp}_k[n + k - 1]. \tag{1.88}$$

Il s'ensuit que le cardinal cherché est

$$|\mathcal{M}_k[n]| = \binom{n+k-1}{k}. \tag{1.89}$$

C'est ce qu'on appelle le **coefficient binomial de 2-ième sorte** :

$$\left(\!\!\binom{n}{k}\!\!\right) := \binom{n+k-1}{k}. \tag{1.90}$$

Fonctions et opérations. Une **bijection** $f : (A, \mu) \to (B, \nu)$, entre deux multi-sous-ensembles (A, μ) et (B, ν), est une fonction bijective de A vers B telle que la multiplicité de $f(x)$ est égale à la multiplicité de x, c.-à-d. : $\nu(f(x)) = \mu(x)$. On dit que f **respecte la multiplicité**. En particulier, deux multi-sous-ensembles ont même cardinal, si et seulement si il existe une bijection entre les deux.

Les opérations sur les ensembles s'étendent aux multi-sous-ensembles de façon assez directe. En fait, la situation est même parfois plus simple. Ainsi, la **somme** est plus naturelle dans ce contexte, puisqu'on pose

$$(A, \mu) + (B, \nu) := (A \cup B, \tau), \tag{1.91}$$

avec la fonction de multiplicité τ définie comme

$$\tau(x) := \begin{cases} \mu(x) + \nu(x) & \text{si, } x \in A \cap B \\ \mu(x) & \text{si, } x \in A \quad \text{et} \quad x \notin B \\ \nu(x) & \text{si } x \notin A \quad \text{et} \quad xt \in B. \end{cases}, \tag{1.92}$$

D'autre part, le **produit cartésien** se définit en posant

$$(A, \mu) \times (B, \nu) := (A \times B, \tau), \tag{1.93}$$

avec la fonction de multiplicité τ définie comme

$$\tau(x,y) := \mu(x)\,\nu(y), \tag{1.94}$$

C'est définitions font en sorte qu'on a encore

Proposition 1.12. *Si (A,μ) et (B,ν) sont des multi-sous-ensembles finis, alors on a les égalités suivantes :*

$$\text{(i) } |A+B|_\tau = |A|_\mu + |B|_\nu, \quad \text{(ii) } |A\times B|_\tau = |A|_\mu\,|B|_\nu. \tag{1.95}$$

Bien entendu les définitions de somme généralisée (1.15) et produit cartésien généralisé (1.23) s'adaptent de façon analogue au contexte des multi-sous-ensembles.

1.6 Suite et séries génératrices

Lorsqu'on cherche à trouver une formule pour le nombre a_n de structures construites sur un ensemble à n éléments, des outils adéquats facilitent grandement le travail. L'objectif visé par l'introduction (C'est une idée qui remonte au moins à Euler.) de la **série génératrice (ordinaire)**, et de la **série génératrice exponentielle**,

$$\sum_{n=0}^{\infty} a_n\, z^n, \quad \text{et} \quad \sum_{n=0}^{\infty} a_n\, \frac{z^n}{n!}, \tag{1.96}$$

d'une suite de nombres $(a_n)_{n\in\mathbb{N}}$, est de faciliter ces manipulations. En effet, un phénomène fascinant se produit alors, puisque des calculs très classiques sur les séries (et les fonctions associées) correspondent à des manipulations combinatoires très naturelles. Nous aurons plusieurs fois l'occasion de le constater, mais ce n'est qu'au chapitre sur la théorie des « espèces de structures » qu'on pourra véritablement bien mettre en évidence cette relation intime entre l'algèbre des fonctions et celle des opérations combinatoires.

Leonhard Euler
(1707–1783)

Pour cette approche, l'un des principes fondamentaux est le **critère d'égalité** est que deux séries ne peuvent être égales que si leurs coefficients coïncident. Autrement dit,

$$\sum_{n=0}^{\infty} a_n\, z^n = \sum_{n=0}^{\infty} b_n\, z^n$$

si et seulement si

$$a_n = b_n, \qquad \text{pour tout } n \in \mathbb{N}.$$

C'est donc dire que la série (1.96) caractérise entièrement la suite $(a_n)_{n\in\mathbb{N}}$. Lorsque le développement en série de Taylor d'une fonction $f(z)$ (sur les réels) est

$$f(z) = \sum_{n=0}^{\infty} a_n\, z^n \qquad \left(\text{resp.} \qquad f(z) = \sum_{n=0}^{\infty} a_n\, z^n\right), \tag{1.97}$$

on dit que $f(t)$ est la **fonction génératrice ordinaire** de la suite des nombres a_n (respectivement **fonction génératrice exponentielle**). Pour bien mettre en évidence l'intérêt de travailler avec de tels outils, nous allons commencer par étudier un exemple.

Considérons l'identité bien connue

$$e^{(s+t)\,z} = e^{s\,z} \cdot e^{t\,z}.$$

En développant en série chaque membre de l'égalité, on obtient le calcul (Voir (1.102) pour le produit de séries)

$$\begin{aligned} \sum_{n\geq 0} (s+t)^n\, \frac{z^n}{n!} &= \sum_{n\geq 0} s^n\, \frac{z^n}{n!} \sum_{n\geq 0} t^n\, \frac{z^n}{n!} \\ &= \sum_{n\geq 0} \left(\sum_{k=0}^{n} \binom{n}{k} s^k\, t^{n-k} \right) \frac{z^n}{n!}. \end{aligned}$$

Selon le critère d'égalité de séries, on doit avoir l'identité

$$(s+t)^n = \sum_{k=0}^{n} \binom{n}{k} s^k\, t^{n-k}. \tag{1.98}$$

C'est là très exactement l'identité du binôme de Newton (1.77). Pour faciliter les calculs à venir, il est bon de rappeler [8] qu'on a

$$(1+z)^t = \sum_{k=0}^{\infty} t_{(k)}\, \frac{z^k}{k!}. \tag{1.99}$$

où on peut même considéré t comme étant une variable quelconque.

8. Voir votre cours de calcul.

Opérations sur les séries génératrices. Les séries que nous considérons ici sont des **séries formelles**, c'est-à-dire que les préoccupations habituelles (convergence, etc) de l'Analyse ne s'appliquent pas. Le point de vue est celui de l'Algebre, et nous nous préoccupons plutôt des manipulations [9] qu'il est possible d'effectuer sur ces séries (qu'on conçoit plus comme étant des polynômes de degré infini).

Étant données deux séries formelles $f(z) = \sum_{n\geq 0} a_n\, z^n$ et $g(z) = \sum_{n\geq 0} b_n\, z^n$, on a considéré les opérations

a) la **somme** :

$$f(z) + g(z) := \sum_{n\geq 0} (a_n + b_n)\, z^n, \tag{1.100}$$

b) le **produit** (ou **produit de Cauchy**)

$$f(z)g(z) := \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) z^n, \tag{1.101}$$

b') dans le cas exponentiel, on a plutôt

$$f(z)g(z) := \sum_{n\geq 0} \left(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \right) \frac{z^n}{n!}, \tag{1.102}$$

c) la **puissance** n-ième d'une série :

$$f(z)^n := \begin{cases} f(z)\, f(z)^{n-1} & \text{si, } n > 0 \\ 1 & \text{si, } n = 0, \end{cases} \tag{1.103}$$

d) la **dérivée**

$$f'(z) = \sum_{n\geq 0} (n+1)\, a_{n+1}\, z^n, \qquad \text{ou} \qquad f'(z) = \sum_{n\geq 0} a_{n+1}\, \frac{z^n}{n!} \tag{1.104}$$

e) et l'**intégrale**

$$\int_0^z f(t)\, dt = \sum_{n\geq 0} \frac{a_n}{n+1}\, z^{n+1}., \qquad \text{ou} \qquad \int_0^z f(t)\, dt = \sum_{n\geq 0} a_n\, \frac{z^{n+1}}{(n+1)!} \tag{1.105}$$

9. Lorsque la situation est essentiellement la même pour les deux notions de séries, nous ne présentons que le cas ordinaire.

On a ensuite des opérations un peu plus complexes comme

f) l'**inverse**[10] pour le produit, $(f(z))^{-1} = 1/f(z)$, que l'on ne considère que dans le cas où $a_0 = 1$ dans $f(z)$:

$$(f(z))^{-1} := \sum_{n\geq 0} c_n\, z^n, \tag{1.106}$$

où $c_0 = 1$, et les c_n satisfont les équations

$$c_n = \sum_{k=0}^{n-1} c_k\, a_{n-k}. \tag{1.107}$$

Le système d'équations (1.107) est triangulaire :

$$\begin{aligned}
c_0 &= 1,\\
c_1 &= -c_0\, a_1,\\
c_2 &= -c_0\, a_2 - c_1\, a_1,\\
c_3 &= -c_0\, a_3 - c_1\, a_2 - c_2\, a_1,\\
c_4 &= -c_0\, a_4 - c_1\, a_3 - c_2\, a_2 - c_3\, a_1,\\
c_5 &= -c_0\, a_5 - c_1\, a_4 - c_2\, a_3 - c_3\, a_2 - c_4\, a_1,\\
&\vdots
\end{aligned}$$

On trouve que c_k s'exprime comme un polynôme en les a_i :

$$\begin{aligned}
c_0 &= 1,\\
c_1 &= -a_1,\\
c_2 &= {a_1}^2 - a_2,\\
c_3 &= -{a_1}^3 + 2\, a_1\, a_2 - a_3,\\
c_4 &= {a_1}^4 - 3\, {a_1}^2 a_2 + 2\, a_1\, a_3 + {a_2}^2 + a_4,\\
c_5 &= -{a_1}^5 + 4\, a_2\, {a_1}^3 - 3\, a_3\, {a_1}^2 - 3\, a_1\, {a_2}^2 + 2\, a_1 a_4 + 2\, a_2\, a_3 - a_5,\\
&\vdots
\end{aligned}$$

L'opération la plus riche est très certainement la **substitution** qui n'est définie que lorsque $g(0) = b_0 = 0$,

g) et alors

$$\begin{aligned}
f(g(x)) &= \sum_{n\geq 0} a_n\, (g(x))^n. \qquad (1.108)\\
&= a_0 + a_1 b_1 x + \left(a_2 {b_1}^2 + a_1 b_2\right) x^2 + \left(a_3 {b_1}^3 + 2\, a_2 b_1 b_2 + a_1 b_3\right) x^3\\
&\qquad + \left(a_4 {b_1}^4 + 3\, a_3 {b_1}^2 b_2 + 2\, a_2 b_1 b_3 + a_2 {b_2}^2 + a_1 b_4\right) x^4 + \ \ldots
\end{aligned}$$

10. Attention de ne pas confondre avec l'inverse pour la composition.

Pour plus de détails sur l'utilisation de séries génératrices et de fonctions génératrices, voir [44].

1.7 Exercices

1.1. Montrer que, pour tous ensembles A et B on a

a) $A = A \cup B$ si et seulement si $B = A \cap B$.

b) $A \cup (A \cap B) = A$, et $A \cap (A \cup B) = A$,

1.2. Montrer que, pour tous ensembles A, B et C deux à deux disjoints, on a

a) $A + \emptyset = A$,

b) $A + B = B + A$,

c) $A + (B + C) = (A + B) + C$.

Pour une famille $\{A_k\}_{i \in I+J}$ d'ensembles deux à deux disjoints, avec I et J disjoint, alors on a aussi

d) $$\sum_{k \in I+J} A_k = \left(\sum_{i \in I} A_i\right) + \left(\sum_{j \in J} A_j\right).$$

1.3. Montrer l'identité (1.24) en considérant la bijection qui associe à deux suites $(x_i)_{i \in I}$ et $(y_j)_{j \in J}$, pour I et J disjoints, la nouvelle suite $(z_k)_{k \in K}$, avec $K = I + J$, où

$$z_k := \begin{cases} x_k & \text{si, } k \in I \\ y_k & \text{si, } k \in J. \end{cases}$$

Suggestion : Observer que lorsque $I = [n]$ et $J = [m]$, alors la bijection prend la forme

$$((x_1, \ \ldots \ , x_n), (y_1, \ \ldots \ , y_m)) \qquad \mapsto \qquad (x_1, \ \ldots \ , x_n, y_1, \ \ldots \ , y_m).$$

1.4. Montrer que les ensembles à un élément (les singletons) sont des identités pour le produit cartésien (à une bijection près).

1.5. Montrer que, pour des familles d'ensembles $\{A_i\}_{i \in I}$ et $\{B_i\}_{i \in I}$, avec A_i disjoint de B_i pour tout i, on a (a une bijection près)

$$\prod_{i \in I} (A_i + B_i) = \sum_{K \subseteq I} \left(\prod_{k \in K} A_k\right) \times \left(\prod_{j \in \overline{K}} B_j\right). \tag{1.109}$$

1.6. Montrer que

a) $f : A \to B$ est injective ssi il existe $g : B \to A$ tel que $g \circ f = \mathrm{Id}_A$.

b) Le composé de fonctions injectives est injectif.

c) Donner un exemple d'une fonction injective de $\{a, b\}$ dans $\{1, 2, 3\}$, ainsi que deux inverses à gauche distincts de cette fonction.

d) $f : A \to B$ est surjective ssi il existe $g : B \to A$ tel que $f \circ g = \mathrm{Id}_B$.

e) Le composé de fonctions surjectives est surjectif.

c) Donner un exemple d'une fonction surjective de $\{a, b, c\}$ dans $\{1, 2\}$, ainsi que deux inverses à droite distincts de cette fonction.

1.7. Démontrer les Propositions 1.4 et 1.5. Suggestion : Montrer que $f^+ \circ f^- = \mathrm{Id}_{\mathcal{P}[A]}$, et utiliser l'exercice 1.6.

1.8. Vérifier que la correspondance

$$C \longleftrightarrow \chi_C$$

donne une bijection entre l'ensemble $\mathcal{P}[A]$ et l'ensemble $\mathsf{Fonct}[A, \{0, 1\}]$.

1.9. Montrer que $n!$ est le nombre de bijections entre deux ensembles de cardinal n.

1.10 (Coefficients binomiaux).

a) Montrer directement (à partir de la définition 1.70) qu'on a les identités

$$\text{i)}\ \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \quad \text{et} \quad \text{ii)}\ \binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}. \tag{1.110}$$

b) Montrer que ii) se déduit aussi de l'identité (1.17).

c) Montrer qu'on déduit

$$\binom{n+k}{j} = \sum_{i=0}^{j} \binom{n}{i}\binom{k}{j-i}. \tag{1.111}$$

de la bijection (1.19).

d) Utiliser la formule du binôme de Newton (1.77) pour montrer que

$$\sum_{i=0}^{n} \frac{1}{i+1}\binom{n}{i} = \frac{2^{n+1}-1}{n+1}. \tag{1.112}$$

Suggestion : Intégrer chaque membre de la formule du binôme.

e) Montrer par récurrence les identités

$$\text{i)}\ \sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}, \quad \text{et} \quad \text{ii)}\ \sum_{i=0}^{k} \binom{n+i}{i} = \binom{n+k+1}{k}. \tag{1.113}$$

1.11. Soit s et t des variables quelconques, et n dans $\mathbb{N}$. Prouver les formules :

a) $t^{(n)} = (-1)^n\,(-t)_{(n)}$,

b) $(t+s)_{(n)} = \displaystyle\sum_{k=0}^{n} \binom{n}{k}\, t_{(k)}\, s_{(n-k)}$,

c) $(t+s)^{(n)} = \displaystyle\sum_{k=0}^{n} \binom{n}{k} t^{(k)}\, s^{(n-k)}$.

1.12.$^{(*)}$ Soit A et B deux ensembles, avec $|A| = n$ et $|B| = k$, et x tel que $x \notin A$.

a) Montrer qu'on a l'identité

$$\begin{aligned} \mathsf{Surj}[A+\{x\}, B] \;&=\; \sum_{y\in B} \Big\{ f + \{(x,y)\} \mid f \in \mathsf{Surj}[A,B] \Big\} \\ &\qquad + \sum_{y\in B} \Big\{ f + \{(x,y)\} \mid f \in \mathsf{Surj}[A, B\setminus\{y\}] \Big\} \end{aligned} \tag{1.114}$$

b) Décrire l'identité (1.114) au moyen d'un dessin.

c) En déduire que les nombres $T(a,b) := |\mathsf{Surj}[A,B]|$ satisfont la récurrence

$$T(n,k) = k\,T(n-1,k) + k\,T(n-1,k-1), \tag{1.115}$$

avec les conditions initiales, $T(n,1) = 1$, $T(0,0) = 1$, et $T(n,k) = 0$ lorsque $n < k$.

1.13. Soit A de cardinal n, et B de cardinal k. Considérons l'ensemble $\mathsf{Fonct}_j[A,B]$ des fonctions dont l'image est de cardinal j :

$$\mathsf{Fonct}_j[A,B] := \{ f : A \to B \mid |\mathrm{Im}(f)| = j \}.$$

Montrer que

a) $\mathsf{Fonct}_j[A,B] = \displaystyle\sum_{C\in\mathcal{P}_j[B]} \mathsf{Surj}[A,C]$,

b) En déduire l'identité

$$k^n = \sum_{j=1}^{k} \binom{k}{j}\, T(n,j), \tag{1.116}$$

où les nombres $T(n,k)$ sont tels que définit en (1.115).

1.14. Rappelons qu'une composition de n en k parts est une solution en entiers positifs non nuls à l'équation

$$\nu_1 + \nu_2 + \;\ldots\; + \nu_k = n.$$

a) Trouver toutes les compositions de n, pour k allant de 1 à n, avec $n \leq 4$.

b) Prouver que le nombre total de compositions de n est 2^{n-1}.

c) Trouver une bijection explicite entre l'ensemble des compositions de n en k parts, et l'ensemble des compositions de n en $n-k+1$ parts.

1.15. Généraliser une construction de la preuve du Théorème 1.7 en montrant que, pour A de cardinal n, on peut construire explicitement une bijection

$$\mathsf{Inj}[A,C] \xrightarrow{\sim} \sum_{B\in\mathcal{P}_n[C]} \mathsf{Bij}[B,C]. \tag{1.117}$$

1.16 (Ensembles pondérés).(*) Soit $\mathcal{R}$ un anneau commutatif. Un **ensemble pondéré**, à valeur dans $\mathcal{R}$, est un couple (A,α), où A est un ensemble fini, et $\alpha : A \to \mathcal{R}$ est une fonction qui associe un **poids** $\alpha(x)$ à chaque élément x de A. Si la fonction de poids est clairement identifiée, on désigne plus simplement par A l'ensemble pondéré en question. Le **cardinal (pondéré)** d'un tel ensemble pondéré A est

$$|A| := \sum_{x\in A} \alpha(x).$$

On définit la **somme disjointe** et le **produit cartésien** d'ensembles pondérés (A,α) et (B,β), en posant

$$(A,\alpha)+(B,\beta) := (A+B,\omega), \quad \text{et} \quad (A,\alpha)\times(B,\beta) := (A\times B,\gamma),$$

avec

$$\omega(z) := \begin{cases} \alpha(z) & \text{si, } z\in A \\ \beta(z) & \text{si } z\in B. \end{cases}, \quad \text{et} \quad \gamma((x,y)) := \alpha(x)\,\beta(y).$$

a) Montrer qu'on a alors

$$|A+B| = |A|+|B|, \quad \text{et} \quad |A\times B| = |A|\,|B|.$$

b) On pondère les ensembles $\mathcal{P}[S]$ et $\mathcal{P}_k[S]$ en donnant le poids t^k aux parties à k éléments de S. Montrer que, si S contient n éléments, on a

$$|\mathcal{P}[S]| = (1+t)^n, \quad \text{et} \quad |\mathcal{P}_k[S]| = \binom{n}{k} t^k,$$

c) En déduire, via (1.16), la formule du **binôme de Newton** :

$$(1+t)^n = \sum_{k=0}^{n} \binom{n}{k} t^k. \tag{1.118}$$

1.17. Quel que soit les ensembles A, B, et C, respectivement de cardinal n, k, et m,

a) trouver des bijections explicites :

$$\begin{aligned} &\text{i) } \mathsf{Fonct}[A+B,C] \xrightarrow{\sim} \mathsf{Fonct}[A,C] \times \mathsf{Fonct}[B,C], \\ &\text{ii) } \mathsf{Fonct}[A,B\times C] \xrightarrow{\sim} \mathsf{Fonct}[A,B] \times \mathsf{Fonct}[A,C], \\ &\text{iii) } \mathsf{Fonct}[A,\mathsf{Fonct}[B,C]] \xrightarrow{\sim} \mathsf{Fonct}[A\times B,C]. \end{aligned} \tag{1.119}$$

b) En déduire que

$$\text{i) } m^{n+k} = m^k\, m^n, \qquad \text{ii) } (m\cdot k)^n = m^n\, k^n, \quad \text{et} \quad \text{iii) } (m^k)^n = m^{k\,n} \tag{1.120}$$

1.18. Prouver que $e^{-x}\cdot e^x = 1$ implique l'identité

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0,$$

pour $n \geq 1$.

1.19. Montrer que

$$\text{a) } \left(\frac{1}{1-z}\right)^t = \sum_{k=0}^{\infty} t^{(k)}\,\frac{z^k}{k!}, \qquad \text{b) } \left(\frac{1}{1-z}\right)^n = \sum_{k=0}^{\infty} \left(\!\!\binom{n}{k}\!\!\right) z^k, \qquad \text{c) } \log\frac{1}{1-z} = \sum_{k=1}^{\infty} \frac{z^k}{k}. \tag{1.121}$$

Programmation mathématique

1.20 (Génération de sous-ensembles).

a) Au moyen de la formule (1.17), écrire une procédure récursive qui calcule l'ensemble des parties à k éléments d'un ensemble.

b) Utiliser la bijection entre $\mathcal{P}[A]$ et $\mathsf{Fonct}[A,\{0,1\}]$ pour construire une autre procédure de calcul de $\mathcal{P}[A]$.

c) Écrire une procédure qui engendre aléatoirement (avec distribution uniforme [11]) un élément de $\mathcal{P}_k[A]$.

1.21. Concevoir des procédures [12] qui, étant donnés des ensembles finis A et B, et k dans $\mathbb{N}$, engendrent les ensembles :

$$\text{a) } \mathsf{Rel}_k[A,B], \quad \text{b) } \mathsf{Fonct}[A,B], \quad \text{c) } \mathsf{Bij}[A,B], \quad \text{d) } \mathsf{Inj}[A,B], \quad \text{e)}^{(*)}\ \mathsf{Surj}[A,B]$$

Attention, ces ensembles deviennent rapidement très grands.

11. Chaque élément doit avoir la même probabilité d'être engendré, à savoir $1/N$, où N est le nombre d'éléments de l'ensemble concerné.

12. Les exercices marqués d'une étoile $(*)$ sont plus difficiles.

1.22. Concevoir des procédures de calcul formel qui, étant donnés des ensembles finis A et B, engendrent aléatoirement (avec distribution uniforme) un élément de :

a) $\mathsf{Rel}_k[A, B]$, b) $\mathsf{Fonct}[A, B]$, c) $\mathsf{Bij}[A, B]$, d) $\mathsf{Inj}[A, B]$, e)$^{(*)}$ $\mathsf{Surj}[A, B]$

Ces procédures devraient pouvoir fonctionner pour des ensembles beaucoup plus grands que ceux de l'exercice précédent.

Chapitre 2

Relations et graphes

2.1 Introduction

Nous allons maintenant étudier plus en profondeur les relations sur un ensemble A, c.-à-d. : de A vers A. Pour celles-ci, on a plusieurs propriétés intéressantes. Les relations possédant certaines de ces propriétés donnent lieu à de nouveaux concepts importants. L'un d'entre eux est très certainement la notion de graphe, mais plusieurs autres notions vont apparaître naturellement dans ce contexte.

2.2 Relations sur un ensemble

La notion de relation sur un ensemble correspond au cas particulier de relation entre ensembles (au sens du chapitre précédent), avec la particularité que les deux ensembles impliqués coïncident. Ainsi, une **relation** R sur un ensemble A est simplement une relation de A vers A, c.-à-d. : $R \subseteq A \times A$. Il y a donc $2^{(n^2)}$ relations de A vers A, lorsque A contient n éléments. Ainsi, pour $A = \{a, b\}$, on a les 16 relations

$$
\begin{aligned}
\mathsf{Rel}[A, A] = \{\ & \emptyset, \\
& \{(a,a)\}, && \{(a,b)\}, && \{(b,a)\}, && \{(b,b)\}, \\
& \{(a,a),(a,b)\}, && \{(a,a),(b,a)\}, && \{(a,a),(b,b)\}, \\
& \{(a,b),(b,a)\}, && \{(a,b),(b,b)\}, && \{(b,a),(b,b)\}, \\
& \{(a,a),(a,b),(b,a)\}, && \{(a,a),(a,b),(b,b)\}, \\
& \{(a,a),(b,a),(b,b)\}, && \{(a,b),(b,a),(b,b)\}, \\
& \{(a,a),(a,b),(b,a),(b,b)\}\ \}.
\end{aligned}
$$

Si le couple (x, y) est un élément de R, on dit que x est en relation R avec y. On écrit parfois $x\,R\,y$. Il est aussi courant de « dessiner » les couples (x, y) sous la forme d'« arcs » allant du point x au

point y.

Chaque relation donne alors lieu à un dessin qu'on appelle **graphe orienté** sur A. Dans ce contexte, les éléments de A sont appelés **sommets**, et chaque couple (x, y) est un **arc** du graphe. Il est traditionnel de présenter un graphe orienté G comme étant un couple (A, R), avec $R \subseteq A \times A$, pour souligner le rôle de l'ensemble A des sommets. Les graphes orientés de sommets A, et les relations sur A, sont donc deux points de vue différents pour un même objet mathématique. La Figure 2.1 illustre par un dessin [1] cette notion de graphe orienté. On dit d'un arc (x, x) que c'est une **boucle**

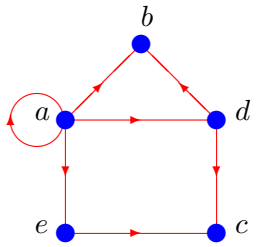


FIGURE 2.1 – Le graphe orienté $\{(a,a),(a,b),(a,d),(a,e),(d,b),(d,c),(a,c)\}$.

du graphe.

On désigne par $\mathsf{Gro}[A]$ l'ensemble des graphes orientés sur A, c.-à-d. :

$$\mathsf{Gro}[A] = \mathcal{P}[A \times A]. \tag{2.1}$$

Ce n'est donc qu'un autre nom pour les relations de A vers A. Les graphes orientés de sommets $\{\bullet, \bullet\}$ sont les 16 graphes de la Figure 2.2.

Une relation R sur A est dite

(a) **réflexive** si pour chaque x dans A, on a $(x, x) \in R$,

(b) **symétrique** si $(x, y) \in R$ entraine $(y, x) \in R$,

(c) **antisymétrique** si $(x, y) \in R$ et $(y, x) \in R$ entraine $x = y$,

(d) **transitive** si $(x, y) \in R$ et $(y, z) \in R$ entraine $(x, z) \in R$.

La plus simple des relations réflexives, sur un ensemble A, est la **relation d'égalité** entre éléments de A. Le sous-ensemble correspondant de $A \times A$ est clairement $\{(x, x) \mid x \in A\}$. Il est parfois dénoté Δ, ou encore Id_A. On dit que deux éléments x et y sont **comparable** pour la relation R, si au moins l'un des deux couples (x, y) ou (y, x) appartiennent à R.

1. Bien entendu, plusieurs dessins différents peuvent correspondent au même graphe. Nous y reviendrons.

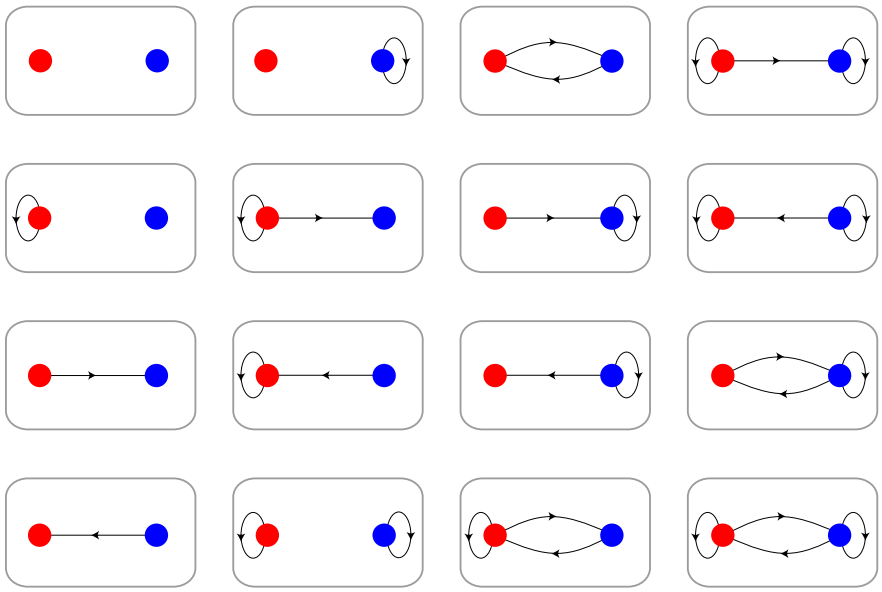


FIGURE 2.2 – Les 16 graphes orientés à deux sommets.

Le graphe orienté correspondant à une relation réflexive contient une boucle en chacun de ses sommets. Lorsque la relation est symétrique, le graphe contient un arc allant de x à y, si et seulement si il contient un arc allant de y à x.

En passant à la fonction caractéristique (comme en (1.40)), on transforme une relation R sur $[n]$ en une matrice carrée $n \times n$, de 1 et de 0, dénoté χ_R. Si la relation R est réflexive, alors la matrice χ_R a des 1 sur sa diagonale principale, c.-à-d. : $\chi_R(i,i) = 1$; et si R est symétrique, alors la matrice χ_R est symétrique. Nous allons voir plus loin que les puissances de la matrice χ_R (pour le produit usuel) ont une signification très naturelle. La matrice associée à la relation d'égalité $\mathrm{Id}_{[n]}$, est la matrice identité $n \times n$. Pour un graphe orienté $G = (A, R)$, on dénote aussi χ_G la matrice de la relation R. On dit que χ_G est la **matrice d'adjacence** du graphe.

On désigne par $\mathsf{Trans}[A]$ l'ensemble des relations réflexives transitives sur A. Il s'ensuit directement des définitions que l'intersection $R_1 \cap R_2$, de deux relations réflexives et transitives R_1 et R_2, est aussi une relation réflexive transitive. Cela implique que

Proposition 2.1. *Pour toute relation R sur A, il existe une unique relation réflexive et transitive $\widehat{R}$ sur A qui est minimale parmi toutes les relations réflexives transitives contenant R.*

Preuve. Il suffit de prendre $\widehat{R}$ égal à l'intersection de toutes les relations réflexives et transitives

sur A qui contiennent R. Autrement dit,

$$\widehat{R} := \bigcap_{\substack{R \subseteq T \\ T \in \mathsf{Trans}[A]}} T. \tag{2.2}$$

Observons que toute relation R est contenue dans la relation transitive $A \times A$. L'intersection en (2.2) a donc lieu sur une famille non vide. ■

On dit que $\widehat{R}$ est la **fermeture transitive** de la relation R. Observons que la fermeture transitive d'une relation symétrique est une relation symétrique. En principe, la Proposition 2.1 fournit une méthode pour calculer la fermeture transitive d'une relation. Cependant, cette méthode est essentiellement impraticable. On verra à la Section 2.6 une méthode efficace pour ce calcul.

Fonctions compatibles avec des relations. Il est fréquent qu'on ait à considérer des fonctions entre deux ensembles, chacun muni d'une relation, et que cette fonction « traduise » une relation dans l'autre. Plus précisément, soit R_1 et R_2 des relations respectivement sur les ensembles A_1 et A_2. On dit alors que $f : A_1 \to A_2$ est **compatible** avec les relations R_1 et R_2, si

$$(x, y) \in R \quad \Longrightarrow \quad (f(x), f(y)) \in S. \tag{2.3}$$

On dit aussi que f est un **morphisme** du graphe orienté $G_1 = (A_1, R_1)$ vers le graphe orienté $G_2 = (A_2, R_2)$, et on écrit $f : G_1 \to G_2$. Le composé de morphismes de graphes est un morphisme de graphe. Intuitivement, f envoie un arc de G_1 sur un arc de G_2, en respectant les notions de source et de but. Par exemple, avec $A_1 = \{a, b, c\}$ et $A_2 = \{1, 2, 3, 4\}$, la fonction

$$f(a) = 1, \qquad f(b) = 3, \quad \text{et} \quad f(c) = 1,$$

donne un morphisme (voir la Figure 2.3) entre les graphes orientés correspondant aux relations

$$\begin{aligned} R_1 &= \{(a, b), (b, b), (b, c)\} \\ R_2 &= \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4)\}. \end{aligned}$$

Si la fonction inverse de f est aussi un morphisme de graphe, alors on dit qu'on a un **isomorphisme** de graphe, c.-à-d. : les deux graphes sont de même forme. Nous allons développer l'étude de toutes ces notions au Chapitre 6.

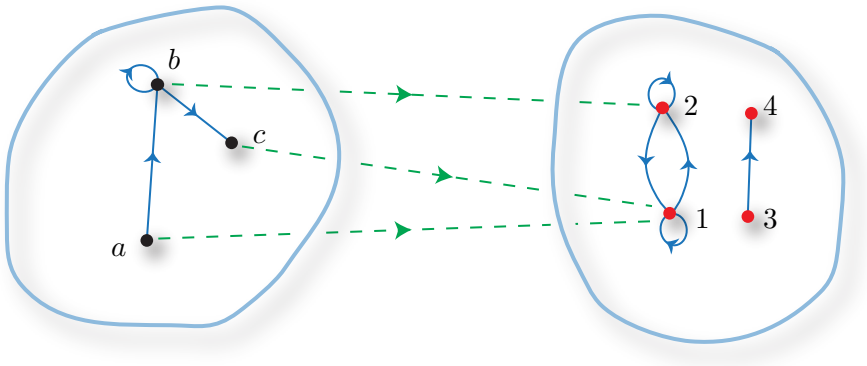


FIGURE 2.3 – Un morphisme de graphe orienté

Relations réflexives symétriques, et graphes simples. Plusieurs relations sont réflexives, mais parmi celles-ci les relations symétriques jouent un rôle particulier. Pour alléger la discussion les concernant, il est courant de simplifier leur présentation de la façon suivante. Puisque tous les couples (x, x) apparaissent dans la relation, on convient de ne pas les écrire (leur présence étant sous-entendue). De plus, pour $x \neq y$, on remplace les deux couples (x, y) et (y, x) par la **paire** $\{x, y\}$ (dont on exploite ici la symétrie $\{x, y\} = \{y, x\}$). Modulo ces simplifications (qui ne nous font pas perdre d'information), une relation réflexive symétrique sur A devient tout simplement un sous-ensemble de $\mathcal{P}_2[A]$. Réciproquement, tout tel sous-ensemble détermine clairement une relation réflexive symétrique.

On rend plus imagée l'étude de ces objets en les dessinant, comme on l'a fait pour les relations en général. On obtient alors la notion de **graphe** (ou **graphe simple**) sur A. Encore une fois, les éléments de A sont les sommets du graphe, mais on a maintenant des **arêtes** (non orientées) $\{x, y\}$, plutôt que des arcs. On dit qu'on a une arête $\{x, y\}$ entre les sommets x et y, et alors les sommets x et y sont dits **adjacents**. Un graphe sur A est donc un couple (A, R), avec R dans $\mathcal{P}[\mathcal{P}_2[A]]$. La Figure 2.4 donne une représentation par dessin du graphe $G = (A, R)$ sur l'ensemble de sommets

$$A = \{a, b, c, d, e\},$$

avec comme arêtes les éléments de l'ensemble

$$R = \{\{a, b\}, \{a, d\}, \{a, e\}, \{b, d\}, \{c, d\}, \{c, e\}\}.$$

Encore une fois, plusieurs dessins différents peuvent correspondent au même graphe. Ainsi le graphe de la Figure 2.4 peut tout aussi bien se dessiner comme à la Figure 2.5 (qui est cependant un peu moins jolie). De plus, il se peut que le graphe soit si complexe qu'un dessin ne soit d'aucune utilité (voir Figure 2.6), sauf peut-être pour les esthètes. Il est classique de souligner qu'un des premiers

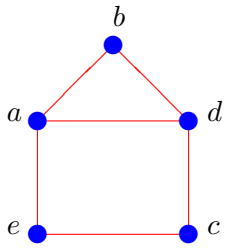


FIGURE 2.4 – Un graphe.

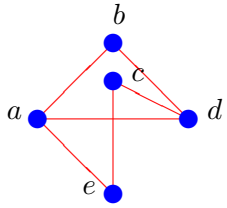


FIGURE 2.5 – Autre représentation du graphe de la Figure 2.4.

problèmes connus de la théorie des graphes (résolut par Euler), consiste à trouver une façon de traverser les 7 ponts de la ville de Konigsberg (telle qu'elle était au 17-ième siècle, voir Figure 2.7) sans passer deux fois par le même pont (Voir Exercice 2.3).

On dénote $\mathsf{Gra}[A]$ l'ensemble des graphes sur A, et on a donc

$$\mathsf{Gra}[A] := \mathcal{P}[\mathcal{P}_2[A]]. \tag{2.4}$$

De même, l'ensemble des graphes sur A qui contiennent exactement k arêtes est

$$\mathsf{Gra}_k[A] := \mathcal{P}_k[\mathcal{P}_2[A]], \tag{2.5}$$

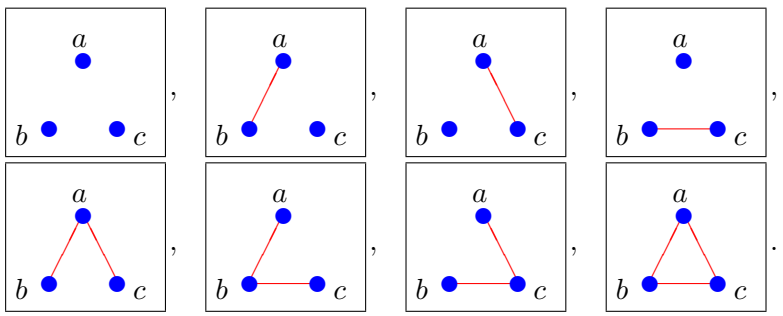
et on a évidemment

$$\mathsf{Gra}[A] = \sum_{k=0}^{n} \mathsf{Gra}_k[A].$$

Le nombre de graphes à a sommets est

$$|\mathsf{Gra}[A]| = 2^{\binom{a}{2}}. \tag{2.6}$$

Pour $A = \{a, b, c\}$, on a les 8 graphes :



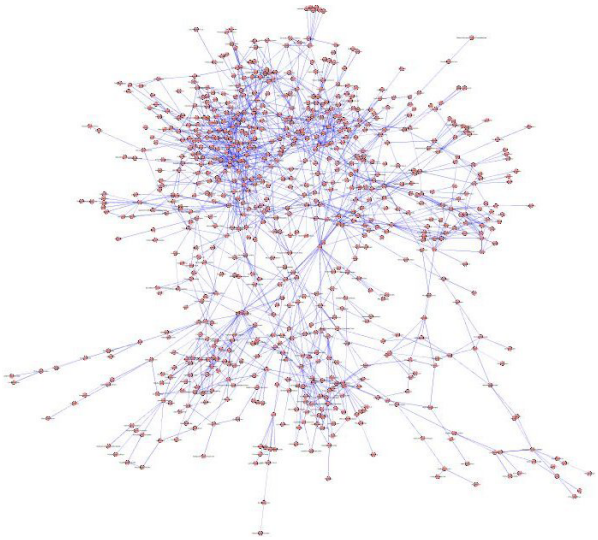


FIGURE 2.6 – Un grand graphe.

Deux graphes très particuliers ressortent, le **graphe discret** $(A, \emptyset)$, qui ne contient aucune arête, et le **graphe complet** $(A, \mathcal{P}_2[A])$, qui contient toutes les arêtes possibles.

L'étude des graphes, et de leurs propriétés, est un vaste domaine sur lequel nous allons revenir.

2.3 Relation d'équivalence

Un autre type important de relation sur un ensemble est celui de **relation d'équivalence** R sur A. C'est une relation qui est à la fois réflexive, symétrique et transitive. Plutôt que d'écrire $(x, y) \in R$, on écrit souvent $x \sim y$, et on dit que x est équivalent à y. Ainsi, $\ll \sim \gg$ est une relation d'équivalence si et seulement si, pour tout x, y et z dans A, on a

(a) $x \sim x$,

(b) si $x \sim y$, alors $y \sim x$,

(c) si $x \sim y$ et $y \sim z$, alors $x \sim z$.

On désigne par $\mathsf{Equiv}[A]$ l'ensemble des relations d'équivalences sur A. Ainsi, pour $A = \{a, b, c\}$, on a les 5 relations d'équivalence

$$\begin{aligned}\mathsf{Equiv}[A] = \{\quad & \{(a,a),(b,b),(c,c)\},\\ & \{(a,a),(b,b),(c,c),(a,b),(b,a)\},\\ & \{(a,a),(b,b),(c,c),(a,c),(c,a)\},\\ & \{(a,a),(b,b),(c,c),(b,c),(c,b)\},\\ & \{(a,a),(b,b),(c,c),(a,b),(b,a),(a,c),(c,a),(b,c),(c,b)\} \quad \}.\end{aligned}$$

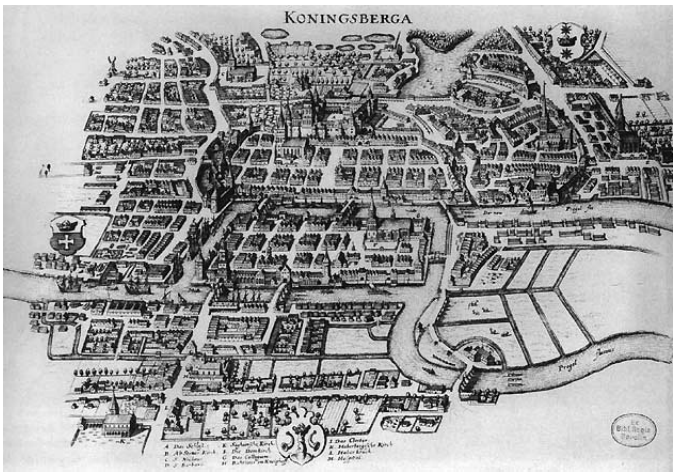


FIGURE 2.7 – Les 7 ponts de Konigsberg en 1652.

La première relation dans cet ensemble est le relation d'égalité entre éléments de A. Il découle de la Proposition 2.1 qu'on peut considérer la notion de relation d'équivalence engendrée par une relation R. C'est la fermeture réflexive, symétrique et transitive de R. Par exemple, la relation d'égalité est la relation d'équivalence engendrée par la relation vide.

Le graphe simple associé à une relation d'équivalence a une structure très particulière. Il se décompose en graphes disjoints qui sont tous complets. Cela mène naturellement à la notion suivante.

Une **classe d'équivalence**, pour une relation d'équivalence $\ll \sim \gg$ sur A, est un sous-ensemble B, de A, qui a tous ses éléments équivalents deux à deux. Autrement dit, on a

(a) pour chaque x, y dans B, on a $x \sim x$,

(b) pour x dans B, si $x \sim x$ alors on a forcément $y \in B$.

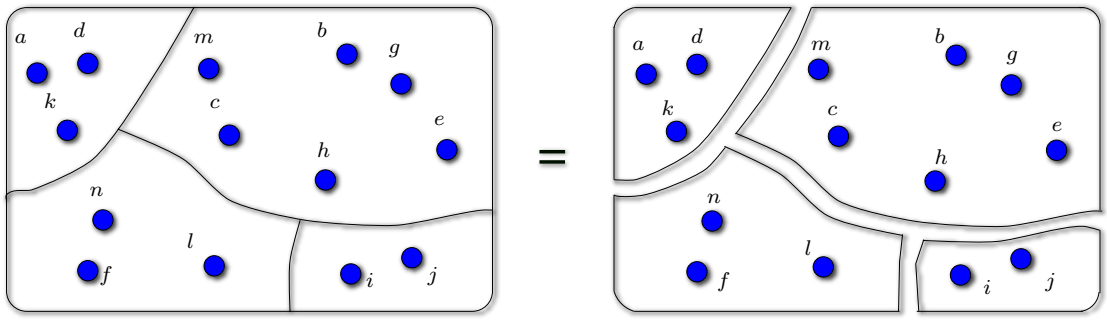


FIGURE 2.8 – Une partition est un recouvrement en parties non vides disjointes.

On dénote $[x]_\sim$ la classe d'équivalence (selon « $\sim$ ») contenant x, et

$$(A/\sim) := \{[x]_\sim \mid x \in A\}, \tag{2.7}$$

dénote **l'ensemble des classes d'équivalences** (on dit aussi que $A/\sim$ est le **quotient** de A par la relation d'équivalence) selon la relation « $\sim$ » sur A. On vérifie que

(a) chaque classe d'équivalence est non-vide,

(b) pour B et C dans $(A/\sim)$, on a $B \cap C \neq \emptyset$ si et seulement si $B = C$,

(c) les classes d'équivalences recouvrent A, c.-à-d. :

$$\bigcup_{B \in (A/\sim)} B = A.$$

Un tel recouvrement est une « partition » de A. Plus généralement, on dit d'une famille $P = (B_i)_{i \in I}$, de sous-ensembles non vides B_i de A, qu'elle forme une **partition** de A si et seulement si

$$B_i \cap B_j = \emptyset, \text{ si } i \neq j, \quad \text{et} \quad A = \bigcup_{i \in I} B_i.$$

Chaque élément de la famille P est une **part** (ou un **bloc**) de la partition P. La notion de partition est illustrée à la Figure 2.8. On vérifie facilement que la donnée d'une partition P de A est équivalente à la donnée d'une relation d'équivalence sur A. En effet, il suffit de poser $a \sim b$ si et seulement si a et b sont dans la même partie de P. Autrement dit, les classes d'équivalence correspondent exactement aux parts de la partition. La Proposition 1.1 affirme que l'ensemble des fibres d'une fonction $f : A \to B$ forme une partition de l'ensemble A. Autrement dit,

Proposition 2.2. *Pour toute fonction $f : A \to B$, on a une relation d'équivalence sur A définie par*

$$x \sim_f y, \quad \text{ssi} \quad f(x) = f(y). \tag{2.8}$$

Les classes d'équivalences correspondantes sont les fibres non vides de f.

On dit de la partition de A donnée par les classes d'équivalences de la relation « $\sim_f$ », que c'est la **partition en fibre** de la fonction f.

Inversement, pour une relation d'équivalence donnée, on peut toujours construire une fonction particulière, la **projection sur le quotient**, dont les fibres sont les classes d'équivalence de cette relation. Cette fonction, dénotée $\pi_\sim : A \to A/\sim$ est simplement définie en posant que $\pi_\sim(x) := [x]_\sim$. C'est clairement une surjection. Avant d'énoncer la proposition reliant ces notions, convenons de dire qu'une fonction $f : A \to B$ est **compatible avec la relation d'équivalence** si et seulement si, pour tout x et y dans A,

$$x \sim y \qquad \Longrightarrow \qquad f(x) = f(y). \tag{2.9}$$

On a alors que

Proposition 2.3. *Si l'ensemble A est muni d'une relation d'équivalence « $\sim$ », et $f : A \to B$ est une fonction compatible avec cette relation, alors, on a une unique fonction $f_\sim : (A/\sim) \longrightarrow B$, telle que $f = f_\sim \circ \pi_\sim$. En fait, on a*

$$f_\sim([x]_\sim) = f(x). \tag{2.10}$$

Pour illustrer tout ceci, considérons sur $A = [6]$ la relation d'équivalence pour laquelle $x \sim y$ si et seulement si $y - x$ se divise par 4. Cette relation contient donc les couples

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

On a donc $(A/\sim) = \{\{1,5\},\{2,6\},\{3\},\{4\}\}$. La fonction $\pi_\sim$ est telle que

$$\pi_\sim(1) = \pi_\sim(5) = \{1,5\}, \qquad \pi_\sim(2) = \pi_\sim(6) = \{2,6\}, \qquad \pi_\sim(3) = \{3\}, \quad \text{et} \quad \pi_\sim(4) = \{4\}.$$

La fonction $f(x) := (-1)^x$ est compatible avec cette relation d'équivalence, puisqu'on a

$$f(1) = f(5) = -1, \qquad f(3) = -1, \qquad f(2) = f(6) = 1, \quad \text{et} \quad f(4) = 1.$$

Quant à elle, la fonction $f_\sim$ est telle que

$$f_\sim(\{1,5\}) = -1 \qquad f_\sim(\{3\}) = -1, \qquad f_\sim(\{2,6\}) = 1,, \quad \text{et} \quad f_\sim(\{4\}) = 1,$$

et on voit bien que $f = f_\sim \circ \pi_\sim$.

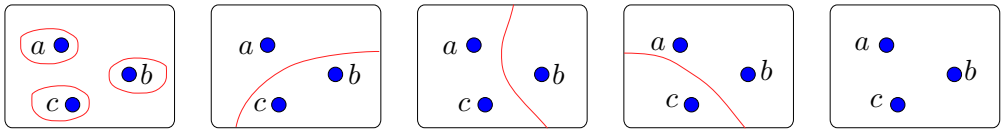
Partitions. On désigne par $\mathsf{Part}[A]$ l'ensemble des partitions de A. Pour $A = \{a,b,c\}$, on a les 5 partitions suivantes :

$$\begin{aligned}\mathsf{Part}[A] = \{ \quad & \{\{a\},\{b\},\{c\}\}, \quad \{\{a\},\{b,c\}\}, \\ & \{\{b\},\{a,c\}\}, \quad \{\{c\},\{a,b\}\}, \quad \{\{a,b,c\}\} \quad \}.\end{aligned}$$

Si les éléments de l'ensemble ordonné A s'y prêtent, on utilise parfois une notation plus compacte (sous forme de mots) pour les partitions sur A. Pour chaque part, on forme un mot en disposant les éléments de la part en ordre croissant, les parts sont placées en ordre lexicographique (l'ordre de leur plus petit élément) et séparé par des tirets. Ainsi, on a

$$\mathsf{Part}[A] = \Big\{a\text{-}b\text{-}c, a\text{-}bc, ac\text{-}b, ab\text{-}c, abc\Big\}.$$

De façon plus imagée, ces mêmes partitions se représentent comme suit :



On a alors la proposition suivante, qui raffine (d'une certaine façon) la Proposition 2.2. Comme nous allons le voir plus explicitement ci-dessous, elle correspond à dire qu'une fonction est caractérisée par sa partition en fibre, et par le choix d'images, distincte deux à deux, pour ces fibres. La proposition est donc une « traduction » du dessin de la Figure 1.2.

Proposition 2.4. *On a une bijection naturelle*[2]

$$\mathsf{Fonct}[A,B] \xrightarrow{\sim} \sum_{P\in\mathsf{Part}[A]} \mathsf{Inj}[P,B]. \tag{2.11}$$

Bien que la notion de « bijection naturelle », dont il est question ici, puisse être formalisée (on en discute un peu en Section 2.4), nous n'allons que l'illustrer en décrivant explicitement comment elle correspond à une traduction évidente des éléments de l'ensemble $\mathsf{Fonct}[A,B]$ en éléments de l'ensemble $\sum_{P\in\mathsf{Part}[A]} \mathsf{Inj}[P,B]$. Un exemple donne une idée claire du processus. Soit donc

$$A=\{a,b,c,d,e,f\}, \quad \text{et} \quad B=\{1,2,3,4\}$$

Considérons la relation fonctionnelle

$$\{(a,1),(b,2),(c,1),(d,2),(e,4),(f,1)\} \qquad \text{dans} \qquad \mathsf{Fonct}[A,B].$$

Les fibres non vides pour cette relation fonctionnelle sont les ensembles

$$\{a,c,f\}, \qquad \{b,d\}, \quad \text{et} \quad \{e\},$$

et la partition en fibre correspondante est donc $P=\{\{a,c,f\},\{b,d\},\{e\}\}$. On a aussi une relation bijective

$$\{(\{a,c,f\},1),(\{b,d\},2),(\{e\},4)\}$$

qui donne les images respectives pour chacune de ces fibres. C'est une relation injective de l'ensemble P vers l'ensemble B. La bijection, dont il est question dans (2.11), est donc celle telle que

$$\{(a,1),(b,2),(c,1),(d,2),(e,4),(f,1)\} \qquad \mapsto \qquad \{(\{a,c,f\},1),(\{b,d\},2),(\{e\},4)\}.$$

Plus généralement, pour une fonction $f : A \to B$ quelconque, la bijection en (2.11) est donc explicitement donnée par la relation bijective

$$\{(x,f(x)) \mid x\in A\} \qquad \mapsto \qquad \{(f^{-}(\{y\}),y) \mid y\in \mathrm{Im}(f)\}. \tag{2.12}$$

2. Voir la Section 2.4.

L'ensemble des partitions de A se décompose clairement en la somme disjointe des **partitions à k-parties** :

$$\mathsf{Part}[A] = \sum_{k=1}^{|A|} \mathsf{Part}_k[A], \tag{2.13}$$

où

$$\mathsf{Part}_k[A] := \{P \in \mathsf{Part}[A] \mid |P| = k\}.$$

Proposition 2.5. *Pour tout ensemble fini A, et $x \notin A$, on a l'identité*

$$\begin{aligned} \mathsf{Part}_k[A + \{x\}] \;=\; & \Big\{P + \{\{x\}\} \mid P \in \mathsf{Part}_{k-1}[A]\Big\} + \\ & \Big\{(P \setminus \{B\}) + \{B + \{x\}\} \mid B \in P,\ P \in \mathsf{Part}_k[A]\Big\}. \end{aligned} \tag{2.14}$$

Évidemment, l'ensemble $\mathsf{Part}_k[A]$ ne contient qu'une seule partition, à savoir la partition

$$\{\{x\} \mid x \in A\}.$$

De même, l'ensemble $\mathsf{Part}_1[A]$ ne contient que la partition $\{A\}$.

Preuve. Le premier terme dans le membre de droite correspond à ajouter une nouvelle part, ne contenant que l'élément x, à une partition en $k-1$ parties de A . Il est clair qu'on obtient ainsi une partition de $A + \{x\}$ constituée d'exactement k parties.

Pour chaque partition P (en k parties) de A, on obtient un élément du second terme de (2.14) en ajoutant x à l'une des parts B de P. Autrement dit, on remplace B par $B + \{x\}$ dans P. Pour ce faire, on enlève d'abord B de P par l'opération $P \setminus \{B\}$; puis on ajoute la part $B + \{x\}$ au résultat, pour obtenir la partition

$$(P \setminus \{B\}) + \{B + \{x\}\}$$

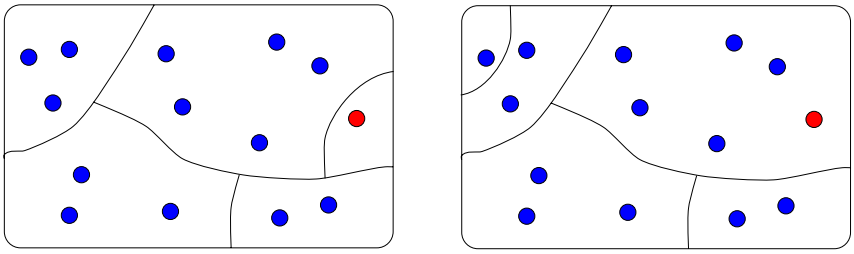
de $A + \{x\}$.

La Figure 2.9, présente de façon un peu plus imagée le processus décrit en (2.14). Les éléments de A sont les points bleus, et le nouvel élément ajouté, x, est représenté par un point rouge. ■

La Proposition 2.5 fournit une procédure récursive (voir Exercice 2.21) pour calculer les partitions en k parties d'un ensemble donné. D'autre part, si on dénote par $\left\{{n \atop k}\right\}$ l'ensemble des partitions en k parties d'un ensemble à n éléments, alors on déduit de (2.14) la récurrence

$$\left\{{n \atop k}\right\} = \left\{{n-1 \atop k-1}\right\} + k \left\{{n-1 \atop k}\right\}, \tag{2.15}$$

avec les conditions initiales $\left\{{n \atop n}\right\} = 1$, $\left\{{n \atop 1}\right\} = 1$, et $\left\{{n \atop k}\right\} = 0$ lorsque $k > n$. Les nombres $\left\{{n \atop k}\right\}$ sont connus sous le nom de **nombres de Stirling de 2-ième sorte**. On a les valeurs suivantes pour ces nombres



$P + \{\{x\}\}$
Ajouter une nouvelle part $\{x\}$.

$(P \setminus \{B\}) + \{B + \{x\}\}$
Ajouter x à une part existante.

FIGURE 2.9 – La construction de l'identité (2.14)

$n \setminus k$	1	2	3	4	5	6	7	8	9	10
1	1									
2	1	1								
3	1	3	1							
4	1	7	6	1						
5	1	15	25	10	1					
6	1	31	90	65	15	1				
7	1	63	301	350	140	21	1			
8	1	127	966	1701	1050	266	28	1		
9	1	255	3025	7770	6951	2646	462	36	1	
10	1	511	9330	34105	42525	22827	5880	750	45	1

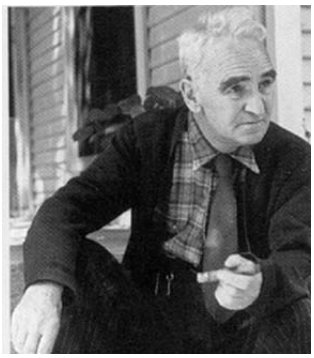
TABLE 2.1 – Les nombres de Stirling de 2-ième sorte : $\left\{ {n \atop k} \right\}$.

En vertu de la formule (2.13), nombre de partitions d'un ensemble à n éléments est donné par la somme

$$B_n := \sum_{k=0}^{n} \left\{ {n \atop k} \right\}. \tag{2.16}$$

On donne le nom de **nombre de Bell** à cette somme, on la dénote B_n. Les premières valeurs des nombres de Bell sont les suivantes

n	0	1	2	3	4	5	6	7	8	9	10	...
B_n	1	1	2	5	15	52	203	877	4140	21147	115975	...



Eric Temple Bell
(1883–1960)

L'énumération pondérée (voir Exercice 1.13) des partitions d'un ensemble à n éléments, avec poids t^k pour les partitions ayant k classes, donne le **polynôme de Bell** :

$$B_n(t) := \sum_{k=0}^{n} \left\{ n \atop k \right\} t^k. \tag{2.17}$$

Ainsi, on a (par le biais de la Table 2.1) que

$$\begin{aligned} B_0(t) &= 1, \\ B_0(t) &= 1+t, \\ B_0(t) &= 1+3t+t^2, \\ B_0(t) &= 1+7t+6t^2+t^3, \vdots \end{aligned}$$

Nous allons revenir au chapitre 6 sur ces polynômes pour en donner une « description » plus explicite. Pour l'instant, voici certaines propriétés des nombres de Stirling, et des nombres de Bell, qu'on peut obtenir par des arguments combinatoires directs.

Proposition 2.6. *On a les formules :*

$$\left\{ n+1 \atop k \right\} = \sum_{j=0}^{n} \binom{n}{j} \left\{ j \atop k-1 \right\}, \tag{2.18}$$

$$B_{n+1} = \sum_{j=0}^{n} \binom{n}{j} B_j. \tag{2.19}$$

Preuve. Pour montrer (2.18), il suffit de considérer, pour une partition de $\{1,2,\ldots,n+1\}$ en k partie, la partie contenant l'élément $n+1$ et, disons, $n-j$ éléments de $\{1,2,\ldots,n\}$. Les j éléments restants de $\{1,2,\ldots,n\}$ doivent être partionnés en $k-1$ parties.

Pour montrer (2.19), on somme (2.18) avec k allant de 1 à $n+1$. Ou encore, on reprend l'argument précédent avec une partition arbitraire cette fois des j éléments restants de $\{1,2,\ldots,n\}$. ■

Proposition 2.7. *Le nombre de fonctions surjectives d'un ensemble, A, à n éléments vers un ensemble, B, à k éléments est $k!\left\{ n \atop k \right\}$. Ainsi :*

$$|\mathsf{Surj}[A,B]| = k! \left\{ n \atop k \right\}. \tag{2.20}$$

Preuve. Ceci découle directement de (2.21). ■

2.4 Bijections naturelles(*)

Comme dans la Proposition 2.11, il se produit souvent qu'on ait deux ensembles qui sont « égaux », au détail près que leurs éléments ne sont pas vraiment les mêmes (à strictement parlé). C'est souvent seulement parce que ces éléments se décrivent de façon légèrement différente, mais cela suffit pour que les ensembles soient différents. Pour illustrer, considérons les ensembles

$$A = \{a, b, c, d, e\}, \quad \text{et} \quad B = \{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\},$$

pour lesquels on a l'élément x dans A si et seulement si l'ensemble $\{x\}$ est dans B. On a $x \neq \{x\}$, et ces deux ensembles sont en fait disjoint. Cela est normal, et même désirable si l'on veut pouvoir faire correctement toute sorte d'autres constructions.

Cependant, il y a clairement façon de passer de l'ensemble A à l'ensemble B par une bijection qui s'impose presque comme allant de soi, c.-à-d. :

$$x \mapsto \{x\}.$$

En comparaison, toutes les autres bijections entre A et B (il y en a 119 autres) semblent totalement « artificielles ».

On dit informellement [3] qu'on a une **bijection naturelle** entre A et B. Par exemple, en généralisant l'exemple ci-dessus, on a une bijection naturelle entre les ensembles A et $\mathcal{P}_1[A]$:

$$A \xrightarrow{\sim} \mathcal{P}_1[A].$$

Il serait en fait catastrophique d'avoir une véritable égalité entre ces deux ensembles, mais la bijection naturelle joue presque un rôle analogue (sans les conséquences fâcheuses qu'aurait une égalité). Une autre façon de penser aux bijections naturelles est de considérer qu'elles décrivent un processus de traduction évident des éléments d'un ensemble en ceux d'un autre.

Donnons maintenant un autre exemple plus élaboré, mais aussi plus intéressant.

Proposition 2.8. *Pour tout ensemble fini A et B, avec B de cardinal k, on a une bijection naturelle*

$$\mathsf{Surj}[A, B] \xrightarrow{\sim} \sum_{p \in \mathsf{Part}_k[A]} \mathsf{Bij}[P, B] \tag{2.21}$$

La bijection naturelle sous-jacente est en fait exactement comme en (2.12).

3. Dans le contexte de la théorie des catégories (qui n'est ni présentée ni utilisée dans ce texte) on peut donner un sens précis à la notion de « bijection naturelle ».

2.5 Ordres

Mettre en ordre les éléments d'un ensemble est non seulement naturel, mais cela est parfois essentiel pour pouvoir analyser et comprendre un problème. De plus, lorsqu'on cherche à compter les éléments d'un ensemble de structures, le fait de savoir les énumérer (les présenter successivement) dans un certain ordre facilite grandement le travail. Bref, la notion d'ordre est essentielle pour toutes sortes de raisons [4].

Une **relation d'ordre** (on dit aussi un **ordre**) « $\preceq$ » sur un ensemble A, est n'importe quelle relation qui est à la fois réflexive, antisymétrique et transitive. Si le couple (x, y) fait partie de la relation d'ordre, on écrit $x \preceq y$, et on dit que x est plus petit ou égal à y. On a donc que « $\preceq$ » est un ordre sur A si et seulement si, pour tout x, y et z dans A, on a

(a) $x \preceq x$,

(b) si $x \preceq y$ et $y \preceq x$, alors $x = y$.

(c) si $x \preceq y$ et $y \preceq z$, alors $x \preceq z$.

Un **ensemble ordonné** [5] est un couple $(A, \preceq)$, où « $\preceq$ » est un ordre sur A. Si l'ordre sous-jacent « $\preceq$ » est clair, on écrit aussi plus simplement A, plutôt que $(A, \preceq)$. On écrit $x \prec y$ lorsque $x \preceq y$ et $x \neq y$. Un exemple typique d'ensemble ordonné est obtenu en considérant la relation d'inclusion sur l'ensemble $\mathcal{P}[A]$, des parties de A. En effet, il découle de (1.6) que l'inclusion est bien une relation d'ordre. La Figure 2.13 présente [6] l'ensemble ordonné $(\mathcal{P}[\{a, b, c\}], \subseteq)$.

Attention, la définition d'ensemble ordonné ne signifie pas que l'on puisse comparer tous les éléments de l'ensemble, et cette notion mathématique ne coïncide donc pas avec la notion utilisée « dans la vie courante ». Cette dernière correspond plutôt au concept d'ordre total au sens ci-dessous.

Un **ordre total** (ou **linéaire**) « $\leq$ », est un ordre sur A pour lequel tous les éléments de A sont comparables deux à deux, c.-à-d. : pour chaque a et b dans A, on a soit $a \leq b$ ou $b \leq a$. On dit alors que $(A, \leq)$ (ou simplement A) est un ensemble totalement ordonné, ou encore qu'on a **listé** les éléments de A.

La Figure 2.10 présentes [7] tous les ordres totaux sur l'ensemble $A = \{a, b, c\}$. Les ordres possibles sur $\{a, b, c\}$ incluent non seulement ces 6 ordres totaux, mais aussi les 13 autres de la Figure 2.11, pour un total de 19.

On désigne par $\mathsf{Ord}[A]$ l'ensemble des ordres sur A, et par $\mathbb{L}[A]$ l'ensemble des ordres linéaires sur

4. Pensez au côté peu pratique d'un dictionnaire dans lequel les mots seraient disposés au hasard.
5. Les anglophones parlent de « partially ordered set », et utilisent le néologisme « poset ».
6. Sous la forme du diagramme de Hasse de l'ordre, au sens défini un peu plus loin.
7. Pour simplifier la présentation, on ne dessine pas les boucles qui sont en principe présentes pour tous les sommets.

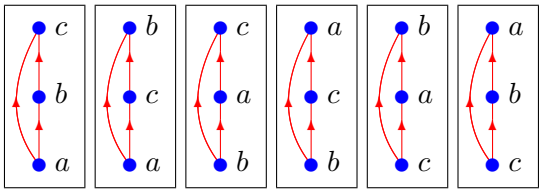


FIGURE 2.10 – Les 6 ordres totaux sur $\{a, b, c\}$.

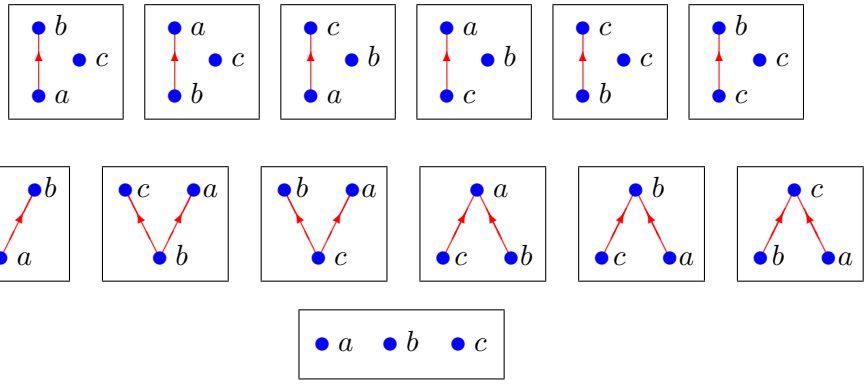


FIGURE 2.11 – Les 13 autres ordres sur $\{a, b, c\}$.

A. Sur l'ensemble $\{a, b\}$, on a les 3 ordres

$$\begin{aligned}\mathsf{Ord}[A] = \{\quad & \{(a,a),(b,b)\},\\ & \{(a,a),(a,b),(b,b)\},\\ & \{(b,b),(b,a),(a,a)\}\quad\}.\end{aligned}$$

La proposition suivante relie la notion d'ordre linéaire sur A aux bijections entre A et $[n]$, où n est le cardinal de A.

Proposition 2.9. *Pour un ensemble A à n éléments, il y a des bijections naturelles*

$$\mathsf{Bij}[n, A] \xrightarrow{\sim} \mathbb{L}[A]. \tag{2.22}$$

Le nombre d'ordres linéaires sur A est donc est $n!$, c.-à-d. :

$$|\mathbb{L}[A]| = n!. \tag{2.23}$$

Preuve. Étant donnée une bijection $f : [n] \xrightarrow{\sim} A$, on pose $f(i) \preceq f(j)$ si et seulement si $i < j$ selon l'ordre usuel sur les entiers. Il est facile de vérifier que cela définit une relation d'ordre linéaire sur A. ■

La **restriction** $\preceq_B$ d'un ordre $\preceq_A$ sur A à un sous-ensemble B de A est une relation d'ordre qui est définie, pour x et y dans B, par le fait que

$$x \preceq_B y \quad \text{ssi} \quad x \preceq_A y. \tag{2.24}$$

On dit aussi que $(B, \preceq_B)$ est un **sous-ordre** de $(A, \preceq_A)$. Si l'ordre est total sur A, alors la restriction de l'ordre à B est un ordre total.

Lorsque A, est un ensemble de cardinal n, on peut décrire les éléments de $\mathbb{L}[A]$ (qui sont tous les ordres totaux sur A) sous la **forme de mots**. Cette description d'un ordre prend la forme

$$x_1 x_2 \ \cdots \ x_n, \tag{2.25}$$

avec $x_i = x(i)$ pour $x : [n] \xrightarrow{\sim} A$, et l'ordre est $x_i < x_i$ ssi $i < j$. Dans cette notation, on a les 6 ordres totaux sur [3] :

$$\mathbb{L}[3] = \{123, 132, 213, 231, 312, 321\}$$

Il n'y a pas encore de formule connue pour le nombre $\mathcal{O}_n$, d'ordres sur un ensemble à n éléments. On connaît au moins les valeurs suivantes :

n	0	1	2	3	4	5	6	7	8	9	...
$\mathcal{O}_n$	1	1	3	19	219	4231	130023	6129859	431723379	44511042511	...

Apparemment, la plus grande valeur connue est pour $n = 16$, et c'est :

$$2419393925972011766028978201480850 23.$$

On n'a jusqu'ici décrit certaines constructions (comme les matrices d'adjacences) que dans le cas de l'ensemble $[n]$. On peut maintenant étendre toutes ces notions aux ensembles totalement ordonnés, en exploitant (2.22).

Pour des éléments distincts x et y d'un ensemble ordonné $(A, \preceq)$, on dit que y **couvre** x, si il n'y a aucun élément de A, autre que x et y, se situant entre x et y. Autrement dit, si $x \preceq z \preceq y$, alors forcément $z = x$ ou $z = y$. On écrit alors $x \to_{\preceq} y$ (ou plus simplement $x \to y$). Toute l'information sur la relation d'ordre peut-être entièrement récupérée (voir Section 2.6) à partir de la **relation de couverture**, $\mathcal{C}_{\preceq}$ (ou plus simplement $\mathcal{C}$), constituée des couples (x, y) pour lesquels x est couvert par y, c.-à-d. :

$$(x, y) \in \mathcal{C}, \quad \text{ssi} \quad x \to y, \tag{2.26}$$

et donc $x \neq y$. Une relation de couverture est **antitransitive**, c.-à-d. :

$$((x, y) \in \mathcal{C} \quad \text{et} \quad (y, z) \in \mathcal{C}) \quad \Longrightarrow \quad (x, z) \notin \mathcal{C}.$$

Une relation d'ordre est tout simplement la fermeture transitive de sa relation de couverture, c'est-à-dire que

$$x \preceq y, \quad \text{ssi} \quad (x, y) \in \widehat{\mathcal{C}}. \tag{2.27}$$

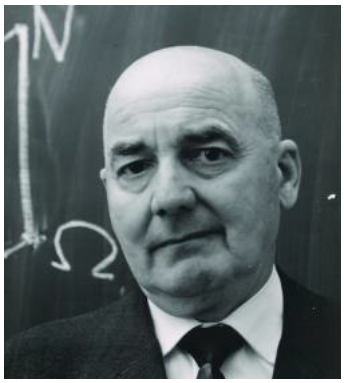
Autrement dit, on a $x \preceq y$ si et seulement si il existe une suite de la forme

$$x = x_0 \to x_1 \to \cdots \to x_k = y,$$

pour un certain $k \geq 0$.

Un ordre est très fréquemment présenté en ne décrivant que la relation de couverture associée, parce que celle-ci est beaucoup plus compacte, où plus simple à présenter. Pour illustrer, observons que n'importe quelle relation d'ordre linéaire sur n éléments contient $n(n+1)/2$ couples, tandis que la relation de couverture correspondante n'en contient que $n-1$.

Le graphe orienté correspondant à la relation de couverture d'un ordre porte habituellement le nom de **diagramme de Hasse** de l'ordre. Pour en simplifier un peu la présentation, on dispose le dessin de façon à ce que les arcs soient tous orientés du bas vers le haut. Du coup, on peut négliger de dessiner la flèche qui indique le sens de parcours de l'arc.



Helmut Hasse
(1898–1979)

Ainsi, on a le diagramme de Hasse de la Figure 2.12, qui décrit une relation de couverture dont les éléments sont

$$\{(123, 213), (123, 132), (213, 231), (132, 312), (231, 321), (312, 321))\},$$

sur l'ensemble $\{123, 132, 213, 231, 312, 321\}$.

Nous allons revoir cet exemple au Chapitre 5. Lorsque la relation d'ordre est totale, le diagramme

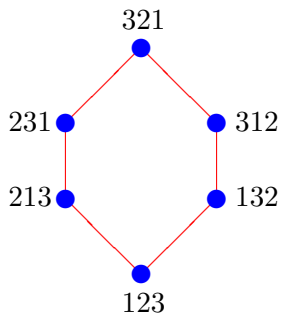


FIGURE 2.12 – Un diagramme de Hasse

de Hasse correspondant est une **chaîne**.

Un **interval** $[x, y]_\preceq$ (ou $[x, y]$), d'un ensemble ordonné $(A, \preceq)$, est l'ensemble des éléments de A qui se trouve entre x et y, c.-à-d. :

$$[x, y]_\preceq := \{z \mid x \preceq z, \quad \text{et} \quad z \preceq y\}. \tag{2.28}$$

En particulier, $[x, y] = \emptyset$ si $x \not\preceq y$, et $[x, y]$ contient exactement deux éléments si et seulement si $x \to y$.

Pour un ensemble ordonné A, on dit que $s \in A$ est le **supremum** de deux éléments x et y de A, si s est le plus petit élément de A qui est à la fois plus grand que x et plus grand que y. S'il existe, le supremum est unique, et on le dénote $x \vee y$. Autrement dit, on a

$$(s \preceq x \quad \text{et} \quad s \preceq y) \quad \text{ssi} \quad s \preceq (x \vee y). \tag{2.29}$$

De façon analogue, on a la notion **d'infimum** de x et y, dénoté $x \wedge y$, avec

$$(x \preceq t \quad \text{et} \quad y \preceq t) \quad \text{ssi} \quad (x \wedge y) \preceq t. \tag{2.30}$$

S'il n'existe aucun élément de A qui soit plus petit que x, alors on dit que x est un **élément minimal** de A, c.-à-d. : $y \preceq x$ implique $y = x$. De façon semblable, x est un **élément maximal** de A, c.-à-d. : $x \preceq y$ implique $x = y$. S'il existe x dans A tel que $x \preceq y$ (resp. $y \preceq x$), pour tout y dans A, on dit que x est le **maximum** (resp. le **minimum**) de A. On désigne souvent par 1 (resp. par 0) le maximum (resp. minimum) d'un ensemble ordonné (qui en a un). Un ensemble ordonné peut ne pas avoir de maximum, ou de minimum (voir Exercice 2.12), mais il a toujours au moins un élément minimal, et au moins un élément maximal.

Graduation. On dit qu'un ensemble ordonné $(A, \preceq)$ est **gradué**, si A est muni d'une **fonction de rang**

$$\rho : A \to \mathbb{Z}, \tag{2.31}$$

avec $\rho(y) = \delta(x) + 1$, si y couvre x dans A. Les ensembles ordonnés n'admettent pas tous des fonctions de rang. Pour voir quand cela est possible, on considère la notion de **chaîne**, i.e : une suite $(x_0, x_1, \ \ldots \ , x_k)$ d'éléments de A telle que $x_i \prec x_{i+1}$. On dit que k est la **longueur** de la chaîne. Une chaîne est dite **maximale** s'il est impossible d'y insérer un élément. Autrement dit, on a que x_{i+1} couvre x_i, pour tout $i < k$. On montre (voir Exercice 2.11) que

Proposition 2.10. *Un ensemble ordonné peut être gradué, si et seulement si toutes les chaînes maximales entre deux éléments ont la même longueur.*

Comme les ensembles que nous manipulons sont toujours finis, on peut toujours choisir la fonction de rang pour que les valeurs soient dans $\mathbb{N}$ (quitte à tout décaler les valeurs). Si A admet un

minimum, on s'arrange de plus pour que son rang soit 0. **L'énumérateur de rang** de A est le polynôme défini comme

$$R_A(t) := \sum_{x \in A} t^{\rho(x)}. \tag{2.32}$$

Un **treillis** est un ensemble ordonné dans lequel toute paire d'éléments admet un infimum et un supremum. Comme nous nous restreignons aux treillis finis, il en découle qu'on a forcément un minimum, et un maximum. Un exemple « typique » de treillis est donné par l'ordre d'inclusion sur l'ensemble des parties de A. Le supremum est l'union, et l'infimum est l'intersection. Ainsi pour les parties de $\{a, b, c\}$, on a le treillis dont le diagramme de Hasse est donné à la figure 2.13.

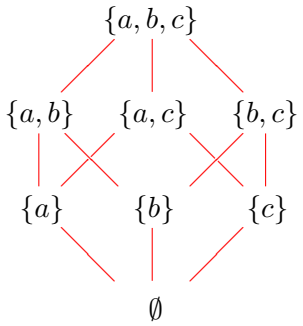


FIGURE 2.13 – Treillis des sous-ensembles de $\{a, b, c\}$

Le treillis des sous-ensembles d'un ensemble A à n éléments, peut-être muni de la fonction de rang

$$\rho : \mathcal{P}[A] \to \mathbb{N},$$

en posant $\rho(B) = k$, si B est un sous-ensemble de cardinal k de A. Le polynôme énumérateur de rang associé est donc

$$\begin{aligned} R_{\mathcal{P}[A]}(t) &= \sum_{k=0}^{n} \binom{n}{k} t^k \\ &= (1+t)^n. \end{aligned} \tag{2.33}$$

Opérations. Si $(A_i, \preceq_i)$ des ensembles ordonnés, avec $i = 1, 2, \ldots, n$, alors on construit les ensembles ordonnés :

1) **somme** : $A_1 + A_2$, où la relation d'ordre est $\preceq := \preceq_1 + \preceq_2$. C'est donc dire que, pour x et y dans $A_1 + A_2$, on a

$$x \preceq y \quad \text{ssi} \quad \begin{cases} x \preceq_1 y, & \text{avec } x \text{ et } y \text{ appartenant à } A_1, \text{ ou} \\ x \preceq_2 y, & \text{avec } x \text{ et } y \text{ appartenant à } A_2. \end{cases}$$

2) **somme ordonnée** : $A_1 \overrightarrow{+} A_2$, avec la relation d'ordre :

$$x \preceq y \quad \text{ssi} \quad \begin{cases} x \preceq_1 y, & \text{avec} \quad x \text{ et } y \text{ appartenant à } A_1, \text{ ou} \\ x \preceq_2 y, & \text{avec} \quad x \text{ et } y \text{ appartenant à } A_2, \text{ ou} \\ x \in A_1 & \text{et} \quad y \in A_2. \end{cases}$$

Si A_1 et A_2 sont totalement ordonnés, alors $A_1 \overrightarrow{+} A_2$ l'est aussi.

3) **produit cartésien général** : $A_1 \times A_2 \times \cdots \times A_n$, avec l'ordre **composantes à composantes** :

$$(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n) \quad \text{ssi} \quad (\forall i)\ x_i \preceq_i y_i.$$

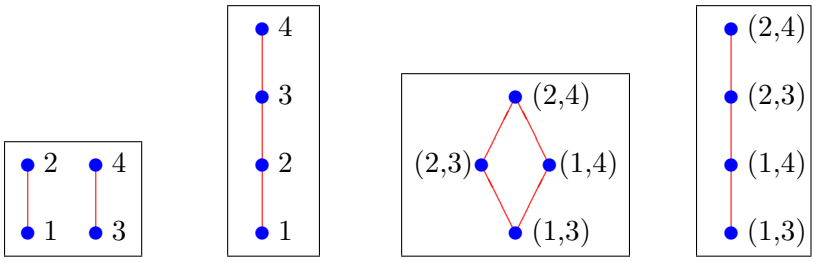


FIGURE 2.14 – Les opérations.

4) **produit lexicographique** : $A_1 \times_\ell A_2$, avec l'ordre :

$$(x_1, x_2) \preceq (y_1, y_2) \quad \text{ssi} \quad \begin{cases} x_1 \preceq_1 y_1, \text{ ou} \\ x_1 = y_1 \quad \text{et} \quad x_2 \preceq_2 y_2. \end{cases}$$

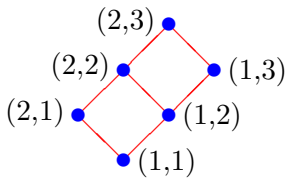
Si A_1 et A_2 sont totalement ordonnés, alors $A_1 \overrightarrow{+} A_2$ l'est aussi.

5) **produit lexicographique général** : $A_1 \times_\ell A_2 \times_\ell \cdots \times_\ell A_n$, avec l'ordre :

$$(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n) \quad \text{ssi} \quad (\exists i)\ x_1 = y_1, \ \ldots, \ x_{i-1} = y_{i-1}, \quad \text{et} \quad x_i \preceq_i y_i.$$

Si les A_i sont totalement ordonnés, alors leur produit lexicographique l'est aussi.

En guise d'exemple, si $A_1 = \{1, 2\}$ et $A_2 = \{3, 4\}$ (chacun avec l'ordre usuel), alors on a les divers ordres présentés à la Figure 2.14, donnés en terme du diagramme de Hasse correspondant. Comme autre exemple, on a aussi le diagramme de Hasse suivant pour $[2] \times [3]$:



Fonctions croissantes. Si A et B sont deux ensembles ordonnés, avec les ordres respectifs $\preceq_A$ et $\preceq_B$. On dit d'une fonction $f : A \to B$ qu'elle est **croissante** si et seulement si, pour tout élément x et y dans A, on a

$$x \preceq_A y \qquad \Longrightarrow \qquad f(x) \preceq_B f(y). \tag{2.34}$$

On désigne par $\mathsf{Croi}[A, B]$ l'ensemble des fonctions croissantes de A vers B. Convenons d'écrire $x \prec y$, lorsque $x \preceq y$ et $x \neq y$. On dit d'une fonction croissante $f : A \to B$ qu'elle est **strictement croissante**, si

$$x \prec_A y \qquad \Longrightarrow \qquad f(x) \prec_B f(y), \tag{2.35}$$

et $\mathsf{Strict}[A, B]$ désigne l'ensemble des fonctions strictement croissantes de A vers B. Bien entendu, on a l'inclusion

$$\mathsf{Strict}[A, B] \subseteq \mathsf{Croi}[A, B]. \tag{2.36}$$

Si A et B sont totalement ordonnés, avec $k = |A| \leq |B|$, alors il y a une bijection naturelle

$$\mathsf{Strict}[A, B] \xrightarrow{\sim} \mathcal{P}_k[B]. \tag{2.37}$$

On a donc, si $n = |B|$,

$$|\mathsf{Strict}[A, B]| = \binom{n}{k}. \tag{2.38}$$

Par exemple, les fonctions strictement croissantes de $[3]$ vers $[5]$ sont (sous forme de mots) :

$$\mathsf{Strict}[3, 5] = \{123, 124, 125, 134, 135, 145, 234, 235, 245, 345\}.$$

En particulier, il y a une et une seule fonction strictement croissante entre A et B, si $k = n$, et c'est forcément une bijection. De plus, le nombre de fonctions croissantes (voir (1.84)) entre A (de cardinal k) et B (de cardinal n) est donné par le coefficient binomial de 2-ième sorte :

$$|\mathsf{Croi}[A, B]| = \left(\!\!\binom{n}{k}\!\!\right), \tag{2.39}$$

puisqu'on a une bijection

$$\mathsf{Croi}[A,B] \xrightarrow{\sim} \mathcal{M}_k[B]. \tag{2.40}$$

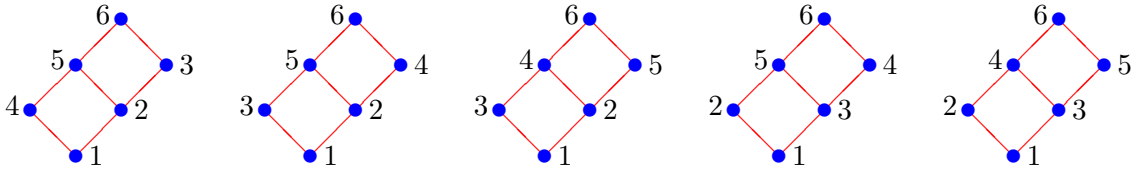
Par exemple, on a

$$\begin{aligned}\mathsf{Croi}[3,4] \;=\; \{&111,\;\; 112,\;\; 113,\;\; 114,\;\; 122,\;\; 123,\;\; 124,\;\; 133,\;\; 134,\;\; 144,\\ &222,\;\; 223,\;\; 224,\;\; 233,\;\; 234,\;\; 244,\;\; 333,\;\; 334,\;\; 344,\;\; 444\}.\end{aligned}$$

Nous allons voir à la section 4.6 que le nombre de fonctions strictement croissantes allant de $[2]\times[n]$ vers $[2\,n]$ est égal au n-ième nombre de Catalan. En formule :

$$|\mathsf{Strict}[[2]\times[n],2\,n]| = \frac{1}{n+1}\binom{2\,n}{n}. \tag{2.41}$$

Par exemple, si on décrit une telle fonction en donnant l'étiquette $f(i,j)$ au sommet correspondant de $[2]\times[3]$ (via la fonction), on obtient les 5 fonctions :



2.6 Chemins dans un graphe orienté

Nous allons maintenant résoudre, par une même construction, plusieurs problèmes soulevés par l'étude des relations et des graphes. L'outil principal est la notion de chemin dans un graphe (orienté). Il s'agit ici de formaliser la notion intuitive correspondant au dessin de la Figure 2.15.

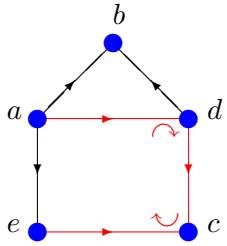


FIGURE 2.15 – Un chemin (en rouge) allant de a à d.

Informellement donc, parcourir un chemin allant de x à y dans un graphe orienté $G=(A,R)$ consiste à suivre une suite d'arcs du graphe, de façon à ce que le but d'un arc soit la source de l'arc suivant. Il est clair que cette notion gagne à être précisée. On en arrive naturellement à la formulation suivante.

Dans un graphe $G = (A, R)$, on dit qu'une suite de sommets

$$\gamma = (x_0, x_1, \ldots, x_k)$$

est un **chemin** allant de x à y, si

a) $x = x_0$,

b) $(x_i, x_{i+1}) \in R$, pour tout i entre 0 et $k-1$.

c) $x_k = y$.

Le sommet $x = s(\gamma)$ est la **source** de γ, $y = b(\gamma)$ est son **but**, et l'entier $\ell(\gamma) := k$ est la **longueur** du chemin. Les chemins de longueur 0 s'identifient aux sommets du graphe. Si on écrit $\mathbb{1}(x, y)$ pour $G^0(x, y)$, alors

$$\mathbb{1}(x,y) = \begin{cases} \{(x)\} & \text{si, } x = y, \\ \emptyset & \text{sinon.} \end{cases}$$

Les chemins de longueur 1 correspondent aux arcs du graphe. Si on écrit simplement $G(x, y)$ pour $G^1(x, y)$, alors

$$G(x,y) = \begin{cases} \{(x,y)\} & \text{si, } (x,y) \in R, \\ \emptyset & \text{sinon.} \end{cases}$$

Il peut y avoir plusieurs chemins (de diverses longueurs) entre deux sommets d'un graphe orienté. On dénote $G^*(x, y)$ l'ensemble de tous les chemins de x à y dans le graphe G, c.-à-d. :

$$G^*(x,y) := \mathbb{1}(x,y) + G(x,y) + G^2(x,y) + \ldots \tag{2.42}$$

En général, cet ensemble est infini. Les définitions suivantes permettent de comprendre dans quels cas tous les ensembles de chemins en question sont finis.

Un **circuit** est un chemin $\gamma = (x_0, x_1, \ldots, x_k)$, avec $k > 0$, dont la source coïncide avec le but, c.-à-d. : $s(\gamma) = b(\gamma)$. On dit qu'un graphe orienté est **acyclique** si et seulement si il ne contient aucun circuit. L'ensemble des graphes acycliques de sommets A est dénoté $\mathsf{Acyc}[A]$. La Figure 2.16 donne un exemple de graphe acyclique. Dans un graphe acyclique G, on dit qu'un sommet x est une **source**, s'l n'y a aucun arc de G dont x soit le but. De même, on dit que x est un **puits**, s'l n'y a aucun arc de G dont x soit la source. Dans le graphe de la Figure 2.16, le somme a est une source, et les sommets b et c sont des puits. Il est facile de montrer que

Proposition 2.11. *Tout graphe acyclique contient au moins une source, et au moins un puits.*

Preuve. On procède par contradiction. Soit G un graphe acyclique sans puits (l'argument est semblable dans le cas des sources). Considérons un chemin $(x_0, x_1, \ldots, x_k)$ dans G. Comme x_k n'est pas un puits, il existe un arc (x, y) dans G via lequel on peut prolonger le chemin ci-haut pour

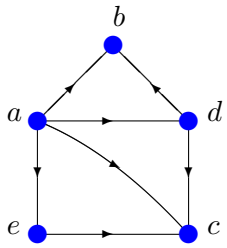


FIGURE 2.16 – Un graphe acyclique.

obtenir le chemin $(x_0, x_1, \ \dots \ , x_k, y)$. Ceci montre qu'il y a un chemin de longueur arbitraire dans G. Par le principe des tiroirs, tout chemin assez long contient forcément deux sommets du chemin qui coïncident, disons $x_i = x_j$ avec $i < j$. On a donc un circuit $(x_i, \ \dots \ , x_j)$ dans le graphe, ce qui contredit l'hypothèse d'acyclicité. ■

En précisant l'idée de cette preuve[8], on peut montrer (voir [39]) que le nombre $\alpha_n := |\mathsf{Acyc}[A]|$ de graphes acycliques sur un ensemble A à n élément est caractérisé par la récurrence

$$\alpha_n = \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} 2^{k\,(n-k)} \alpha_{n-k}, \tag{2.43}$$

et on a les valeurs

n	0	1	2	3	4	5	6	7	8	...
$\lvert\mathsf{Acyc}[n]\rvert$	1	1	3	25	543	29281	3781503	1138779265	783702329343	...

Pour un graphe (orienté) $G = (A, R)$, et $k \geq 0$, **l'ensemble des chemins** de longueur k dans G, ayant x comme source et y comme but, c.-à-d. : se dénote

$$G^k(x, y) := \{ \ \gamma \mid \ell(\gamma) = k, \quad s(\gamma) = x, \quad \text{et} \quad b(\gamma) = y \}. \tag{2.44}$$

L'argument de la preuve de la Proposition 2.11 montre qu'on a aussi

Proposition 2.12. *Dans un graphe acyclique G sur A, de cardinal n, les chemins ont une longueur bornée par le nombre de sommets. On a donc $G^k = \emptyset$ pour tout k n. Il en découle que pour tout sommet x et y, on a :*

$$G^*(x, y) := \mathbb{1}(x, y) + G(x, y) + G^2(x, y) + \ldots + G^n(x, y). \tag{2.45}$$

8. Avec un argument d'inclusion-exclusion qui exploite le choix d'un sous-ensemble de sources.

Composition de chemins. On a une opération de **composition de chemins** $\gamma_1 \cdot \gamma_2$, entre chemins dans un graphe orienté G, défini comme suit. Soit $\gamma_1 = (x_0, x_1, \ldots, x_k)$ de but z et $\gamma_2 = (y_0, y_1, \ldots, y_j)$ de source z (donc $x_k = z = y_0$), on dit alors que γ_1 et γ_2 sont **composables**. Le **composé** de γ_1 et γ_2 est le chemin de de longueur $k + j$

$$\gamma_1 \cdot \gamma_2 := (x_0, x_1, \ldots, x_k, y_1, \ldots, k_j), \tag{2.46}$$

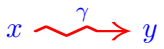
dont la source est la source de γ_1, et le but est le but de γ_2. L'unique chemin (x) de longueur 0, source et de but x, est dénoté 1_x. On a donc que la composition est une fonction

$$G^k(x, y) \times G^j(y, k) \to G^{k+j}(x, z). \tag{2.47}$$

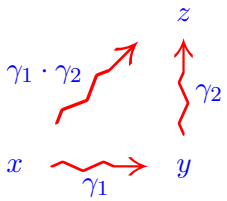
L'opération de composition de chemins (définie entre chemins composables) est associative, avec les chemins 1_x comme identités. Plus précisément, pour des chemins γ_1, γ_2 et γ_3, avec $b(\gamma_1) = s(\gamma_2)$ et $b(\gamma_2) = s(\gamma_3)$, on a

$$\begin{aligned} &\text{i) } 1_x \cdot \gamma_1 = \gamma_1 \cdot 1_y = \gamma_1, \\ &\text{ii) } \gamma_1 \cdot (\gamma_2 \cdot \gamma_3) = (\gamma_1 \cdot \gamma_2) \cdot \gamma_3, \end{aligned} \tag{2.48}$$

si $x = s(\gamma_1)$ et $y = b(\gamma_1)$. On écrit



pour indiquer qu'on a un chemin γ de x à y. La composition de chemins peut alors se représenter comme suit :



(2.49)

Dénotons simplement F^n (plutôt que $F^n(1, 1)$) l'ensemble des chemins de longueur n allant de 1 à 1 dans le graphe orienté :

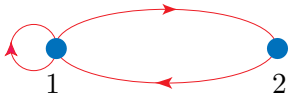


FIGURE 2.17 – F : le graphe de Fibonacci.

On ainsi les chemins suivants, ici écrits sous forme de mot.

n	F^n : chemins de longueur n de 1 à 1
0	$\{1\}$
1	$\{11\}$
2	$\{111, 121\}$
3	$\{1111, 1211, 1121\}$
4	$\{11111, 12111, 11211, 11121, 12121\}$
$\vdots$	$\vdots$

Leonardo Fibonacci
(1170 – 1250)

Observons que, pour chaque chemin γ dans F^{n-1}, on peut construire un chemin dans F^n, en prolongeant γ par 1. En terme de composition de chemins, c'est le chemin $\gamma \cdot 11$. D'autre part, pour chaque chemin γ dans F^{n-2}, on peut construire un chemin dans F^n, en prolongeant γ par 21. En terme de composition de chemins, c'est le chemin $\gamma \cdot 121$. Tous les chemins dans F^n sont ainsi obtenus de façon unique. En résumé,

$$F^{(n)} = \Big\{\gamma \cdot 11 \;\Big|\; \gamma \in F^{n-1}\Big\} \;+\; \Big\{\gamma \cdot 121 \;\Big|\; \gamma \in F^{n-2}\Big\}.$$

Si F_n désigne le nombre d'éléments de $F^{(n)}$, on a donc la récurrence

$$F_n = F_{n-1} + F_{n-2}, \qquad \text{avec} \quad F_0 = F_1 = 1, \tag{2.50}$$

Les nombres F_n sont donc les fameux **nombres de Fibonacci**, dont les premières valeurs sont

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	...

La matrice d'adjacence du graphe de Fibonacci est :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

On vérifie facilement par récurrence que

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{pmatrix}, \tag{2.51}$$

au moyen de l'égalité

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n-1} & F_{n-2} \\ F_{n-2} & F_{n-3} \end{pmatrix} = \begin{pmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{pmatrix},$$

qui découle de (2.50). En passant, soulignons que les nombres de Fibonacci admettent de nombreuses autres interprétations combinatoires.

Plus généralement, on vérifie récursivement facilement la proposition suivante.

Proposition 2.13. *Soit $G = (A, R)$ un graphe orienté sur un ensemble totalement ordonné A. Pour x et y dans A, alors le nombre de chemins allant de x à y dans G est égal au coefficient (x, y) de la k-ième puissance de la matrice d'adjacence χ_G. Autrement dit,*

$$\left|G^k(x, y)\right| = (\chi_G)^k (x, y), \tag{2.52}$$

où $(\chi_G)^k$ dénote la k-ième puissance de la matrice χ_G.

L'une des raisons fondamentales pour étudier les chemins dans un graphe orienté est exprimée par la proposition suivante.

Proposition 2.14. *Pour qu'un couple (x, y) (avec x et y dans A) appartienne à la fermeture transitive d'une relation R sur A, il faut et il suffit qu'il existe un chemin de x à y dans le graphe (A, R).*

Nous allons utiliser cette proposition pour rendre effectif le calcul de la fermeture transitive d'une relation donnée R sur A. On commence par introduire la relation $R^{\leq k}$, contenant les couples (x, y) dans A pour lesquels il existe un chemin de longueur inférieur ou égal à k allant de x à y, c.-à-d. :

$$R^{\leq k} = \{(x, y) \mid \exists j \leq k,\ G^j(x, y) \neq \emptyset\}. \tag{2.53}$$

Observons d'abord que, si A est de cardinal n, alors il existe un chemin de longueur au plus égal à $n - 1$ allant de x à y, si et seulement si (x, y) est dans la fermeture transitive $\widehat{R}$. On a donc

$$R^{\leq k} = \widehat{R} \qquad \text{lorsque} \qquad k \geq n - 1. \tag{2.54}$$

Pour poursuivre, on peut soit choisir un ordre linéaire sur A, ou simplement supposer que $A = [n]$. Nos calculs, qui se feront de façon booléennes (avec $1 + 1 = 1$), débutent avec la matrice χ de R. Étant donné la Proposition 2.13, la matrice de $R^{\leq k}$ est tout simplement

$$\mathrm{Id} + \chi + \chi^2 + \ \ldots\ + \chi^k = (\mathrm{Id} + \chi)^k, \tag{2.55}$$

puisque les opérations matricielles (booléennes) sont telles que

$$(M\,N)(i, j) = \sum_{s=1}^{n} M(i, s)N(s, j) = 1, \quad \text{ssi} \quad \exists s\ M(i, s) = 1, \quad \text{et} \quad N(s, j) = 1.$$

Dans notre cas, cela correspond au fait évident que tout chemin de longueur au plus k peut s'obtenir en composant un chemin de longueur au plus s avec un chemin de longueur au plus $k - s$. En fait, le calcul de (2.55) peut se faire (voir Exercice 2.25) en au plus $\lfloor \log_2(n) \rfloor + 1$ étapes, en exploitant le simple fait que $(\mathrm{Id} + \chi)^{2k} = ((\mathrm{Id} + \chi)^k)^2$.

2.7 Arbres

Parmi les structures classiques de la combinatoire, les arbres (qui sont des graphes simples) jouent un rôle particulièrement important en informatique théorique, en plus d'apparaître dans toutes sortes d'autres contextes mathématiques. Afin de les définir, introduisons d'abord quelques notions. Dans le contexte des graphes simples la notion analogue à celle de chemin, dans un graphe orienté, est celle de chaîne. en remplaçant les arcs par des arêtes. Autrement dit, pour des sommets x et y de $G = (A, R)$ (avec R dans $\mathcal{P}_2[A]$), une **chaîne** γ de longueur $\ell(\gamma) = k$ entre x et y, est une suite

$$\gamma = (x_0, x_1, \ldots, x_k)$$

de sommets de G, avec chaque $\{x_i, x_{i+1}\}$ une arête de G. Tout comme pour le cas des chemins dans les graphes orientés, $s(\gamma) = x = x_0$ est la source de γ, et $b(\gamma) = x_k = y$ en est le but.

Une **composante connexe** d'un graphe G est un ensemble de sommets de G qui sont tous reliées entre eux par des chaînes. Plus précisément, la composante connexe G_x de $G = (A, R)$ qui contient un sommet x est :

$$G_x := \{y \mid \text{il existe une chaîne dans } G \text{ allant de } x \text{ vers } y\}. \tag{2.56}$$

Un graphe est dit **connexe** s'il est constitué d'une seule composante connexe, c.-à-d. : pour tout x dans A, on a $G_x = A$. Autrement dit, un graphe simple est **connexe** si on peut joindre toute paire de sommets par une chaîne.

On dit qu'un sommet y qu'il est **voisin** d'un sommet x, dans le graphe G, si l'arête $\{x, y\}$ appartient au graphe. Un **cycle premier** est une chaîne $\gamma = (x_0, x_1, \ldots, x_k)$, avec $k > 2$, dans lequel tous les sommets sont distincts, sauf la source et le but qui coïncident, c.-à-d. : on a $x_i \neq x_j$ pour tout $i \neq j$, avec $1 \leq i, j \leq k$. Un graphe est dit **sans cycle** s'il ne contient aucun cycle premier.

Un **arbre** est tout simplement un graphe connexe sans cycle (voir Figure 2.18). De façon équivalente,

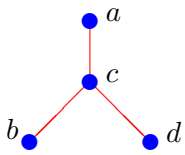


FIGURE 2.18 – Un arbre.

un arbre est un graphe dans lequel il existe une et une seule chaîne reliant toute paire de sommets. On appelle aussi souvent **noeuds** les sommets d'un arbre. Tous les noeuds d'un arbre ont au moins un voisin. Ceux qui n'en n'ont qu'un seul sont appelés **feuilles** de l'arbre.

Lorsqu'on dessine un arbre dans le plan, la disposition des voisins d'un noeud autour de celui-ci n'a pas d'importance. Autrement dit, les deux arbres de la Figure 2.19 sont les mêmes. On dénote

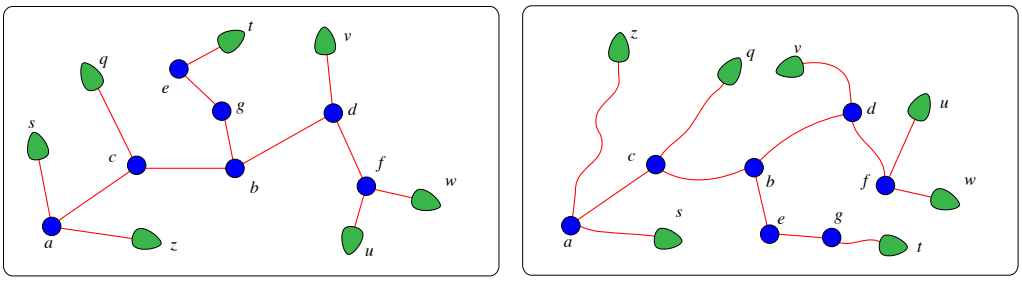


FIGURE 2.19 – Deux présentations du même arbre.

$\mathsf{Arb}[A]$ l'ensemble des arbres qui ont l'ensemble A comme ensemble de noeuds. Par définition, il n'y a pas d'arbre sur l'ensemble vide, et un seul arbre sur un singleton. On montre facilement (par récurrence sur le nombre de noeuds) que

Proposition 2.15. *Tout arbre à n noeuds contient exactement $n-1$ arêtes.*

On a les 16 arbres de l'ensemble suivant sur $\{a,b,c,d\}$:

$$\begin{aligned}\mathsf{Arb}[A] = \{&\{\{a,b\},\{b,c\},\{c,d\}\}, \quad \{\{a,b\},\{b,d\},\{d,c\}\}, \quad \{\{a,c\},\{c,b\},\{b,d\}\},\\ &\{\{a,c\},\{c,d\},\{d,b\}\}, \quad \{\{a,d\},\{d,b\},\{b,c\}\}, \quad \{\{a,d\},\{d,c\},\{c,b\}\},\\ &\{\{b,a\},\{a,c\},\{c,d\}\}, \quad \{\{b,a\},\{a,d\},\{d,c\}\}, \quad \{\{c,a\},\{a,b\},\{b,d\}\},\\ &\{\{c,a\},\{a,d\},\{d,b\}\}, \quad \{\{d,a\},\{a,b\},\{b,c\}\}, \quad \{\{d,a\},\{a,c\},\{c,b\}\},\\ &\{\{a,b\},\{a,c\},\{a,d\}\}, \quad \{\{b,a\},\{b,c\},\{b,d\}\}, \quad \{\{c,a\},\{c,b\},\{c,d\}\},\\ &\{\{d,a\},\{d,b\},\{d,c\}\}\}.\end{aligned}$$

Ces mêmes arbres sont dessinés à la Figure 2.20.

On montrera plus loin (voir Chapitre 6) qu'il y a n^{n-2} arbres ayant n noeuds, c.-à-d. :

$$|\mathsf{Arb}[A]| = n^{n-2}. \tag{2.57}$$

Une **arborescence** (on dit aussi arbre avec **racine**, ou arbre **enraciné**) est un arbre dans lequel on a choisi un des noeuds (n'importe lequel) pour qu'il joue le rôle de **racine**. Plus précisément, une arborescence est un couple (x,α) avec α un arbre sur A, et x un élément de A (c'est la racine). Pour chaque arbre on a donc n arborescences distinctes. La Figure 2.21 présente une arborescence. En formule, on a donc

$$\mathcal{A}[A] = A \times \mathsf{Arb}[A], \tag{2.58}$$

si on désigne par $\mathcal{A}[A]$ l'ensemble des arborescences ayant comme noeuds les éléments de l'ensemble A. La formule (2.57) est donc équivalente au fait qu'il y a n^{n-1} arborescences à n noeuds, i.e :

$$|\mathcal{A}[A]| = n^{n-1}. \tag{2.59}$$

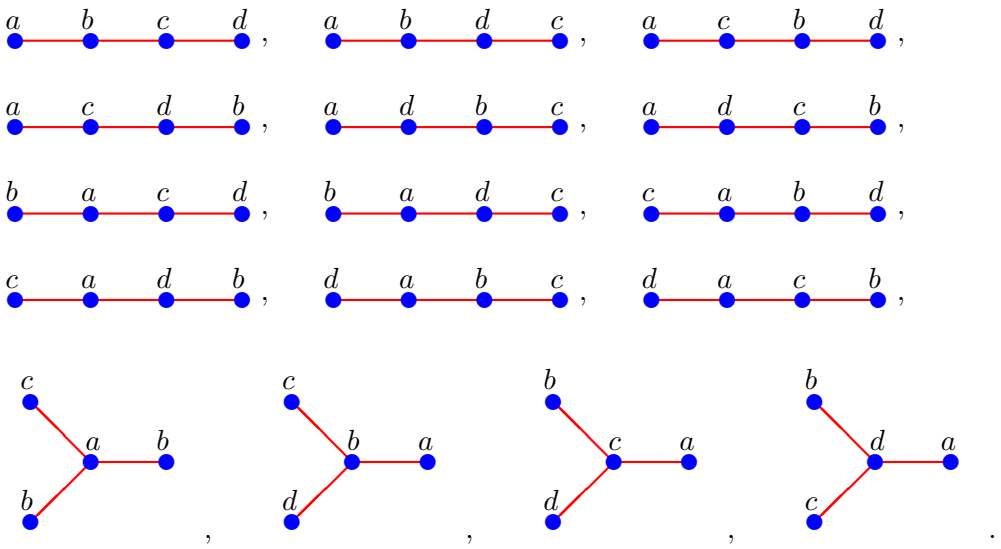


FIGURE 2.20 – Les 16 arbres sur $\{a, b, c, d\}$.

En exploitant le fait qu'il y a une et une seule chaîne allant d'un noeud quelconque à la racine, on peut orienter les arêtes d'une arborescence « vers » la racine. Autrement dit, l'arête $\{x, y\}$ d'une arborescence α est remplacée par le couple (x, y), si et seulement si l'unique chaîne allant de x à la racine (dans α) commence par le pas (x, y). Par abus de langage, on dénote aussi α le graphe orienté ainsi obtenu. La **branche** attachée en un noeud y d'une arborescence (x, α), est l'arborescence $(y, \beta(y))$ (de racine y) obtenue à partir de α en ne conservant que les noeuds z pour lesquels il existe un chemin allant de z à y dans le graphe orienté (x, α). En formule, on a la description récursive

$$\beta(y) := \sum_{\substack{z \\ (z,y)\in\alpha}} \{(z, y)\} + \beta(z). \tag{2.60}$$

Les branches[9] d'un arbre (x, α) sont les arborescences $(y, \beta(y))$ avec y voisin de la racine x.

Avec l'orientation introduite ci-haut, il est maintenant possible de « condenser » la présentation d'une arborescence de la façon suivante. L'étape de base du processus consiste à réécrire bijectivement un ensemble de couples, ayant tous la même seconde coordonnée, sous la forme[10] :

$$\{(y, x) \mid y \in B\} \qquad \longleftrightarrow \qquad (x, B). \tag{2.61}$$

9. Sans spécifier de racine.
10. Ce n'est que pour des raisons esthétiques qu'on inverse l'ordre dans la position de x.

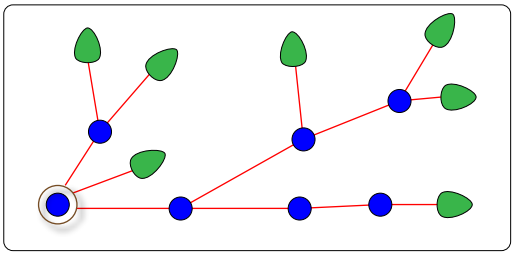


FIGURE 2.21 – Une arborescence.

Par exemple,

$$\{(1,a),(2,a),(3,a)\} \qquad \longleftrightarrow \qquad (a,\{1,2,3\}).$$

On **condense** la présentation d'une arborescence en appliquant récursivement cette transformation de base. La description d'une arborescence prend alors la forme récursive $\alpha = (x, \mathsf{B}_x)$, où x est la racine de l'arborescence, et B_x est l'ensemble des branches de α qui sont rattachées à x :

$$\mathsf{B}_x := \{(y, \mathsf{B}_y) \mid (y,x) \in \alpha\}, \tag{2.62}$$

avec $\mathsf{B}_y := y$, lorsque y est une feuille. Les 9 arborescences sur $\{a,b,c\}$, qui sont originalement décrites comme

$$\begin{aligned}\mathcal{A}[A] = \quad &\{(a,\{\{a,b\},\{b,c\}\}), \quad (b,\{\{a,b\},\{b,c\}\}), \quad (c,\{\{a,b\},\{b,c\}\}),\\ &(a,\{\{a,c\},\{c,b\}\}), \quad (b,\{\{a,c\},\{c,b\}\}), \quad (c,\{\{a,c\},\{c,b\}\}),\\ &(a,\{\{b,a\},\{a,c\}\}), \quad (b,\{\{b,a\},\{a,c\}\}), \quad (c,\{\{b,a\},\{a,c\}\})\},\end{aligned}$$

se traduisent (respectivement) sous la forme plus condensée

$$\begin{aligned}\mathcal{A}[A] = \quad &\{(b,\{a,c\}), \quad (a,\{(b,c)\}), \quad (c,\{(b,a)\}),\\ &(c,\{a,b\}), \quad (a,\{(c,b)\}), \quad (b,\{(c,a)\}),\\ &(a,\{b,c\}), \quad (b,\{(c,c)\}), \quad (c,\{(a,b)\})\}.\end{aligned}$$

L'arborescence $(b,\{a,c\})$ est de racine b avec deux branches réduites à ne contenir qu'une seule feuille ; tandis que l'arborescence $(b,\{(a,c)\})$, aussi de racine b, n'a qu'une seule branche dont la racine est a, à laquelle est attachée la feuille c.

2.8 Endofonctions

On dit d'une fonction $f : A \longrightarrow A$, de source et de but A, que c'est une **endofonction** sur A. Comme on l'a déjà souligné à la section 1.2, il y a n^n endofonctions sur en ensemble A à n éléments. Le graphe orienté associé à une endofonction porte parfois le nom de **graphe sagittal** de

l'endofonction. C'est donc le graphe dont l'ensemble des sommets est A, avec un arc de a à $f(a)$, pour chaque $a \in A$. On désigne par $\mathsf{End}[A]$ l'ensemble des endofonctions sur A.

Un élément x dans A est dit **récurrent** (pour f) s'il existe $k > 0$ tel que $x = f^k(x)$. Ici f^k désigne l'**itéré** de f pour la composition, qui est définie récursivement comme suit

$$f^k := \begin{cases} \mathrm{Id}_A & \text{si, } k = 0 \\ f \circ f^{k-1} & \text{sinon.} \end{cases} \tag{2.63}$$

Comme A est fini, A contient forcément (voir Exercice 2.1) au moins un élément récurrent pour f. On peut décomposer une endofonction sur A par le biais de la relation d'équivalence

$$x \sim y, \qquad \text{s'il existe } k \text{ et } m \in \mathbb{N}, \text{ tels que} \qquad f^k(x) = f^m(y). \tag{2.64}$$

Si B est une classe d'équivalence pour cette relation, alors $f^{-1}(B) = B$. Inversement, les sous-ensembles B de A qui sont minimaux pour l'inclusion, et tels que $f^{-1}(B) = B$ sont exactement les classes d'équivalences pour la relation $\ll \sim \gg$. On dit de la restriction de f, à l'un de ces sous-ensembles minimaux, que c'est une **composante connexe** de f. Deux éléments x et y sont dans une même composante connexe, si et seulement si il existe z et deux chemins : l'un allant de x à z, et l'autre allant de y à z.

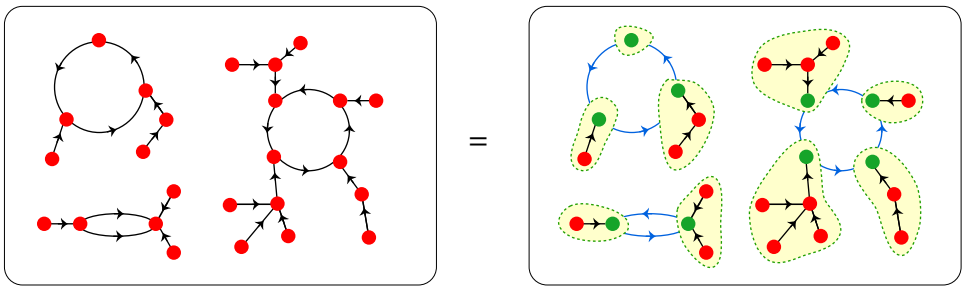


FIGURE 2.22 – Une endofonction et sa décomposition

Voici un exemple de graphe sagittal où on a mis en évidence la partition de l'ensemble sous-jacent qui correspond à la relation $\sim$. Les éléments récurrents apparaissent en grisé dans le dessin de droite, et une décomposition plus fine des endofonctions y est illustrée. à chaque élément récurrent x est attachée une arborescence, dont x est la racine, et dont tous les autres sommets sont non récurrents. Les sommets récurrents sont permutés entre eux par f. Nous reviendrons au Chapitre 6 à l'étude de cette décomposition d'une endofonction.

2.9 Exercices

2.1. Montrer que toute endofonction admet au moins un élément récurrent.

2.2. Soit A un ensemble fini, avec $|A| = n$. Combien y a-t-il de relations R sur A qui sont symétriques ?

2.3. Dans un graphe simple, on dit qu'un cycle constitue un **circuit eulérien** si et seulement si le cycle contient chaque arête du graphe une et une seule fois. Un **parcours eulérien** est une chaîne qui contient chaque arête du graphe une et une seule fois ; on admet donc que la source et le but de la chaîne puissent être distincts.

a) Donner une condition nécessaire et suffisante pour qu'il existe un circuit eulérien dans un graphe.

a) Donner une condition nécessaire et suffisante pour qu'il existe un parcours eulérien dans un graphe.

2.4. En exploitant la récurrence (2.50), montrer que la fonction génératrice

$$F(z) := F_0 + F_1\, z + F_2\, z^2 + F_3\, z^3 + \ \dots\ ,$$

des nombres de Fibonacci est donnée par la formule

$$F(z) = \frac{1}{1 - z - z^2}. \tag{2.65}$$

Généraliser au cas de la récurrence $F_n = a\, F_{n-1} + b\, F_{n-2}$, avec $F_0 = 1$ et $F_1 = a$.

2.5. Pour les nombres de Stirling $\left\{ {n \atop k} \right\}$, prouver que :

$$\text{a)]}\ \left\{ {n \atop 2} \right\} = 2^{n-1} - 1, \quad \text{et} \quad \text{b)}\ \left\{ {n \atop n-1} \right\} = \binom{n}{2}. \tag{2.66}$$

2.6. Prouver bijectivement la formule

$$\left\{ {n+1 \atop k} \right\} = \sum_{j=0}^{n} \binom{n}{j} \cdot \left\{ {j \atop k-1} \right\}, \tag{2.67}$$

où $k \geq 1$.

2.7. En décomposant la somme dans le membre de droite de (2.11) selon le nombre de parties, montrer qu'on a l'identité

$$m^n = \sum_{k=1}^{n} \left\{ {n \atop k} \right\} m_{(k)}, \tag{2.68}$$

avec $n = |A|$ et $m = |B|$.

2.8. Montrer que

$$\text{a)}\ \sum_{k=0}^{n} (-1)^{n-k} \left\{ {n \atop k} \right\} t^{(k)} = t^n, \quad \text{et} \quad \text{b)}\ \sum_{k=0}^{n} \left\{ {n \atop k} \right\} t_{(k)} = t^n. \tag{2.69}$$

2.9. Prouver la formule

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k, \tag{2.70}$$

où B_n est le n^e nombre de Bell.

2.10. Pour $\{A_i\}_{i\in I}$ une famille d'ensembles ordonnés (avec ordres respectifs dénotés $\preceq_i$), généraliser les constructions

a) de somme $\sum_{i\in I} A_i$,

b) de produit cartésien $\prod_{i\in I} A_i$.

Si de plus, si I est totalement ordonné, définir une notion de

c) de somme ordonnée $\overrightarrow{\sum_{i\in I}} A_i$,

d) de produit lexicographique $\prod^{(\ell)}_{i\in I} A_i$.

2.11. Montrer la Proposition 2.10 dans le cas où l'ensemble ordonné A admet un minimum x. Suggestion : Pour montrer que la condition sur les chaînes maximales est suffisante, montrer qu'on peut construire une fonction de rang δ sur A en choisissant de poser $\delta(x) = 0$. Pouvez-vous généraliser au cas d'un ensemble ordonné (mais fini) quelconque.

2.12. Si A admet un minimum et un maximum respectivement dénotés 0_A et 1_A ; de même pour B, eux dénotés par 0_B et 1_B. Calculer les éléments minimaux et maximaux respectifs des ensembles ordonnés suivants, et trouver (s'il existe) le minimum et le maximum. S'il n'existe pas, expliquer pourquoi et donner un exemple explicite.

a) $A + B$, b) $A \overrightarrow{+} B$,

c) $A \times B$, et d) $A \times_\ell B$.

2.13. Si A et B sont respectivement munis de fonction de rang ρ_A et ρ_B. Peut-on munir naturellement les ensembles suivants de fonctions de rang ?

a) $A + B$, b) $A \overrightarrow{+} B$,

c) $A \times B$, et d) $A \times_\ell B$.

Si possible exprimer les fonctions de rang correspondant à chacun de ces ensembles ordonnés, en terme des fonction de rang ρ_A et ρ_B.

2.14. Montrer qu'il y a une bijection naturelle entre $[k] \overrightarrow{+} [n]$ et $[k + n]$.

2.15. Montrer que, si A et B sont A et B totalement ordonnés, alors $A \overrightarrow{+} B$ est totalement ordonné, mais que $A + B$ ne l'est pas nécessairement.

2.16. Pour A et B totalement ordonnés, calculer le cardinal de $\mathsf{Croi}[A \overrightarrow{+} B, A + B]$.

2.17. Compter le nombre de chemins de longueur k, allant de 1 à n dans le graphe orienté sur $[n]$, dont l'ensemble d'arcs est

a) $\{(i, j) \mid 1 \leq i \leq n, \quad \text{et} \quad 1 \leq j \leq n\}$.

b) $\{(i, j) \mid 1 \leq i \leq j \leq n\}$.

c) $\{(i, j) \mid j - i \leq 2\}$.

2.18. Montrer qu'un graphe orienté est acyclique si et seulement si la matrice $(\mathrm{Id} - \chi_G)$ est inversible. Suggestion : Montrer que pour un graphe acyclique, les coefficients de la matrice $(\mathrm{Id} - \chi_G)^{-1}$ (qui existe) correspondent aux nombres de chemins reliant les sommets dans le graphe.

2.19. Montrer que la description condensée des arborescences décrite à la Section 2.7 correspond à la description ensembliste suivante. Si $|A| \leq 1$ alors $\mathcal{A}[A] := A$, sinon

$$\mathcal{A}[A] = \sum_{x \in A} \sum_{P \in \mathsf{Part}[A \setminus \{x\}]} \{x\} \times \prod_{B \in P} \mathcal{A}[B]. \tag{2.71}$$

2.20. Soit $\mathsf{Con}[A]$ l'ensemble des endofonctions sur A qui n'ont qu'une seule composante connexe. Montrer qu'on a une bijection naturelle

$$\mathsf{End}[A] \xrightarrow{\sim} \sum_{P \in \mathsf{Part}[A]} \prod_{B \in P} \mathsf{Con}[B]. \tag{2.72}$$

Programmation mathématique

2.21. Concevoir des procédures qui, pour un ensemble fini A donné, engendrent toutes

a) les relations reflexives sur A,

b) les relations symétriques sur A,

c) les relations antisymétriques sur A.

d) les relations d'ordre linéaire sur A.

2.22. Pour deux ensembles ordonnés A et B, construire une procédure qui construit toutes les fonctions croissantes de $A \overrightarrow{+} B$ vers $A + B$.

2.23. Pour deux graphes orientés donnés $g_1 = (A_1, R_1)$ et $g_2 = (A_2, R_2)$, écrire une procédure qui engendre tous les morphismes de g_1 vers g_2.

2.24. Pour un graphe orienté donné $G = (A, R)$ et x, y dans A, écrire une procédure récursive qui engendre tous les chemins de x vers y dans G. Suggestion : exploiter la composition de chemins.

2.25 (Fermeture transitive). Concevoir une procédure récursive qui calcule (en au plus $\lfloor \log_2(n) \rfloor$ étapes) la fermeture transitive d'une relation sur un ensemble à n éléments.

2.26. Concevoir une procédure qui, pour un ensemble fini A donné, engendre toutes

a) les relations d'équivalence sur A,

b) les relations d'ordre sur A.

2.27. Utiliser la Proposition 2.5 pour construire une procédure qui, pour un ensemble fini A donné, engendre toutes les partitions en k parties de A.

2.28. Construire une procédure qui, pour un ensemble fini A donné, engendre

a) tous les arbres[11] sur A,

b) toutes les arborescences sur A,

c) toutes les endofonctions sur A.

d) aléatoirement (avec distribution uniforme) ces mêmes structures.

2.29. Construire une procédure qui transforme une arborescence présentée sous la forme (x, α), avec α un arbre présenté sous la forme d'un graphe simple, dans sa forme condensée (voir Section 2.7).

2.30. Concevoir une procédure qui, étant donnée une endofonction $f : A \to A$, calcule sa décomposition en composantes connexes.

11. Plus tard, cela sera plus facile à faire.

Chapitre 3

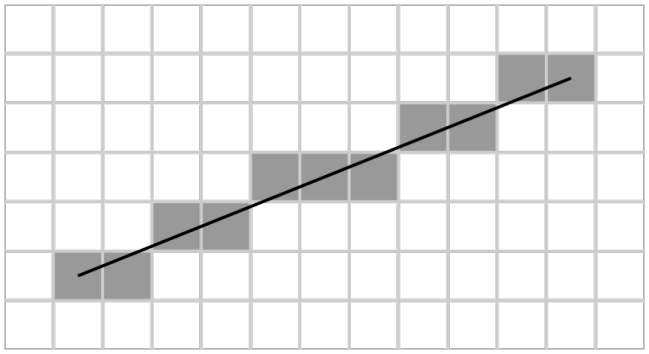
Mots, langages, automates et chemins

3.1 Introduction.

Nous avons déjà eu l'occasion d'utiliser des mots pour coder des structures combinatoires. Plusieurs autres applications des mots ont fait en sorte qu'on a même introduit la « combinatoire des mots », comme l'un des domaines de recherche en combinatoire. Les applications sont multiples, par exemple informatique pour décrire la syntaxe des langages de programmation, ou encore en génomique pour l'étude du séquençage de l'ADN, qui se présente comme un long mot :

$$\cdots\ ACAGATACACCTGATAGATTCGAATAG\ \cdots$$

avec les lettres A (Adénine), C (Cytosine), G (Guanine) et T (Thymine) codant les nucléobases dont l'ADN est constitué. Une autre application classique concerne le traçage d'une droite sur un écran qui, lorsqu'on la regarde de très près, ressemble aux pixels grisés de l'illustration ci-dessous.



3.2 Mots

Pour introduire la notion de mot, on commence par choisir un **alphabet** A, qui est simplement un ensemble fini (quelconque) de **lettres**. En pratique, il est bien plus agréable de choisir A de façon à ce que ses éléments se prêtent bien aux constructions suivantes, mais cela n'est qu'une question de goût. Tout ensemble fini peut servir d'alphabet. Par exemple, on pourra choisir A comme étant l'un des ensembles suivants

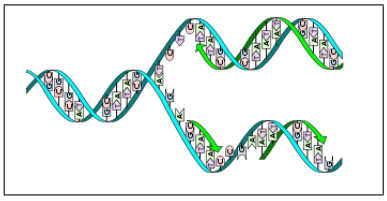


Illustration d'une molécule d'ADN.

$$\{a,b,c,d,\ \ldots\ ,z\},\qquad \{0,1\},\qquad \{A,C,G,T\},\qquad \{\bullet,\bullet,\bullet\},\qquad \text{ou}\qquad \{\clubsuit,\ \diamondsuit,\ \heartsuit,\ \spadesuit\}.$$

Un **mot** de longueur n sur l'alphabet A est une suite de n lettres

$$w = w_1\, w_2\, w_3\, \ldots\, w_n, \qquad \text{avec} \qquad w_i \in A, \tag{3.1}$$

qui sont écrites successivement, sans virgules séparatrices. Autrement dit, au détail près de la présentation, ce sont les éléments de A^n. Le **mot vide** est noté 1 (ou encore ε, par exemple dans le cas où 1 est une lettre de l'alphabet). Sur l'alphabet $A = \{a,b,c\}$, on a

$$A^0 = \{1\}, \qquad A^1 = \{a,b,c\}, \quad \text{et}$$
$$A^2 = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}.$$

On dénote A^* l'ensemble de tous les mots, c.-à-d. :

$$A^* = \sum_{n=0}^{\infty} A^n. \tag{3.2}$$

Avec $A = \{0,1\}$, on a donc

$$A^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111,\ \ldots\}$$

Bien entendu la **longueur** $|w|$ d'un mot w est le nombre de lettres qu'il contient, et les mots de longueur 1 s'identifient aux lettres. On dit qu'il y a **occurrence** de la lettre x en position i dans w, si $w_i = x$. Pour w un mot sur l'alphabet A, et x une lettre de A, on désigne $|w|_x$ le nombre d'occurrences de x dans w.

Clairement, pour un alphabet de k lettres, on a k^n mots de longueur n. Observons en passant que, via la bijection naturelle entre A^n et $A^{[n]}$, un mot de longueur n peut aussi être considéré comme la donnée d'une fonction

$$w : \{1, \ldots, n\} \longrightarrow A, \tag{3.3}$$

dont la valeur en i est la i^{e} lettre du mot, c.-à-d. : $w(i) = w_i$.

L'opération de **concaténation** (dénotée multiplicativement) entre deux mots $u = u_1\, u_2\, u_3\, \ldots\, u_n$ et $v = v_1\, v_2\, v_3\, \ldots\, v_k$ est le mot

$$u \cdot v = u_1\, u_2\, u_3\, \ldots\, u_n\, v_1\, v_2\, v_3\, \ldots\, v_k, \tag{3.4}$$

dont la longueur est la somme des longueurs de u et de v. Elle correspond à la bijection naturelle

$$A^n \times A^k \xrightarrow{\sim} A^{n+k}, \tag{3.5}$$

et, si l'on considère un mot comme une fonction (voir (3.3)), la concaténation $w = u \cdot v$ correspond à la fonction $w : [n+k] \to A$ telle que

$$w(i) := \begin{cases} u(i) & \text{si } 1 \leq i \leq n \\ v(i-n) & \text{si } n+1 \leq i \leq n+k. \end{cases} \tag{3.6}$$

La concaténation est associative, et admet le mot vide comme élément neutre. Munissant A^* de cette opération de concaténation, on obtient le **monoïde**[1] **des mots** sur A.

Avec ce point de vue algébrique, il devient naturel de considérer la **puissance k-ième** d'un mot w, défini récursivement comme :

$$w^k := \begin{cases} w \cdot w^{k-1} & \text{si } k > 0 \\ 1 & \text{si } k = 0. \end{cases} \tag{3.7}$$

On a donc $(ba)^4 = babababa$.

Si un mot w s'écrit sous la forme $w = u \cdot v$, on dit que u est **préfixe** de w, et que v est un **suffixe** de w. Ainsi, tous les préfixes possibles du mot $abbabaab$ (sur l'alphabet A) sont

$$\{1, a, ab, abb, abba, abbab, abbaba, abbabaa, abbabaab\},$$

tandis que ses suffixes sont

$$\{1, b, ab, aab, baab, abaab, babaab, bbabaab, abbabaab\},$$

Une autre notion intéressante (et apparemment utile pour la physique) est la notion de « palindrome ». Pour l'introduire, on considère d'abord la notion d'**image miroir** d'un mot

$$w = w_1 w_2 \cdots w_n,$$

1. Un ensemble muni d'une opération associative avec un élément neutre est appelé monoïde.

c'est-à-dire le mot

$$\widetilde{w} := w_n \ \cdots \ w_2 w_1. \tag{3.8}$$

Un **palindrome** w est un mot qui est égal à son image miroir, c.-à-d. :

$$w = \widetilde{w}. \tag{3.9}$$

En terme de la présentation fonctionnelle pour les mots, $w \in A^n$ est un palindrome si et seulement si on a $w(i) = w(n+1-i)$ pour tout i allant de 1 à n. Par défaut, le mot vide est un palindrome. C'est la généralisation directe de la notion du dictionnaire, et on a des exemples comme :

radar, kayak, ressasser ...

Si on ignore la ponctuation, les espaces, les accents, et la différence entre lettres majuscules et minuscules, certaines phrases forment des palindromes. Ainsi, on a la phrase (apparemment due à Victor Hugo) :

« Tu l'as trop écrasé, César, ce Port-Salut ! »

George Perec (membre du groupe OuLiPo) a écrit une phrase palindrome contenant 1247 mots.

Georges Perec.
(1936-1982)

Pour un alphabet A, on dénote $\mathsf{Pal}_k[A]$ l'ensemble des palindromes de longueur k sur A, et on pose

$$\mathsf{Pal}[A] := \sum_{k=0}^{\infty} \mathsf{Pal}_k[A]. \tag{3.10}$$

Ainsi, pour $A = \{a, b\}$, on a

$$\mathsf{Pal}_5[A] = \{aaaaa, aabaa, ababa, abbba, baaab, babab, bbabb, bbbbb\}$$

3.3 Langages

Dans plusieurs contextes, on est mené à considérer des ensembles de mots particuliers. C'est certainement le cas en informatique ou en génomique. Ces sous-ensembles sont appelés **langages** sur A. Ainsi, un langage $\mathcal{L}$ sur A est

$$\mathcal{L} \subseteq A^*. \tag{3.11}$$

Pour un alphabet quelconque, disons $A = \{a, b\}$, on a des langages finis comme

$$\emptyset, \qquad \{a, b\}, \qquad \mathsf{Pal}_k[A], \qquad \text{ou encore} \qquad \{w \mid |w|_a = k \text{ et } |w|_b = n - k\},$$

et des langages infinis comme

$$\{a^n b^n \mid n \in \mathbb{N}\}, \qquad \mathsf{Pal}[A], \qquad \text{ou encore} \qquad \{1, a, aa, aaa, \ \ldots\ \}.$$

On convient d'écrire $\mathcal{L}_k$ pour le langage ne contenant que les mots de longueur k dans $\mathcal{L}$, c.-à-d. :

$$\mathcal{L}_k := \{\ w \in \mathcal{L} \ \mid\ |w| = k\}. \tag{3.12}$$

Les opérations d'union, de **produit**, et d'**étoile** permettent de construire de nouveaux langages à partir de langages donnés. Plus précisément, soit $\mathcal{L}$ et $\mathcal{L}'$ deux langages sur l'alphabet A, le produit est

$$\mathcal{L} \cdot \mathcal{L}' := \{u \cdot v \ \mid\ u \in \mathcal{L} \quad \text{et} \quad v \in \mathcal{L}'\}, \tag{3.13}$$

et on a les identités (voir Exercice 3.2

$$\mathcal{L} \ = \ \sum_{k=0}^{\infty} \mathcal{L}_k, \tag{3.14}$$

$$\mathcal{L} \cdot \mathcal{L}' \ = \ \sum_{k=0}^{\infty} \left(\bigcup_{j=0}^{k} \mathcal{L}_j \cdot \mathcal{L}'_{k-j} \right). \tag{3.15}$$

Remarquons qu'on a des sommes disjointes dans les membres de droite de ces identités. Quant à l'étoile, on la définit en posant

$$\mathcal{L}^* := \bigcup_{k=0}^{\infty} \mathcal{L}^k, \tag{3.16}$$

avec $\mathcal{L}^0 := \{1\}$, et

$$\mathcal{L}^k := \mathcal{L} \cdot \mathcal{L}^{k-1}, \tag{3.17}$$

si $k > 0$. En passant, on remarque qu'il y a compatibilité entre cette définition et nos usages précédents, puisque l'ensemble A est lui-même un langage (dont les mots sont les lettres de l'alphabet). Pour illustrer l'opération d'étoile, considérons le langage $\mathcal{L} = \{ab, ba\}$. On a alors

$$\mathcal{L}^* = \{1, ab, ba, abab, abba, baab, baba, \ \ldots\ \}.$$

La **série génératrice** d'un langage $\mathcal{L}$ contient toute l'information concernant le nombre de mots de longueur k dans $\mathcal{L}$, pour tout k dans $\mathbb{N}$. On la dénote $\mathcal{L}(z)$, et elle est définie en posant

$$\mathcal{L}(z) := \sum_{k=0}^{\infty} \ell_k \, z^k, \tag{3.18}$$

où ℓ_k est le nombre de mots dans $\mathcal{L}_k$.

On dit qu'un produit de langage est **non-ambigue** si et seulement si chaque mot $w \in \mathcal{L} \cdot \mathcal{L}'$ se décompose de façon unique comme produit d'un mot u dans $\mathcal{L}$ avec un mot v dans $\mathcal{L}'$, c.-à-d. : pour tout u, u' dans $\mathcal{L}$, et v, v' dans $\mathcal{L}'$, on a

$$u \cdot v = u' \cdot v', \quad \text{ssi} \quad (u = u' \quad \text{et} \quad v = v'). \tag{3.19}$$

On dit aussi qu'un langage $\mathcal{L}$ est un **code** si et seulement si chaque mot dans $\mathcal{L}^*$ se décompose de façon unique comme produit de mots dans $\mathcal{L}$. Avec ces définitions, on a la proposition :

Proposition 3.1. *Le passage à la série génératrice est compatible avec les opérations sur les langages, c.-à-d. :*

$$\begin{aligned} &\text{i)} && (\mathcal{L} + \mathcal{L}')(z) = \mathcal{L}(z) + \mathcal{L}'(z), && \text{si} \quad \mathcal{L} \cap \mathcal{L}' = \emptyset, \\ &\text{ii)} && (\mathcal{L} \cdot \mathcal{L}')(z) = \mathcal{L}(z)\, \mathcal{L}'(z), && \textit{si le produit est non-ambigue}, \\ &\text{iii)} && \mathcal{L}^*(z) = \frac{1}{1 - \mathcal{L}(z)}, && \textit{si } \mathcal{L} \textit{ est un code}. \end{aligned} \tag{3.20}$$

Il est habituel (mais potentiellement peu clair, voir Exercice 3.3) de simplifier la notation en écrivant simplement w pour le langage $\mathcal{L} = \{w\}$, qui ne contient que le mot w. Avec cette convention [2], on obtient une **notation additive** pour les langages, qui se présentent maintenant sous la forme de la somme (formelle) des mots qu'ils contiennent :

$$\sum_{w \in \mathcal{L}} w. \tag{3.21}$$

Ainsi, on a

$$(a + b)^3 = aaa + aab + aba + abb + baa + bab + bba + bbb.$$

En guise d'autre illustration, le langage sur $\{a, b\}$, constitué de tous les mots qui contiennent exactement une occurrence de deux a consécutifs, admet la description

$$\mathcal{L} = (ab + b)^*\, a\, a\, (ba + b)^*. \tag{3.22}$$

Résoudre des équations. Nous allons maintenant voir qu'on peut définir des langages intéressants en résolvant des équations « algébriques », écrites au moyen des opérations introduites ci-haut. Plutôt que de développer une théorie générale, illustrons l'approche par un exemple classique. Le langage $\mathcal{D}$ des **mots de Dyck** sur l'alphabet $\{a, b\}$, est caractérisé par l'équation

$$\mathcal{D} = 1 + a\, \mathcal{D}\, b\, \mathcal{D}. \tag{3.23}$$

2. Très utilisée dans les milieux de l'informatique théorique.

Autrement dit, les mots de Dyck sont : soit le mot vide 1, soit un mot de la forme $a\,u\,b\,v$, où u et v sont des mots de Dyck (évidemment plus courts). On a donc

$$\mathcal{D} = \{1, ab, abab, aabb, ababab, abaabb, aabbab, aababb, aaabbb, \ \dots\ \}$$

Une conséquence fascinante de toute notre démarche est que l'équation 3.23 se traduit en une équation algébrique pour la série génératrice $\mathcal{D}(z)$ du langage des mots de Dyck. En effet, en passant aux séries génératrices de chaque membre de cette identité, on trouve

$$\mathcal{D}(z) = 1 + z^2\,\mathcal{D}(z)^2. \tag{3.24}$$

On considère alors $\mathcal{D}(z)$ comme une inconnue dans cette équation quadratique, qui a les deux solutions

$$\frac{1-\sqrt{1-4z^2}}{2\,z^2}, \quad \text{et} \quad \frac{1+\sqrt{1-4z^2}}{2\,z^2}.$$

Seule la première possibilité admet un développement en série de puissances à l'origine, et on conclut qu'on doit avoir

$$\mathcal{D}(z) = \frac{1-\sqrt{1-4z^2}}{2\,z^2}. \tag{3.25}$$

Dénotons C_n les coefficients de cette série génératrice des mots de Dyck, c.-à-d. :

$$\mathcal{D}(z) = \sum_{n=0}^{\infty} C_n\,z^{2\,n}. \tag{3.26}$$

on dit que les C_n sont les **nombres de Catalan**, et on montre (voir Exercice 3.6) qu'on a la formule

$$C_n = \frac{1}{n+1}\binom{2\,n}{n}. \tag{3.27}$$

Comme nous allons le voir plus tard, les nombres de Catalan apparaissent dans toutes sortes de contextes. Nous verrons plus loin (voir Exercice 3.8) que les nombres de Catalan satisfont à la récurrence :

$$C_n = \sum_{i=0}^{n-1} C_i\,C_{n-i-1}, \tag{3.28}$$

lorsque $n \geq 1$.

Eugène Charles Catalan (1814–1894)

Les premières valeurs des nombres de Catalan sont

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
C_n	1	1	2	5	14	42	132	429	1430	4862	16796	58786	208012	742900	...

3.4 Automates

Une autre façon de spécifier un langage est par le bais d'un « automate », c.-à-d. : un modèle abstrait de machine de calcul[3]. L'histoire des modèles mathématiques de machines de calculs est longue et pleine de rebondissements. Elle culmine (pour l'instant) avec l'introduction des ordinateurs modernes. Les automates considérés ici sont des machines beaucoup plus limitées dans leur capacité de calculs. Il y en a plusieurs variantes, mais nous ne considérerons que le cas des automates dits déterministes.

Soit A un alphabet, et E un ensemble fini dont les éléments seront appelés **états**. Un **automate** α est simplement une fonction $\alpha : A \to \mathsf{End}[E]$, qui associe à chaque lettre x de A une endofonction $\alpha_x : E \to E$. Lorsqu'on les représente en termes de graphes sagittaux, on place la lettre x sur chaque arc de la fonction associée. Ainsi, pour $A = \{a, b\}$ et $E = \{\bullet, \bullet\}$, l'automate

$$\alpha_a = \{(\bullet, \bullet), (\bullet, \bullet)\}, \quad \text{et} \quad \alpha_b = \{(\bullet, \bullet), (\bullet, \bullet)\},$$

se représente comme indiqué à la Figure 3.1. C'est un **multigraphe** orienté, dont les arcs sont

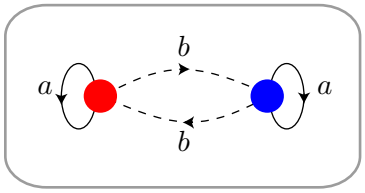


FIGURE 3.1 – Un automate.

étiquetés par les lettres de l'alphabet A. On dit multigraphe, parce qu'il y a potentiellement plusieurs arcs allant d'un sommet x à un sommet y. Techniquement, un tel multigraphe (qui n'est pas nécessairement un automate) est simplement un sous-ensemble du produit cartésien $A \times E \times E$. On interprète alors le triplet (x, e, f) comme étant un arc allant de e à f, portant l'étiquette a.

Il est naturel de désigner par x la fonction α_x. On fait « fonctionner » un automate au moyen des mots sur l'alphabet A. En effet, on considère un mot comme fonction composée à partir des fonctions associées à chacune de ses lettres. L'habitude dans ce domaine est de composer de gauche à droite, plutôt que de droite à gauche comme on a l'habitude de le faire pour des fonctions. Ainsi, pour un automate fixé, un mot $w = w_1 w_2 \cdots w_n$ devient synonyme de la fonction $w = w_n \circ \cdots \circ w_2 \circ w_1$, selon la convention usuelle de composition de fonction. On évite d'avoir à continuellement tout retourner, en convenant dorénavant de désigner par $e \cdot_\alpha w$, ou plus simplement par $e \cdot w$, l'effet (via

3. Attention, ce ne sont pas tous les langages qui peuvent être obtenus ainsi. La « complexité » du langage est liée au pouvoir de calcul du modèle de machine choisi. De plus, certains langages ne peuvent être obtenus par aucune machine.

l'automate) du mot w sur un état e dans E. On a alors, pour chaque $w \in A^*$ et $e \in E$:

$$\begin{aligned} &\text{a)} \qquad e \cdot 1 = e, \\ &\text{b)} \qquad e \cdot (u\,v) = (e \cdot u) \cdot v. \end{aligned} \tag{3.29}$$

L'interprétation imagée du calcul $e \cdot w$ est la suivante. Partant de l'état e, on suit le chemin, dans le multigraphe orienté, qui correspond au mot w. Plus précisément, pour chaque lettre x, il y a un seul arc du multigraphe (l'automate) de la forme (x, e, f). L'effet de x sur e est d'aller à f, c.-à-d. : $e \cdot x = f$. Le processus se déroule ensuite récursivement, en exploitant le fait que

$$e \cdot (x\,u) = (e \cdot x) \cdot u = f \cdot u.$$

Le chemin associé à $e \cdot w$, pour $w = w_1 w_2 \cdots w_n$, est donc

$$(e_0, e_1, \ldots, e_n), \qquad \text{avec} \qquad e = e_0, \qquad e \cdot w = e_n,$$

et $e_i = e_{i-1} \cdot w_i$, pour i allant de 1 à n. Le but e_n du chemin est donc la valeur de $e \cdot w$.

Par exemple, avec l'automate de la Figure 3.1, on obtient le résultat suivant [4]

$$\begin{aligned} \bullet \cdot aabaab &= \bullet \cdot abaab \\ &= \bullet \cdot baab \\ &= \bullet \cdot aab \\ &= \bullet \cdot ab \\ &= \bullet \cdot b \\ &= \bullet \end{aligned}$$

Le lien entre la notion d'automate et celle de langage s'établit de la façon suivante. Soit $\alpha : A \to E$ un automate donné, et $e \in E$ un état fixé que l'on va appeler **initial**. On choisit aussi un sous-ensemble F de E, et on dit que les éléments de F sont des états **finaux**. Un langage $\mathcal{L}$, sur l'alphabet A, est **reconnu** par l'automate $\alpha : A \to E$, avec le choix de e comme état initial et des états finaux F, si et seulement si on a

$$w \in \mathcal{L} \qquad \Longleftrightarrow \qquad e \cdot_\alpha w \in F. \tag{3.30}$$

S'il existe un automate (avec choix d'état initial et d'états finaux) qui reconnaît un langage $\mathcal{L}$, on dit que le langage est **reconnaissable**. Un célèbre théorème lie cette notion à celle des langages qu'on peut décrire avec les opérations introduites ci-haut. En voici l'énoncé, sans démonstration :

Théorème 3.2 (Kleene, 1954)**.** *Un langage est reconnaissable si et seulement si peut être engendré, à partir des lettres de l'alphabet, à l'aide des trois opérations somme, produit et étoile.*

4. Il est facile du suivre les étapes en déplaçant son doigt sur le dessin.

Avec un peu de travail supplémentaire, on peut montrer qu'il découle de ce théorème, en conjonction avec la Proposition 3.1, que la série génératrice d'un langage reconnaissable $\mathcal{L}$ est nécessairement de la forme

$$\mathcal{L}(z) = \frac{P(z)}{Q(z)}, \tag{3.31}$$

avec $P(z)$ et $Q(z)$ des polynômes dans $\mathbb{Z}(z)$. En particulier, ceci montre que le langage de Dyck n'est pas reconnaissable.

3.5 Chemins dans le réseau $\mathbb{N} \times \mathbb{N}$

Nous avons vu plusieurs notions combinatoires liées à des chemins dans des graphes. Une notion très parente est celle de chemins dans le réseau $\mathbb{N} \times \mathbb{N}$. Elle intervient en physique statistique, dans l'étude des marches aléatoires, des chaînes de Markov, etc. Le **plan combinatoire** (ou **réseau**) $\mathbb{N} \times \mathbb{N}$ est l'ensemble des points à coordonnées entières positives (ou nulles) du plan cartésien, comme illustré à la Figure 3.2. Dans cette section, nous allons voir que plusieurs des nombres

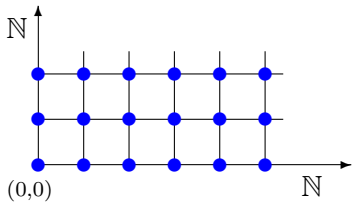


FIGURE 3.2 – Le réseau $\mathbb{N} \times \mathbb{N}$.

que nous avons déjà rencontrés apparaissent aussi comme énumérateurs de chemins dans le plan combinatoire. Ainsi, les coefficients binomiaux $\binom{n}{k}$ énumèrent l'ensemble les chemins dans $\mathbb{N} \times \mathbb{N}$ allant de $(0,0)$ à $(n-k,k)$, et constitués de k pas verticaux et de $(n-k)$ pas horizontaux.

Un **chemin** γ dans le réseau $\mathbb{N} \times \mathbb{N}$ est une suite

$$\gamma = (p_0, p_1, \ \ldots \ , p_n), \tag{3.32}$$

de **points** $p_i = (x_i, y_j)$ dans $\mathbb{N} \times \mathbb{N}$ avec

$$p_{i+1} = \begin{cases} p_i + (1,0) & \text{ou,} \\ p_i + (0,1), \end{cases}$$

pour $0 \leq i \leq n-1$. Le point p_0 est la **source** du chemin, et le point p_n est son **but**. La Figure 3.3 donne l'illustration d'un chemin de longueur 13 allant de $(0,0)$ à $(9,4)$. Habituellement (sauf mention explicite du contraire) la source d'un chemin est le point $(0,0)$. On dénote simplement par

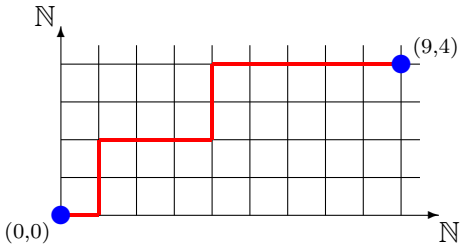


FIGURE 3.3 – Un chemin allant de $(0,0)$ à $(9,4)$.

$\Gamma(k,n)$ l'ensemble des chemins de but $p = (k,n)$ et de source $(0,0)$, et plus généralement par $\Gamma_{a,b}(k,n)$ l'ensemble des chemins allant de (a,b) à (k,n). On a une bijection naturelle

$$\eta : \Gamma_{a,b}(a+k, b+n) \xrightarrow{\sim} \Gamma(k,n), \tag{3.33}$$

obtenue tout simplement en translatant par $(-a,-b)$ les points des chemins dans $\Gamma_{a,b}(a+k,b+n)$. On dit de l'image d'un chemin γ par cette translation, que c'est le **normalisé** $\eta(\gamma)$ de γ. L'inverse de la bijection (3.33) transforme (par translation) tout chemin γ dans $\Gamma(k,n)$ en chemin allant de (a,b) à $(a+n, b+k)$. On dénote $\tau_{a,b}(\gamma)$ ce **translaté** de γ. L'idée intuitive [5] est que les chemins sont considérés comme égaux à « translation près ».

On observe qu'il y a une bijection naturelle

$$\Gamma(k,n) \xrightarrow{\sim} \Gamma(k-1,n) + \Gamma(k,n-1), \tag{3.34}$$

qui correspond au fait que l'avant-dernier point de tout chemin de $(0,0)$ à (k,n) est : soit le point $(k-1,n)$, soit le point $(k,n-1)$. Ceci est illustré à la Figure 3.4.

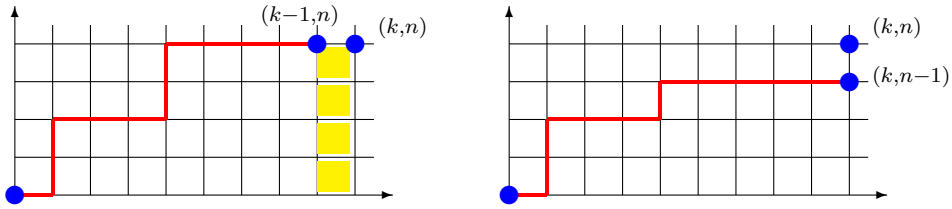


FIGURE 3.4 – Un chemin se terminant en $(k-1,n)$ ou $(k,n-1)$.

On dit que le chemin est de **longueur** n. Autrement dit, il est constitué de n **pas**, chacun allant du point p_i au point p_{i+1}. Si $p_{i+1} = p_i + (1,0)$, on dit qu'on a un **pas horizontal**. De façon tout à fait semblable, on dit qu'on a un **pas vertical**, si $p_{i+1} = p_i + (0,1)$. Les chemins dans $\Gamma(k,m)$ sont ceux qui contiennent k pas horizontaux et m pas verticaux.

5. En considérant une relation d'équivalence judicieuse, on peut rendre tout ceci rigoureusement correct.

En général, un chemin γ est donc une suite de pas verticaux et de pas horizontaux. On peut le coder sous la forme d'un mot sur l'alphabet $\{x, y\}$, avec x dénotant un pas horizontal, et y un pas vertical. Plus explicitement, le mot associé au chemin $\gamma = (p_0, p_1, \ \dots \ , p_n)$ est le mot $w(\gamma) = w_0 w_1 \dots w_{n-1}$ obtenu en posant

$$w_i := \begin{cases} x & \text{si } (p_i, p_{i+1}) \text{ est un pas horizontal,} \\ y & \text{si } (p_i, p_{i+1}) \text{ est un pas vertical.} \end{cases} \tag{3.35}$$

Par abus de langage, on désigne aussi par γ le mot associé au chemin γ. Ainsi le chemin de la Figure 3.3 correspond au mot $xyyxxxyyxxxxx$. À son tour, le mot d'un chemin correspond bijectivement à la fonction caractéristique d'un sous-ensemble à k élements de $[n]$, comme on l'a déjà décrit en (3.3). Les chemins de $(0, 0)$ à $(k, n-k)$ codent donc bijectivement les parties à k éléments de $[n]$, c.-à-d. : il y a une bijection naturelle

$$\Gamma(k, n-k) \xrightarrow{\sim} \mathcal{P}_k[n]. \tag{3.36}$$

On en déduit aussitôt que

$$|\Gamma(k, m)| = \binom{k+m}{k}, \tag{3.37}$$

de la bijection (3.33) on trouve facilement combien il y a de chemins allant de (a, b) à (n, k).

Composition de chemins. Soit γ et γ' deux chemins dans $\mathbb{N} \times \mathbb{N}$ respectivement de sources (s, t) et (s', t'), et de buts (k, n) et (k', n'), On dénote $\gamma \cdot \gamma'$ le chemin obtenu en concaténant γ avec le translaté de γ' selon le vecteur $(a, b) := (k - s', n - t')$. Autrement dit, on translate γ' de façon à ce que sa source coïncide avec le but de γ, ce qui permet de composer au sens usuel. Plus explicitement, si

$$\gamma_1 = (p_0, p_1, \ \dots \ , p_\ell) \quad \text{et} \quad \tau_{a,b}(\gamma_2) = (q_0, q_1, \ \dots \ , q_m),$$

alors on pose

$$\gamma_1 \cdot \gamma_2 := (p_0, p_1, \ \dots \ p_\ell, q_1, \ \dots \ , q_m), \tag{3.38}$$

et c'est bien un chemin dans $\mathbb{N} \times \mathbb{N}$. On dit que c'est le **composé** (ou **produit**) de γ et γ'. C'est un chemin dont la source est (s, t), et le but est $(k - s' + k', n - t' + n')$. Le chemin **nul**, égal à $((0, 0))$, agit comme élément neutre pour le produit de chemin.

3.6 Aire de chemin

Considérons les pas horizontaux d'un chemin $\gamma = (p_0, \dots, p_n)$, c'est-à-dire les couples de points successifs $\gamma_i := (p_i, p_{i+1})$ pour lesquels on a $p_{i+1} = p_i + (1, 0)$. Pour chacun de ces pas horizontaux,

on a la **hauteur** du pas :

$$h(\gamma_i) := y_i, \qquad \text{lorsque} \qquad p_i = (x_i, y_i). \tag{3.39}$$

Autrement dit, $h(\gamma_i)$ est le nombre de « cases » qui se trouve sous le pas en question. Rappelons qu'une **case** de $\mathbb{N} \times \mathbb{N}$ est un carré délimité par les 4 points adjacents (x, y), $(x+1, y)$, $(x, y+1)$, et $(x+1, y+1)$. Notre objectif est ici de compter les chemins avec un poids donné par l'**aire** sous le chemin, c.-à-d. :

$$\text{aire}(\gamma) := \sum_{\gamma_i \text{ horizontal}} h(\gamma_i). \tag{3.40}$$

L'aire de γ est donc le nombre de cases (dont l'aire est l'unité de surface) qui se trouvent sous le chemin. Pour notre exemple de la Figure 3.3 on a une aire de 26, comme l'illustre la région en jaune de la Figure 3.5.

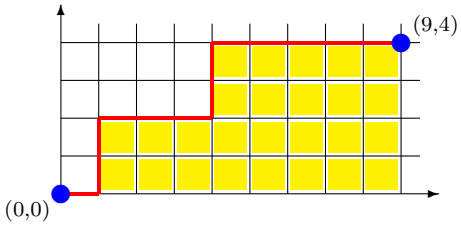


FIGURE 3.5 – Aire sous un des chemins de $(0, 0)$ à $(9, 4)$.

L'**énumération** selon l'aire d'un ensemble fini $\mathcal{C}$ de chemins prend la forme du **polynôme énumérateur d'aire** :

$$\mathcal{C}(q) := \sum_{\gamma \in \mathcal{C}} q^{\text{aire}(\gamma)}. \tag{3.41}$$

Ce polynôme contient l'information sur la distribution de l'aire des chemins considérés. On observe que

$$\mathcal{C}(1) = |\mathcal{C}|. \tag{3.42}$$

Ainsi, pour $\mathcal{C} = \Gamma(3, 2)$, on a les $10 = \binom{3+2}{3}$ chemins de la Figure 3.6, et le polynôme correspondant est donc

$$\begin{aligned} \mathcal{C}(q) &= 1 + q + 2\,q^2 + 2\,q^3 + 2\,q^4 + q^5 + q^6 \\ &= (1+q)(1 + q + q^2 + q^3 + q^4) \end{aligned}$$

Pour $\mathcal{C}(q) = \Gamma(k, n-k)$, dénotons

$$\binom{n}{k}_q := \mathcal{C}(q), \tag{3.43}$$

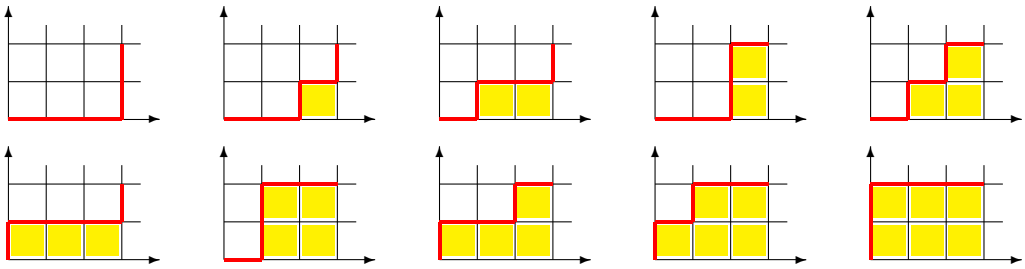


FIGURE 3.6 – Tous les chemins de $(0,0)$ à $(3,2)$.

le polynôme énumérateur d'aire associé. Ce sont les **coefficients q-binomiaux**. En tenant compte du défaut d'aire introduit dans le premier terme (voir la région en jaune de la Figure 3.4), la bijection (3.34) donne la récurrence suivante pour ces polynômes

$$\binom{n}{k}_q = q^{n-k}\binom{n-1}{k-1}_q + \binom{n-1}{k}_q, \tag{3.44}$$

avec les valeurs initiales

$$\binom{n}{0}_q = 1, \quad \text{et} \quad \binom{n}{n}_q = 1. \tag{3.45}$$

Le facteur q^{n-k} qui apparaît dans (3.44) vient de ce que l'aire d'un chemin allant de $(0,0)$ à $(k-1,n-k)$ diffère exactement d'une quantité $n-k$, de l'aire du chemin obtenu en ajoutant un pas horizontal à un tel chemin pour obtenir un chemin (passant par $(k-1,n-k)$) qui termine en $(k,n-k)$. On a les valeurs de la Table 3.1 pour les coefficients q-binomiaux :

$n \setminus k$	0	1	2	3	4
0	1				
1	1	1			
2	1	$q+1$	1		
3	1	q^2+q+1	q^2+q+1	1	
4	1	q^3+q^2+q+1	$q^4+q^3+2\,q^2+q+1$	q^3+q^2+q+1	1

TABLE 3.1 – Les coefficients q-binomiaux $\binom{n}{k}_q$.

3.7 Chemins de Dyck

Un **chemin de Dyck** est un chemin $\gamma = (p_0, \ldots, p_{2\,n})$ dans le réseau $\mathbb{N} \times \mathbb{N}$

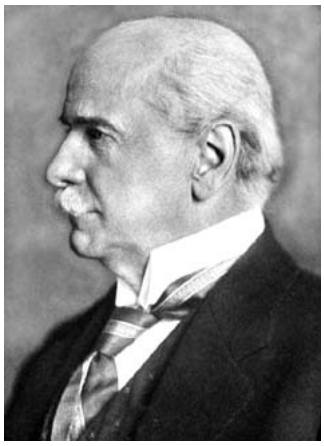
a) qui démarre (en $(0,0)$) et se termine sur la diagonale, au point

$$p_{2\,n} = (n, n),$$

b) qui reste toujours au-dessus de la diagonale, c.-à-d. :

$$p_i = (x_i, y_i), \quad \text{avec} \quad y_i \geq x_i.$$

La Figure 3.7 illustre un tel chemin de Dyck. On dit de l'entier n que c'est la **hauteur** du chemin (qui est de longueur $2\,n$).



Walter Von Dyck
(1856–1934)

L'unique chemin de Dyck de hauteur 0 est le chemin nul. On désigne par Dyck$[n]$ l'ensemble des chemins de Dyck de hauteur n. (Observez qu'il n'y a que des chemins de Dyck de longueur paire.) Les cinq chemins de Dyck de hauteur 3 sont ceux qui apparaissent à la Figure 3.8.

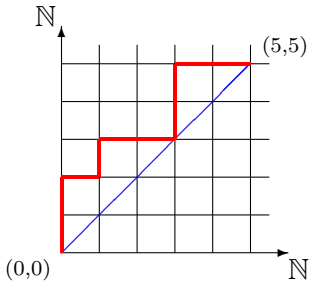


FIGURE 3.7 – Un chemin de Dyck.

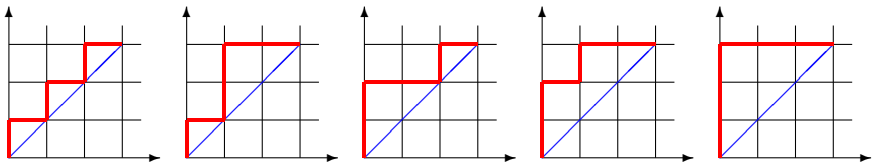


FIGURE 3.8 – Les 5 chemins de Dyck de hauteur 3.

En codant sous forme de mot les chemins de Dyck de hauteur n, on obtient exactement les mots

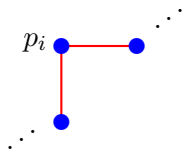
de Dyck (sur l'alphabet $\{y, x\}$) de longueur $2\,n$. Autrement dit, on a une bijection

$$\mathsf{Dyck}[n] \xrightarrow{\sim} \mathcal{D}_{2\,n}. \tag{3.46}$$

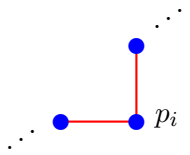
Ainsi, aux 5 chemins de Dyck de la Figure 3.8, il correspond les mots de Dyck :

$$\mathcal{D}_6 = \{yxyxyx, yxyyxx, yyxxyx, yyxyxx, yyyxxx\}$$

Un **coin extérieur** d'un chemin de Dyck $\gamma = (p_0, \ \dots \ , p_{2\,n})$ est un point p_i pour lequel on a $p_{i-1} = p_i - (0,1)$ et $p_{i+1} = p_i + (1,0)$. De façon analogue, on considère la notion de **coin intérieur** de γ. C'est un point p_i pour lequel on a $p_{i-1} = p_i - (1,0)$ et $p_{i+1} = p_i + (0,1)$. De façon imagée, on a donc



(p_i coin extérieur)



(p_i coin intérieur)

Manifestement, un chemin de Dyck est entièrement caractérisé (voir Exercices 3.10 et 3.15) par la position de ses coins extérieurs et de ses coins intérieurs.

Décomposition des chemins de Dyck. Tout chemin de Dyck

$$\gamma = (p_0, p_1, \ \dots \ , p_{2\,n})$$

de hauteur n, admet une décomposition unique en produit (composé) de chemins de Dyck

$$\gamma = \gamma' \cdot \gamma'' \tag{3.47}$$

avec γ' non nul de hauteur minimale, disons égale à k. Le chemin γ'' est alors de hauteur $n-k$, et c'est potentiellement le chemin nul. Plus précisément, si les coordonnés des p_i sont (x_i, y_i), alors $x_k = y_k$. On dit que le point $p_k = (x_k, y_k)$ est le point de **premier retour** de γ à la diagonale $y = x$. C'est le but du chemin γ'. Le chemin γ'' (translaté adéquatement) est la partie de γ allant de ce point de premier retour au point (n, n).

Le chemin γ', est un chemin de Dyck particulier en ce qu'il ne touche à la diagonale qu'en ses extrémités. On dit d'un tel chemin qu'il est **premier**, et on voit facilement que

Lemme 3.3. *Un chemin de Dyck $\gamma = (p_0, p_1, \ \dots \ , p_{2\,n})$ est premier, si et seulement si on a $\gamma = Y \cdot \gamma' \cdot X$, avec $Y = ((0,0),(0,1))$, $X = ((0,0),(1,0))$ et γ' un chemin de Dyck quelconque.*

Cet énoncé correspond à dire que le chemin obtenu, en enlevant le premier et le dernier pas de γ, est un chemin de Dyck (une fois translaté pour démarrer à l'origine).

En décomposant γ'' de même manière qu'en (3.47), et ainsi de suite, il s'ensuit que

Proposition 3.4. *Tout chemin de Dyck se décompose de façon unique comme produit de chemins de Dyck premiers.*

Cette décomposition correspond à découper le chemin selon ses divers retours à la diagonale. Nous allons maintenant démonter directement, avec une approche en terme de chemins, que

Proposition 3.5. *Le nombre de chemins de Dyck de hauteur n est donné par le n-ième nombre de Catalan, c.-à-d. :*

$$|\mathsf{Dyck}[n]| = \frac{1}{n+1}\binom{2\,n}{n}. \tag{3.48}$$

La démonstration apparaît comme un cas particulier de l'étude du « problème du scrutin ».

Le problème du scrutin. On s'imagine qu'il y a une élection entre deux candidats X et Y, et qu'à la fin du vote l'un des candidats, disons Y, reçoit k votes, et X reçoit n votes, avec $k > n$. C'est donc Y qui est élu. Le problème du scrutin consiste à calculer la probabilité qu'au cours du dépouillement des votes le gagnant Y demeure toujours en avance sur X. Autrement dit, chaque fois que le scrutateur comptabilise un vote, le nombre de votes pour Y demeure plus grand que le nombre des votes pour X. On peut dire que cela est un dépouillement « sans stress » pour Y.

On cumule les votes au moyen d'un vecteur (x, y), avec x égal au nombre de votes pour X, et y égal au nombre de votes pour Y. Pour chaque vote comptabilisé, le nouveau cumul de votes est soit $(x, y) + (1, 0)$, soit $(x, y) + (0, 1)$, selon que le vote dépouillé est pour X ou Y. L'histoire complète d'un dépouillement correspond donc à un chemin dans le réseau $\mathbb{N} \times \mathbb{N}$, se terminant au point (n, k). Comme on l'a vu, il y a $\binom{k+n}{n}$ tels chemins.

Au sens de notre problème, un dépouillement sans stress pour Y correspond à un chemin qui reste au-dessus de la diagonale, et n'y revient jamais après l'avoir quitté en passant de $(0, 0)$ à $(0, 1)$. C'est donc dire que dans le chemin $\gamma = (p_0, \ldots, p_{n+k})$ codant le dépouillement, on a d'abord $p_1 = (0, 1)$; puis, tous les $p_i = (x_i, y_i)$ subséquents sont tels que

$$y_i > x_i, \qquad \text{pour tout } i > 0. \tag{3.49}$$

Puisqu'on a toujours $p_1 = (0, 1)$, il est pratique de ne considérer que les chemins de source $(0, 1)$. L'ensemble des chemins $\Gamma_{0,1}(n, k)$, de source $(0, 1)$, se partage en l'union disjointe des deux en-

sembles :

$$\begin{aligned}\mathcal{T}(n,k) &:= \{\gamma \in \Gamma_{0,1}(n,k) \mid \gamma = ((x_i,y_i))_{1\le i\le k+n},\ \exists i>0 \quad \text{avec } y_i = x_i\},\\ \mathcal{R}(n,k) &:= \{\gamma \in \Gamma_{0,1}(n,k) \mid \gamma = ((x_i,y_i))_{1\le i\le k+n},\ \forall i>0 \quad \text{on a } y_i > x_i\}.\end{aligned}$$

Les éléments de $\mathcal{T}(n,k)$ sont donc les chemins qui « touchent » à la diagonale $y=x$, et ceux de $\mathcal{R}(n,k)$ sont les chemins qui « restent » au-dessus de la diagonale $y=x$, et on a

$$|\mathcal{T}(n,k)| + |\mathcal{R}(n,k)| = \binom{k+n-1}{n}.$$

Reste maintenant à calculer le nombre d'éléments $\mathcal{R}(n,k)$ qui correspond au nombre de dépouillements sans stress pour Y.

On obtient ce nombre indirectement en calculant plutôt $|\mathcal{T}(n,k)|$ par le biais du « principe de réflexion » attribué habituellement à Désiré André[6]. Tout simplement, ce principe donne une bijection entre $\mathcal{T}(n,k)$ et l'ensemble $\Gamma_{1,0}(n,k)$ des chemins allant du point $(1,0)$ au point (n,k). Pour un chemin γ dans $\mathcal{T}(n,k)$, la bijection consiste à remplacer la portion du chemin γ allant de $(0,1)$ jusqu'à son premier retour la droite $y=x$, par sa réflexion par rapport à cette droite. Plus précisément, on commence par décomposer γ en produit de chemin

$$\gamma = \gamma' \cdot \gamma'',$$

avec γ' se terminant au premier point p_i pour lequel $y_i = x_i$, c.-à-d. : i minimal et ≥ 1.

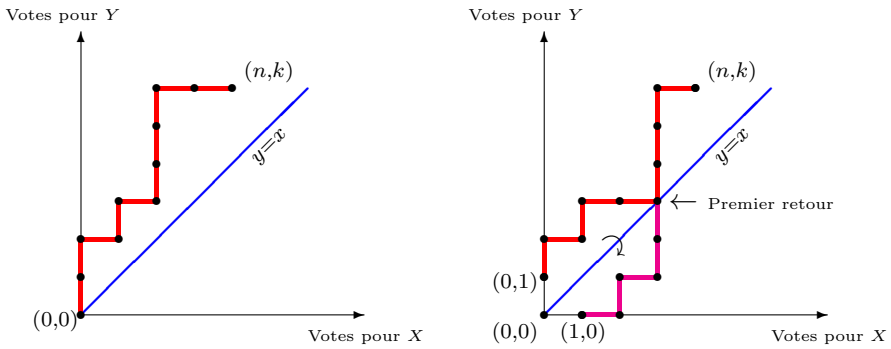


FIGURE 3.9 – Chemins sans ou avec stress.

Le **principe de réflexion** consiste à envoyer γ sur

$$\rho(\gamma) := \widehat{\gamma'} \cdot \gamma'', \tag{3.50}$$

6. Désiré André (1840–1910). Apparemment il n'aurait pas utilisé de réflexion comme telle, mais l'idée de sa preuve est semblable.

où $\widehat{(x,y)} := (y,x)$ est la réflexion selon la diagonale $y = x$. Il est clair que ρ est une bijection qui est son propre inverse. Ce processus est illustré dans la partie de droite de la Figure 3.9. Le fait que cela soit une bijection est facile à vérifier. On en déduit que

$$|\mathcal{T}(n,k)| = \binom{k+n-1}{n-1}.$$

Un calcul direct donne alors

$$|\mathcal{R}(n,k)| = \frac{k-n}{k+n}\binom{k+n}{n}. \tag{3.51}$$

Comme le nombre total de dépouillements est $\binom{n+k}{n}$, la probabilité que Y demeure sans stress est donc :

$$\frac{|\mathcal{R}(n,k)|}{|\Gamma(n,k)|} = \frac{k-n}{k+n}. \tag{3.52}$$

Preuve de la Proposition 3.5. Supposons $k = n$ et cherchons le nombre de dépouillements où le candidat Y est toujours en avance ou à égalité avec le candidat X. (voir la Figure 3.10). Dans ce cas, on trouve $\binom{2n}{n}$ chemins au total, et $\binom{2n}{n-1}$ d'entre eux (ceux qui touchent à la droite $y = x-1$) sont à rejeter. Le nombre de chemins cherché est donc

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

et on trouve que ces chemins sont comptés par les nombres de Catalan. ■

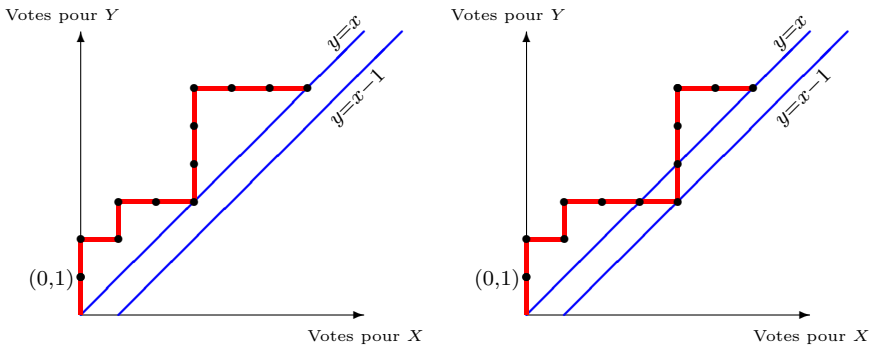


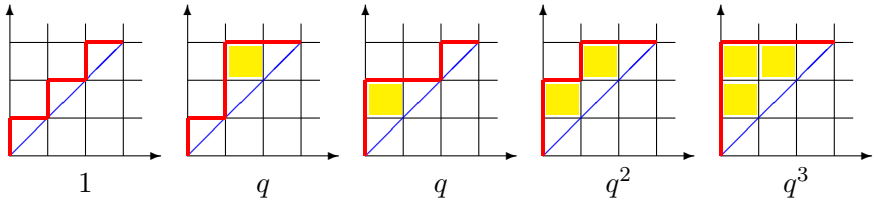
FIGURE 3.10 – Chemins de Dyck.

3.8 Chemins de Dyck avec poids

On peut énumérer les chemins de Dyck en tenant compte de l'aire de la façon suivante. On adapte légèrement la notion d'aire sous le chemin en ne tenant compte que des cases qui se situent au-dessus de la diagonale. On s'intéresse donc au calcul de

$$\mathcal{C}_n(q) := \sum_{\gamma \in \mathsf{Dyck}[n]} q^{\alpha(\gamma)}, \tag{3.53}$$

où $\alpha(\gamma)$ désigne l'aire (le nombre de cases) de la région entre le chemin et la diagonale $y = x$. Bien entendu, si l'on pose $q = 1$, on obtient $\mathcal{C}_n(q) = C_n$. On dit que les $\mathcal{C}_n(q)$ sont des **q-analogues des nombres de Catalan**. Les 5 chemins de Dyck de hauteur 3 ont les poids $q^{\alpha(\gamma)}$ respectifs :



En répertoriant les configurations analogues, on trouve :

$$\begin{array}{rcl}
\mathcal{C}_0(q) &=& 1, \\
\mathcal{C}_1(q) &=& 1, \\
\mathcal{C}_2(q) &=& q+1, \\
\mathcal{C}_3(q) &=& q^3+q^2+2\,q+1 \\
\mathcal{C}_4(q) &=& q^6+q^5+2\,q^4+3\,q^3+3\,q^2+3\,q+1, \\
\mathcal{C}_5(q) &=& q^{10}+q^9+2\,q^8+3\,q^7+5\,q^6+5\,q^5+7\,q^4+7\,q^3+6\,q^2+4\,q+1.
\end{array} \tag{3.54}$$

Au moyen de la décomposition selon le premier retour, on obtient (voir Exercice 3.9) que les polynômes $\mathcal{C}_n(q)$ satisfont la récurrence

$$\mathcal{C}_n(q) = \sum_{i=0}^{n-1} q^i \mathcal{C}_i(q)\, \mathcal{C}_{n-i-1}(q), \tag{3.55}$$

qui se spécialise en la récurrence (3.28) lorsqu'on pose $q = 1$.

3.9 Exercices

3.1. Combien il y a-t-il de palindromes de longueur k sur l'alphabet $\{a, b\}$?

3.2. Montrer les identités (3.14) et (3.15).

3.3. (*) Pour rendre rigoureux la notation additive des langages, on considère l'anneau des séries $\mathbb{Q}\langle\langle A\rangle\rangle$ en les variables non commutatives correspondant aux éléments de A, c.-à-d. : $x\,y \neq y\,x$, pour x et y dans A. Par définition, les éléments de cet anneau sont les sommes formelles

$$\sum_{w\in A^*} c_w\, w, \qquad \text{avec} \qquad c_w \in \mathbb{Q}, \tag{3.56}$$

avec coefficients rationnels.

a) Montrer qu'en posant

$$\begin{aligned}\Big(\sum_{w\in A^*} c_w\, w\Big) + \Big(\sum_{w\in A^*} d_w\, w\Big) &:= \sum_{w\in A^*} (c_w + d_w)\, w,\\ \Big(\sum_{w\in A^*} c_w\, w\Big)\cdot\Big(\sum_{w\in A^*} d_w\, w\Big) &:= \sum_{w\in A^*} \Big(\sum_{u\cdot v=w} c_u\, d_v\Big)\, w\end{aligned}$$

on obtient un anneau (non commutatif).

b) Montrer qu'on a un unique homorphisme d'anneau $\Psi : \mathbb{Q}\langle\langle A\rangle\rangle \to \mathbb{Q}[\![z]\!]$, vers l'anneau des séries formelles en la variable z, pour lequel $\Psi(x) = z$ pour chaque variable x dans A, et que $\Psi(\mathcal{L}) = \mathcal{L}(z)$, pour tout langage $\mathcal{L}$.

3.4. Montrer qu'il y a bijection entre les mots du langage $(a+b)^n$, et les sous-ensembles de $[n]$.

3.5. Montrer que les mots de Dyck correspondent aux parenthèsages « équilibrés », pour lesquels à chaque parenthèse ouvrante « (», il correspond une parenthèse fermante «) » bien placée. Par exemple, les 5 parenthèsages

$$(\,)(\,)(\,), \qquad (\,)((\,)), \qquad ((\,))(\,), \qquad ((\,)(\,)), \quad \text{et} \quad (((\,))).$$

correspondent aux 5 mots de Dyck : $yxyxyx$, $yxyyxx$, $yyxxyx$, $yyxyxx$, et $yyyxxx$. Plus précisément, un **parenthésage** est un mot sur l'alphabet constitué des deux lettres « (» et «) ». Pour chaque i entre 1 et n, on calcule la différence

$$\begin{aligned} d_i \;:=\; &(\text{nombre de parenthèses ouvrantes avant la position } i)\\ &-(\text{nombre de parenthèses fermantes avant la position } i).\end{aligned}$$

Le parenthèsage est dit **équilibré** si et seulement si on a $d_i \geq 0$ pour tout i, et si $d_n = 0$.

3.6. Utiliser (1.99) pour montrer, à partir de (3.25), que les nombres de Catalan sont bien donnés par la formule

$$C_n = \frac{1}{n+1}\binom{2\,n}{n}. \tag{3.57}$$

3.7. Construire un automate qui reconnaît le langage de l'exemple (3.22).

3.8. En comparant les coefficients de z^n de chacun des membres de l'équation (3.25), déduire la récurrence (3.28). Une autre approche consiste à montrer d'abord que, pour $n > 1$, on a

$$\mathcal{D}_{2\,n} = \sum_{k=0}^{n-1} a\,\mathcal{D}_{2\,k}\,b\,\mathcal{D}_{2\,n-2\,k-2}, \tag{3.58}$$

puis on applique la Proposition 3.1.

3.9. Montrer la récurrence (3.55) en décomposant les chemins de Dyck selon leur premier retour à la diagonale. Suggestion : Tenir compte du fait que la première composante est un chemin de Dyck premier. Utiliser ensuite le Lemme 3.3 en tenant compte du calcul de l'aire.

3.10. Donner les conditions que doivent satisfaire deux ensembles de points A et B (dans $\mathbb{N} \times \mathbb{N}$) pour qu'ils correspondent respectivement à l'ensemble des coins extérieurs, et l'ensemble des coins intérieurs, d'un même chemin de Dyck. Suggestion : Il y a d'abord une condition liant les cardinaux de ces ensembles, puis une condition sur la position relative de leurs éléments.

Programmation mathématique

3.11. Construire une procédure qui construit tous les palindromes de longueur k sur un alphabet A.

3.12. Traduire l'équation 3.23 en une procédure récursive qui génère tous les mots de Dyck de longueur n.

3.13. Construire une procédure qui, avec comme données un automate, un état et un mot, calcule le résultat obtenu en appliquant la fonction associée à ce mot à l'état donné.

3.14. Construire une procédure qui, avec comme données un automate, un état initial et des états finaux fixés, calcule tous les mots de longueur n du langage reconnu par cet automate, avec cet état initial et ces états finaux.

3.15. Construire une procédure qui calcule tous les points d'un chemin de Dyck, étant donné la position de ses coins extérieurs et de ses coins intérieurs.

Chapitre 4

Diverses structures combinatoires

4.1 Introduction.

Bien entendu, il y a une grande variété de structures combinatoires, chacune adaptée à la solution de problèmes particuliers. Certaines structures sont si importantes qu'elles méritent un chapitre à elles seules. Nous allons ici faire un rapide survol de structures variées, sans prétendre couvrir tout le spectre des objets intéressants en combinatoire. D'autres structures seront étudiées plus en profondeur dans des chapitres ultérieurs.

4.2 Arbres binaires

Un **arbre binaire**[1] sur l'ensemble A peut se décrire récursivement de la façon suivante. Il est

a) soit l'arbre binaire vide, dans le cas $A = \emptyset$; soit l'arbre binaire réduit à un seul noeud, lorsque $|A| = 1$;

b) soit constitué d'un noeud (la racine, qui est un élément x de A) auquel sont attachées une branche gauche et une branche droite (qui sont chacun des arbres binaires, respectivement sur des ensembles B et C tels que $B + C = A \setminus \{x\}$).

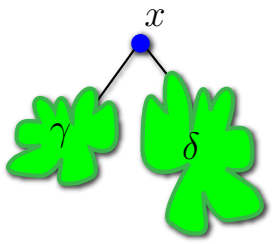
On dénote $\mathcal{B}[A]$ l'ensemble des arbres binaires sur A, et la définition donnée ci-haut correspond plus formellement à dire que

$$\mathcal{B}[A] = \sum_{x \in A} \sum_{B+C=A\setminus\{x\}} \{x\} \times \mathcal{B}[B] \times \mathcal{B}[C], \qquad \text{si} \qquad A \neq \emptyset, \tag{4.1}$$

1. On devrait plutôt dire « arborescence binaire », mais ce n'est pas la tradition.

avec $\mathcal{B}[\emptyset] := \{0\}$, où 0 dénote l'arbre vide. Autrement dit, un arbre binaire est simplement un triplet $\alpha = (x, \gamma, \delta)$, avec $x \in A$, γ un arbre binaire sur B, δ un arbre binaire sur C, et $B + C = A \setminus \{x\}$. On dit que x est la **racine** de α, à laquelle sont rattachées deux branches : γ la **branche gauche**, et δ est la **branche droite**. On dénote respectivement $\gamma(\alpha)$ et $\delta(\alpha)$ les branches gauche et droite de α.

Tous les éléments de A sont des **noeuds** de l'arbre, et ceux qui n'ont pas de descendants (c.-à-d. : de la forme $(x, 0, 0)$) sont les **feuilles** de l'arbre. Pour simplifier la présentation, élimine les 0 qui sont attachés à une feuille. Ainsi les arbres réduits à une feuille prennent la forme (x), plutôt que $(x, 0, 0)$.On dessine habituellement les arbres binaires comme suit :



La racine se retrouve donc toute en haut, et les deux branches issues de la racine pointent vers le bas, l'une vers la gauche, l'autre vers la droite. Les noeuds de l'arbre sont représentés par des points (bleus) accompagnés d'une **étiquette**, qui est tout simplement l'élément de A correspondant. La Figure 4.1 donne un exemple complet. Le noeud étiqueté c est la racine, et ceux portant les étiquettes a, d et f sont les feuilles. Les noeuds internes sont b et e. La branche gauche de l'arbre est réduite au seul noeud a, et la branche droite est celle portée par les noeuds b, d, e, et f.

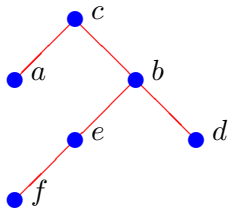


FIGURE 4.1 – L'arbre binaire $(c, (a), (b, (e, (f), 0), (d)))$.

Il est courant de présenter des arbres sans étiquettes. On dit alors qu'on a dessiné la **forme**[2] de l'arbre. À chaque forme d'arbre binaire à n noeuds, il correspond en fait $n!$ arbres qui peuvent s'obtenir en étiquetant (de toutes les façons possibles) les n noeuds par les éléments de A. Comme nous le verrons plus tard, le nombre de formes d'arbres binaires à n noeuds est le n-ième nombre

2. Nous allons rendre tout ceci plus précis au Chapitre 6.

de Catalan :

$$C_n = \frac{1}{n+1}\binom{2\,n}{n}. \tag{4.2}$$

Le nombre total d'arbres binaires sur A, de cardinal n, est donc

$$|\mathcal{B}[A]| = \frac{n!}{n+1}\binom{2\,n}{n}. \tag{4.3}$$

Les 5 formes d'arbres binaires à $n = 3$ noeuds sont celles illustrées à la Figure 4.2.

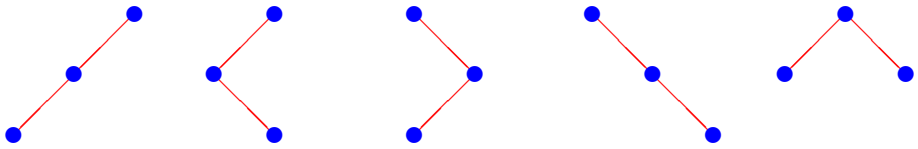


FIGURE 4.2 – Les formes d'arbres binaires à 3 noeuds.

La **profondeur** $\pi_\alpha(y)$ d'un noeud y, d'un arbre binaire α, est la distance entre ce noeud et la racine. Autrement dit, c'est la longueur de l'unique chemin qui relie ce noeud à la racine. La profondeur $\pi(\alpha)$, d'un arbre α, est la profondeur maximale d'un noeud :

$$\pi(\alpha) := \max_{y\in\alpha} \pi_\alpha(y). \tag{4.4}$$

4.3 Arbres binaires croissants

Parmi les arbres binaires sur un ensemble totalement ordonné A, on a ceux pour lesquels les

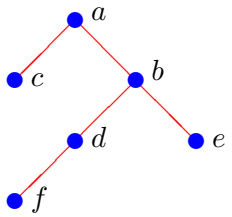


FIGURE 4.3 – Arbre binaire croissant, avec $a < b < c < d < e < f$.

étiquettes vont en croissant le long de tout chemin allant de la racine aux feuilles. On dit de ces arbres binaires qu'ils sont **croissants**, et on dénote $\mathsf{Abc}[A]$ l'ensemble des arbres binaires croissants dont les noeuds sont étiquetés par les éléments de A. Plus précisément, si $\min(A)$ désigne l'élément minimal de A, alors on a la description récursive

$$\mathsf{Abc}[A] = \sum_{B+C=A\setminus\{\min(A)\}} \{\min(A)\} \times \mathsf{Abc}[B] \times \mathsf{Abc}[C], \qquad \text{si} \qquad A \neq \emptyset, \tag{4.5}$$

où on suppose que sur l'ensemble vide, il n'y a qu'un arbre binaire croissant : l'arbre vide. L'ordre sur B, ainsi que celui sur C, sont obtenus par restriction de celui sur A.

Autrement dit, un arbre binaire croissant sur A est un triplet $(\min(A), \gamma, \delta)$, où γ est un arbre binaire croissant sur $B \subseteq A \setminus \{\min(A)\}$, et δ est un arbre binaire croissant sur le complément de B dans $A \setminus \{\min(A)\}$. Sur l'ensemble $A = \{1, 2, 3\}$, on a les 6 arbres binaires croissants de la Figure 4.4.

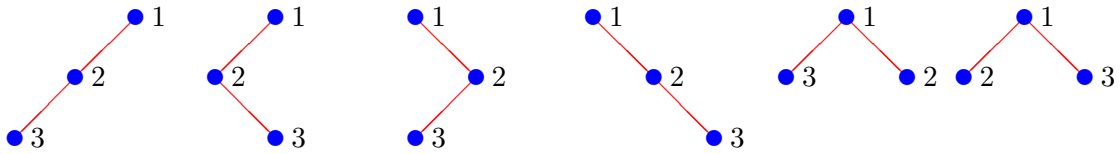


FIGURE 4.4 – Les arbres binaires croissants sur $\{1, 2, 3\}$.

En fait, le nombre d'arbres binaires croissants à n-sommets est exactement $n!$. Ceci découle de la bijection

$$\pi : \mathsf{Abc}[A] \xrightarrow{\sim} \mathbb{L}[A], \tag{4.6}$$

qui se définit récursivement comme suit, en utilisant la notation sous forme de mots pour les ordres totaux sur A. On dit que $\pi(\alpha)$ est la **projection** de α. Soit a l'élément minimal de A. Pour un arbre croissant $\alpha = (a, \gamma, \delta)$ (avec branche gauche γ et branche droite δ), on pose

$$\pi(\alpha) := \pi(\gamma)\, a\, \pi(\delta). \tag{4.7}$$

On récupère l'arbre α à partir de $\ell = \pi(\alpha)$ en calculant le **déployé** $\Delta(\ell)$ de ℓ. Plus précisément, pour un ordre total $\ell = x_1 x_2 \cdots x_n$ sur A, on pose

$$\delta(\ell) := (a, \delta(u), \delta(v)), \tag{4.8}$$

où u et v sont les mots qui sont uniquement caractérisés par le fait que ℓ se décompose comme comme produit (de concaténation) de la façon suivante :

$$\ell = u\, a\, v.$$

On voit facilement que la fonction δ est l'inverse de π. Par exemple, le mot $cabfde$ est la projection de l'arbre binaire croissant de la Figure 4.3. On dit aussi parfois qu'on a obtenu le mot $\pi(\alpha)$ par lecture **infixe** de l'arbre α.

Il découle directement de la construction de la bijection π que

$$|\mathsf{Abc}[A]| = n!, \tag{4.9}$$

si A est un ensemble totalement ordonné de cardinal n.

4.4 Arbres plans

Un **arbre plan** (ou **arbre ordonné**) est un arbre (une arborescence) soit réduit à un seul noeud, soit constitué d'un noeud (la racine) auquel est rattaché une suite non vide d'arbres plan. Ce sont les branches de l'arbre, et elles sont ordonnées de gauche à droite. La Figure 4.5 présente les formes d'arbres plans à 4 noeuds. Plus techniquement, un arbre plan sur A est soit réduit à (x) si $A = \{x\}$,

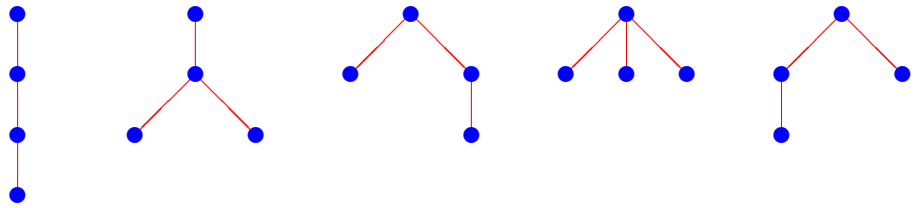


FIGURE 4.5 – Formes d'arbres plans à quatre noeuds

soit un couple (x, B), où x (dans A) est la racine de l'arbre, et $B = (\alpha_1, \alpha_2, \ \dots \ , \alpha_k)$ est une suite non vide ($k > 0$) d'arbres plans. Il n'y a pas d'arbre plan sur l'ensemble vide.

Plus synthétiquement, si $\mathsf{Plan}[A]$ désigne l'ensemble des arbres plans sur A, on a donc $\mathsf{Plan}[\emptyset] = \emptyset$; $\mathsf{Plan}[\{x\}] = \{x\}$; et

$$\mathsf{Plan}[A] = \sum_{x\in A} \sum_{k\geq 1} \sum_{B_1+\ldots+B_k=A\setminus\{x\}} \{x\} \times \mathsf{Plan}[B_1] \times \cdots \times \mathsf{Plan}[B_k], \tag{4.10}$$

dans les autres cas. Par exemple, on a les 12 arbres plans

$$\begin{aligned} \mathsf{Plan}[3] = \ \{&(1,(2,(3))), \quad (1,(3,(2))), \quad (2,(1,(3))),\\ &(2,(3,(1))), \quad (3,(1,(2))), \quad (3,(2,(1))),\\ &(1,((2),(3))), \quad (1,((3),(2))), \quad (2,((1),(3))),\\ &(2,((3),(1))), \quad (3,((1),(2))), \quad (3,((2),(1)))\}, \end{aligned}$$

L'arbre $(1,(2,(3)))$ n'a qu'une feuille qui est 3 ; et l'arbre $(1,((2),(3))$ à 2 et 3 comme feuilles. Le nombre d'arbres plan à n noeuds est

$$|\mathsf{Plan}[A]| = (n-1)!\binom{2\,n-2}{n-1}, \qquad (|A| = n). \tag{4.11}$$

4.5 Triangulations d'un polygone

Une triangulation d'un polygone régulier à n sommets, est un découpage du polygone en $n-2$ triangles dont les sommets sont les sommets du polygone. On demande que deux triangles de la triangulation aient au plus un côté ou un sommet en commun.

Plus explicitement, supposons que les sommets du polygone sont étiquetés de 1 à n dans le sens des aiguilles d'une montre. Autrement dit, on considère le polygone comme étant un graphe simple avec les arêtes

$$\{\{i, (i+1 \bmod n)\} \mid 1 \leq i \leq n\}.$$

Un **triangle** d'une triangulation est la donnée d'un ensemble $\{a, b, c\}$ de trois sommets du polygone. On dit que deux triangles $T_1 = \{a, b, c\}$ et $T_2 = \{d, e, f\}$ (avec $T_1 \cap T_2 = \emptyset$) se **croisent** si on a deux des sommets de T_1, disons a et b, et deux sommets de T_2, disons c et d qu'on rencontre dans l'ordre a, c, b, d lorsqu'on tourne autour du polygone dans le sens des aiguilles d'une montre. Bien entendu, les triangles sont dits **sans croisement** s'ils ne se croisent pas.

Une **triangulation** τ est la donnée d'une famille

$$\tau = \{\, \{a_i, b_i, c_i\} \,\}_{1 \leq i \leq n-2} \tag{4.12}$$

de triangles qui recouvrent $[n]$, et qui sont deux à deux sans croisements. On désigne par $\Delta[n]$ l'ensemble des triangulations d'un polygone à n-cotés. Par exemple, pour $n = 5$, on a les 5 triangulations

$$\Delta[5] = \{\{123, 134, 145\},\ \{123, 135, 345\},\ \{125, 234, 245\},\ \{124, 145, 234\},\ \{125, 235, 345\}\},$$

où on a écrit abc pour le triangle $\{a, b, c\}$. Ces 5 triangulations du pentagone sont présentées de façon plus imagée à la Figure 4.6. Comme nous allons le montrer plus loin, le nombre de triangulations

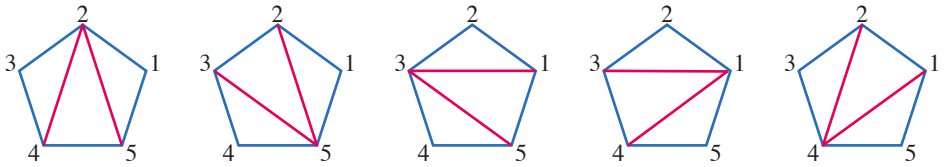


FIGURE 4.6 – Triangulations du pentagone

d'un polygone à $n + 2$ cotés est donné par le n-ième nombre de Catalan. En passant, ces nombres ont été découverts par Euler, longtemps avant Catalan. Dans une lettre adressée à Goldbach en 1751, Euler les considère dans le contexte de l'énumération des triangulations d'un polygone. Il y donne la formule (3.27), et la série génératrice (3.25). Goldbach répond en soulignant que la série satisfait l'équation (3.24).

4.6 Configurations de Catalan

Un fait expérimental, peut-être un peu étonnant a priori, est qu'il y a souvent un grand nombre de familles de structures combinatoires différentes qui sont comptées par la même famille de nombres.

Ci-dessous, nous allons discuter plus en détail le cas des nombres de Catalan. Pour l'instant, on peut mentionner un autre cas bien connu : celui des nombres de Fibonacci. En effet, ces nombres semblent jouer tellement de rôles différents, qu'on a même mis sur pied une association officielle les concernant. On peut trouver plus de détails sur cette association à l'adresse

http://www.mathstat.dal.ca/fibonacci/.

Cette association publie un journal spécialisé s'intitulant : ≪ The Fibonacci Quaterly ≫, qui se consacre exclusivement aux nombres de Fibonacci.

Le fait de reconnaître que de mêmes nombres interviennent dans deux (ou plusieurs) contextes différents peut s'avérer un indice précieux pour révéler qu'il y a des liens inattendus entre les sujets concernés. C'est cette idée qui a poussé N.J.A. Sloane à rédiger un livre, *The Handbook of Integer Sequences* (paru en 1973), dans lequel il a répertorié 2372 suites de nombres jouant un rôle dans un ou plusieurs domaines des mathématiques et d'autres sciences, avec une (ou des) référence bibliographique donnant l'origine des suites. De nombreux chercheurs ont depuis eu l'occasion d'exploiter cette ressource pour assister leurs travaux de recherche. Devant tant de succès, 22 ans plus tard Sloane, avec la collaboration de Simon Plouffe (de l'UQAM), a récidivé en publiant *The Encyclopedia of Integer Sequences* (1995), avec maintenant 5488 suites répertoriées. De plus (c'est là une des contributions de Simon Plouffe), la nouvelle version contient des formules explicites nouvelles obtenues au moyen d'outils de calcul formel spécialisés (voir la Section A.3). On trouve maintenant en ligne le site **The Online Encyclopedia of Integer Sequences** :

http://www.research.att.com/ njas/sequences/,

qui permet de consulter cette base de données. On peut aussi y retrouver des exemples d'utilisation de ces informations pour l'avancement de recherches théoriques. Il y a une liste de 1705 articles spécialisés mentionnant avoir utilisé ces outils.

Lorsqu'une suite de nombre sentiers

$$a_0,\ a_1,\ a_2,\ a_3,\ \ldots,$$

compte des structures combinatoires, on dit qu'on en a une ≪ interprétation combinatoire ≫. On peut aussi en avoir une interprétation algébrique, par exemple s'ils apparaissent comme dimensions d'une famille d'espaces vectoriels.

Les nombres de Catalan jouent divers rôles importants autant en combinatoire énumérative qu'en combinatoire algébrique. Dans son livre *Enumerative Combinatorics*[3], Richard Stanley, sous la forme d'exercices, en énumère 66 interprétations combinatoires et 9 interprétations algébriques. Sur son site web

www-math.mit.edu/∼rstan/ec

3. Cambridge University Press, 1999

on trouve de plus au moins 110 autres interprétations des nombres de Catalan. Voici seulement quelques-unes des configurations en question. Ce sont en fait celles que nous avons rencontrées jusqu'ici.

(1) Formes d'arbres binaires ayant n noeuds.

(2) Formes d'arbres plans ayant $n+1$ noeuds.

(3) Mots de Dyck de longueur $2\,n$.

(4) Chemins de Dyck de hauteur $2n$.

(5) Fonctions strictement croissantes de $[2] \times [n]$ vers $[2\,n]$.

(6) Triangulations d'un polygone à $(n+2)$ sommets.

On va voir qu'on a de jolies bijections entre ces différentes configurations. Il en découle qu'elles sont toutes comptées par les nombres de Catalan C_n, puisqu'on a déjà vu que c'est le cas pour les chemins de Dyck de hauteur n.

Les bijections

(**1**)↔(**2**). Le passage d'un arbre binaire à un arbre ordonné peut se décrire aisément en terme de filiation. On ajoute un nouveau noeud comme « père »[4] de la racine, et on interprète le fait de descendre dans la branche gauche d'un arbre binaire comme le passage de « père » en « fils ». Descendre dans la branche droite s'interprète comme le passage de « frère » à « frère cadet ». Ce processus est illustré à la Figure 4.6. Le noeud supplémentaire est celui qui est étiqueté x. On enlève de part et d'autre les étiquettes des noeuds, pour obtenir la correspondance en terme de forme d'arbres.

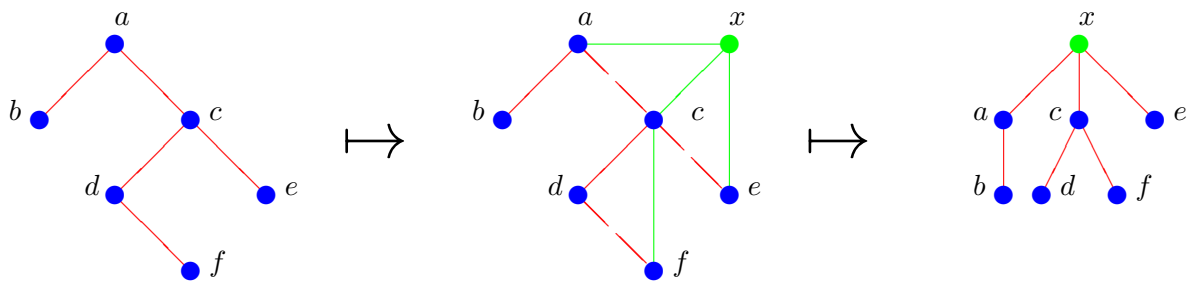


FIGURE 4.7 – Un arbre binaire et l'arbre plan correspondant.

Pour $n = 3$, la bijection de la Figure 4.8.

4. Selon le goût du lecteur, on peut substituer « mère » pour « père » et « fille » pour « fils », ou même encore utiliser les plus neutres de termes « parent » et « enfant ».

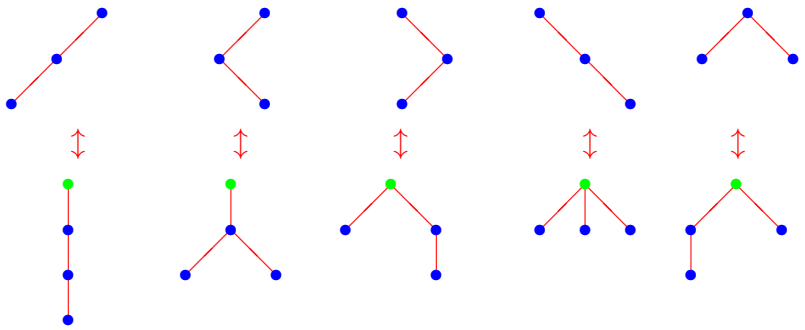
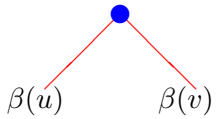


FIGURE 4.8 – La bijection (**1**)↔(**2**) pour $n = 3$.

(**1**)↔(**3**). On décrit cette bijection de façon récursive, en exploitant la décomposition (3.23) des mots de Dyck. Rappelons que tout mot de Dyck (non vide) w admet une décomposition unique de la forme

$$w = a\,u\,b\,v, \qquad \text{où} \quad u, v \quad \text{sont des mots de Dyck sur } \{a, b\},$$

avec u de longueur minimale. La forme d'arbre binaire $\beta(w)$, associée à w, est construite récursivement [5] en posant

$\beta(w) :=$ 

lorsque w est différent du mot vide. Sinon $\beta(w)$ est l'arbre vide. Pour $n = 3$, on a la bijection de la Figure 4.9.

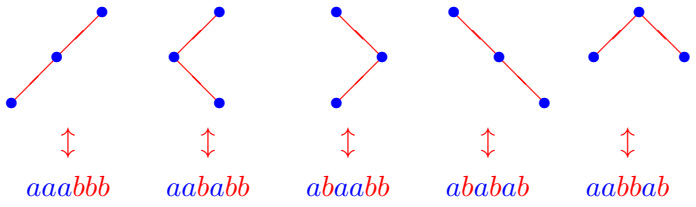


FIGURE 4.9 – La bijection (**1**)↔(**3**) pour $n = 3$.

(**3**)↔(**4**). On a déjà montré comment passer d'un mot de Dyck à un chemin de Dyck. Pour $n = 3$, on a la bijection de la Figure 4.10.

5. Voir la Section 6.9 pour plus de détails à ce sujet.

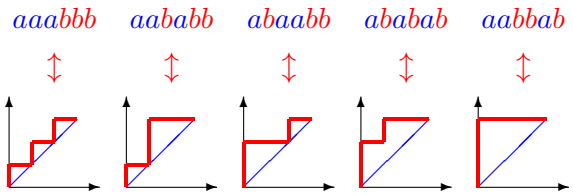


FIGURE 4.10 – La bijection (**3**)↔(**4**) pour $n = 3$.

(**3**)↔(**5**). On passe d'un mot de Dyck de longueur $2\,n$ à une fonction croissante de $[2] \times n]$ vers $[2\,n]$, en procédant comme suit. Pour un mot de Dyck $w = w_1\, w_2 \cdots w_{2\,n}$, avec w_i égal à a ou b. La fonction cherchée s'obtient en plaçant dans l'ordre croissant les i tels que $w_i = a$ dans la ligne du bas, et les i tels que $w_i = b$ dans la ligne du haut. Pour $n = 3$, on a la bijection de la Figure 4.11. Autrement dit, les valeurs sur la ligne du bas correspondent aux positions des a dans le mot.

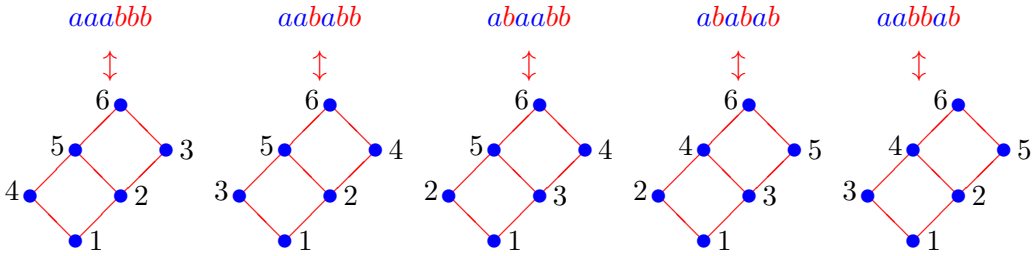


FIGURE 4.11 – La bijection (**3**)↔(**5**) pour $n = 3$.

(**1**)↔(**6**). Voir Exercice 4.1.

4.7 Fonction de stationnement$^{(*)}$

Supposons que n « conducteurs » ont chacun opté d'avance pour une des n places de stationnement, toutes situées du même coté d'une rue à sens unique et numéroté consécutivement de 1 à n. Autrement dit, on a une fonction ψ de l'ensemble $\mathcal{C}$ des conducteurs vers l'ensemble $\{1, 2, \ldots, n\}$, qui rend compte des préférences de stationnement de chaque conducteur, avec $\psi(c) = k$ si le conducteur c préfère la place k. On peut tout aussi bien numéroter les conducteurs de 1 à n, et donc on suppose dorénavant que $\mathcal{C} = [n]$, c.-à-d. : $\psi : [n] \to [n]$. On dit que ψ est la **fonction de préférence**. Il n'y a aucune restriction sur ces préférences. Par exemple, les conducteurs peuvent avoir tous choisi la place 1 comme place préférée.

Pour une fonction de préférence ψ fixée, on suppose que les conducteurs arrivent l'un après l'autre, dans un ordre quelconque, et s'avancent jusqu'à leur place préférée. Ils s'y garent si elle est libre, ou se garent à la première place libre qui suit leur place préférée. Dans le cas illustré à la Figure 4.12, le prochain conducteur désire se garer à la place numérotée 8, qui est occupée. Il se garera donc à la donc la place 9, qui est libre. S'il existe un ordre d'arrivée des conducteurs pour lequel un des

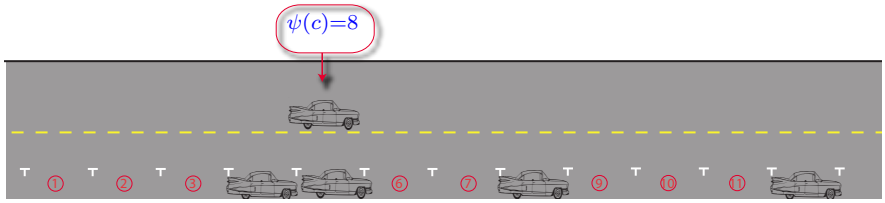


FIGURE 4.12 – Un conducteur cherchant sa place préférée.

conducteurs n'arrive pas à se trouver une place (suivant cette procédure) avant de parvenir à la fin de la rue, on dit que la fonction de préférence ψ n'est pas une fonction de stationnement. Au contraire, on dit avoir une **fonction de stationnement** si chaque conducteur réussit à se garer, quelque soit l'ordre d'arrivée. On montre facilement que ψ est une fonction de stationnement [6] si et seulement si, pour tout k entre 1 et n, l'image inverse

$$\psi^-([k]) = \{c \in \mathcal{C} \mid \psi(c) \leq k\}.$$

contient au moins k éléments, c.-à-d. :

$$\mathsf{Sta}[n] := \{\psi : [n] \to [n] \mid (\forall k) \ \left|\psi^-([k])\right| \geq k \ \}. \tag{4.13}$$

Autrement dit, pour chaque k il y a au moins k conducteurs qui désirent se garer dans les k premières places.

La **type** $\tau(\psi)$ d'une fonction $\psi : [n] \to [n]$, est le vecteur dans $\mathbb{N}^n$ dont les coordonnés correspondent aux cardinaux des fibres de ψ. Plus précisément, on calcule pour chaque k entre 1 et n, le cardinal $d_k := |\psi^-(k)|$, et le type de ψ est le vecteur

$$\tau(\psi) := (d_1, d_2, \ \ldots \ , d_n). \tag{4.14}$$

On a que ψ est une fonction de stationnement si et seulement si son type satisfait la condition

$$d_1 + d_2 + \ldots + d_k \geq k, \tag{4.15}$$

pour tout k entre 1 et n. La **forme** $\lambda(v)$ d'un vecteur $v \in \mathbb{N}^n$ est la suite obtenue en réordonnant en ordre décroissant les coordonnés non nulles de v. Ainsi, on a $\lambda(2, 1, 0, 3, 0, 0) = 321$. Nous allons

6. Apparemment cette notion est en fait dû à R. Pyke (voir [30]). Elle a été redécouverte par A.G. Konheim et B. Weiss (voir [23]) dans un contexte informatique.

voir que le nombre de fonctions de stationnement d'un type donné ne dépend que de la forme du type.

On dénote $\mathsf{Sta}[n]$ l'ensemble des fonctions de stationnement. C'est un sous-ensemble de $\mathsf{End}[n]$. Comme on l'a déjà fait dans d'autres circonstances, on peut décrire une fonction de stationnement comme un mot $\psi = p_1 p_2 \cdots p_n$, avec $p_i = \psi(i)$. Ainsi, les 3 fonctions de stationnement qui correspondent au cas $n = 2$ sont :

$$\mathsf{Sta}[2] = \{11, 12, 21\}.$$

Pour $n = 3$, on a les 16 fonctions de stationnement :

$$\begin{aligned}\mathsf{Sta}[3] = \{&111,\ 112,\ 121,\ 211,\ 113,\ 131,\ 311,\ 122,\\ &212,\ 221,\ 123,\ 132,\ 213,\ 231,\ 312,\ 321\}\end{aligned}$$

Dans cette notation, le type de la fonction de stationnement 241144 est $\tau(241144) = (2, 1, 0, 3, 0, 0)$. C'est donc la suite des multiplicités des lettres du mot.

Le problème posé consiste à compter le nombre de fonctions de stationnement en terme de n. Pour ce faire [7] on déforme la rue pour en faire un cercle, et on ajoute une place de stationnement étiquetée $n + 1$, comme illustré à l Figure 4.13. qui peut aussi être l'une des places préférées. Il

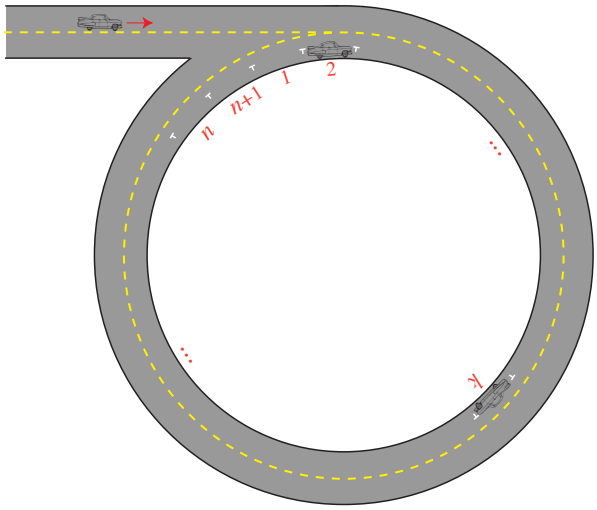


FIGURE 4.13 – Stationnement circulaire.

en résulte donc que ψ prend maintenant des valeurs entre 1 et $n + 1$. Toutes les voitures peuvent toujours se stationner, quitte à repasser par le début ; et, à la fin, il reste toujours exactement une place de libre. La fonction ψ est une fonction de stationnement si la seule place libre est la place

7. Cette approche est due à Pollak (voir [32, Sec. 2]).

numérotée $n+1$. Pour chaque fonction de préférence ψ, et chaque j entre 0 et n, on a une fonction de préférence ψ_j définie comme :

$$\psi_j(c) := (\psi(c) + j \bmod n+1).$$

Parmi les $(n+1)^n$ fonctions de préférences, il y en a $n+1$ qui s'écrivent comme ψ_j, pour chaque fonction de stationnement ψ. Une seule d'entre elles laisse la place $n+1$ libre. On a donc $(n+1)^n/(n+1) = (n+1)^{n-1}$ fonctions de stationnement :

$$|\mathsf{Sta}[n]| = (n+1)^{n-1}. \tag{4.16}$$

Décomposition selon le type. Si $\mathcal{T}_n$ est l'ensemble des types possibles pour des fonctions de stationnement, on a la décomposition

$$\mathsf{Sta}[n] = \sum_{\gamma \in \mathcal{T}_n} \mathsf{Sta}_\gamma, \tag{4.17}$$

où Sta_γ dénote l'ensemble des fonctions de stationnement de type γ. Pour étudier cette décomposition de l'ensemble $\mathsf{Sta}[n]$ selon le type, on exploite le fait qu'il y a une bijection naturelle entre l'ensemble $\mathcal{T}_n$ des types de fonctions dans $\mathsf{Sta}[n]$, et l'ensemble $\mathsf{Dyck}[n]$ des chemins de Dyck de hauteur n.

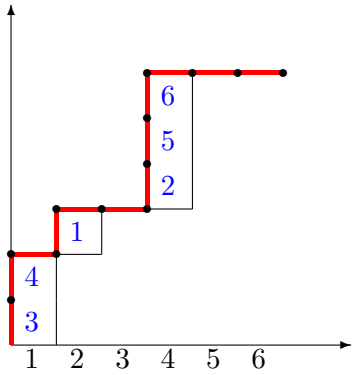


FIGURE 4.14 – Chemin de Dyck de la fonction de stationnement 241144.

Pour un chemin de Dyck de hauteur n :

$$\gamma = (p_0, p_1, \ \ldots \ , p_{2n}), \qquad \text{avec} \qquad p_i = (x_i, y_i),$$

on considère l'ensemble Vert_γ des points (x_i, y_i) pour lesquels $(x_{i-1}, y_{i-1}) = (x_i, y_i - 1)$. Autrement dit, on ne considère que les points du chemin qui sont l'extrémité supérieure de pas verticaux,

et on dit que Vert_γ est **l'ensemble des pas verticaux** de γ. Comme le chemin est de hauteur n, l'ensemble Vert_γ est de cardinal n. En fait, pour chaque hauteur j (avec $1 \leq i \leq n$), il y a exactement un point de γ qui appartient à Vert_γ. Parmi les points de même hauteur, c'est le point du chemin le plus à gauche qui appartient à Vert_γ. Pour l'exemple de la Figure 4.14, on a

$$\mathsf{Vert}_\gamma = \{(0,1),(0,2),(1,3),(3,4),(3,5),(3,6)\}.$$

Pour chaque k entre 1 et n, l'ensemble Vert_γ contient un certain nombre de points ayant $k-1$ comme première coordonnée. On dénote d_k ce nombre de points, c.-à-d. :

$$d_k := |\{(k-1,i) \mid (k-1,i) \in \mathsf{Vert}_\gamma\}|,$$

et bien sûr $n = d_1 + d_2 + \ldots + d_n$. Pour notre exemple de la Figure 4.14, on a

$$(d_1,d_2,d_3,d_4,d_5,d_6) = (2,1,0,3,0,0).$$

Ce vecteur caractérise entièrement γ. De plus, le fait que γ soit un chemin de Dyck correspond au fait que le vecteur $\tau(\gamma) := (d_1, d_2, \ \ldots \ , d_n)$ satisfasse (4.15) pour tout k. Autrement dit, il y a une bijection entre les chemins de Dyck, et les types de fonctions de stationnement.

Pour chaque chemin de Dyck, on construit l'ensemble Sta_γ des fonctions de stationnement dont le type correspond à $\tau(\gamma)$, de la façon suivante. Pour chaque bijection φ entre $[n]$ et Vert_γ, on construit tout simplement une fonction de stationnement en posant $\psi := \pi \circ \varphi$, où $\pi : \mathsf{Vert}_\gamma \to [n]$ est la fonction telle que $\pi(x,y) := x+1$. En effet, les conditions (4.15) assurent que la fonction résultante est bien une fonction de stationnement.

On observe ensuite que plusieurs bijections $\varphi : [n] \xrightarrow{\sim} \mathsf{Vert}_\gamma$ donnent la même fonction de stationnement. En effet, si on permute entre elles les valeurs associées aux points de Vert_γ ayant même premières coordonnées, on obtient très exactement le même résultat final $\psi = \pi \circ \varphi$. On en conclu que

$$|\mathsf{Sta}_\gamma| = \frac{n!}{d_1! d_2! \cdots d_n!}, \tag{4.18}$$

où $(d_1, d_2, \ \ldots \ , d_n) = \tau(\gamma)$. On écrit parfois $\binom{n}{\tau(\gamma)}$ pour le membre de droite de (4.18). Il résulte de tout ceci que

$$(n+1)^{n-1} = \sum_{\gamma \in \mathsf{Dyck}[n]} \binom{n}{\tau(\gamma)}. \tag{4.19}$$

4.8 Polyominos$^{(*)}$

Un **polyomino** est un ensemble fini « connexe » de cases de $\mathbb{N} \times \mathbb{N}$, à translation près. Plus précisément, un polyomino π est un sous-ensemble fini de $\mathbb{N} \times \mathbb{N}$, tel qu'il existe un chemin

reliant toute case à toute autre, et qui est constitué de pas de la forme $(x, y) \rightsquigarrow (x \pm 1, y)$ ou $(x, y) \rightsquigarrow (x, y \pm 1)$. On dit que le nombre de cases du polyomino est son **aire**. Par exemple, on a le polyomino d'aire 36 de la Figure 4.15.

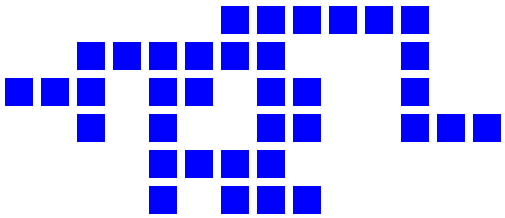


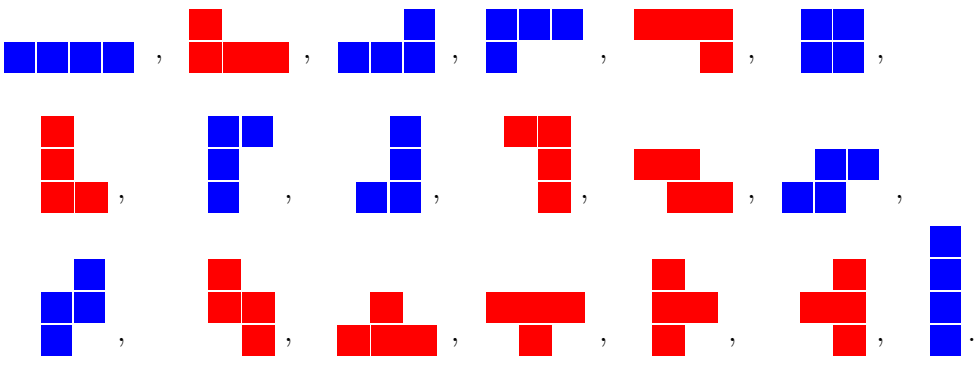
FIGURE 4.15 – Un polyomino d'aire 36.

Il n'y a qu'un seul polyomino d'aire 1 (aussi appelé **monomino**) :

Il y a deux polyominos d'aire 2 (les **dominos**) :

On a les 6 polyominos d'aire 3 (les **triominos**) :

et les 19 polyominos d'aire 4 (les **tétraminos**)[8] :



8. Ce sont les formes qui apparaissent dans le jeux de Tétris.

On ne connaît pas encore de formule donnant p_n, le nombre de polyominos d'aire n. Les premières valeurs de ces nombres sont

n	1	2	3	4	5	6	7	8	9	10	11	12	13	...
p_n	1	2	6	19	63	216	760	2725	9910	36446	135268	505861	1903890	...

Cependant, pour certaines familles particulières de polyominos on a de jolis résultats. Ces le cas des polyominos parallélogrammes définit comme suit.

Polyominos parallélogrammes. Considérons deux chemins γ et γ' du plan $\mathbb{N}\times\mathbb{N}$, allant de $(0,0)$ à $(n-k,k)$ (pour $n>k$), et qui ne se croisent pas. C'est donc dire qu'il n'ont aucun point en commun, sauf leurs extrémités. L'ensemble des cases de $\mathbb{N}\times\mathbb{N}$ qui se situent entre les deux chemins forme un polyomino qui est dit **parallélogramme**. Sans perte de généralité, on peut supposer que

$$\mathsf{Vert}_\gamma = \{(x_1,1),(x_2,2),\ \dots\ ,(x_k,k)\},\quad \text{et}\quad \mathsf{Vert}_{\gamma'} = \{(y_1,1),(y_2,2),\ \dots\ ,(y_k,k)\},$$

avec $x_i < y_i$, $x_1 = 0$, et $y_k = (n-k,k)$. Les cases du polyomino parallélogramme, dénoté $\pi_{\gamma\gamma'}$, associé au couple de chemins (γ,γ') sont alors

$$\pi_{\gamma\gamma'} := \{(z,i) \mid x_i < z \le y_i,\ 1\le i\le k\}. \tag{4.20}$$

On observe que tous ces polyominos ont **périmètre** égal à $2\,n$, quelque soit k. On dénote $\mathsf{Pol}_{/\!/}[n]$ l'ensemble de ces polyominos parallélogrammes de périmètre $2\,n$, sans tenir compte de l'aire. Les polyominos parallélogrammes d'aire ≤ 4 sont ceux qui apparaissent en bleu dans les listes plus haut. On a 5 polyominos de périmètre 8, 4 d'entres eux sont d'aire 3, et il y en a un seul d'aire 4.

Un polyomino parallélogramme est caractérisé (voir Exercice 4.3) par les deux suites

$$\alpha = (a_1,a_2,\ \dots\ ,a_k),\quad \text{et}\quad \beta = (b_1,b_2,\ \dots\ ,b_{k-1})$$

qui donnent respectivement le nombre de cases dans chaque ligne du polyomino, et le nombre de **contacts** entres deux colonnes consécutives. Autrement dit, avec les mêmes notations que ci-haut, on a

$$a_i := y_i - x_i,\quad \text{et}\quad b_i := x_{i+1} - y_i. \tag{4.21}$$

On peut bijectivement coder les deux suites α et β sous la forme d'un chemin de Dyck γ de hauteur $n-1$, en spécifiant (voir Exercice 4.4) la position des coins extérieurs et des coins intérieurs de γ au moyen des entrés de ces suites. Il s'ensuit que :

Proposition 4.1. *Le nombre de polyominos parallélogrammes de périmètre $2\,n$ est le $(n-1)$-ième nombre de Catalan :*

$$\left|\mathsf{Pol}_{/\!/}[n]\right| = \frac{1}{n}\binom{2\,n-2}{n-1}. \tag{4.22}$$

4.9 Exercices

4.1. Décrire une bijection directe entre les arbres binaires sur n noeuds, et les triangulations d'un polygone à $n+2$ sommets. Suggestion : Les noeuds de l'arbre correspondent aux triangles, et deux noeuds sont reliés si les triangles correspondants ont une arête en commun. On place la racine dans le triangle contenant l'arête $\{1,2\}$. Pour $n=3$, on aura la bijection de la Figure 4.16.

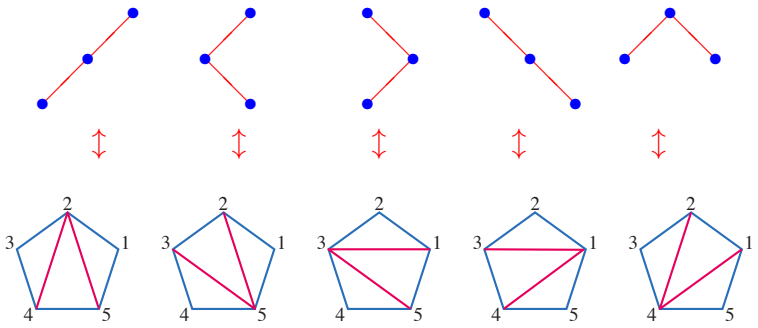


FIGURE 4.16 – La bijection (**1**)↔(**6**) pour $n=3$.

4.2. Montrer que la séries génératrice $f(x)$, pour les arbres ordonnés,est telle que

a)
$$f(x) = x + x\,f(x) + x\,(f(x))^2 + \ldots + x\,(f(x))^k + \ldots = x\,\frac{1}{1-f(x)}$$

b) En déduire l'équation
$$(f(x))^2 - f(x) + x = 0.$$
et donc que
$$f(x) = \frac{1-\sqrt{1-4x}}{2}.$$

c) Vérifier que le nombre de tels arbres sur n noeuds est C_{n-1}.

4.3. Montrer que les suites $(a_1, a_2, \ldots, a_k)$ et $(b_1, b_2, \ldots, b_{k-1})$, définies en (4.21) caractérisent le polyomino parallélogramme sous-jacent. Suggestion : Étant donnés les a_i et b_i, résoudre les équations (4.21) en fonction des x_i et y_i en utilisant le fait que $x_1 = 0$ et $y_k = (n-k, k)$.

4.4. Montrer qu'on peut construire un unique chemin de Dyck, en ne spécifiant que la suite des distances entre les coins (extérieurs et intérieurs) du chemin et la diagonale $y = x$. Achever de montrer la Proposition 4.1 en appliquant ceci au cas où les distances en question sont données par $(a_1, a_2, \ldots, a_k)$, pour les coins extérieurs, et par $(b_1 - 1, b_2 - 1, \ldots, b_{k-1} - 1)$, pour les coins intérieurs.

Programmation mathématique

4.5. Utiliser l'identité (4.1) pour construire une procédure qui calcule tous les arbres binaires sur un ensemble A.

4.6. Construire une procédure qui calcule la profondeur $\pi(\alpha)$ (voir (4.4)) d'un arbre binaire α sur un ensemble A, et utiliser cette procédure pour calculer les premiers termes de la série **indicatrice de profondeur** :

$$\mathcal{B}_\pi(z) := \sum_{n=1}^{\infty} \sum_{\alpha \in \mathcal{B}[n]} t^{\pi(\alpha)} \, \frac{z^n}{n!}. \tag{4.23}$$

4.7. Utiliser l'identité (4.5) pour construire une procédure qui calcule tous les arbres binaires croissants sur un ensemble totalement ordonné A.

4.8. Construire une procédure qui calcule la profondeur d'un arbre binaire croissant sur un ensemble totalement ordonné A, et utiliser cette procédure pour calculer les premiers termes de la série indicatrice de profondeur $\mathsf{Abc}_\pi(z)$ (définie de façon analogue à (4.23).

4.9. Utiliser l'identité (4.10) pour construire une procédure qui calcule tous les arbres plans sur un ensemble A.

4.10. Construire une procédure qui calcule toutes les triangulations d'un polygone à n sommets. Chaque triangulation sera présentée sous la forme (4.12).

4.11. Construire une procédure qui transforme un arbre binaire en arbre plan, comme il est décrit à la Figure 4.7.

4.12. Construire une procédure qui génère toutes les fonctions de stationnement sur $[n]$, dont le type correspond à un chemin de Dyck donné (comme dans la discussion autour de la Figure4.14).

4.13. Construire une procédure qui génère toutes les polyominos parallélogrammes de périmètre $2\,n$.

Chapitre 5

Permutations et partitions

5.1 Introduction.

Parmi les problèmes typiques d'énumération, une situation que nous n'avons pas encore assez discutée concerne l'étude des structures ≪ non étiquetée ≫, ou encore construite avec des atomes qu'on ne peut pas ≪ distinguer ≫ les uns des autres. Encore une fois, nous avons là affaire à une notion pour l'instant assez floue. Tout ceci sera complètement clarifié au Chapitre 6, en considérant la notion de permutation des éléments d'un ensemble. C'est très certainement l'une des raisons pour lesquelles la notion de permutation est importante, mais c'est loin d'être la seule. En fait le groupe des permutations joue un rôle fondamental en combinatoire, comme dans de très nombreux autres domaines des mathématiques et de la physique.

5.2 Permutations

Rappelons qu'une **permutation** de A est simplement une bijection de A vers A, et qu'on dénote $\mathbb{S}[A]$ l'ensemble des permutations de A, c'est-à-dire

$$\mathbb{S}[A] := \{\sigma : A \xrightarrow{\sim} A \mid \sigma \text{ est une bijection}\}.$$

Un permutation σ de A (de cardinal n) est donc un ensemble de n couples :

$$\sigma = \{(x, \sigma(x)) \mid x \in A\}.$$

Nous allons aussi écrire $\mathbb{S}_A$ pour $\mathbb{S}[A]$, et $\mathbb{S}_n$ pour $\mathbb{S}[n]$. Le cardinal de $\mathbb{S}_A$ est $n!$, si A est de cardinal n.

Si A est muni d'un ordre linéaire fixé (voir Proposition 2.22), on peut identifier les permutations de A aux façons de « réordonner » les éléments de A. Ainsi, dans le cas $A = [n]$, en écrivant plus simplement σ_i pour $\sigma(i)$, on présente les permutations sous la forme

$$\sigma = \sigma_1\sigma_2\cdots\sigma_n.$$

Par exemple, on a l'ensemble des 24 permutations :

$$\begin{aligned}\mathbb{S}_4 = \{\ & 1234,\ 1243,\ 1324,\ 1342,\ 1423,\ 1432,\\ & 2134,\ 2143,\ 2314,\ 2341,\ 2413,\ 2431,\\ & 3124,\ 3142,\ 3214,\ 3241,\ 3412,\ 3421,\\ & 4123,\ 4132,\ 4213,\ 4231,\ 4312,\ 4321\ \}.\end{aligned}$$

De façon un peu plus imagée, on représente encore une permutation σ comme il est illustré à la Figure 5.1. Chacune de ses représentations permet de mettre en évidence des propriétés particulières.

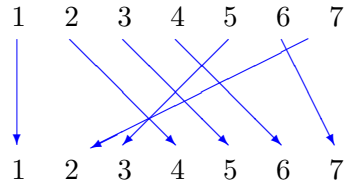


FIGURE 5.1 – Une permutation

Décomposition en cycles. Comme les permutations sont aussi des endofonction, on peut les présenter sous la forme de graphe orienté (graphe sagittal, voir Figure 5.2). Il devient alors naturel

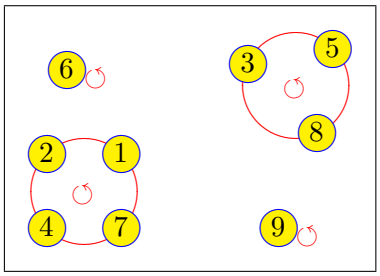


FIGURE 5.2 – La décomposition de la permutation 248736159 en cycles disjoints.

de les décomposer en composantes connexes. Plus précisément, une permutation de A (de cardinal n) est dite **cyclique** si en l'itérant (voir (2.63)) on peut passer de n'importe quel élément de A à

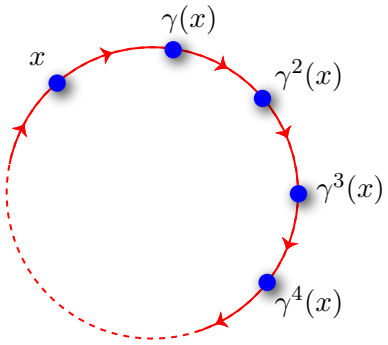


FIGURE 5.3 – Un cycle γ, contenant x.

n'importe quel autre. Plus techniquement, cela signifie que γ est cyclique si et seulement si, pour chaque x et y dans A, il existe $k \in \mathbb{N}$ tel que

$$\gamma^k(x) = y.$$

L'ensemble A peut alors s'écrire sous la forme

$$A = \{\gamma^i(x) \mid 0 \leq i \leq n-1\},$$

avec x un élément quelconque de A. Observons que $\gamma^n = \mathrm{Id}_A$. Cette situation est illustrée à la Figure 5.3, et il est courant, dans ce cas, d'utiliser une **notation cyclique** [1] :

$$\gamma = (x, \gamma(x), \gamma^2(x), \ \ldots \ , \gamma^{n-1}(x)), \tag{5.1}$$

avec la convention (Voir Exercice 5.2) que les deux suites

$$(x_1, x_2, \ \ldots \ , x_{n-1}, x_n) \quad \text{et} \quad (x_2, x_3, \ \ldots \ , x_n, x_1),$$

représente le même cycle. Ainsi, on a donc les écritures équivalentes

$$(1,3,2,4) = (3,2,4,1) = (2,4,1,3) = (4,1,3,2).$$

Dans le cas plus particulier où A est muni d'un ordre linéaire fixé, on peut convenir de présenter les cycles sous la forme (5.1), avec x égal au plus petit élément du cycle.

On désigne par $\mathcal{C}[A]$ l'ensemble des permutations cycliques de A, et (voir Exercice 5.1) il y a $(n-1)!$ permutations cycliques d'un ensemble à n éléments. Les 6 permutations cycliques de $[4]$ (sous forme de mot) forment l'ensemble $\mathcal{C}[4]$ $(= \mathcal{C}[[4]])$:

$$\mathcal{C}[4] = \{2341, 2413, 3421, 3142, 4312, 4123\}.$$

1. Notez l'utilisation de parenthèse et de virgules qui différencient cette notation de la notation sous forme de mot.

Le même ensemble, décrit en utilisant la notation cyclique, est :

$$\mathcal{C}[4] = \{(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2)\}.$$

Les composantes connexes d'une permutation σ, sont les « cycles » de σ. Plus précisément, à chaque σ on associe la partition $\mathcal{O}_\sigma$ de A, qui a comme parts les sous-ensembles

$$\sigma^*(x) := \{\sigma^k(x) \mid k \in \mathbb{N}\}. \tag{5.2}$$

On dit que $\sigma^*(x)$ est l'**orbite de** x selon σ. Pour $B = \sigma^*(x)$ (avec $x \in A$), la restriction $\sigma\big|_B$, de σ à B, est une permutation cyclique des éléments de B. On dit que $\sigma\big|_B$ est un **cycle** de σ. Toute permutation σ d'un ensemble A se décompose ainsi uniquement en cycles disjoints. L'ordre d'écriture des cycles n'ayant pas vraiment d'importance, on a que

$$\mathsf{Cycles}(\sigma) := \{\sigma\big|_B\}_{B\in\mathcal{O}_\sigma}. \tag{5.3}$$

est la **décomposition en cycles** de σ.

La liste, en ordre décroissant, des longueurs de chacun des cycles de $\mathsf{Cycles}(\sigma)$ est la **structure cyclique** (ou **forme**) de σ. On la dénote $\lambda(\sigma)$, et elle souvent écrite sous forme de mot [2]

$$\lambda(\sigma) = \mu_1\mu_2\cdots\mu_k, \tag{5.4}$$

avec les $\mu_i \in \mathbb{N}$, et $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_k > 0$. Il est clair que $n = \mu_1 + \mu_2 + \ \ldots\ + \mu_n$.

Pour l'exemple de la Figure 5.2, on a une permutation 248736159 dont la décomposition en cycles est

$$\sigma = 248736159 \quad \mapsto \quad \mathsf{Cycles}(\sigma) = \{(1,2,4,7),(3,5,8),(6),(9)\}.$$

Il s'ensuit que la structure cyclique de 248736159 est $\lambda(\sigma) = 4311$. Dans le cas $A = \{1,2,3\}$, on a les structures cycliques possibles :

$\lambda(\sigma)$	σ
111	123,
21	213, 132, 321,
3	231, 312.

2. Nous allons revenir plus en profondeur sur cette notion, à la Section 5.3.

Les décompositions en cycles correspondantes sont :

σ	$\mathsf{Cycles}(\sigma)$
123	$\{(1),(2),(3)\}$,
213	$\{(1,2),(3)\}$,
132	$\{(1),(2,3)\}$,
321	$\{(1,3),(2)\}$,
231	$\{(1,2,3)\}$,
312	$\{(1,3,2)\}$.

Utilisons la notation exponentielle pour la répétition de lettres dans les mots. La forme d'une permutation σ s'écrit alors sous la forme [3]

$$\lambda(\sigma) = 1^{d_1} 2^{d_2} \ \cdots \ n^{d_n}, \tag{5.5}$$

avec d_i égal au nombre de cycles de longueur i dans la décomposition cyclique de σ. Nous allons étudier cette notion plus en profondeur à la Section 5.3.

Énumeration selon le nombre de cycles. On désigne par $\mathbb{S}_k[A]$ l'ensemble des permutations de A qui sont composées de k cycles, c.-à-d. : $|\mathsf{Cycles}(\sigma)| = k$. Observons que

$$\mathbb{S}_n[A] = \{\mathrm{Id}_A\}, \tag{5.6}$$

si $n = |A|$. On a

$$\mathbb{S}_k[A] \xrightarrow{\sim} \sum_{P \in \mathsf{Part}_k[A]} \prod_{B \in P} \mathcal{C}[B]. \tag{5.7}$$

Pour A de cardinal n, le nombre d'éléments de $\mathbb{S}_k[A]$ est dénoté $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$. Ce sont les **nombres de Stirling de 1-ère sorte** (non signés [4]). Il découle immédiatement de cette définition que

$$\text{a)} \ \left[\begin{smallmatrix} n \\ n \end{smallmatrix}\right] = 1, \quad \text{pour tout } n \geq 0, \quad \text{et} \quad \text{b)} \ \left[\begin{smallmatrix} n \\ 0 \end{smallmatrix}\right] = 0, \quad \text{si} \quad n > 0, \tag{5.8}$$

D'autre part, puisque

$$\mathbb{S}[A] = \sum_{k=0}^{n} \mathbb{S}_k[A], \tag{5.9}$$

3. Encore une fois, il faut faire attention ici d'interpréter $4^2\,5^3$ comme le mot 44555, et non comme l'entier $16 \cdot 125 = 2000$.

4. Il existe dans la littérature une version avec un signe.

on a

$$n! = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}. \tag{5.10}$$

La Table 5.1 donne les petites valeurs de ces nombres. On donne à l'exercice 5.3 plusieurs formules

$n \setminus k$	1	2	3	4	5	6	7	8	9	10
1	1									
2	1	1								
3	2	3	1							
4	6	11	6	1						
5	24	50	35	10	1					
6	120	274	225	85	15	1				
7	720	1764	1624	735	175	21	1			
8	5040	13068	13132	6769	1960	322	28	1		
9	40320	109584	118124	67284	22449	4536	546	36	1	
10	62880	1026576	1172700	723680	269325	63273	9450	870	45	1

TABLE 5.1 – Les nombres de Stirling de 1-ère sorte : $\begin{bmatrix} n \\ k \end{bmatrix}$.

concernant ces nombres. Entre autres, on y montre une récurrence qui en permet le calcul. Celle-ci est basée sur l'identité suivante qui permet le calcul récursif de $\mathbb{S}_k[A]$, avec $A = B + \{x\}$:

$$\begin{aligned} \mathbb{S}_k[B + \{x\}] \;=\; & \{\sigma + \{(x,x)\} \mid \sigma \in \mathbb{S}_{k-1}[B]\} \\ & + \sum_{y \in A} \{(\sigma \setminus \{(y,z)\}) + \{(y,x),(x,z)\} \mid \sigma \in \mathbb{S}_k[B]\}, \end{aligned} \tag{5.11}$$

où $z = \sigma(y)$. Dans le premier du terme de droite, on ajoute un cycle de longueur un (envoyant x sur x). Dans le second, on insère x après y dans le cycle contenant y. Autrement dit, on remplace dans σ le couple (y,z) par les deux couples (y,x) et (x,z).

Dérangements. Un élément x de A est un **point fixe** de σ si et seulement si $\sigma(x) = x$. Dans la décomposition cyclique d'une permutation, un point fixe x donne un cycle de longueur 1, égal à (x). On désigne par $\mathrm{fix}(\sigma)$ l'ensemble des points fixes de σ.

Un **dérangement** est une permutation de A sans point fixe. C'est donc une permutation ayant tous ses cycles de longueur plus grande ou égale à deux. On désigne par $\mathrm{Der}[A]$ l'ensemble des

dérangements de A. Par exemple, l'ensemble $\mathsf{Der}[n]$ des dérangements de $[n]$, pour $n = 4$, contient 9 permutations :

$$\mathsf{Der}[4] = \{2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321\}.$$

Le cardinal de $d_n := \mathsf{Der}[n]$, prend les valeurs :

n	0	1	2	3	4	5	6	7	8	9	10	11	...
d_n	1	0	1	2	9	44	265	1854	14833	133496	1334961	14684570	...

La bijection naturelle suivante exploite le fait qu'en enlevant à une permutation ses points fixes, on obtient un dérangement.

$$\mathbb{S}[A] \xrightarrow{\sim} \sum_{B \in \mathcal{P}[A]} \mathsf{Der}[B]. \tag{5.12}$$

Elle associe donc à une permutation σ, le dérangement $\sigma\big|_B$ sur l'ensemble $B = A \setminus \mathsf{fix}(\sigma)$. L'identité suivante découle automatiquement de cette bijection.

$$n! = \sum_{k=0}^{n} \binom{n}{k} d_k, \tag{5.13}$$

avec (comme plus haut) d_k désignant le nombre de dérangements sur un ensemble de cardinal k. On peut alors utiliser l'exercice 5.4 pour déduire [5] la formule

$$d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \tag{5.14}$$

Une des conséquences souvent mentionnées de cette identité est que :

« *la probabilité d'obtenir un dérangement, lorsqu'on choisit une permutation de n éléments au hasard, tend vers e^{-1} lorsque n tend vers l'infini.* »

La proposition suivante permet de calculer effectivement les dérangements de A.

Proposition 5.1. *On a une la bijection naturelle (identifiant une permutation à sa décomposition en cycles)*

$$\begin{aligned} \mathsf{Der}[A + \{y\}] \quad = \quad & \sum_{x \in A} \Big\{ \sigma + \{(x,y),(y,x)\} \mid \sigma \in \mathsf{Der}[A \setminus \{x\}] \Big\} + \\ & \sum_{(x,z) \in \sigma} \Big\{ (\sigma \setminus \{(x,z)\}) + \{(x,y),(y,z)\} \mid \sigma \in \mathsf{Der}[A] \Big\}. \end{aligned} \tag{5.15}$$

5. On redémontrera ceci plus combinatoirement plus tard.

Autrement dit, pour le premier terme du membre de droite, on ajoute un nouveau cycle de longueur deux : $\{(x,y),(y,x)\}$, à un dérangement de $A\setminus\{x\}$; et, dans le second terme de membre de droite, on insère y entre x et son image $z=\sigma(x)$, dans un dérangement de A.

Il s'ensuit que

Corollaire 5.2. *On a les identités*

$$d_n = (n-1)(d_{n-2}+d_{n-1}), \quad \text{et} \tag{5.16}$$
$$d_n = n\,d_{n-1}+(-1)^n. \tag{5.17}$$

Transpositions. Une **transposition** τ sur A est une permutation qui laisse fixe tous les éléments de A sauf deux, disons x et y, pour lesquels on a

$$\tau(x)=y \quad \text{et} \quad \tau(y)=x. \tag{5.18}$$

Tous les cycles de σ ont donc longueur 1, sauf un qui est de longueur 2. Comme il suffit de choisir ces deux éléments parmi les n éléments de A, il y a $\binom{n}{2}$ transposition de A. Si $\mathcal{T}[A]$ dénote l'ensemble des transpositions sur A, on a donc une bijection naturelle

$$\mathcal{T}[A] \xrightarrow{\sim} \mathcal{P}_2[A]. \tag{5.19}$$

On dénote souvent (x,y) la transposition qui échange x et y. Bien entendu $(x,y)=(y,x)$. Lorsque A est totalement ordonné, on dit d'une transposition τ qu'elle est **adjacente**, si les deux éléments sont transposés, sont consécutifs dans l'ordre, c.-à-d. : y couvre x. Dans le cas $A=[n]$, avec l'ordre usuel, les transpositions adjacentes sont donc celles de la forme $(i,i+1)$, pour i allant de 1 à $n-1$. Il est coutume de dénoter s_i la transposition adjacente $(i,i+1)$:

$$s_i := (i,i+1). \tag{5.20}$$

Ainsi, pour $A=[6]$, on a les 5 transpositions adjacentes

$$(1,2)=213456, \quad (2,3)=132456, \quad (3,4)=124356,$$
$$(4,5)=123546, \quad (5,6)=123465.$$

Toutes les transpositions d'un ensemble A, de cardinal n, sont de même forme

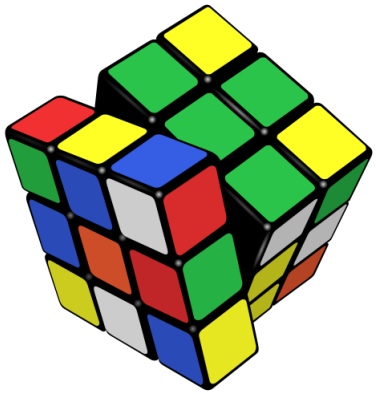
$$\lambda(\tau) = 2\underbrace{11\cdots 1}_{n-2 \text{ copies}}$$
$$= 2\,1^{n-2}.$$

Rappelons qu'en terme de mots, 1^k désigne le mot constitué de k copies de la lettre 1. Pour mieux approfondir la notion de transposition, on considère maintenant la notion de composition de permutations.

Structure de groupe. Rappelons que le composé de deux permutations de A, σ et τ, est aussi une permutation de A. De même, l'inverse d'une permutation de A, est une permutation de A L'ensemble $\mathbb{S}_A$ des permutations de A devient donc un groupe pour la composition, avec la permutation identité Id_A comme élément neutre. Il est courant d'utiliser une notation multiplicative, et on écrit $\sigma\,\tau$ pour le composé $\sigma \circ \tau$.
Dans $\mathbb{S}_A$, le **conjugué** d'une permutation σ, par une permutation θ, est la permutation $\theta\,\sigma\,\theta^{-1}$. La **conjugaison**, notée $\ll \sim \gg$, est la relation d'équivalence pour laquelle on a

$$\sigma \sim \tau, \quad \text{ssi} \quad (\exists\ \theta \in \mathbb{S}_A)\ \tau = \theta\,\sigma\,\theta^{-1}. \tag{5.21}$$

On vérifie directement (Voir Exercice 5.6) que c'est bien une relation d'équivalence, et on montre que



Cube de Rubik (1974),
$(2^{10}\,3^7\,8!\,12!)$ permutations.

Proposition 5.3. *Deux permutations sont conjuguées si et seulement si elles ont la même structure cyclique, c.-à-d. :* $\sigma \sim \tau$ ssi $\lambda(\sigma) = \lambda(\tau)$.

Preuve. Observons d'abord que l'image de $\theta(x)$ par

$$\begin{aligned} \tau^i &= (\theta\,\sigma\,\theta^{-1})^i, \\ &= \underbrace{(\theta\,\sigma\,\theta^{-1})\ (\theta\,\sigma\,\theta^{-1})\ \cdots\ (\theta\,\sigma\,\theta^{-1})}_{i \text{ times}}, \\ &= \theta\,\sigma^i\,\theta^{-1}. \end{aligned}$$

Pour tout i on a donc

$$\theta(\sigma^i(x)) = \tau^i(\theta(x)). \tag{5.22}$$

Il en résulte la correspondance suivante, entre les cycles de σ et ceux de τ :

$$(x,\ \ldots\ , \sigma^i(x),\ \ldots) \longleftrightarrow (\theta(x),\ \ldots\ , \theta(\sigma^i(x)),\ \ldots). \tag{5.23}$$

Cela donne une traduction claire entre la structure cyclique de σ et celle de τ.

Inversement, si σ et τ ont la même forme, on construit de la façon suivante une permutation θ telle que $\theta\sigma\theta^{-1} = \tau$. Les permutations ayant même forme, on peut ordonner [6] les cycles γ_i de σ, ainsi

6. Il y a plusieurs façons de faire

que les cycles ρ_i de τ, de façon à ce que la longueur de γ_i soit la même que celle de ρ_i. On choisit ensuite un élément x_i dans chaque cycle γ_i, et un élément y_i dans chaque cycle ρ_i. Puis on pose $\theta(x_i) := y_i$. Comme on l'a vu en (5.22), la relation $\tau = \theta\sigma\theta^{-1}$ si et seulement si $\tau^i\theta = \theta\sigma^i$ pour tout i. Pour avoir la relation désirée, on doit forcément étendre θ au reste du cycle γ_i (pour chaque i) en posant

$$\begin{array}{cccc} (x_i, & \sigma(x_i), & \sigma^2(x_i), & \dots \;) \\ \downarrow & \downarrow & \downarrow & \dots \\ (y_i, & \tau(y_i), & \tau^2(y_i), & \dots \;) \end{array}$$

Ceci définit entièrement θ, et par construction on a la relation désirée. ■

Une **involution** σ sur A est une permutation qui est sont propre inverse, c.-à-d. : $\sigma^{-1} = \sigma$. Autrement dit, σ est une involution si et seulement si $\sigma^2 = \mathrm{Id}$. Il s'ensuit que, pour tout x et y dans A, on a

$$y = \sigma(x) \quad \text{ssi} \quad \sigma(y) = x.$$

Les cycles de la décomposition cyclique correspondant aux involutions sont donc forcément, soit de longueur 1, soit de longueur 2. La forme d'une involution σ est donc

$$\lambda(\sigma) = 2^k\, 1^{n-2\,k}, \qquad \text{avec} \qquad 0 \le k \le n/2. \tag{5.24}$$

En fait, σ est une involution si et seulement si c'est une permutation de forme (5.24). On dénote $\mathsf{Inv}[A]$ l'ensemble des involutions sur A.

En particulier, les transpositions sont toutes des involutions, et les transpositions adjacentes $s_i = (i, i+1)$ satisfont les **relations de Coxeter** :

$$\begin{array}{lrcll} 1) & s_i^2 & = & \mathrm{Id}, & \\ 2) & s_i\, s_j & = & s_j, s_i, & \text{si } |j-i| \ge 2, \\ 3) & s_i\, s_{i+1}\, s_i & = & s_{i+1}\, s_i\, s_{i+1}. & \end{array} \tag{5.25}$$

De plus, toutes les transpositions sont conjuguées deux à deux.

Inversions d'une permutation de $[n]$. Dans le cas où A est totalement ordonné, on dit qu'un couple (x, y) (dans $A \times A$) forme une **inversion** de la permutation σ, si

$$x < y \quad \text{et} \quad \sigma(x) > \sigma(y). \tag{5.26}$$

Soulignons que les inversions de σ correspondent aux croisements des segments dans la figure 5.1. Il s'ensuit qu'on a la proposition suivante, où on dénote $\mathrm{Inv}(\sigma)$ l'ensemble des inversions de σ, et

$\ell(\sigma)$ son cardinal, c.-à-d. : son **nombre d'inversions**. On a la distribution suivante pour la nombre d'inversions des permutations de $A = [4]$:

$\ell(\sigma)$	σ
0	1234,
1	1243, 1324, 2134,
2	1342, 1423, 2143, 2314, 3124,
3	1432, 2341, 2413, 3142, 3214, 4123,
4	2431, 3241, 3412, 4132, 4213
5	3421, 4231, 4312
6	4321.

Pour la suite de notre discussion, nous allons supposer que $A = [n]$.

Polynôme énumérateur d'inversions. Pour énumérer les permutations de $[n]$ selon leur nombre d'inversions, nous allons utiliser une jolie technique de la combinatoire énumérative. L'idée, qui remonte à Euler, est de coder l'information sur la distribution de la « statistique », $\ell(\sigma)$, sous une forme algébrique qui facilite le calcul. Plus précisément, on pose

$$\mathsf{Inv}_n(q) := \sum_{\sigma \in \mathbb{S}[n]} q^{\ell(\sigma)}. \tag{5.27}$$

C'est le **polynôme énumérateur** pour les inversions des permutations de $[n]$. Bien entendu, on a

$$\mathsf{Inv}_n(1) = \sum_{\sigma} 1 = n! \tag{5.28}$$

Pour les petites valeurs de n, ces polynômes sont :

$$\begin{aligned}
\mathsf{Inv}_1(q) &= 1 \\
\mathsf{Inv}_2(q) &= q + 1 \\
\mathsf{Inv}_3(q) &= q^3 + 2\,q^2 + 2\,q + 1 \\
\mathsf{Inv}_4(q) &= q^6 + 3\,q^5 + 5\,q^4 + 6\,q^3 + 5\,q^2 + 3\,q + 1 \\
\mathsf{Inv}_5(q) &= q^{10} + 4\,q^9 + 9\,q^8 + 15\,q^7 + 20\,q^6 + 22\,q^5 + 20\,q^4 + 15\,q^3 + 9\,q^2 + 4\,q + 1
\end{aligned}$$

La Figure 5.4 donne la distribution de probabilités [7] pour le nombre d'inversions des permutations de [12].

7. Nombre de permutations ayant k inversions divisé par $n!$.

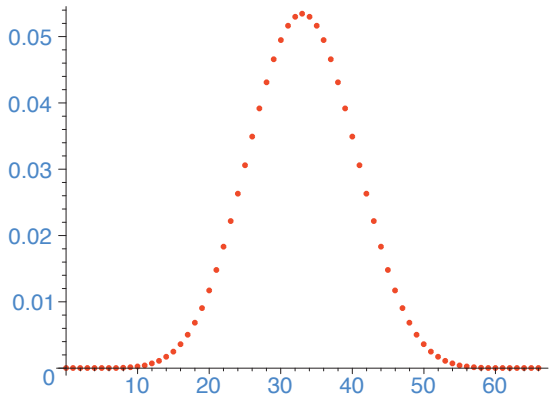


FIGURE 5.4 – Distribution des inversions.

Il y a en fait une formule très simple pour $\mathsf{Inv}_n(q)$. En effet, dans une permutation $\sigma = \sigma_1\,\sigma_2\,\cdots\,\sigma_n$ la valeur n apparaît en une certaine position i, et on a

$$\sigma = \sigma_1\,\sigma_2\,\cdots\,\sigma_{i-1}\;n\;\sigma_{i+1}\,\cdots\,\sigma_n. \tag{5.29}$$

Chaque valeur à droite de n (il y en a $n-i$) cause une inversion avec n, et ce sont les seules inversions impliquant n. Si τ désigne la permutation

$$\tau = \sigma_1\,\sigma_2\,\cdots\,\sigma_{i-1}\,\sigma_{i+1}\,\cdots\,\sigma_n$$

des nombres de 1 à $n-1$. On a donc

$$\ell(\sigma) = \begin{cases} (n-i) + \ell(\tau), & \text{si } n > 1, \\ 0, & \text{si } n \leq 1, \end{cases} \tag{5.30}$$

Inversement, pour chaque permutation τ de $[n-1]$, il y a n permutations distinctes obtenues en insérant n dans $\tau = \tau_1\,\tau_2\,\cdots\,\tau_{n-1}$

$$\begin{array}{c} \tau_1\,\tau_2\,\cdots\,\tau_i\quad\tau_{i+1}\,\cdots\,\tau_{n-1}, \\ \uparrow \\ n \end{array}$$

une pour chaque position i entre 0 à $n-1$, en convenant que position $i=0$ correspond à ajouter n en tête de la permutation. La récurrence (5.30) caractérise donc complètement $\ell(\sigma)$. Il en découle que

$$\mathsf{Inv}_n(q) = (q^{n-1} + \ldots + q + 1)\,\mathsf{Inv}_{n-1}(q). \tag{5.31}$$

Puisque

$$\begin{aligned}
\mathsf{Inv}_n(q) &= \sum_{\sigma\in\mathbb{S}[n]} q^{\ell(\sigma)} \\
&= \sum_{\tau\in\mathbb{S}[n-1]} \sum_{i=0}^{n} q^{(n-i)+\ell(\tau)} \\
&= (q^{n-1}+\ldots+q+1) \sum_{\sigma\in\mathbb{S}[n]} q^{\ell(\tau)} \\
&= (q^{n-1}+\ldots+q+1)\,\mathsf{Inv}_{n-1}(q).
\end{aligned}$$

Il s'ensuit que

Proposition 5.4. *Pour tout $n>0$, le polynôme énumérateur d'inversions est donné par la formule*

$$\mathsf{Inv}_n(q) = \prod_{k=1}^{n-1}(q^k+\ldots+q+1) \tag{5.32}$$

$$= \prod_{k=1}^{n}\frac{q^k-1}{q-1}. \tag{5.33}$$

Le nombre d'inversions d'une permutation apparaît naturellement en liaison avec l'étude de la décomposition d'une permutation en produit de transpositions adjacentes. Pour le voir, on peut procéder comme suit. Étant donné une permutation $\sigma = \sigma_1\,\sigma_2\cdots\sigma_n$ dans $\mathbb{S}[n]$, on considère l'opération qui consiste à déplacer vers la droite la plus grande valeur qui cause une inversion. Par exemple, si on a n en position $i<n$ (c.-à-d. : $\sigma_i = n$), on procède à la transformation

$$\sigma_1\ \cdots\ \sigma_{i-1}\ n\ \sigma_{i+1}\ \cdots\ \sigma_n \qquad \mapsto \qquad \sigma_1\ \cdots\ \sigma_{i-1}\ \sigma_{i+1}\ n\ \cdots\ \sigma_n.$$

qui consiste à échanger n et σ_{i+1}. La permutation résultante, appelons-la τ, a une inversion de moins, et on a $\tau = \sigma\, s_i$, ce qui est équivalent à

$$\sigma = \tau\, s_i. \tag{5.34}$$

Par récurrence, on en déduit la proposition suivante.

Proposition 5.5. *Toute permutation s'exprime comme produit de transpositions adjacentes*[8]*. Le nombre minimal*[9] *de transpositions adjacentes nécessaires est exactement $\ell(\sigma)$.*

8. En général de plusieurs façons différentes.
9. Le nombre de façons, d'exprimer une permutation σ comme produit de $\ell(\sigma)$ transpositions, est difficile à calculer.

Le **signe** $\varepsilon(\sigma)$ d'une permutation σ est

$$\varepsilon(\sigma) := (-1)^{\ell(\sigma)}. \tag{5.35}$$

Une des propriétés fondamentales du signe est que

$$\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau). \tag{5.36}$$

5.3 Partages

La forme des permutations et des partitions fait intervenir la notion de partage au sens suivant. Nous allons en étudier les propriétés plus en détail. Un **partage** d'un entier $n > 0$ est une liste décroissante d'entiers positifs (> 0) dont la somme donne n. Ainsi, $(7, 7, 4, 4, 4, 2, 1, 1)$ (aussi dénoté 77444211) est un partage de

$$30 = 7 + 7 + 4 + 4 + 4 + 2 + 1 + 1.$$

Par convention, l'entier 0 admet le partage **vide** qu'on dénote 0. Un partage

$$\mu = (\mu_1, \mu_2, \ldots, \mu_k), \qquad \text{ou plus simplement} \qquad \mu = \mu_1\, \mu_2 \ldots \mu_k,$$

de $n > 0$, est donc tel que

1. $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_k > 0$,
2. $n = \mu_1 + \mu_2 + \ldots + \mu_k$.

On dénote $\mu \vdash n$ le fait que μ soit un partage de n. Les entiers μ_i, $1 \leq i \leq k$, sont les **parts** de μ, et k est la **longueur** (dénotée $\ell(\mu)$) du partage μ.

On désigne par $\Lambda[n]$ l'ensemble des partages de n, et on a

$$\begin{aligned}
\Lambda[0] &= \{0\} \\
\Lambda[1] &= \{1\} \\
\Lambda[2] &= \{2, 11\} \\
\Lambda[3] &= \{3, 21, 111\} \\
\Lambda[4] &= \{4, 31, 22, 211, 1111\} \\
\Lambda[5] &= \{5, 41, 32, 311, 221, 2111, 11111\} \\
\Lambda[6] &= \{6, 51, 42, 411, 33, 321, 3111, 222, 2211, 21111, 111111\} \\
&\vdots
\end{aligned}$$

On dénote $p(n)$ le nombre de partages de n. Les premières valeurs des $p(n)$ sont

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$p(n)$	1	1	2	3	5	7	11	15	22	30	42	56	77	101	...

On calcule récursivement l'ensemble $\Lambda_{\leq k}[n]$, des partages de n en parts plus petites ou égales à k, au moyen de l'identité

$$\Lambda_{\leq k}[n] = \sum_{j=1}^{\min(k,n)} \{(j, \mu_1, \ \dots \ , \mu_r) \mid (\mu_1, \ \dots \ , \mu_r) \in \Lambda_{\leq j}[n-j]\}, \tag{5.37}$$

avec la condition initiale :

$$\Lambda_{\leq k}[0] = \{0\}. \tag{5.38}$$

La **forme** $\lambda(P)$, d'une partition P d'un ensemble à n éléments, est la liste (décroissante) de la taille de ses parts. C'est un partage de n. On justifie cette terminologie de « forme » par les deux propositions suivantes.

Proposition 5.6. *Deux partitions P et P' d'un ensemble A ont même forme, c.-à-d. : $\lambda(P) = \lambda(P')$, si et seulement si il existe une bijection $f : A \xrightarrow{\sim} A$, telle que*

$$\rho = \{f^+(B) \mid B \in \pi\}.$$

Preuve. Clairement, s'il y a une bijection telle que $\rho = \{f^+(B) \mid B \in \pi\}$, alors la liste des tailles des parts de π est la même que celle de ρ.

Inversement, si π est ρ ont même forme, on peut ordonner les parts B_i de π, et C_i de ρ, de façon à ce que $|B|_i = |C|_i$. Il existe alors donc des bijections $f_i : B_i \xrightarrow{\sim} C_i$, qu'on peut « recoller » en une bijection globale $f : A \xrightarrow{\sim} A$ telle que la restriction de f à B_i soit f_i. ■

La classification des classes de conjugaison de permutations, ou celle des types de partitions se ramènent donc à l'étude des partages.

5.4 Diagrammes de Ferrers

On représente souvent un partage par son **diagramme de Ferrers** [10] défini ci-dessous. On introduit d'abord la notion plus générale de **diagramme**, qui est tout simplement un sous ensemble fini D de $\mathbb{N} \times \mathbb{N}$. Les éléments de D, sont les **cases** du diagramme. Ainsi, le diagramme

$$\{(0,0), (2,0), (2,1), (1,3), (0,2), (0,3), (3,1)\}$$

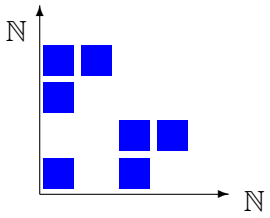
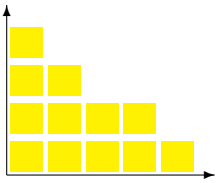


FIGURE 5.5 – Un diagramme.

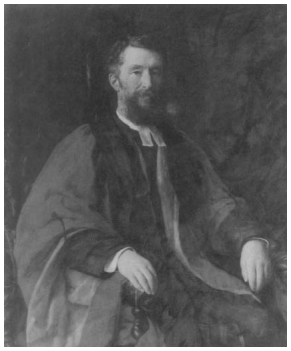
corresponds à l'illustration de la Figure 5.5. On fait d'un diagramme D un ensemble ordonné en considérant la relation d'ordre **composante à composante** sur les cases, c.-à-d. :

$$(x_1, y_1) \leq (x_2, y_2) \quad \text{ssi} \quad (x_1 \leq x_2 \quad \text{et} \quad y_1 \leq y_2). \tag{5.39}$$

C'est donc la restriction à D de l'ordre $\mathbb{N} \times \mathbb{N}$ considéré comme carré cartésien de l'ensemble ordonné $\mathbb{N}$, avec l'ordre usuel. Un diagramme D est dit **de Ferrers** s'il est en forme d'escalier, comme suit :



Autrement dit, si $(i, j) \in D$ alors chaque case (x, y), avec $x \leq i$ et $y \leq j$, est aussi dans D. Une **ligne** d'un diagramme de Ferrers est l'ensemble des cases qui ont même seconde coordonnée.



N. M. Ferrers
(1829–1903)

Tout naturellement, la **longueur** d'une ligne est le nombre de cases de celle-ci. La liste des longueurs des lignes d'un diagramme de Ferrers, ordonnée du bas vers le haut, est clairement décroissante. C'est donc un partage. On établit ainsi une correspondance entre partages et diagrammes de Ferrers. Le diagramme de la Figure ci-haut correspond au partage 5421 de l'entier 12. Plus généralement, au partage $\mu = \mu_1 \cdots \mu_k$ correspond le diagramme de Ferrers (aussi dénoté μ)

$$\mu := \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid 0 \leq y \leq k - 1, \quad \text{et} \quad 0 \leq x \leq \mu_y - 1\}. \tag{5.40}$$

Bien entendu, une **colonne** du diagramme de Ferrers μ est l'ensemble des cases qui ont même première coordonnée, et sa **hauteur** est le nombre de ces cases.

La liste des hauteurs des colonnes d'un diagramme de Ferrers à n cases, ordonnées de gauche à droite, est aussi un partage de n qui est dénoté μ'. C'est le **conjugué** de μ. Le diagramme de μ' est obtenu de celui de μ par réflexion par rapport à la diagonale $y = x$. C'est donc l'ensemble

$$\mu' := \{(y, x) \mid (x, y) \in \mu\}. \tag{5.41}$$

10. Nommés ainsi en l'honneur de Norman Macleod Ferrers (1829-1903).

La Figure 5.6 donne le diagramme de Ferrers du conjugé du partage 5421. Le conjugé de $\mu = 5421$

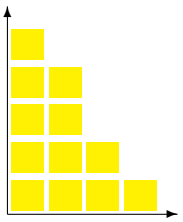


FIGURE 5.6 – Le conjugé du partage 5421.

est donc $\mu' = 43221$.

Si le partage μ contient d_i parts de **taille** i, on écrit encore

$$\mu = 1^{d_1} 2^{d_2} \cdots m^{d_m}.$$

C'est le partage décrit sous forme de mot. On dit alors que d_i est la **multiplicité** de la part i dans μ. Pour notre exemple courant, on a $\mu = 1^1 2^1 4^1 5^1$ et $\mu' = 1^1 2^2 3^1 4^1$.

5.5 Énumération de partages

Il est naturel de considérer le problème de l'énumération des partages d'entiers dans le contexte plus général de l'énumération de partages avec restrictions. Ces restrictions peuvent être sur la taille des parts, ou sur le nombre de parts d'une certaine taille.

Plus précisément, soit K un sous-ensemble de $\mathbb{N}^+$ (l'ensemble des entiers positifs > 0). Pour chaque n, on considère l'ensemble $\Lambda_K[n]$ des partages de n dont toutes les parts sont dans K. Par exemple, si on choisit K égal au sous-ensemble des entiers impairs :

$$I := \{2\,k + 1 \mid k \in \mathbb{N}\},$$

on a alors

$$\begin{aligned}
\Lambda_I[1] &= \{1\} \\
\Lambda_I[2] &= \{11\} \\
\Lambda_I[3] &= \{3, 111\} \\
\Lambda_I[4] &= \{31, 1111\} \\
\Lambda_I[5] &= \{5, 311, 11111\} \\
\Lambda_I[6] &= \{51, 33, 3111, 111111\} \\
&\vdots
\end{aligned}$$

Le cardinal de $\Lambda_K[n]$ est dénoté $p_K(n)$, et simplement p_n dans le cas $K = \mathbb{N}^+$. On considère aussi souvent l'ensemble $\Lambda_{K;\neq}[n]$ des partages de n en parts dans K, avec au plus une part de de chaque taille (c.-à-d. : des parts distinctes). On note alors $p_{K;\neq}(n)$ le nombre d'éléments de cet ensemble. Dans le cas où $K = \mathbb{N}^+$, on écrit simplement $\Lambda_{\neq}[n]$ et $p_{\neq}[n]$.

A chacune de ces familles de partages, on associe une série génératrice qui contient toute l'information concernant l'énumération des partages de la famille. Ces séries sont respectivement

$$\Lambda(z) := \sum_{n=0}^{\infty} p(n) z^n, \qquad \text{(tous les partages)}, \tag{5.42}$$

$$\Lambda_K(z) := \sum_{n=0}^{\infty} p_K(n) z^n, \qquad \text{(parts dans } K\text{)}, \tag{5.43}$$

$$\Lambda_{\neq}(z) := \sum_{n=0}^{\infty} p_{\neq}(n) z^n, \qquad \text{(parts distinctes)}, \tag{5.44}$$

$$\Lambda_{K;\neq}(z) := \sum_{n=0}^{\infty} p_{K;\neq}(n) z^n, \qquad \text{(parts distinctes dans } K\text{)}. \tag{5.45}$$

Les formules suivantes pour les séries génératrices des partages avec parts dans K, avec ou sans répétitions possibles, ont été trouvées il y a déjà longtemps par Euler.

Théorème 5.7 (Euler). *Pour $K \subseteq \mathbb{N}^+$, on a les fonctions génératrices*

$$\Lambda_K(z) = \prod_{k \in K} \frac{1}{1 - z^k}, \tag{5.46}$$

et

$$\Lambda_{K;\neq}(z) = \prod_{k \in K} (1 + z^k). \tag{5.47}$$

Preuve. Soit $K = \{k_1, k_2, \ldots\}$ alors

$$\begin{aligned} \prod_{k \in K} \frac{1}{1 - z^k} &= (1 + z^{k_1} + z^{2k_1} + \ldots) \cdot (1 + z^{k_2} + z^{2k_2} + \ldots) \cdots \\ &= \sum_{\sum n_i < \infty} z^{n_1 k_1} \, z^{n_2 k_2} \ldots \\ &= \sum_{n \geq 0} p_K(n) \, z^n \end{aligned}$$

Ici les $x^{n_i k_i}$ signifie qu'on a pris n_i fois une part de taille k_i. On montre la seconde formule de façon similaire. Dans le développement du produit $\prod_{k \in K}(1 + z^k)$, on prend z^k dans le facteur $1 + z^k$ si

la part k apparaît dans le partage, sinon on prend le 1. On a donc au plus une part de chacune des tailles apparaissant dans K. ■

Exemples classiques. En comparant l'énumération des partages en parts impaires et l'énumération des partages en parts distinctes, on constate que, pour les premières valeurs, on a $p_I(n) = p_{\neq}(n)$:

$$\begin{array}{lcl} \Lambda_{\neq}[1] & = & \{1\} \\ \Lambda_{\neq}[2] & = & \{2\} \\ \Lambda_{\neq}[3] & = & \{3, 21\} \\ \Lambda_{\neq}[4] & = & \{4, 31\} \\ \Lambda_{\neq}[5] & = & \{5, 41, 32\} \\ \Lambda_{\neq}[6] & = & \{6, 51, 42, 321\} \\ \vdots & & \end{array} \qquad \begin{array}{lcl} \Lambda_{I}[1] & = & \{1\} \\ \Lambda_{I}[2] & = & \{11\} \\ \Lambda_{I}[3] & = & \{3, 111\} \\ \Lambda_{I}[4] & = & \{31, 1111\} \\ \Lambda_{I}[5] & = & \{5, 311, 11111\} \\ \Lambda_{I}[6] & = & \{51, 33, 3111, 111111\} \\ \vdots & & \end{array}$$

Ceci peut se démontre par le calcul formel suivant sur les séries génératrices.

$$\begin{aligned} \sum_{n\geq 0} p_{\neq}(n)\, z^n &= (1+z)\,(1+z^2)\,(1+z^3)\cdots \\ &= \left(\frac{1-z^2}{1-z}\right)\cdot\left(\frac{1-z^4}{1-z^2}\right)\cdot\left(\frac{1-z^6}{1-z^3}\right)\cdots \\ &= \frac{(1-z^2)\cdot(1-z^4)\cdot(1-z^6)\cdots}{(1-z)\cdot(1-z^2)\cdot(1-z^3)\cdots} \\ &= \frac{1}{(1-z)}\,\frac{1}{(1-z^3)}\,\frac{1}{(1-z^5)}\cdots \\ &= \sum_{n\geq 0} p_I(n)\, z^n \end{aligned}$$

On peut aussi montrer ce fait en exhibant une bijection φ entre l'ensemble $\Lambda_I[n]$ des partages de n en parts impaires et l'ensemble $\Lambda_{\neq}[n]$ des partages de n en parts distinctes. Rappelons que chaque entier m s'écrit de façon unique en base 2 comme

$$m = \sum \varepsilon_i\, 2^i$$

où les ε_i sont égaux à 0 ou 1, avec $\{i \mid \varepsilon_i = 1\}$ fini. Pour un partage μ en parts impaires, supposons que la part i apparaît n_i fois et écrivons n_i en base 2 :

$$n_i = \varepsilon_{i0} + \varepsilon_{i1}\, 2 + \ldots + \varepsilon_{ij}\, 2^i + \ldots$$

On associe ainsi une « table » $(\varepsilon_{ij})_{i,j}$ au partage μ, et on a

$$\begin{aligned} n &= \sum_i i\, n_i \\ &= \sum_{i,j} \varepsilon_{ij}\, i\, 2^j. \end{aligned}$$

Le partage $\varphi(\mu)$ est simplement constitué des parts $i\,2^j$, pour lesquelles $\varepsilon_{ij} \neq 0$. Ces parts sont bien deux à deux distinctes puisque les parts i de μ sont impaires, et l'écriture d'un nombre sous la forme $(2\,k+1)\,2^m$ est unique. Par exemple, cette bijection transforme le partage

$$\mu = (7,7,7,5,5,3,3,3,3,3), \qquad \text{en} \qquad \varphi(\mu) = (14,12,10,7,3).$$

Une autre proposition de ce type est la suivante.

Proposition 5.8. *Le nombre de partages de n en au plus k parts est égal au nombre de partages de n en parts de taille inférieure ou égale à k. La série génératrice correspondante est donc*

$$\Lambda_{\leq k}(z) = \prod_{m=1}^{k} \frac{1}{1-z^m}. \tag{5.48}$$

Preuve. Pour μ un partage de n en au plus k parts, la plus grande part de μ', le conjugué de μ, est clairement de taille inférieure ou égale à k. Le passage au conjugué établit donc une bijection entre les ensembles considérés. ■

On a les développements suivants pour diverses séries considérées jusqu'ici :

$$\begin{aligned}
\Lambda(z) &= 1 + z + 2\,z^2 + 3\,z^3 + 5\,z^4 + 7\,z^5 + 11\,z^6 + 15\,z^7 + 22\,z^8 + 30\,z^9 + 42\,z^{10} + \dots && (5.49)\\
\Lambda_{\neq}(z) &= \Lambda_I = 1 + z + z^2 + 2\,z^3 + 2\,z^4 + 3\,z^5 + 4\,z^6 + 5\,z^7 + 6\,z^8 + 8\,z^9 + 10\,z^{10} + \dots && (5.50)\\
\Lambda_{\leq 2}(z) &= 1 + z + 2\,z^2 + 2\,z^3 + 3\,z^4 + 3\,z^5 + 4\,z^6 + 4\,z^7 + 5\,z^8 + 5\,z^9 + 6\,z^{10} + \dots && (5.51)\\
\Lambda_{\leq 3}(z) &= 1 + z + 2\,z^2 + 3\,z^3 + 4\,z^4 + 5\,z^5 + 7\,z^6 + 8\,z^7 + 10\,z^8 + 12\,z^9 + 14\,z^{10} + \dots && (5.52)
\end{aligned}$$

5.6 Théorème pentagonal d'Euler

Euler (encore lui !) a donné une formule qui permet, entre autres, de calculer efficacement le nombre de partages. Pour pouvoir énoncer cette formule, on doit d'abord introduire la notion de nombres **pentagonaux**. à cette fin, rappelons d'abord la propriété bien connue des nombres carrés :

$$n^2 = 1 + 3 + 5 + \dots + (2\,n-1),$$

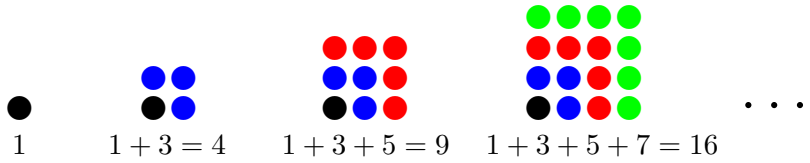


FIGURE 5.7 – Nombres carrés.

dont la véracité découle de l'illustration à la Figure 5.7.

Par analogie, on convient d'appeler **pentagonaux** les nombres

$$\omega(k) := \frac{k(3k-1)}{2}, \tag{5.53}$$

en raison du fait qu'ils apparaissent comme nombre de points dans un pentagone, comme l'illustre la Figure 5.8.

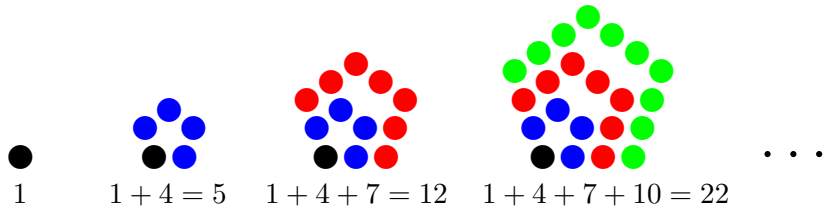


FIGURE 5.8 – Nombres pentagonaux.

On étend la définition de nombres pentagonaux au cas $k < 0$ en utilisant la formule ci-haut :

k	1	2	3	4	5	6	7	8
$\omega(k)$	1	5	12	22	35	51	70	92
$\omega(-k)$	2	7	15	26	40	57	77	100

Observons que

$$\omega(-k) = \frac{k(3k+1)}{2}. \tag{5.54}$$

Le théorème d'Euler s'exprime alors comme suit

Théorème 5.9 (Pentagonal d'Euler). *Soit* $\Lambda(z) = \sum_{n\geq 0} p(n)\, z^n = \prod_{m\geq 1} \frac{1}{1-z^m}$ *alors :*

$$\Lambda(z)^{-1} = \prod_{m\geq 1} (1-z^m) = 1 + \sum_{k\geq 1} (-1)^k \left(z^{\omega(k)} + z^{\omega(-k)}\right). \tag{5.55}$$

Avant de passer à une élégante démonstration de ce théorème, considérons en la conséquence suivante de (5.55), montrant comment calculer récursivement $p(n)$.

$$p(n) = \sum_{k\geq 1} (-1)^{k+1} \left(p(n-\omega(k)) + p(n-\omega(-k))\right). \tag{5.56}$$

Plus explicitement, on a :

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - p(n-22) - p(n-26) \dots$$

L'avantage de cette récurrence pour calculer les nombres $p(n)$est que le nombre de termes apparaissant dans le membre de droite de l'égalité est relativement petit (de l'ordre de la racine carrée de n).

En guise de préparation à la preuve, on adapte d'abord la formule (5.55), en ajoutant une variable y qui **marque** le nombre de parts, pour obtenir les formules suivantes

$$\sum_{n\geq 0} \left(\sum_{k=0}^{n} p_k(n)\, y^k \right) z^n \;=\; \prod_{m\geq 1} \frac{1}{1-y\, z^m} \tag{5.57}$$

$$\sum_{n\geq 0} \left(\sum_{k=0}^{n} p_{k;\neq}(n)\, y^k \right) z^n \;=\; \prod_{m\geq 1} (1+y\, z^m), \tag{5.58}$$

où $p_k(n)$ désigne le nombre de partages de n en k parts, et $p_{k;\neq}(n)$ le nombre de partages de n en k parts distinctes.

Preuve du théorème pentagonal. Soient $p^+_{\neq}(n)$ (resp. $p^-_{\neq}(n)$) le nombre de partages de n en un nombre pair (resp. impair) de parts distinctes et soient $\Lambda^+_{\neq}[n]$ et $\Lambda^-_{\neq}[n]$ les ensembles de partages correspondants. Bien sûr $p_{\neq}(n) = p^+_{\neq}(n) + p^-_{\neq}(n)$ et l'on a :

$$\Lambda(z)^{-1} = \prod_{m\geq 1} (1+(-1)\, z^m) = \sum_{n\geq 0} \sum_{k=0}^{n} (-1)^k\, p_{k;\neq}(n)\, z^n = \sum_{n\geq 0} (p^+_{\neq}(n) - p^-_{\neq}(n))\, z^n.$$

Nous allons voir que, pour presque toutes les valeurs de n, il y a une bijection entre $\Lambda^+_{\neq}[n]$ et $\Lambda^-_{\neq}[n]$. En fait, il y a bijection lorsque n n'est pas de la forme $\omega(k)$. Dans le cas où $n = \omega(k)$, il y a aussi presque une bijection entre $\Lambda^+_{\neq}[n]$ et $\Lambda^-_{\neq}[n]$, un seul partage posant problème.

Plus explicitement soit $\mu \in \Lambda^+_{\neq}[n]$. Pour les besoins de la preuve, traçons le diagramme de Ferrers de μ avec des points. Notons $\min(\mu)$ la plus petite part de μ. D'autre part, soit $d = d(\mu)$ le plus grand entier tel que $\mu_j = \mu_1 - j + 1$ pour chaque $j \leq d$. On appelle **diagonale** de μ l'ensemble des derniers points de chacune des lignes de μ_1 jusqu'à μ_d.

La bijection (sauf exception) procède en déplaçant certains points de la façon suivante.

1. Si $\min(\mu) \leq d(\mu)$, on déplace les points de la plus petite part pour les ajouter le long de la diagonale.
2. Si $\min(\mu) > d(\mu)$, on déplace les points de la diagonale pour les ajouter au-dessus de la plus petite part.

La figure 5.9 illustre cette bijection. On fait ici correspondre au partage

$$\mu = (8, 7, 6, 4, 3, 2)$$

dans $\Lambda^+_{\neq}(30)$, le partage $\mu = (9, 8, 6, 4, 3)$ dans $\Lambda^-_{\neq}(30)$. Cette bijection (sur son ensemble de

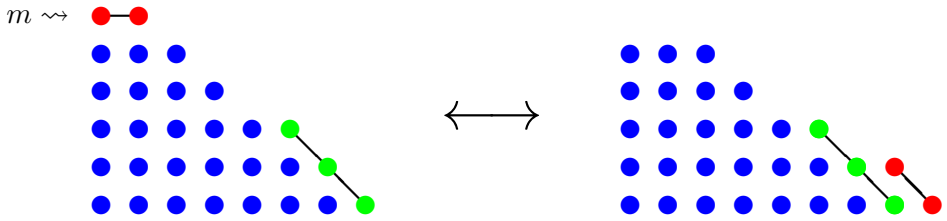


FIGURE 5.9 – Bijection.

définitions) est son propre inverse.

Le résultat de cette construction donne un partage en parts distinctes dans tous les cas, sauf lorsque la diagonale de μ partage un point avec la plus petite part et que cette part est de taille égale (ou un de plus) au nombre de parts. Ces exceptions sont donc de la forme

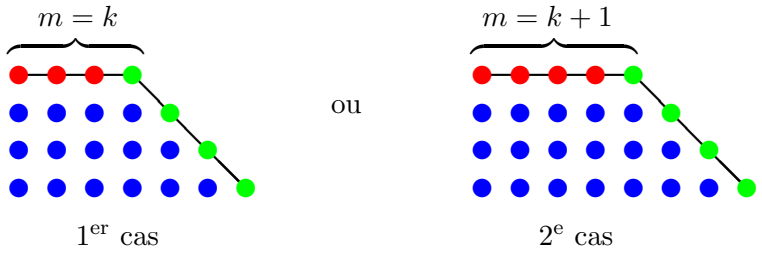


FIGURE 5.10 – Exceptions.

avec k égal au nombre de parts. Dans le premier cas, il y a

$$n = k + (k + 1) + \ldots + (2\,k - 1) = \omega(k)$$

points, et dans le second, il y en a

$$n = (k + 1) + (k + 2) + \ldots + 2\,k = \omega(-k).$$

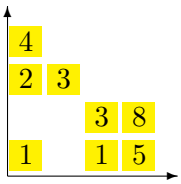
On a donc en général $p^+_{\neq}(n) - p^-_{\neq}(n) = 0$ sauf si $n = \omega(k)$ ou $n = \omega(-k)$. Dans ce cas, il y a un et un seul partage de n pour lequel on ne peut pas utiliser la bijection. En examinant les formules ci-dessus, on se convainc que $p^+_{\neq}(n) - p^-_{\neq}(n) = (-1)^k$, ce qui termine la démonstration. ■

5.7 Tableaux de Young$^{(*)}$

Les tableaux de Young [11], introduits dans cette section, se construisent à partir de diagrammes et sont la source de multiples problématiques fascinantes en combinatoire. Pour un diagramme D, un **tableau** τ de **forme** $\lambda(\tau) = D$, avec valeurs dans un ensemble totalement ordonné A, est tout simplement une fonction

$$\tau : D \longrightarrow A$$

On représente souvent un tel tableau en remplissant chaque case c de D avec le valeur $\tau(c)$. Par exemple, on a le tableau :

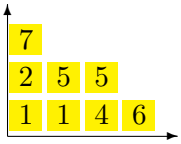


Le tableau τ est **injectif** si la fonction sous-jacente est injective.

On dit qu'on a un tableau **semi-standard** si ses valeurs vont en croissant faiblement sur chaque ligne lue de la gauche vers la droite, et vont en croissant strictement sur chaque colonne lue du bas vers le haut. Plus techniquement, on a donc

$$\begin{aligned} &\tau(i,j) \leq \tau(i',j), \quad \text{si} \quad i < i', \quad \text{et} \\ &\tau(i,j) < \tau(i,j'), \quad \text{si} \quad j < j'. \end{aligned}$$

Ainsi, on a le tableau semi-standard :



On dénote $\mathsf{Semi}_D[A]$ l'ensemble des tableaux semi-standards de forme D à valeur dans A. Un tableau τ, de forme $\mu \vdash n$, est dit **standard** (on dit aussi que c'est un **tableau de Young** [12]) s'il est semi-standard et injectif à valeur dans $\{1, 2, \ldots, n\}$. Autrement dit,

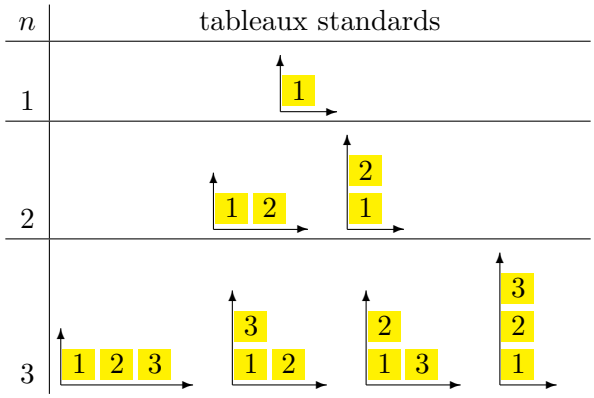
$$\tau(i,j) < \tau(i',j') \qquad \text{si} \qquad (i,j) < (i',j'). \tag{5.59}$$

Un tableau standard correspond donc à la donnée d'une fonction strictement croissante de l'ensemble ordonné μ (munit de l'ordre (5.39)) vers $[n]$. On dénote $\mathsf{Young}[\mu]$ l'ensemble des tableaux standards de forme μ. Rapellons (voir section 4.6) que c'est sous cette forme qu'on a vu (voir (2.41)

11. Alfred Young (1973-1940).
12. Pour Alfred Young (1873-1940), l'un des fondateurs de la théorie de la représentation des groupes.

et Section 4.6) que le nombre de tableaux standards de forme rectangulaire $2 \times n$ est exactement le n^{e} nombre de Catalan.

Pour $n \leq 3$, on a les tableaux standards



5.8 Formule des équerres(*)

Pour $\mu \vdash n$, le nombre f_μ de tableaux standards de forme μ :

$$f_\mu := |\mathsf{Young}[\mu]|, \tag{5.60}$$

est donné par la formule dite **des équerres** [13] (qui n'est pas prouvée ici) :

$$f_\mu = \frac{n!}{\prod_{c \in \mu} h_c}, \tag{5.61}$$

où, pour c une case de μ, h_c dénote la **longueur d'équerre** de la case $c = (i-1, j-1)$, à savoir

$$h_c := (\mu_j - i) + (\mu'_i - j) + 1. \tag{5.62}$$

C'est le nombre de cases, incluant c, qui se situent à droite de c (sur la même ligne) et haut de c (sur la même colonne). Dans l'exemple de la Figure 5.11, on illustre la notion d'équerre (dans ce cas de longueur 8). Pour le partage 3 2 1 on a les valeurs d'équerres

$$\begin{array}{ccc} 1 & & \\ 3 & 1 & \\ 5 & 3 & 1 \end{array}.$$

On a donc les $16 = \frac{6!}{5 \cdot 3 \cdot 3}$ tableaux standards de la forme 3 2 1.

13. Due à Frame-Robinson-Thrall [15].

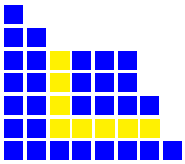


FIGURE 5.11 – L'équerre d'une case.

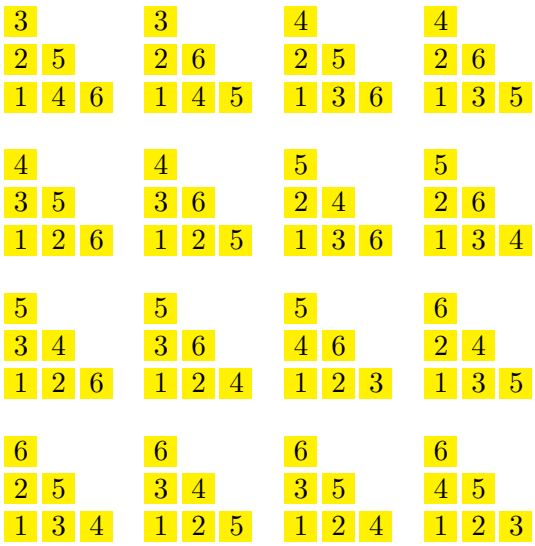


FIGURE 5.12 – Tous les tableaux standards de forme 321.

5.9 Correspondance de Robinson-Schensted-Knuth(*)

La correspondance de Robinson-Schensted-Knuth (RSK), dénoté ρ, associe bijectivement à chaque permutation (d'un ensemble totalement ordonné, habituellement $[n]$) un couple de tableaux standards de même forme :

$$\rho : \mathbb{S}[n] \xrightarrow{\sim} \sum_{\mu \vdash n} \mathsf{Young}[\mu] \times \mathsf{Young}[\mu] \tag{5.63}$$

Elle est liée à de nombreuses facettes de la combinatoire des permutations, et joue un rôle fondamental dans l'étude de l'interaction entre le groupe des permutations et les autres groupes (en théorie de la représentation des groupes).

Comme le nombre de tableaux standards de forme μ est donné par f_μ (qu'on peut calculer avec la

formule des équerres), la bijection [14] (5.63) entraîne qu'on a la très jolie formule

$$n! = \sum_{\mu \vdash n} f_\mu^2. \tag{5.64}$$

Cette formule admet de nombreuses généralisations dans le contexte de la théorie de la représentation des groupes, et dans celui de la théorie des fonctions symétriques. C'est comme la proverbiale pointe de l'iceberg.

G. de B. Robinson (1906-1992)

Une autre formule (discutée plus en détail à la section suivante) affirme que

$$|\mathsf{Inv}[n]| = \sum_{\mu \vdash n} f_\mu. \tag{5.65}$$

Rappelons que $\mathsf{Inv}[n]$ est l'ensemble des involutions sur $[n]$.

La correspondance [15] associe à chaque permutation σ un couple de tableaux

$$(P(\sigma), Q(\sigma)) = (P_\sigma, Q_\sigma),$$

qui sont respectivement appelés **P-tableau** et **Q-tableau** de σ. Si la permutation σ (décrite sous forme de mot) prend la forme

$$\sigma = \sigma_1\, \sigma_2 \cdots \sigma_n,$$

ces tableaux sont obtenus en « insérant » successivement les valeurs σ_i et i, respectivement dans le P-tableau et dans le Q-tableau. On commence avec deux tableaux vides. L'insertion suit un processus différent pour chacun des deux tableaux. Ce sont les valeurs σ_i qui sont insérées dans le P-tableau, tandis que ce sont les positions i qui s'insèrent dans le Q-tableau. D'une façon grossière, on peut dire que l'insertion dans le P-tableau consiste en une cascade de remplacement de valeurs, culminant par l'ajout d'une nouvelle case à l'une des lignes ; et l'insertion dans le Q-tableau enregistre les étapes de croissance du P-tableau.

Il est courant de commencer la présentation de la correspondance par un exemple, plutôt que de décrire formellement le processus d'entrée de jeu. Ainsi donc, pour la permutation

$$\sigma = 5\,4\,8\,2\,3\,6\,1\,7,$$

on a les étapes successives :

14. Gilbert de Beauregard Robinson (1906–1992), Craige Eugene Schensted (voir [36]) et Donald Ervin Knuth (1938–).

15. Plus généralement la correspondance RSK permet d'associer à un couple de mots de même longueur (chacun sur un alphabet ordonné), un couple de tableaux semi-standards.

	σ	$\mapsto$	$(P_\sigma,$	$Q_\sigma)$
(a)	$5\cdots$	$\mapsto$	5	1
(b)	$5\,4\cdots$	$\mapsto$	5 4	2 1
(c)	$5\,4\,8\cdots$	$\mapsto$	5 4 8	2 1 3
(d)	$5\,4\,8\,2\cdots$	$\mapsto$	5 4 2 8	4 2 1 3
(e)	$5\,4\,8\,2\,3\cdots$	$\mapsto$	5 4 8 2 3	3 2 5 1 3
(f)	$5\,4\,8\,2\,3\,6\cdots$	$\mapsto$	5 4 8 2 3 6	3 2 5 1 3 6
(g)	$5\,4\,8\,2\,3\,6\,1\cdots$	$\mapsto$	5 4 2 8 1 3 6	7 3 2 5 1 3 6
(h)	$5\,4\,8\,2\,3\,6\,1\,7$	$\mapsto$	5 4 2 8 1 3 6 7	7 3 2 5 1 3 6 8

Plus spécifiquement maintenant, pour tout mot $\sigma = \sigma_1\,\sigma_2\cdots\sigma_{n-1}\sigma_n$ d'entiers distincts ($\sigma_i \in \mathbb{N}$), la construction procède récursivement comme suit.

1. Si σ est le mot vide, alors $(P_\sigma, Q_\sigma) = (0, 0)$
2. Sinon, σ est de la forme $\sigma = \tau\,a$, pour $\tau = \sigma_1\,\sigma_2\cdots\sigma_{n-1}$, un mot de longueur $n-1$, et $a \in \mathbb{N}$. On suppose avoir déjà construit (P_τ, Q_τ), et on modifie ces deux tableaux de la façon suivante.
   (a) La valeur a remplace la plus petite valeur (qui est éjectée) de la première ligne de P_τ qui est plus grande que a, s'il y en a une. La valeur éjectée est récursivement insérée dans le tableau formé des lignes $2, 3, \ldots$ de P_τ, et ainsi de suite. Si a est plus grand que toute les valeurs de la première ligne, alors on ajoute a dans une nouvelle case à la fin de cette ligne. Le résultat P_σ est donc un tableau standard qui diffère de P_τ, dans sa forme, par une case.
   (b) On modifie le tableau Q_τ en lui ajoutant une case en même position que celle par laquelle P_σ diffère de P_τ, et donne la valeur n à case.

Une étape du processus d'insertion est illustrée à la figure 5.13. On insère 6 dans le premier tableau. Cette insertion éjecte 8 de la première ligne, et on doit l'insérer dans la seconde, etc. Les éléments qui sont «déplacés» par l'insertion sont dans les cases en vert dans le second tableau. La case qui contient 9 est la nouvelle case.

Propriétés de la correspondance RSK. La correspondance de Robinson-Schensted-Knuth a plusieurs propriétés remarquables. Nous n'allons n'en présenter que quelques-unes (sans démontstration).

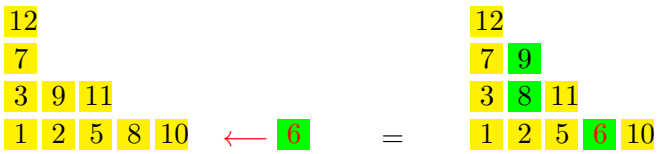


FIGURE 5.13 – Paire de tableaux standards.

L'une des propriétés les plus étonnantes est certainement le fait que la correspondance associe à la permutation σ^{-1} (l'inverse de σ) le couple de tableaux $(Q(\sigma), P(\sigma))$, autrement dit

$$P(\sigma^{-1}) = Q(\sigma), \qquad \text{et} \qquad Q(\sigma^{-1}) = P(\sigma). \tag{5.66}$$

Il en résulte que σ est une involution si et seulement si on a l'égalité $P(\sigma) = Q(\sigma)$. La formule (5.65) :

$$|\mathsf{Inv}[n]| = \sum_{\mu \vdash n} f_\mu$$

découle immédiatement de cette observation, puisque la correspondance RSK établit une bijection entre les involutions et les couples de tableaux $(P(\sigma), Q(\sigma))$ tels que $P(\sigma) = Q(\sigma)$.

Pour une permutation $\sigma = \sigma_1\sigma_2\cdots\sigma_n$, une **sous-suite croissante** de σ est

$$\sigma_{i_1} < \sigma_{i_2} < \ldots < \sigma_{i_k}$$

avec $i_1 < i_2 < \ldots < i_k$. Par exemple, 2 5 7 9 est une sous-suite croissante de longueur 4 de

$$\sigma = 2\,8\,6\,5\,3\,1\,4\,7\,9.$$

Cette dernière permutation admet aussi la sous-suite 2 3 4 7 9 de longueur 5. En fait, 5 est la longueur maximale d'une sous-suite croissante de σ.

Soit σ permutation de $[n]$. Alors, la longueur maximale d'une sous-suite croissante de σ est égale à la longueur de la première ligne du tableau $P(\sigma)$, obtenu par la correspondance RSK. Cette propriété est utilisée pour l'étude de certains algorithmes, plus particulièrement dans le domaine de la bio-informatique en relation avec le séquençage de gènes.

5.10 Exercices

5.1. Montrer qu'il y a $(n-1)!$ permutations cycliques d'un ensemble à n éléments. Suggestion : on peut supposer que l'ensemble en question est $[n]$, et alors, en parcourant le cycle à partir de 1, on trouve un ordre linéaire sur $\{2, 3, \ldots, n\}$.

5.2. Pour un ensemble fini A,

a) Montrer qu'on obtient une relation d'équivalence « $\equiv$ » sur A^n, par fermeture transitive, à partir des équivalences

$$(x_1, x_2, \ \dots \ , x_{n-1}, x_n) \equiv (x_2, x_3, \ \dots \ , x_n, x_1),$$

obtenue pour chaque $(x_1, x_2, \ \dots \ , x_n)$ dans A^n.

b) Montrer que, pour A de cardinal n, il y a une bijection

$$\mathcal{C}[A] \xrightarrow{\sim} A^n / \equiv.$$

5.3. Montrer qu'on a les formules suivantes pour les nombres de Stirling de première sorte.

a) $\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!$.

b) $\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2}$.

c) Si $k > 0$ alors $\begin{bmatrix} n+1 \\ k \end{bmatrix} = \begin{bmatrix} n \\ k-1 \end{bmatrix} + n \begin{bmatrix} n \\ k \end{bmatrix}$.

d) En notant le fait que $t^{(n+1)} = t^{(n)}\,(t+n)$ (Voir (1.69)), vérifier que

$$t^{(n)} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} t^k.$$

5.4. Soit $(a_n)_{n\geq 0}$ et $(b_n)_{n\geq 0}$ deux suites de nombres réels (ou même des polynômes). Prouver que,

$$a_n = \sum_{k=0}^{n} \binom{n}{k} b_k \qquad \Longleftrightarrow \qquad b_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} a_k. \tag{5.67}$$

5.5. Prouver bijectivement la formule

$$\begin{bmatrix} n+1 \\ k+1 \end{bmatrix} = \sum_{j=k}^{n} \binom{j}{k} \cdot \begin{bmatrix} n \\ j \end{bmatrix}, \tag{5.68}$$

où $k \geq 1$.

5.6. Montrer que la relation de conjugaison est une relation d'équivalence sur $\mathbb{S}_A$.

5.7. Montrer que, pour toute permutation σ et τ, on a

a) Le nombre de permutations θ, telles que $\theta\sigma\theta^{-1} = \tau$, est égal au nombre de permutations ρ telles que $\rho\sigma\rho^{-1} = \sigma$. Suggestion : Construire une bijection entre les deux ensembles en exploitant le fait que, lorsque $\theta\sigma\theta^{-1} = \psi\sigma\psi^{-1}$, alors $\rho = \psi^{-1}\theta$ est tel que $\rho\sigma\rho^{-1} = \sigma$.

b) Montrer que lorsque la forme de σ est $\lambda(\sigma) = \mu = 1^{d_1} 2^{d_2} \cdots n^{d_n}$ le nombre de permutations ρ telles que $\rho\sigma\rho^{-1} = \sigma$ est donné par la formule

$$z_\mu := 1^{d_1}\, d_1!\, 2^{d_2}\, d_2!\ \cdots\ n^{d_n}\, d_n!. \tag{5.69}$$

Bien entendu, on doit lire cette dernière expression en interprétant la notation exponentielle de la façon usuelle pour les entiers.

5.8. Combien y a-t-il de partages de n en parts au plus égales à 2 ?

5.9. a) Soit $K = \{2, 4, 6, \ldots\}$ l'ensemble des entiers pairs. Prouver que $p(n) = p(2n, K)$, bijectivement et par les séries génératrices.

b) Soit $I = \{1, 3, 5, \ldots\}$ l'ensemble des entiers impairs. Prouver que $p_I(n) = p_{\neq}(n)$, bijectivement et par les séries génératrices.

5.10. Soit $K = \{1, 2, 4, 8, \ldots\}$. Prouver directement que pour tout n, $p_{K;\neq}(n) = 1$. Donner une autre preuve, en terme de séries.

5.11. Prouver que la série génératrice des partages en exactement k parts, $k \geq 1$, est :

$$\frac{x^k}{(1-x)\,(1-x^2)\cdots(1-x^k)}$$

5.12. Trouver une bijection entre l'ensemble des compositions de n en parts égales à un ou deux et l'ensemble des compositions de $n+2$ à parts au moins égales à deux. En déduire que ces deux ensembles sont de cardinalité F_n, le n^e nombre de Fibonacci.

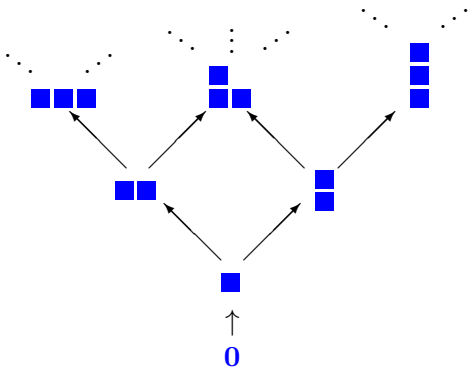
5.13. Trouver la série génératrice (en n) des partages en au moins k parts, $k \geq 1$.

5.14. Montrer, au moyen de la formule des équerres, que le nombre de tableaux standards à deux lignes, chacune de longueur n, est le n-ième nombre de Catalan :

$$\frac{1}{n+1}\binom{2\,n}{n}.$$

5.15. On peut ordonner l'ensemble de tous les diagrammes de Young par inclusion (en tant que sous-ensembles de $\mathbb{N} \times \mathbb{N}$). On obtient ce qu'on appelle le **treillis de Young**, dont voici une petite

partie du début de son diagramme de Hasse



Montrer qu'il y a bijection entre tableaux standards de forme μ (un partage), et chemins allant de 0 à μ dans ce treillis, et en déduire qu'on a la récurrence

$$f_\mu = \sum_{\nu \to \mu} f_\nu, \tag{5.70}$$

où $\nu \to \mu$ dénote la relation de couverture de l'ordre de Young.

5.16. Pour les partages d'un même entier n, on a l'ordre (partiel) de **dominance**, pour lequel on a $\nu \preceq \mu$ si

$$\begin{aligned} \nu_1 &\leq \mu_1, \\ \nu_1 + \nu_2 &\leq \mu_1 + \mu_2, \\ &\vdots \\ \nu_1 + \nu_2 + \cdots + \nu_k &\leq \mu_1 + \mu_2 + \cdots + \mu_k, \end{aligned}$$

où $\mu_i = 0$ si $i > \ell(\mu)$, avec une convention similaire pour ν. Le diagramme de Hasse de cet ordre sur l'ensemble des partages de 3 est : Trouver le diagramme de Hasse de cet ordre sur l'ensemble des partages de 7. Attention, ce n'est pas un ordre total.

5.17. L'ordre (total) **lexicographique**, sur les partages de n, est celui pour lequel $\nu < \mu$, si la première différence non nulle, $\mu_i - \nu_i$, est positive. Pour $n = 4$, on a donc

$$1111 < 211 < 22 < 31 < 4$$

Montrer que l'ordre lexicographique est une extension linéaire de l'ordre de dominance. C'est-à-dire que l'ordre lexicographique est un ordre total tel que

$$\nu \preceq \mu \qquad \text{implique} \qquad \nu \leq \mu.$$

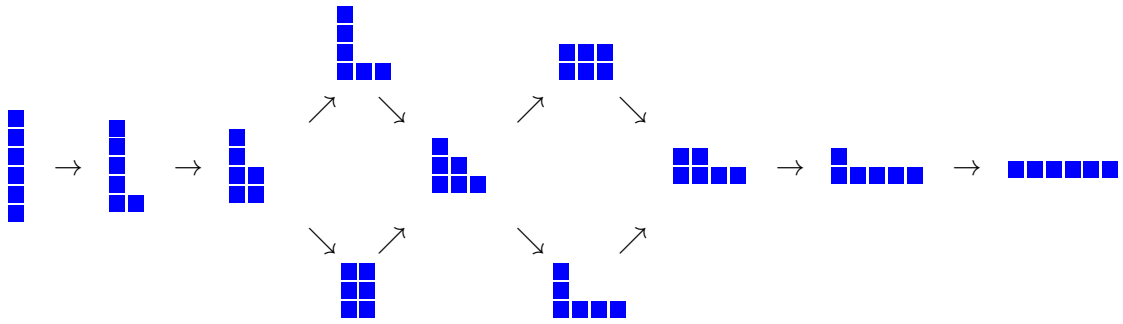


FIGURE 5.14 – L'ordre de dominance pour $n = 6$

5.18. Le **contenu**, $\gamma(t)$, d'un tableau t, est

$$\gamma(t) = 1^{m_1}2^{m_2}3^{m_3}\cdots$$

où m_i est la multiplicité de l'entier i dans t. Ainsi le contenu du tableau t :

3	3	4		
2	2	2		
1	1	1	1	2

est $\gamma(t) = 1^4 2^4 3^2 4^1$. Il y a exactement quatre tableaux semi-standards de forme 321 et de contenu 2211. Ce sont :

4				3				4				3					
2	3			2	4			2	2			2	2				
1	1	2		1	1	2		1	1	3		1	1	4			

Pour ν et μ des partages de n, le **nombre de Kostka**, $K_{\nu\mu}$, est le nombre de tableaux semi-standard de forme ν et de contenu

$$1^{\mu_1}2^{\mu_2}\cdots k^{\mu_k}.$$

1. Montrer que $K_{\nu,1^n} = f_\nu$.
2. Montrer que $K_{\nu\nu} = 1$.

5.19. Si l'on ordonne les partages de 4 lexicographiquement comme à l'exercice 5.17, on obtient que la matrice des nombres de Kostka (voir exercice précédent) :

$$(K_{\nu\mu})_{\nu,\mu\vdash 4} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{5.71}$$

Calculer la matrice de Kostka pour $n = 5$.

5.20. Sachant que, pour un partage μ de n, le nombre de tableaux semi-standard de forme μ à valeur dans $[k]$ est donné par la formule

$$s_\mu(k) = \prod_{(i,j)\in\mu} \frac{k+j-i}{h_{ij}}, \tag{5.72}$$

où on a posé $s_\mu(k) := |\mathsf{Semi}_\mu[k]|$, déduire de l'exercice 5.27 qu'on a l'identité

$$k^n = \sum_{\mu\vdash n} f_\mu\, s_\mu(k). \tag{5.73}$$

Programmation mathématique

5.21. Concevoir des procédure qui, pour une permutation σ de $[n]$ donnée sous forme de mot,

a) calcule la partition de $[n]$

b) calcule la décomposition cyclique de σ.

c) trouve une représentation de σ comme produit de transpositions adjacentes.

d) trouve toutes les représentations (de longueur minimale) de σ comme produit de transpositions adjacentes.

5.22. Concevoir une procédure qui calcule, sous forme de mot,

a) toutes les permutations cycliques de A,

b) tous les dérangements de A. Suggestion : Utiliser (5.15).

5.23. Utiliser (5.37) pour écrire une procédure qui trouve tous les partages de n en parts plus petites ou égales à k.

5.24. Utiliser le théorème pentagonal d'Euler pour calculer efficacement le nombre de partages de n. Tester l'efficacité de votre procédure pour de grands nombres.

5.25. Concevoir une procédure qui trouve tous les tableaux de Young de forme donnée.

5.26. Concevoir des procédures qui réalise la correspondance RSK, c.-à-d. : calcule le couple (P, Q) à partir de σ. Tester l'énoncé (5.66).

5.27. Étendre la correspondance RSK aux mots w de longueur n sur l'alphabet $[k]$. Le résultat sera un couple (P_w, Q_w), avec P_w est semi-standard et Q_w standard, de même forme que P_w. Les valeurs dans P_w sont les diverses lettres de w (apparaissant avec la même multiplicité).

Chapitre 6

Introduction à la théorie des espèces

6.1 Introduction.

Le concept de structure est fondamental en science et se retrouve dans toutes les branches des mathématiques ainsi qu'en informatique théorique, où il porte le nom de structure de données. Pour en donner une description claire, on introduit la notion d'espèce de structures. Cette définition se fait dans un esprit similaire à celui de la définition de fonction. Rappelons que la notion de fonction a subi une lente et obligatoire évolution, dans l'histoire des mathématiques, pour aboutir à la notion moderne. Cette vision moderne a séparé la définition de la notion de fonction du mode de description de fonctions explicites. Bien entendu, rien n'empêche ensuite de décrire une fonction particulière par une formule, un algorithme, comme solution d'une équation, etc. Là où on gagne, c'est dans la possibilité de définir de façon claire des espaces de fonctions. C'est un gain indéniable quand on pense au

C'est de ce niveau de généralité que relève la définition des espèces de structures. Un autre concept important derrière la notion d'espèce est celui d'isomorphisme de structures combinatoires. Il joue un rôle central dans la définition de « type » de structures (ou structures « non étiquetées »). Le but de la théorie des espèces est principalement de fournir une approche synthétique à la notion de structures combinatoires. Nous allons constater que plusieurs des identités déjà rencontrées dans ce texte se reformulent agréablement dans le contexte de la théorie des espèces.

6.2 Espèces de structures.

En fait, nous avons déjà rencontré plusieurs espèces tout au cours des chapitres précédents, et tout ce qui nous reste à faire maintenant est d'en donner une définition formelle. Le but de cette

définition est de donner un critère précis permettant de vérifier qu'une espèce donne une description claire d'une construction combinatoire sur les éléments d'un ensemble fini.

La notion **espèce de structures**[1] F contient deux parties.

1) Une première partie qui décrit comment **produire**, pour chaque ensemble fini A, un ensemble fini $F[A]$. On dit que les éléments s de $F[A]$ sont les **structures** d'espèce F sur A, ou encore que ce sont des F-structures.

2) La seconde partie de la règle assure que la description de $F[A]$ peut se traduire **naturellement** (au sens précis décrit plus bas) en une description de $F[B]$, chaque fois que A et B ont la même cardinalité. Plus précisément, on demande que, pour chaque bijection $\sigma : A \to B$, il y a une bijection

$$F_\sigma : F[A] \to F[B]$$

décrivant comment transformer les éléments de $F[A]$ en éléments de $F[B]$. On dit que F_σ est le **transport de structures** le long de σ.

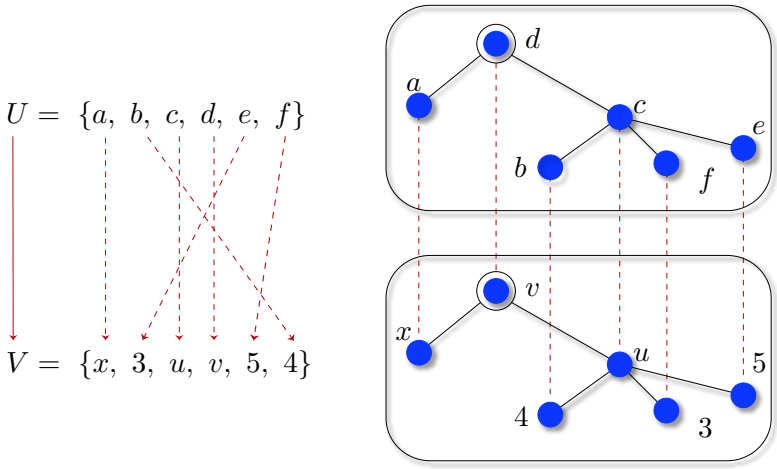


FIGURE 6.1 – Le réétiquetage comme transport.

Très souvent, les éléments de A servent **d'étiquettes** au sein des structures dans $F[A]$, et alors F_σ correspond à remplacer l'étiquette x par l'étiquette $\sigma(x)$, pour chaque x dans A (voir la Figure 6.1). Autrement dit, la bijection F_σ est simplement le **réétiquetage** selon σ. Bien entendu, il y a d'autres possibilités pour F_σ. Quelque soit le cas, pour exclure les situations potentiellement non désirables (contre intuitives), ainsi que pour donner une définition qui soit techniquement aisément manipulable, on impose que les bijections F_σ satisfassent aux conditions de **fonctorialité** :

1. La notion d'espèce de structures a été introduite en combinatoire par A. Joyal et développée par les membres de l'équipe de combinatoire de l'UQAM. On peut trouver une description plus détaillée de la théorie des espèces et de ses applications dans la monographie [6].

i) pour chaque ensemble fini A, la bijection F_{Id_A} est l'identité de l'ensemble $F[A]$.

ii) si $\sigma : A \to B$ et $\tau : B \to C$, alors
$$F_{\tau\circ\sigma} = F_\tau \circ F_\sigma.$$

La meilleure façon de s'habituer à cette définition est de donner un certain nombre d'exemples typiques. Nous en verrons toute une liste après la définition suivante.

Série génératrice. De la définition d'espèce, il suit immédiatement qu'on a forcément

$$|F[A]| = |F[B]|\,,$$

chaque fois qu'il y a une bijection entre les ensembles A et B, puisqu'il y a alors une bijection de $F[A]$ vers $F[B]$. Le nombre de structures d'espèce F sur un ensemble à A est donc simplement une fonction du cardinal de A. Aux fins d'énumération, on peut choisir n'importe quel ensemble de cardinal n, mais usuellement on prend $A = [n]$. Tout comme dans les chapitres précédents, on allège la notation on écrivant simplement $F[n]$ pour l'ensemble des F-structures sur l'ensemble $A = [n]$.

La problématique de la combinatoire énumérative discutée au tout début de ce livre, consiste à calculer la suite de nombres :

$$|F[0]|\,,\quad |F[1]|\,,\quad |F[2]|\,,\quad |F[3]|\,,\quad \cdots\quad |F[n]|\,,\qquad \cdots$$

Comme on la déjà souligné à quelques occasions, une manière efficace de s'attaquer à cette tâche est de considérer la **série génératrice**

$$F(y) := \sum_{n=0}^{\infty} f_n \,\frac{y^n}{n!}\,, \tag{6.1}$$

où f_n est le nombre d'éléments de $F[n]$. Un des aspects fascinants de l'approche par séries génératrices est qu'il y a souvent une fonction classique bien connue dont le développement en série à l'origine correspond précisément à une série génératrice apparaissant ainsi dans un contexte d'énumération. Par calcul direct, on trouve facilement certaines séries.

6.3 Exemples d'espèces

Voici maintenant un liste d'exemples d'espèces et de séries génératrices associées. Dans la plupart de ces exemples, le calcul des séries est direct. Cependant, certaines séries seront obtenues par des techniques présentées plus loin.

Espèces de parties. Au Chapitre 1 (voir (1.9) et (1.42)), on a explicitement décrit les deux composantes de l'espèce des **parties**, en posant

$$\mathcal{P}[A] := \{B \mid B \subseteq A\}, \tag{6.2}$$

$$\mathcal{P}_\sigma : \mathcal{P}[A] \to \mathcal{P}[B], \qquad \mathcal{P}_\sigma(B) := \{\, f(x) \mid x \in B\}. \tag{6.3}$$

Le transport d'une partie B de A, le long d'une bijection $\sigma : A \to B$, est donc l'image $\sigma^+(B)$ de B par σ. On a aussi défini l'espèce des **parties à k éléments**, en posant

$$\mathcal{P}_k[A] := \{B \mid B \subseteq A,\ |B| = k\}, \tag{6.4}$$

avec le transport de structures analogue. Pour la bijection $\sigma(1) = a$, $\sigma(2) = b$, et $\sigma(3) = c$, de $\{1,2,3\}$ vers $\{a,b,c\}$, on a le transport de $\mathcal{P}$-structures :

$$\begin{array}{cccccccc} \emptyset & \{1\} & \{2\} & \{3\} & \{1,2\} & \{1,3\} & \{2,3\} & \{1,2,3\} \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \emptyset & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \end{array}$$

Puisqu'il y a 2^n structures d'espèce $\mathcal{P}$ sur un ensemble à n éléments, on a la série

$$\begin{aligned} \mathcal{P}(y) &= 1 + 2\,y + 4\,\frac{y^2}{2} + 8\,\frac{y^3}{6} + 16\,\frac{y^4}{24} + \ \ldots\ + 2^n\,\frac{y^n}{n!} + \ \ldots \\ &= \exp(2\,y); \end{aligned} \tag{6.5}$$

et puisqu'il y a $\binom{n}{k}$ structures d'espèce $\mathcal{P}_k$ sur un ensemble à n éléments, on a la série

$$\begin{aligned} \mathcal{P}_k(y) &= \frac{y^k}{k!} + (k+1)\,\frac{y^{k+1}}{(k+1)!} + \ \ldots\ + \binom{n}{k}\,\frac{y^n}{n!} + \ \ldots \\ &= \frac{y^k}{k!} + \frac{y^k}{k!}\,y + \ \ldots\ + \frac{y^k\,y^{n-k}}{k!\,(n-k)!} + \ \ldots \\ &= \frac{y^k}{k!}\left(1 + y + \ \ldots\ + \frac{y^n}{n!} + \ \ldots\ \right) \\ &= \frac{y^k}{k!}\,\exp(y). \end{aligned} \tag{6.6}$$

Espèces de graphes. Au Chapitre 2, nous avons défini l'ensemble $\mathsf{Gra}[A]$ des **graphes simples** sur A. C'est là la première partie de la description de l'espèce des graphes simples. Les éléments

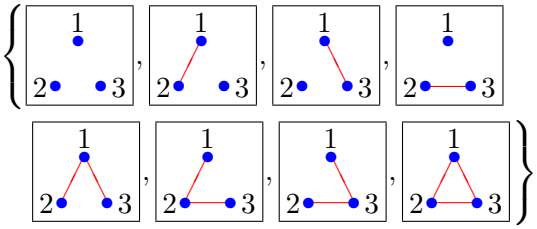


FIGURE 6.2 – L'ensemble des graphes sur $\{1,2,3\}$.

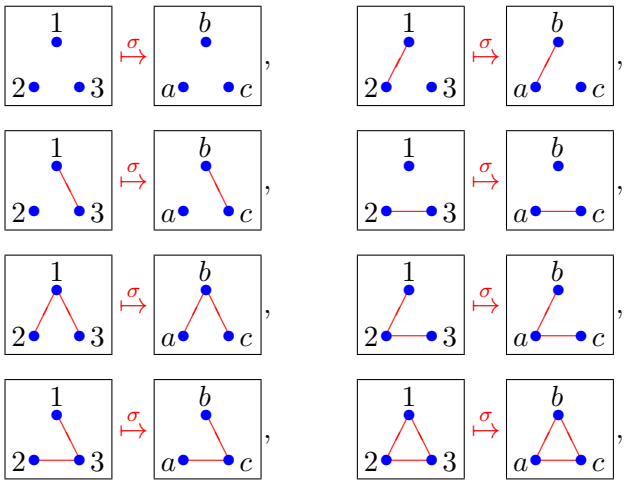
de $\mathsf{Gra}[A]$, qui sont les graphes sur A, sont les structures d'espèce graphe sur A. Par exemple, pour $A = \{1,2,3\}$, on a les structures de la Figure 6.2. Rappelons que, très précisément on a

$$\mathsf{Gra}[A] := \mathcal{P}[\mathcal{P}_2[A]]. \tag{6.7}$$

Reste maintenant à décrire le transport de structures, qui est dans ce cas un réétiquetage. Pour une bijection $\sigma : A \xrightarrow{\sim} B$, le transport Gra_σ d'un graphe G dans $\mathsf{Gra}[A]$ s'obtient en posant :

$$\mathsf{Gra}_\sigma(G) := \{\{\sigma(x), \sigma(x')\} \mid \{x, x'\} \in G\} \tag{6.8}$$

Ceci correspond à changer les étiquettes des sommets, en remplaçant x par $\sigma(x)$. Ainsi, lorsqu'on transporte les graphes sur $\{1,2,3\}$ le long de la bijection $\sigma : \{1,2,3\} \to \{a,b,c\}$, pour laquelle $\sigma(1) = b$, $\sigma(2) = a$ et $\sigma(3) = c$, on obtient le transport :



Au même Chapitre 2, on a aussi décrit l'espèce Gro des **graphes orientés**, en posant

$$\mathsf{Gro}[A] := \mathcal{P}[A \times A]. \tag{6.9}$$

Le transport de structure correspondant est

$$\mathsf{Gro}_\sigma := \mathcal{P}_{\sigma\times\sigma}, \tag{6.10}$$

où $\sigma \times \sigma$ est la bijection qui envoie (x, y), dans $A \times A$, sur

$$(\sigma \times \sigma)(x, y) := (\sigma(x), \sigma(y)).$$

Autrement dit, l'image par Gro_σ d'un graphe orienté G dans $\mathsf{Gro}[A]$, est le graphe orienté :

$$\mathsf{Gro}_\sigma(G) = \{(\sigma(x), \sigma(y)) \mid (x, y) \in G\}.$$

Puisqu'il y a $2^{\binom{n}{2}}$ structures d'espèce Gra sur un ensemble à n éléments, on a la série

$$\begin{aligned}\mathsf{Gra}(y) &= 1 + y + 2\,\frac{y^2}{2} + 8\,\frac{y^3}{6} + 64\,\frac{y^4}{24} + 1024\,\frac{y^5}{120} + \ \ldots \\ &= \sum_{n=0}^{\infty} 2^{\binom{n}{2}}\,\frac{y^n}{n!}.\end{aligned} \tag{6.11}$$

Pour l'espèce des graphes orientés, il y a $2^{(n^2)}$ structures sur un ensemble à n éléments, on a donc la série

$$\begin{aligned}\mathsf{Gro}(y) &= 1 + 2\,y + 16\,\frac{y^2}{2} + 512\,\frac{y^3}{6} + 65536\,\frac{y^4}{24} + 33554432\,\frac{y^5}{120} + \ \ldots \\ &= \sum_{n=0}^{\infty} 2^{(n^2)}\,\frac{y^n}{n!}.\end{aligned} \tag{6.12}$$

Espèces d'endofonctions. Au même Chapitre 5, on a introduit l'espèce $\mathbb{S}$ des **permutations**, en posant

$$\mathbb{S}[A] := \{\tau \mid \tau : A \xrightarrow{\sim} A\}. \tag{6.13}$$

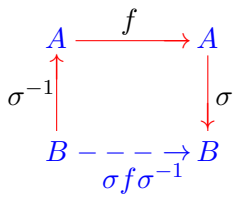
Le transport de structure correspondant à une bijection $\sigma : A \to B$ est tel que

$$\mathbb{S}_\sigma(\tau) := \sigma\,\tau\,\sigma^{-1}, \tag{6.14}$$

pour τ dans $\mathbb{S}[A]$. Autrement dit, le transport de la permutation $\tau : A \to A$ le long de $\sigma : A \to B$ donne une permutation $\theta := \mathbb{S}_\sigma(\tau)$ de B qui est définie de façon à ce qu'on ai

$$\theta(\sigma(x)) = \sigma(y), \quad \text{ssi} \quad \tau(x) = y.$$

Plus généralement, pour une endofonction $f : A \to A$, on a la conjugaison :



(6.15)

Cette conjugaison par σ donne le transport pour les espèces de fonctions :

- l'espèce des **cycles** (ou des **permutations cycliques**) , définie comme

$$\mathcal{C}[A] := \{\sigma \mid \sigma : A \xrightarrow{\sim} A,\ \sigma \text{ cyclique}\}.$$

- l'espèce des **involutions**, définie comme

$$\mathsf{Inv}[A] := \{\sigma \mid \sigma : A \xrightarrow{\sim} A,\ \sigma^2 = \mathrm{Id}_A\}.$$

- l'espèce des **dérangements**

$$\mathsf{Der}[A] := \{\sigma \mid \sigma \text{ est un dérangement}\},$$

- l'espèce des **endofonctions**

$$\mathsf{End}[A] := \{f \mid f : A \to A\}.$$

Puisqu'il y a $n!$ structures d'espèce $\mathbb{L}$ sur un ensemble à n éléments, on a la série

$$\begin{aligned} \mathbb{S}(y) &= 1 + y + 2\,\frac{y^2}{2} + 6\,\frac{y^3}{6} + 24\,\frac{y^4}{24} + \ \dots\ + n!\,\frac{y^n}{n!} + \ \dots \\ &= 1 + y + y^2 + y^3 + y^4 + \ \dots\ + y^n + \ \dots \\ &= \frac{1}{1-y}. \end{aligned} \tag{6.16}$$

Il y a $(n-1)!$ permutations cycliques sur un ensemble à n éléments. On a donc

$$\begin{aligned} \mathcal{C}(y) &= 0 + y + 1\,\frac{y^2}{2} + 2\,\frac{y^3}{6} + 6\,\frac{y^4}{24} + \ \dots\ + (n-1)!\,\frac{y^n}{n!} + \ \dots \\ &= y + \frac{y^2}{2} + \frac{y^3}{3} + \frac{y^4}{4} + \ \dots\ + \frac{y^n}{n} + \ \dots \\ &= \log\frac{1}{1-y}. \end{aligned} \tag{6.17}$$

On montrera plus loin que la série génératrice de l'espèce des involutions est

$$\begin{aligned} \mathsf{Inv}(y) &= 1 + y + 2\,\frac{y^2}{2} + 4\,\frac{y^3}{6} + 10\,\frac{y^4}{24} + 26\,\frac{y^5}{120} + \ \cdots \\ &= \exp(y + y^2/2), \end{aligned} \tag{6.18}$$

et que celle des dérangements est

$$\begin{aligned} \mathsf{Der}(y) &= 1 + 0\,y + \frac{y^2}{2} + 2\,\frac{y^3}{6} + 9\,\frac{y^4}{24} + 44\,\frac{y^5}{120} + \ \cdots \\ &= \frac{\exp(-y)}{1-y}. \end{aligned} \tag{6.19}$$

Comme il y a n^n endofonctions sur un ensemble à n éléments, on a

$$\begin{aligned} \mathsf{End}(y) &= 1 + y + 4\,\frac{y^2}{2} + 27\,\frac{y^3}{6} + 256\,\frac{y^4}{24} + 3125\,\frac{y^5}{120} + \ \cdots \\ &= \sum_{n=0}^{\infty} n^n\,\frac{y^n}{n!}, \end{aligned} \tag{6.20}$$

L'espèce des listes. À la Section 2.5, on a vu l'espèce des **listes** (ou des **ordres linéaires**) :

$$\mathbb{L}[A] := \{\ell \mid \ell : [n] \xrightarrow{\sim} A\} \tag{6.21}$$

qu'on décrit ici en exploitant la Proposition 2.9. Autrement dit, une liste des éléments de A s'identifie à une fonction

$$\ell = \{(1, x_1), (2, x_2), (3, x_3),\ \ldots\ , (n, x_n)\}.$$

On peut alors définir le transport de structures le long de σ tout simplement comme

$$\mathbb{L}_\sigma(\ell) := \sigma \circ \ell. \tag{6.22}$$

Puisqu'il y a $n!$ structures d'espèce $\mathbb{L}$ sur un ensemble à n éléments, on a la série

$$\begin{aligned} \mathbb{L}(y) &= 1 + y + 2\,\frac{y^2}{2} + 6\,\frac{y^3}{6} + 24\,\frac{y^4}{24} + \ \cdots\ + n!\,\frac{y^n}{n!} + \ \cdots \\ &= \frac{1}{1-y}. \end{aligned} \tag{6.23}$$

L'espèce des partitions. On a défini à la Section 2.3 l'ensemble $\mathsf{Part}[A]$ des partitions de A. On en tire l'**espèce des partitions** en considérant de pair le transport de structure défini par

$$\mathsf{Part}_\sigma(P) := \{\sigma^+(B) \mid B \in P\} \tag{6.24}$$

pour P dans $\mathsf{Part}[A]$. Comme on va le voir plus loin, l'espèce des partitions joue un rôle crucial dans la définition de l'opération de substitution d'espèces. On a la série (voir plus loin pour la justification)

$$\begin{aligned} \mathsf{Part}(y) &= 1 + y + 2\,\frac{y^2}{2} + 5\,\frac{y^3}{6} + 15\,\frac{y^4}{24} + 52\,\frac{y^5}{120} + \ \cdots \\ &= \exp(\exp(y) - 1), \end{aligned} \tag{6.25}$$

dont les coefficients sont les nombres de Bell.

6.4 Espèces auxiliaires simples.

Voici quelques autres exemples, parfois presque trop simples, qui seront utiles pour la suite. Dans chaque cas on décrit l'effet de l'espèce sur un ensemble A, et le transport pour $\sigma : A \xrightarrow{\sim} B$. Cependant, lorsque le transport de structures est assez évident, il n'est pas nécessairement décrit explicitement.

(1) $\mathsf{O}[A] = \emptyset$, c'est l'espèce dite **vide**. Le transport de structure est l'unique bijection de l'ensemble vide vers l'ensemble vide. Comme il n'y a aucune structure d'espèce O sur un ensemble de cardinal n, la série génératrice associée est

$$\begin{aligned} \mathsf{O}(y) &= 0 + 0\,y + 0\,\frac{y^2}{2} + 0\,\frac{y^3}{6} + 0\,\frac{y^4}{24} + 0\,\frac{y^5}{120} + \ \cdots \\ &= 0. \end{aligned} \tag{6.26}$$

(2) $\mathsf{E}[A] = \{A\}$, c'est l'espèce **ensemble** (avec une seule structure [2] sur tout ensemble fini). On pose $\mathsf{E}_\sigma(A) := B$. Il y a exactement une structure d'espèce E sur chaque ensemble de cardinal n, on a donc

$$\begin{aligned} \mathsf{E}(y) &= 1 + y + \frac{y^2}{2} + \frac{y^3}{6} + \frac{y^4}{24} + \ \cdots \ + \frac{y^n}{n!} + \ \cdots \\ &= \exp(y). \end{aligned} \tag{6.27}$$

2. Attention ici à la différence entre l'ensemble A, qui peut contenir plusieurs éléments, et l'ensemble $\{A\}$ qui ne contient qu'un seul élément, à savoir l'ensemble A.

(3) $\mathbb{1}[A] = \begin{cases} \{A\} & \text{si , } |A| = 0 \\ \emptyset & \text{sinon.} \end{cases}$

C'est l'espèce **caractéristique de l'ensemble vide**. Le seul ensemble qui admet une structure d'espèce $\mathbb{1}$ est l'ensemble vide, on a donc

$$\begin{aligned} \mathbb{1}(y) &= 1 + 0\,y + 0\,\frac{y^2}{2} + 0\,\frac{y^3}{6} + 0\,\frac{y^4}{24} + 0\,\frac{y^5}{120} + \ \ldots \\ &= 1. \end{aligned} \tag{6.28}$$

(4) $\mathsf{Y}[A] = \begin{cases} \{A\} & \text{si, } |A| = 1 \\ \emptyset & \text{sinon.} \end{cases}$

C'est l'espèce **caractéristique des singletons**. Les seuls ensembles qui admettent des structures d'espèces Y sont les singletons, et il y a alors une seule telle structure. On a donc

$$\begin{aligned} \mathsf{Y}(y) &= 0 + \ y + 0\,\frac{y^2}{2} + 0\,\frac{y^3}{6} + 0\,\frac{y^4}{24} + 0\,\frac{y^5}{120} + \ \ldots \\ &= y. \end{aligned} \tag{6.29}$$

(5) $\text{Élém}[A] = A$, c'est l'espèce **élément**, c.-à-d. : une structure sur A est un élément de A. Il vaut peut-être la peine de réfléchir un peu à la différence entre l'espèce Élém et l'espèce E. Le transport de la structure x (élément de A) est la structure $\sigma(x)$ (qui est un élément de B). Il y a exactement n structure d'espèce Élém sur chaque ensemble de cardinal n, on a donc

$$\begin{aligned} \text{Élém}(y) &= 0 + \ y + 2\,\frac{y^2}{2} + 3\,\frac{y^3}{6} + 4\,\frac{y^4}{24} + \ \ldots \ + n\,\frac{y^n}{n!} + \ \ldots \\ &= y + y^2 + \frac{y^3}{2} + \frac{y^4}{6} + \ \ldots \ + \frac{y^n}{(n-1)!} + \ \ldots \\ &= y\left(1 + y + \frac{y^2}{2} + \frac{y^3}{6} + \ \ldots \ + \frac{y^{n-1}}{(n-1)!} + \ \ldots\right) \\ &= y\,\exp(y). \end{aligned} \tag{6.30}$$

Pour toute espèce F, on peut considérer l'espèce F^+ qui est sa restriction aux ensembles non vides :

$$F^+[A] = \begin{cases} F[A] & \text{si , } |A| \neq 0 \\ \emptyset & \text{sinon.} \end{cases} \tag{6.31}$$

6.5 Isomorphisme d'espèces (bijections naturelles).

L'isomorphisme d'espèces est la formulation précise de la notion de bijection naturelle que nous avons manipulée au cours des chapitres précédents. Un des aspects qui jouent ici un rôle crucial est que pour qu'une bijection soit naturelle, il faut que sa description ne dépende pas de propriétés particulières des éléments (grandeur, valeur ...) qui interviennent dans les structures mises en bijection. Le critère explicite décrit ci-dessous cherche donc à assurer que cela n'est pas le cas. Pour le formuler en termes plus positifs, on demande essentiellement que la bijection soit « compatible » avec les isomorphismes de structures.

Formellement, on dit que deux espèces F et G sont **isomorphes** si et seulement si il existe, pour chaque ensemble A, une bijection θ_A expliquant comment transformer les éléments de $F[A]$ en éléments de $G[A]$, de façon **compatible avec le transport de structure**. C'est-à-dire qu'on demande que le composé $G_\sigma \circ \theta_A$ (c.-à-d. : une traduction $\theta_A : F_\sigma : F[A] \to G[A]$ suivi d'un transport $G_\sigma : G[A] \to G[B]$) donne toujours le même résultat que le composé $\theta_B \circ F_\sigma$ (c.-à-d. : le transport F_σ suivit de la traduction θ_B) :

$$\theta_B \circ F_\sigma = G_\sigma \circ \theta_A, \qquad \forall\ \sigma : A \to B. \tag{6.32}$$

La bijection θ_A est alors dite **naturelle**. C'est donc là très exactement la façon de formaliser cette notion que nous avons utilisée (sans la définir) au cours des chapitres précédents. D'une manière compacte, cette définition assure que la bijection en question s'impose presque comme allant de soi. Très souvent, la vérification de (6.90) est techniquement facile, et le besoin de faire cette vérification ne se fait sentir que dans le cas de bijection ayant une définition un peu complexe.

La propriété (6.90) donne, en cas de besoin, un mécanisme de vérification explicite de la naturalité. Ainsi, grâce à ce critère, on vérifie très facilement que le composé de deux isomorphismes est un isomorphisme, et que l'inverse d'un isomorphisme est un isomorphisme. Il s'ensuit que l'isomorphisme d'espèce est une relation d'équivalence sur les espèces. Il est souvent agréable d'écrire $F \simeq G$, pour signifier qu'il existe un isomorphisme entre F et G sans avoir nécessairement à spécifier lequel. En effet, l'isomorphisme considéré est dans plusieurs situations tellement naturel que cet abus est acceptable. Rien n'empêche cependant qu'il y ait plusieurs isomorphismes naturels différents entre certaines espèces. Un peu plus de soin doit être alors accordé à une description plus explicite.

Un cas spécial d'isomorphisme est celui d'**automorphisme**, c.-à-d. : un isomorphisme d'une espèce vers elle-même. Ainsi, pour l'espèce des listes, on a l'automorphisme

$$\overleftarrow{(\ )} : \mathbb{L}[A] \to \mathbb{L}[A] \tag{6.33}$$

qui envoie une liste $\ell = (a_1, a_2, \ \ldots\ , a_n)$ sur la liste renversée $\overleftarrow{\ell} = (a_n, \ \ldots\ , a_2, a_1)$.

6.6 Somme et produit.

Nous allons maintenant développer l'un des aspects les plus intéressants de la théorie des espèces : « l'algèbre des espèces ». Plus précisément, nous allons introduire des opérations entre espèces qui permettent de manipuler, de construire et de décomposer les espèces. Nous allons constater que plusieurs arguments combinatoires se formulent agréablement en terme de ces opérations.

On a d'abord la **somme** d'espèces :

$$(F+G)[A] := F[A] + G[A], \tag{6.34}$$

Autrement dit, une structure d'espèce $F+G$ sur A est soit une structure d'espèce F, soit une structure d'espèce G. Pour $\sigma : A \xrightarrow{\sim} B$, on pose

$$(F+G)_\sigma(t) := \begin{cases} F_\sigma(t) & \text{si, } t \in F[A] \\ G_\sigma(t) & \text{si, } t \in G[A]. \end{cases}, \tag{6.35}$$

On vérifie facilement que la somme d'espèce est associative et commutative (à isomorphisme d'espèce près), et que l'espèce O agit comme élément neutre. On peut étendre la somme à une famille d'espèces, pour obtenir l'espèce

$$\left(\sum_{i\in I} F_i\right)[A] := \sum_{i\in I} F_i[A], \tag{6.36}$$

qui a un sens clair si I est fini.

Plus intéressant encore est le **produit**, $F \cdot G$, d'espèces qui est défini sur un ensemble A comme

$$(F\cdot G)[A] := \sum_{A=B+C} F[B] \times G[C]. \tag{6.37}$$

De façon équivalente, on a

$$(F\cdot G)[A] := \{(f,g,B) \mid f \in F[B], \quad g \in G[A\setminus B]\}. \tag{6.38}$$

Le transport de structures pour l'espèce $F \cdot G$ se définit en posant

$$(F\cdot G)_\sigma(f,g,B) = (F_\sigma(f), G_\sigma(g), \sigma^+(B)). \tag{6.39}$$

Considérons par exemple le produit d'espèce $\mathsf{E}\cdot\mathsf{E}$. Directement à partir de la définition, on trouve

$$(\mathsf{E}\cdot\mathsf{E})[A] = \{(f,g,B) \mid f \in \mathsf{E}[B], \quad g \in \mathsf{E}[A\setminus B]\}.$$

Comme le seul élément de $\mathsf{E}[B]$ est B, on a donc (avec une petite simplification d'écriture) :

$$(\mathsf{E}\cdot\mathsf{E})[A] = \{(B, A\setminus B) \mid B\subseteq A\}.$$

On observe que, pour chaque ensemble fini A, il y a une bijection évidente entre

$$\pi_A : (\mathsf{E}\cdot\mathsf{E})[A] \xrightarrow{\sim} \mathcal{P}[A], \tag{6.40}$$

simplement définie en posant $\pi_A((B, A\setminus B)) = B$, dont l'inverse est évidemment $\pi^{-1}(B) = (B, A\setminus B)$. On vérifie directement (voir Exercice 6.16) que la famille de ces bijections donne un isomorphisme d'espèces. Pour résumer ceci, on écrit donc

$$\mathsf{E}\cdot\mathsf{E} \;\simeq\; \mathcal{P}. \tag{6.41}$$

À partir des opérations de somme et de produit d'espèces, on peut construire de nouvelles opérations comme la **puissance k-ième**

$$F^k = \begin{cases} \mathbb{1} & \text{si, } k=0 \\ F\cdot F^{k-1} & \text{si } k>0. \end{cases} \tag{6.42}$$

Une structure d'espèce F^k sur A est simplement un k-tuplet de structures d'espèce F. Plus précisément, on commence par découper A en k parties B_1, B_2, … , avec les B_i deux à deux disjointes, et telles que

$$A = B_1 + B_2 + \ldots + B_k. \qquad \text{(de toutes les façons possibles)}$$

Puis on choisit sur chaque B_i une structure d'espèce F. Il découle par récurrence sur k, et du théorème 6.1 (démontré plus loin), que la série génératrice de l'espèce F^k est

$$F^k(y) = \left(F(y)\right)^k. \tag{6.43}$$

Dans le cas où $F[\emptyset] = \emptyset$, c'est-à-dire qu'il n'y a pas de structure d'espèce F sur l'ensemble vide, les ensembles B_k doivent tous être non vides. En conséquence, on a forcément

$$F^k[A] = \emptyset,$$

si $k > |A|$. Cette dernière observation permet d'introduire l'espèce des **listes de F-structures**, lorsque $F[\emptyset] = \emptyset$:

$$\mathbb{L}(F) := \mathbb{1} + F + F^2 + F^3 + \ldots \tag{6.44}$$

puisque notre discussion assure que l'ensemble $\mathbb{L}(F)[A]$ est fini. En effet, on a

$$\mathbb{1}[A] + F[A] + \ldots = \Big(\mathbb{1}[A] + F[A] + \ldots + F^n[A]\Big) + \emptyset + \emptyset + \ldots,$$

si $n = |A|$. Pour l'espèce $\mathbb{L}(F)$, il découle de du théorème 6.1 qu'on a la série

$$\begin{aligned} \mathbb{L}(F)(y) &= \mathbb{1}(y) + F(y) + F^2(y) + F^3(y) + \dots && (6.45)\\ &= 1 + F(y) + (F(y))^2 + (F(y))^3 + \dots && (6.46)\\ &= \frac{1}{1 - F(y)} && (6.47) \end{aligned}$$

Si on choisit $F = \mathsf{Y}$, alors on obtient une décomposition de l'espèce [3] $\mathbb{L}$ des **ordres linéaires** (que nous avons déjà considérée au Chapitre 2) sous la forme :

$$\mathbb{L} = \mathbb{1} + \mathsf{Y} + \mathsf{Y}^2 + \mathsf{Y}^3 + \ \dots \tag{6.48}$$

Ici, Y^k correspondent à l'espèce des **listes de longueur** k. En fait Y^k coïncide avec la restriction $\mathbb{L}_k$ de l'espèce des listes au cardinal k.

6.7 Dessins de structures génériques.

Pour ne pas tomber dans un excès de formalisme risquant d'obscurcir inutilement les raisonnements, il est agréable et efficace de présenter les arguments en terme de dessins qui présentent un exemple typique de structure de l'espèce considérée. C'est d'ailleurs ce que nous avons fait depuis le début pour des espèces spécifiques comme celles des partitions (Part), des graphes orientés (Gro), ou encore des endofonctions (End).

Il est intéressant d'étendre cette habitude aux nouvelles espèces introduites par des opérations combinatoires. Par exemple, il semble tout naturel de présenter une structure d'espèce E^5 (définie en (6.42)) sur l'ensemble [15] comme on le fait à la figure 6.3. Pour systématiser un peu cette

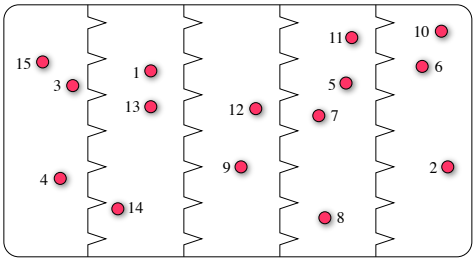


FIGURE 6.3 – Une structure d'espèce E^5.

façon de faire, et afin de décrire diverses opérations et manipulations générales sur les espèces

3. L'égalité énoncée ici est en fait une identité combinatoire comme nous allons le voir à la section sur la substitution des espèces.

de façon plus conviviale, on adopte souvent une présentation « par le dessin » des structures « génériques » d'espèces abstraites F, G, ect.

Le dessin de la Figure 6.4 représente un élément typique de l'ensemble $F[A]$. Ici les divers éléments de A sont apparaissent comme des tiges auxquelles sont rattachées des points rouges. L'arc de cercle (avec son indice F) symbolise abstraitement le fait qu'on a une certaine structure d'espèce F sur ces éléments. Une autre possibilité de représentation abstraite de F-structures sur un ensemble

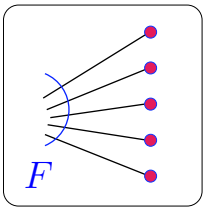


FIGURE 6.4 – Dessin d'une structure générique d'espèce F.

consiste simplement à superposer le symbole F sur cet ensemble, tel qu'illustré à la figure 6.5.

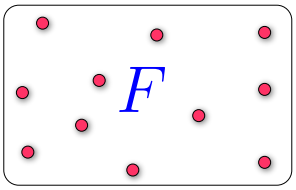


FIGURE 6.5 – Autre présentation d'une structure générique d'espèce F.

On peut alors reformuler, en ces termes plus imagés, la définition d'addition d'espèces, comme on l'a fait à la figure 6.6. De même, soit par la figure 6.7, soit par la figure 6.8, on peut reformuler

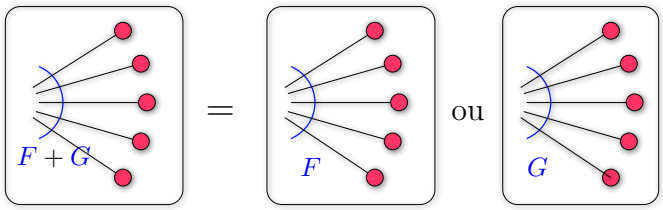


FIGURE 6.6 – Une structure d'espèce $F + G$.

de façon imagée la définition de produit d'espèces : $F \cdot G$. La seconde présentation a l'avantage de mieux mettre en évidence qu'on doit considérer tous les découpages $(A = B + C)$ de l'ensemble A, sans avoir à « déplacer » les éléments de A.

Il y a de nombreux avantages à présenter les choses de ce point de vue plus imagé. En un certain

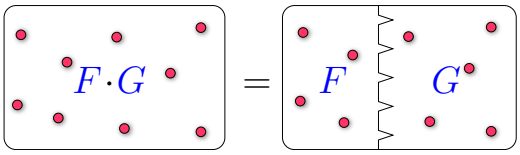


FIGURE 6.7 – Une première façon de présenter une structure d'espèce $F \cdot G$.

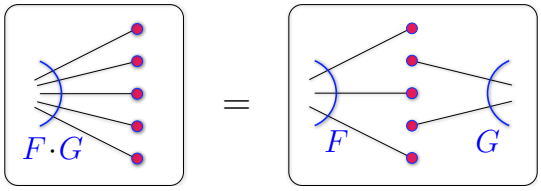


FIGURE 6.8 – Une seconde façon de présenter une structure d'espèce $F \cdot G$.

sens, cela est tout aussi rigoureux si on envisage cette utilisation de figures comme un nouveau genre de formalisme bidimensionnel. En cas de doute, il est toujours possible de revenir à une description rigoureusement ensembliste par une traduction presque directe.

6.8 Passage aux séries.

Observons qu'on a immédiatement $F(y) = G(y)$, si F et G sont des espèces isomorphes. Nous allons maintenant expliquer « pourquoi » la méthode des séries génératrices est si puissante. En fait, en plus d'être compatible avec la notion d'égalité (isomorphisme), une des caractéristiques du passage à la série génératrice est d'être compatible avec les opérations entre espèces. Plus précisément,

Théorème 6.1. *Pour toute espèce F et G, on a*

$$(F+G)(y) = F(y)+G(y), \tag{6.49}$$
$$(F\cdot G)(y) = F(y)\,G(y), \tag{6.50}$$
$$F^n(y) = (F(y))^n, \tag{6.51}$$
$$\mathbb{L}(F)(y) = \frac{1}{1-F(y)}. \tag{6.52}$$

Preuve. La démonstration de ces égalités est directe (modulo les définitions). Par exemple, pour

vérifier (6.50) on procède comme suit

$$\begin{aligned}
(F \cdot G)(y) &= \sum_{n=0}^{\infty} |F \cdot G[n]| \, \frac{y^n}{n!} \\
&= \sum_{n=0}^{\infty} \left| \sum_{B+C=[n]} F[B] \times G[C] \right| \frac{y^n}{n!} \\
&= \sum_{n=0}^{\infty} \sum_{B+C=[n]} |F[B]| \cdot |G[C]| \, \frac{y^n}{n!} \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k} f_k \, g_{n-k} \, \frac{y^n}{n!} \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{f_k}{k!} \, \frac{g_{n-k}}{(n-k)!} \right) y^n \\
&= F(y) \, G(y)
\end{aligned}$$

Les autres démonstrations sont laissées en exercice. ■

6.9 Exemples de calcul de séries.

On a par exemple l'isomorphisme $\text{Élém} \simeq \mathsf{Y} \cdot \mathsf{E}$. En effet la donnée d'un élément a de A est clairement équivalente à la donnée du découpage de A en $\{a\} + B$, où $B = A \setminus \{a\}$. On en déduit donc immédiatement que

$$\text{Élém}(y) = y \, \exp(y)$$

Un exemple beaucoup plus intéressant concerne l'espèce Der des **dérangements**. Toute permutation σ de A se décompose (voir la Figure 6.9) en :

i) l'ensemble, disons B, de ses points fixes, et

ii) un dérangement de $A \setminus B$.

Ceci se traduit en un isomorphisme d'espèces :

$$\mathbb{S} \simeq \mathsf{E} \cdot \mathsf{Der}, \tag{6.53}$$

On en déduit que $\mathbb{S}(y) = \mathsf{E}(y) \, \mathsf{Der}(y)$. Comme on connaît les séries génératrices pour les espèces $\mathbb{S}$ et E, on trouve

$$\mathsf{Der}(y) = \frac{\exp(-y)}{1-y}. \tag{6.54}$$

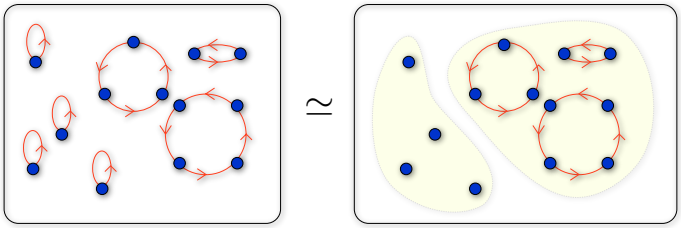


FIGURE 6.9 – Un dérangement.

Il en découle une nouvelle démonstration (sans utiliser le principe d'inclusion-exclusion) du fait que le nombre de dérangements sur un ensemble à n éléments est donné par la formule

$$d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

On peut même définir implicitement une espèce comme solution d'une équation. Par exemple, l'espèce $\mathcal{B}$ des **arbres binaires** (étiquettés) est définie comme étant l'unique [4] solution de l'équation (voir la Figure 6.10)

$$\mathcal{B} = 1 + \mathsf{Y} \cdot \mathcal{B}^2 \tag{6.55}$$

Cette équation est une reformulation directe de l'identité (4.1), et on peut en donner la présentation imagée de la Figure 6.10. Il découle de l'équation (6.55) que

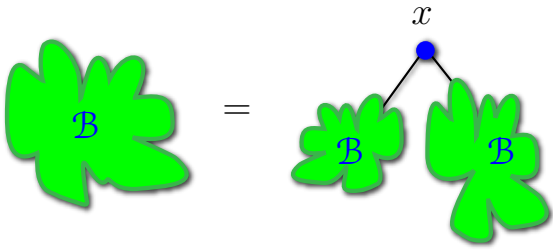


FIGURE 6.10 – Équation pour les arbres binaires.

$$\mathcal{B}(y) = 1 + y\,\mathcal{B}(y)^2$$

dont la solution (la seule admettant un développement en séries à l'origine) est

$$\mathcal{B}(y) = \frac{1 - \sqrt{1 - 4\,y}}{2\,y} = \sum_{n \geq 0} n!\, C_n\, \frac{y^n}{n!}. \tag{6.56}$$

4. Il y a un analogue (à la mode des espèces) du théorème des fonctions implicites qui assure l'existence et l'unicité de cette solution.

Il s'ensuit que le nombre d'arbres binaires (étiquettes) sur $[n]$ est $n!\,C_n$, où C_n est le $n^{\text{ième}}$ nombre de Catalan $\frac{1}{n+1}\binom{2n}{n}$, comme on la vu à la section 4.2.

6.10 Substitution.

L'opération qui est certainement la plus intéressante est celle de **substitution**. Elle a lieu entre une espèce G telle que[5] $G[\emptyset] = \emptyset$, et une espèce F quelconque. On pose

$$F(G)[A] := \sum_{\pi \in \mathsf{Part}[A]} F[\pi] \times \prod_{B \in \pi} G[B], \tag{6.57}$$

où $\mathsf{Part}[A]$ désigne l'ensemble des partitions de A. On peut représenter graphiquement une structure typique d'espèce $F \circ G$ par l'un des dessins de la Figure 6.11.

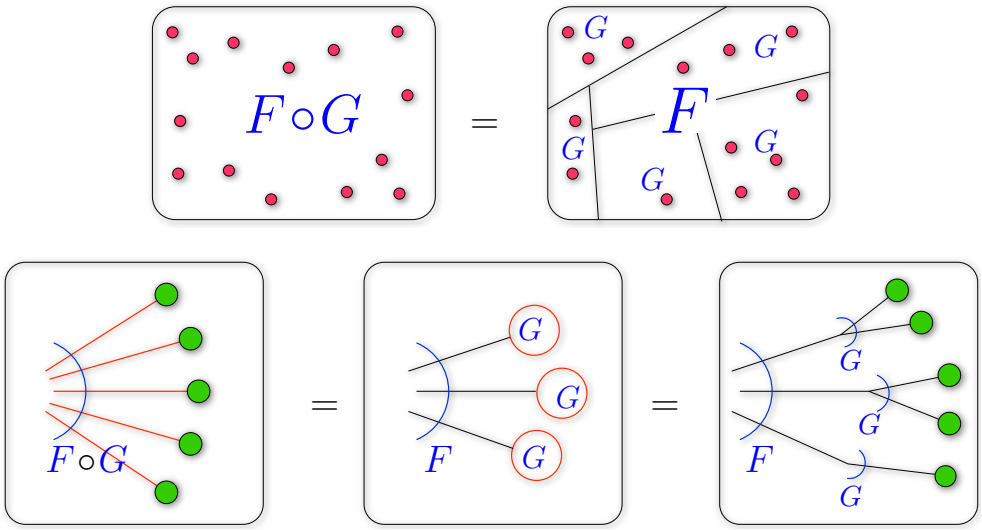


FIGURE 6.11 – Diverses représentations de la substitution.

Il est amusant de constater que nos notations ont été judicieusement choisies pour faire en sorte que

$$F \simeq F(\mathsf{Y}). \tag{6.58}$$

Bien entendu, comme pour les autres opérations, on a compatibilité de la substitution avec le passage aux séries génératrices :

5. Nous allons voir plus loin pourquoi cette condition est nécessaire lorsqu'on veut définir la substitution en toute généralité.

Théorème 6.2. *Pour toute espèce F, et toute espèce G telle que $G[\emptyset] = \emptyset$, on a*

$$(F(G))(y) = F(G(y)). \tag{6.59}$$

Ainsi si

$$F(y) = \sum_{n=0}^{\infty} f_n \frac{y^n}{n!}, \qquad \text{and} \qquad G(y) = \sum_{k=1}^{\infty} g_k \frac{y^k}{k!}$$

alors

$$\begin{aligned} F(G(y)) &= \sum_{n=0}^{\infty} f_n \frac{G(y)^n}{n!}. \\ &= \sum_{n=0}^{\infty} \frac{f_n}{n!} \left(\sum_{k=1}^{\infty} g_k \frac{y^k}{k!} \right)^n \\ &= f_0 + f_1 g_1\, y + (f_2 g_1^2 + f_1 g_2)\frac{y^2}{2!} + (f_3 g_1^3 + 3\, f_2 g_1 g_2 + f_1 g_3)\frac{y^3}{3!} \\ &\qquad + (f_4 g_1^4 + 6\, f_3 g_1^2 g_2 + 4\, f_2 g_1 g_3 + 3\, f_2 {g_2}^2 + f_1 g_4)\frac{y^4}{4!} + \dots \end{aligned}$$

On interprète combinatoirement le terme $6\, f_3\, g_1^2\, g_2$, apparaissant dans le coefficient de $y^4/4!$ du développement de $F(G(y))$, de la façon suivante. Parmi les 15 partitions d'un ensemble à 4 éléments (ici $\{a, b, c, d\}$), il y en a 6 avec deux parties à 1 élément, et une à 2 éléments :

$$\begin{aligned} &\{\{a\}, \{b\}, \{c, d\}\}, \quad \{\{a\}, \{c\}, \{b, d\}\}, \quad \{\{a\}, \{d\}, \{b, c\}\}, \\ &\{\{b\}, \{c\}, \{a, d\}\}, \quad \{\{b\}, \{d\}, \{a, c\}\}, \quad \{\{c\}, \{d\}, \{a, b\}\} \end{aligned}$$

Le nombre de structures d'espèces $F(G)$ pour chacune de ces partitions est $f_3\, g_1^2\, g_2$. On choisit, en effet, une structure d'espèce G sur chacune des parties ce qui peut se faire de $g_1^2\, g_2$ façons. Puis on choisit une structure d'espèce F sur l'ensemble à 3 éléments dont les éléments sont ces parties, ce qui peut se faire de f_3 façons.

6.11 Exemples de substitutions.

1) L'espèce des **partitions** s'obtient comme

$$\mathsf{Part} = \mathsf{E}(\mathsf{E}^+)$$

où E^+ désigne l'espèce des ensembles non vides, c'est-à-dire

$$\mathsf{E}^+[A] = \begin{cases} \{A\} & \text{si} \quad A \neq \emptyset, \\ \\ \emptyset & \text{si} \quad A = \emptyset. \end{cases}$$

Ce qu'on a déjà illustré à la Figure 2.8. On obtient donc

$$\begin{aligned}\mathsf{Part}(y) &= \exp(\exp(y)-1)\\ &= 1+y+2\,\frac{y^2}{2!}+5\,\frac{y^3}{3!}+15\,\frac{y^4}{4!}+52\,\frac{y^5}{5!}+203\,\frac{y^6}{6!}+877\,\frac{y^7}{7!}+4140\,\frac{y^8}{8!}+21147\,\frac{y^9}{9!}+\dots\end{aligned}$$

Les 5 structures d'espèce Part sur l'ensemble $\{a,b,c\}$ sont :

$$\{\{a,b,c\}\},\ \{\{a,b\},\{c\}\},\ \{\{a,c\},\{b\}\},\ \{\{a\},\{b,c\}\},\ \{\{a\},\{b\},\{c\}\}$$

2) La Figure 6.12 montre « comment » l'espèce des permutations est égale à l'espèce des **ensembles de cycles** $\mathsf{E}(\mathcal{C})$ où $\mathcal{C}$ est l'espèce des **cycles** (**permutations circulaires**). Rappelons qu'une

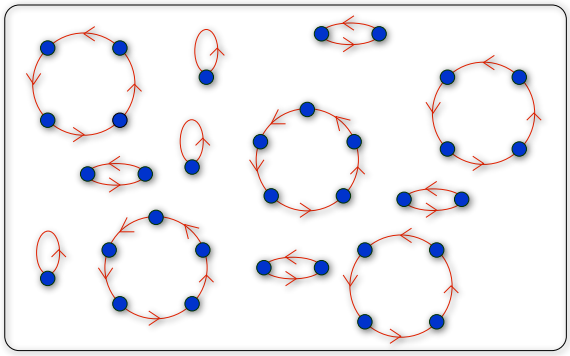


FIGURE 6.12 – Une permutation est un ensemble de cycles.

permutation σ de A est dite circulaire si et seulement si, pour chaque $x,x'\in A$, on peut passer de x à x' en itérant σ, c'est-à-dire qu'il existe un certain entier k tel que

$$\sigma^k(x)=x'.$$

On a donc

$$\begin{aligned}e^{\mathcal{C}(y)} &= \mathbb{S}(y)\\ &= \frac{1}{1-y},\end{aligned}$$

d'où

$$\mathcal{C}(y)=\log\frac{1}{1-y},$$

comme on l'a déjà annoncé. Ce résultat est consistant avec le fait que $|\mathcal{C}[n]|=(n-1)!$, $n\geq 1$, puisque l'égalité

$$-\log(1-y)=\sum_{n\geq 1}\frac{y^n}{n}$$

découle du développement en série bien connu

$$\log(1+y) = \sum_{n\geq 1} (-1)^{n+1} \frac{y^n}{n}.$$

6.12 L'espèce des arborescences.

On peut définir l'espèce $\mathcal{A}$, des **arborescences**, comme solution de l'équation fonctionnelle

$$\mathcal{A} \simeq \mathsf{Y} \cdot \mathsf{E}(\mathcal{A}). \tag{6.60}$$

Ceci correspond à décrire récursivement une arborescence comme étant constituée d'une racine (un point de A) à laquelle sont attachées des branches (arborescences sur des sous-ensembles) comme l'illustre la Figure 6.13. On a donc

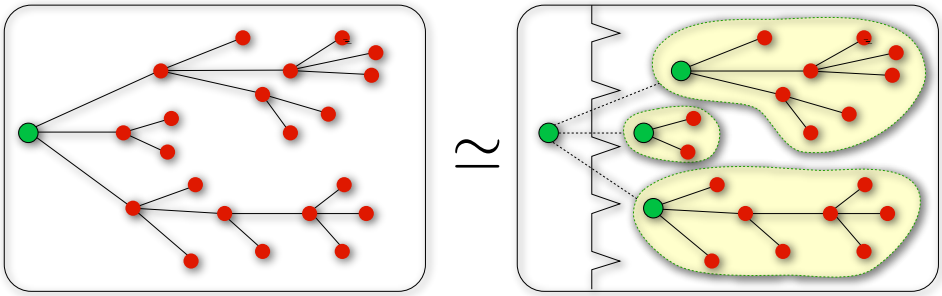


FIGURE 6.13 – Une arborescence « est » un ensemble d'arborescences attachées à une racine.

$$\mathcal{A}(y) = y\, e^{\mathcal{A}(y)}. \tag{6.61}$$

Comme on l'a vu à la Section 2.8, l'espèce des arborescences intervient aussi dans la description de l'espèce des endofonctions. En effet, la décomposition de la Figure 2.22 correspond à l'isomorphisme d'espèce $\mathsf{End} \simeq \mathbb{S}(\mathcal{A})$. En passant aux séries, on trouve ce qui donne

$$\mathsf{End}(y) = \frac{1}{1-\mathcal{A}(y)}. \tag{6.62}$$

Nous allons voir que cette identité permet de calculer le nombre d'arborescences à n noeuds. Introduisons d'abord deux autres opérations de base sur les espèces.

6.13 Dérivée et pointage.

Les dernières opérations que l'on considère ici sont la **dérivée** et le **pointage** d'une espèce. Bien entendu, il y aura encore une fois compatibilité avec le passage aux séries. Pour une espèce quelconque

F, les structures d'espèce F' sur un ensemble fini A sont simplement les structures d'espèces F sur l'ensemble $A + \{*\}$. Une structure typique d'espèce F' peut donc se représenter à la Figure 6.14. Le dessin qui suit montre que la dérivée de l'espèce des cycles peut s'identifier à l'espèce des

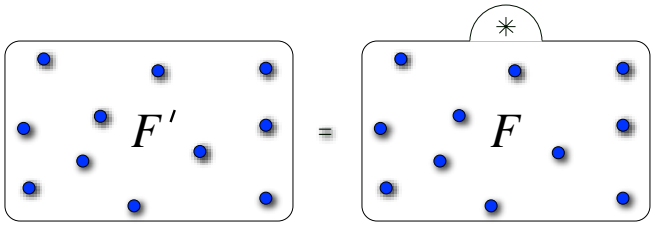
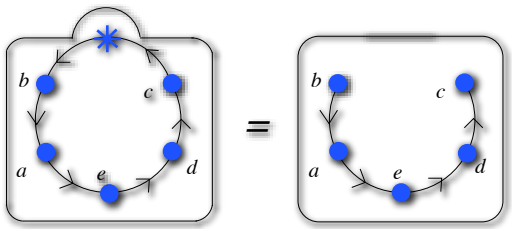


FIGURE 6.14 – Une structure typique d'espèce F'.

ordres linéaires. En formule, $\mathcal{C}' \simeq \mathbb{L}$, ce qui est exactement ce qu'on constate en passant aux séries



génératrices correspondantes :

$$\frac{d}{dy}\log\frac{1}{1-y} = \frac{1}{1-y}.$$

Le **pointage** d'une espèce est défini via la dérivée et la multiplication par Y, de la façon suivante. L'espèce $F^\bullet$ des F structures **pointées** est

$$F^\bullet := \mathsf{Y} \cdot F'.$$

Autrement dit, une $F^\bullet$-structure sur A est la donnée d'une F-structure sur A avec en plus le choix d'un point de A. Cette donnée s'identifie au choix de x dans A avec une F'-structure sur $A \setminus \{x\}$ (voir la Figure 6.15). La justification de cette terminologie peut se voir par la Figure 6.15. La Figure 6.16 montre qu'une arborescence est un arbre [6] pointé. On a donc

$$\mathsf{Arb}^\bullet = \mathsf{Y} \cdot \mathcal{A}', \tag{6.63}$$

si Arb désigne l'**espèce des arbres**. Comme en général, pour $F(y) = \sum_{n=0}^{\infty} f_n\, y^n/n!$, on a

$$F^\bullet(y) = \sum_{n=1}^{\infty} n\, f_n\, \frac{y^n}{n!},$$

6. Graphe simple connexe sans cycle.

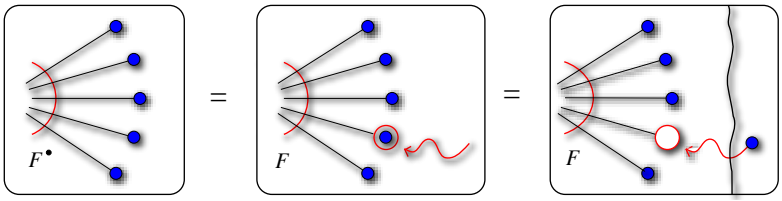


FIGURE 6.15 – Une structure typique d'espèce $F^\bullet$.

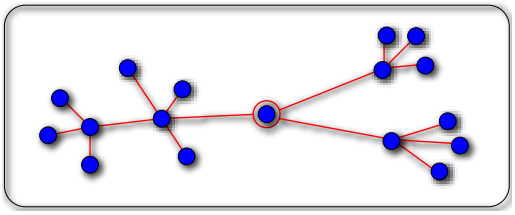


FIGURE 6.16 – Arborescence « est » un arbre pointé.

il découle de (6.63) que le nombre d'arbres à n noeuds est a_n/n (avec $n \geq 1$), où a_n désigne le nombre d'arborescences à n noeuds. Nous allons maintenant calculer a_n.

6.14 Vertébrés.

Notre énumération des arborescences passe par un argument élégant [7], faisant appel à l'espèce des « vertébrés ». Un **vertébré** est une arborescence pointée, c'est-è-dire que l'espèce $\mathcal{V}$ des vertébrés est : $\mathcal{V} := \mathcal{A}^\bullet$. On dit de la racine de l'arborescence que c'est la **tête** du vertébré. La **queue** est le noeud pointé dans l'arborescence. Il est tout à fait possible que ces deux sommets soient confondus. L'unique chemin qui joint la tête à la queue est la **colonne vertébrale** du vertébré. Bien entendu, on dit des noeuds qui se trouvent sur cette colonne vertébrale que ce sont les **vertèbres** du vertébré. (voir Figure 6.17).

Dénotons ν_n, le nombre de vertébrés sur un ensemble de cardinal n. Il est clair que $\nu_n = n\,|\mathcal{A}[n]|$, puisqu'il y a n choix possibles pour la queue. Calculons maintenant ν_n d'une autre façon. On oriente la colonne vertébrale de la tête vers la queue. Puisque à chaque vertèbre est attachée une arborescence, on obtient ainsi une liste non vide d'arborescences disjointes, comme il est illustré à la Figure 6.18).

On met ainsi en évidence l'isomorphisme d'espèces

$$\mathcal{V} \simeq \mathbb{L}^+(\mathcal{A}).\,, \tag{6.64}$$

7. Due à André Joyal.

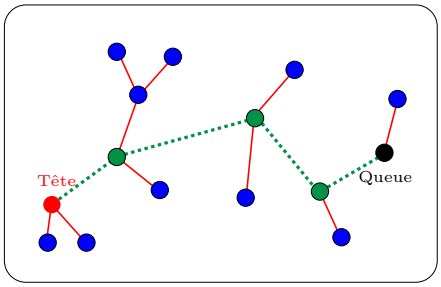


FIGURE 6.17 – Un vertébré.

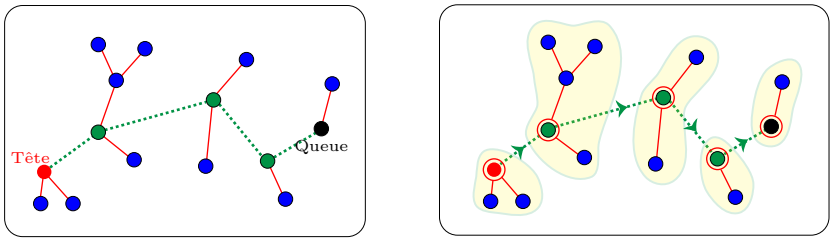


FIGURE 6.18 – Un vertébré transformé en liste d'arborescences.

de façon imagée. En passant aux séries génératrices associées, on trouve

$$\mathcal{V}(y) = \frac{\mathcal{A}(y)}{1 - \mathcal{A}(y)}. \tag{6.65}$$

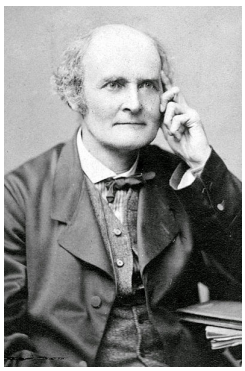
Observons en passant que cette identité se déduit aussi directement de (6.60) par dérivation (voir Exercice 6.12).

D'autre part, il découle directement de (6.62) qu'on a aussi

$$\mathsf{End}^+(y) = \frac{\mathcal{A}(y)}{1 - \mathcal{A}(y)} = \mathcal{V}(y). \tag{6.66}$$

On en déduit donc que le nombre de vertébrés à n sommets est égal au nombre d'endofonctions sur un ensemble à n éléments, c.-à-d. : $\nu_n = n^n$, et finalement on a

Proposition 6.3 (Cayley 1889)**.** *Le nombre d'arborescences à n noeud est n^{n-1}.*



Arthur Cayley
(1821–1895)

6.15 Isomorphisme de structures et types de structures.

On dit que deux structures $s, t \in F[A]$ sont **isomorphes** si et seulement si il existe une permutation $\sigma : A \to A$ qui transporte s sur t. Plus précisément,

$$t = F_\sigma(s).$$

On écrit alors $s \sim t$, et on dit aussi que s et t ont même forme (elles sont $\iota\sigma o$ (iso : « même » en grec) $\mu o \rho \phi \eta$ (morphe : « forme » en grec)). L'isomorphisme de structures est une relation d'équivalence, c'est-à-dire que

1. $s \sim s$
2. si $s \sim t$, alors $t \sim s$
3. si $s \sim t$ et $t \sim r$, alors $s \sim r$

On dit d'une classe d'équivalence, selon la relation $\sim$, que c'est un **type** de F-structures. Décrire un type correspond donc à décrire l'ensemble de toutes les F-structures isomorphes à une F-structures données. **L'ensemble des types de F-structures**, sur un ensemble A, est dont l'ensemble quotient (voir (2.7))

$$F[A]/\sim,$$

de $F[A]$ par la relation d'équivalence considérée ci-haut.

Très souvent [8] les éléments de A apparaissent comme étiquettes dans les structures d'espèce F. Autrement dit, on a $s \sim t$ si et seulement si on peut obtenir t à partir de s en permutant judicieusement ces étiquettes. Dans ce cas, on peut décrire agréablement un type de F-structure en éliminant tout simplement les étiquettes des structures. Les diverses structures d'un type donné s'obtiennent alors en replaçant les étiquettes de toutes les façons possibles. Voilà pourquoi on dit dans ce cas qu'un type (ou une forme) correspond à une structure **non étiquetée**. On identifie donc les éléments de $F[A]/\sim$ et les F-structures non étiquetées.

Par exemple, on a les diverses structures non étiquetées de la Figure 6.19. Dans certains cas ces structures non étiquetées peuvent être décrites plus simplement, puisque le fait d'enlever les étiquettes rend la structure presque inutile. On dit qu'il n'en reste que la **forme**. Ainsi, on a déjà vu que la forme d'une permutation (ainsi que la forme d'une partition) peut être décrite en donnant simplement la liste en ordre décroissant des taille de ses cycles (parts), à savoir comme partage.

6.16 Énumération de structures non étiquetées

L'énumération des types de F-structures (ou des formes de F-structures) correspond donc à l'énumération des structures non-étiquetées. L'outil qui y est adapté est la **série génératrice des**

8. Comme pour l'exemple des arbres binaires de la Section 4.2, ou encore celle des graphes de la Section 6.1.

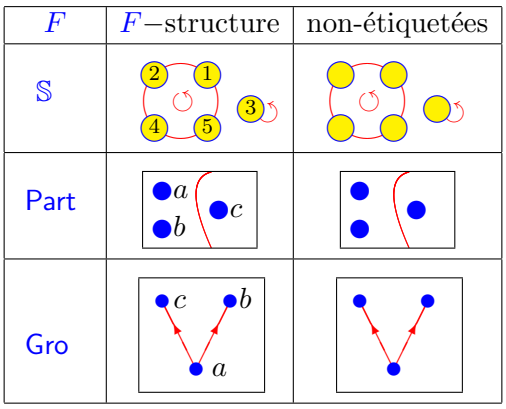


FIGURE 6.19 – F-structures non étiquetées.

types :

$$\widetilde{F}(y) := \sum_{n=0}^{\infty} \widetilde{f}_n \, y^n \,, \tag{6.67}$$

où $\widetilde{f}_n$ correspond au nombre de types de F-structures, c.-à-d. : le cardinal de $F[n]/\sim$. Remarquons qu'on a ici une série génératrice ordinaire (plutôt qu'exponentielle). Nous allons voir ci-dessous en quoi cela est naturel.

En général, il est bien reconnu que le calcul des séries $\widetilde{F}(y)$ est beaucoup plus ardu que celui des séries $F(y)$. C'est Pólya qui a le premier proposé une approche systématique pour ce faire. Une des forces de la théorie des espèces est d'intégrer naturellement son approche. Le lecteur intéressé est référé à [6] pour plus de détails là-dessus.

Bien que la discussion générale de l'approche de Pólya (dans le cadre de la théorie des espèces) dépasse le niveau de notre exposé, un cas est cependant particulièrement facile et accessible. C'est celui des **espèces rigides**. On dit que l'espèce F est rigide si et seulement si, chaque F-structure n'admet qu'un et un seul automorphisme. Il en découle (voir Exercice 6.1) que chaque classe d'équivalence de $F[A]$, selon la relation $\ll \sim \gg$, contient exactement $n!$ F-structures, et on trouve

$$\widetilde{f}_n = \frac{f_n}{n!}.$$

Il en découle que

Proposition 6.4. *Si F est une espèce rigide, alors*

$$\widetilde{F}(y) = F(y). \tag{6.68}$$

Les espèces O, $\mathbb{1}$, Y, $\mathbb{L}$, $\mathcal{B}$, et Plan sont rigides, tandis que les espèces E, $\mathbb{S}$ et Part ne le sont pas. On peut d'ailleurs calculer directement (voir Exercice 6.16) que

$$\widetilde{\mathsf{E}}(y) = \frac{1}{1-y}, \tag{6.69}$$

$$\widetilde{\mathbb{S}}(y) = \widetilde{\mathsf{Part}}(y) = \prod_{k\geq 1} \frac{1}{1-y^k}. \tag{6.70}$$

D'autre part, il est facile de vérifier que

Théorème 6.5. *Pour toute espèce F et G, on a*

$$\widetilde{(F+G)}(y) = \widetilde{F}(y) + \widetilde{G}(y), \tag{6.71}$$

$$\widetilde{(F\cdot G)}(y) = \widetilde{F}(y)\,\widetilde{G}(y), \tag{6.72}$$

$$\widetilde{F^n}(y) = (\widetilde{F}(y))^n, \tag{6.73}$$

$$\widetilde{\mathbb{L}(F)}(y) = \frac{1}{1-\widetilde{F}(y)}. \tag{6.74}$$

Attention cependant, l'énoncé analogue pour la substitution n'est pas vrai en général. C'est-à-dire que, la plupart du temps, on a

$$\widetilde{(F(G))}(y) \neq \widetilde{F}(\widetilde{G}(y)). \tag{6.75}$$

En général, le calcul de la série $\widetilde{(F(G))}(y)$ est difficile et nécessite, sous une forme ou une autre, de passer par la théorie de Pólya. Dans le cadre de la théorie des espèces, une adaptation de cette approche prend la forme des séries indicatrices de cycles de Joyal-Pólya (pour plus de détails, voir [6]). Par le biais de cette approche, on montre par exemple la proposition suivante [9].

Proposition 6.6. *Pour toute espèce G, telle que $G[0] = \emptyset$, on a*

$$\widetilde{\mathsf{E}(G)}(z) = \exp\Big(\sum_{n\geq 1} \widetilde{G}(z^n)/n\Big). \tag{6.76}$$

9. Il est peut-être utile d'insister sur le fait que la Proposition 6.6 n'est qu'un cas très particulier de calculs rendus possibles par les séries indicatrices de cycles. La clé de leurs efficacités passe par le fait qu'on est en mesure de formuler, pour ces séries qui ne sont pas définies ici, une identité concernant la substitution d'espèces en général.

Par exemple, on peut utiliser cette proposition pour calculer que

$$\begin{aligned}
\widetilde{\mathsf{Part}}(y) &= \widetilde{\mathsf{E}(\mathsf{E}^+)}(y) \\
&= \exp\left(\sum_{n\geq 1} \frac{y^n}{n\,(1-y^n)}\right) \\
&= \exp\left(\sum_{n\geq 1}\sum_{k\geq 1} \frac{y^{n\,k}}{n}\right) \\
&= \exp\left(\sum_{k\geq 1}\sum_{n\geq 1} \frac{y^{k\,n}}{n}\right) \\
&= \exp\left(\sum_{k\geq 1} \log\frac{1}{1-y^k}\right) \\
&= \prod_{k\geq 1} \frac{1}{1-y^k}
\end{aligned}$$

ce qui redonne une des identités de (6.70).

6.17 Espèces à plusieurs sortes

Il est naturel et utile d'étendre la notion d'espèces aux cas multi sorte. C'est l'analogue, pour les espèces, des fonctions de plusieurs variables. Considérons le cas des **espèces à deux sortes**. La description est semblable à celle des espèces :

1) pour chaque ensemble, finis A et B, on se donne un ensemble $F[A,B]$, et
2) pour chaque paire de bijections $\sigma_1 : A_1 \to A_2$ et $\sigma_2 : B_1 \to B_2$, on a une bijection

$$F_{\sigma_1,\sigma_2} : F[A_1,B_1] \xrightarrow{\sim} F[A_2,B_2],$$

satisfaisant les conditions

a) la bijection $F[\mathrm{Id}_A,\mathrm{Id}_B]$ est l'identité de $F[A,B]$, et
b) la bijection $F_{\sigma_1\circ\tau_1,\sigma_2\circ\tau_2}$ est toujours égale au composé des bijections F_{σ_1,σ_2} et F_{τ_1,τ_2}.

Par exemple, on a les espèces $\mathsf{Bij}[A,B]$, $\mathsf{Inj}[A,B]$, et $\mathsf{Surj}[A,B]$. Pour une espèce F à deux sortes, on a la série génératrice

$$F(y,z) := \sum_{n,k\geq 0} f_{n,k}\,\frac{y^n}{n!}\,\frac{z^k}{k!}, \tag{6.77}$$

où $f_{n,k}$ est le cardinal de $F[A,B]$, pour A de cardinal n et B de cardinal k. Il est facile de vérifier que

$$\mathsf{Bij}(y,z) = \exp(y\,z), \tag{6.78}$$

L'extension à k sortes de ces définitions est directe. Bien entendu, avec les modifications nécessaires, on étend aussi les opérations entre espèces à ce contexte multi sortes.

En s'inspirant de l'identité (6.58), il devient naturel de dénoter $F(\mathsf{Y},\mathsf{Z})$ une espèce à deux sortes, avec Y pour l'espèce des singletons de la première sorte, et Z celle des singletons de la seconde sorte. C'est-à-dire qu'on a

$$\mathsf{Z}[A,B] := \begin{cases} \{B\} & \text{si, } |B|=1 \quad \text{et} \quad A=\emptyset, \\ \emptyset & \text{sinon,} \end{cases} \tag{6.79}$$

avec une définition analogue pour Y. On a alors les isomorphismes d'espèces à deux sortes :

$$\begin{aligned} \mathsf{Bij}(\mathsf{Y},\mathsf{Z}) &\simeq \mathsf{E}(\mathsf{Y}\cdot\mathsf{Z}), && (6.80)\\ \mathsf{Inj}(\mathsf{Y},\mathsf{Z}) &\simeq \mathsf{E}((\mathbb{1}+\mathsf{Y})\cdot\mathsf{Z}), && (6.81)\\ \mathsf{Surj}(\mathsf{Y},\mathsf{Z}) &\simeq \mathsf{E}(\mathsf{E}^+(\mathsf{Y})\cdot\mathsf{Z}), && (6.82)\\ \mathsf{Fonct}(\mathsf{Y},\mathsf{Z}) &\simeq \mathsf{E}(\mathsf{E}(\mathsf{Y})\cdot\mathsf{Z}). && (6.83) \end{aligned}$$

Il s'ensuit qu'en plus de (6.78), on a

$$\begin{aligned} \mathsf{Inj}(y,z) &= \exp((1+y)\,z), && (6.84)\\ \mathsf{Surj}(y,z) &= \exp((\exp(y)-1)\,z), && (6.85)\\ \mathsf{Fonct}(y,z) &= \exp(\exp(y)\,z). && (6.86) \end{aligned}$$

On peut étendre aux espèces à deux (ou plusieurs) sortes l'énumération selon le type, et une version

étendue de la Proposition 6.6 donne que

$$\begin{aligned}
\widetilde{\mathsf{Inj}}(y,z) &= \exp\left(\sum_{n\geq 1}\frac{(1+y^n)\,z^n)}{n}\right),\\
&= \frac{1}{(1-z)(1-y\,z)}, \qquad (6.87)\\
\widetilde{\mathsf{Surj}}(y,z) &= \exp\left(\sum_{n\geq 1}\frac{y^n\,z^n}{n\,(1-y^n)}\right),\\
&= \prod_{k\geq 1}\frac{1}{1-z\,y^k}, \qquad (6.88)\\
\widetilde{\mathsf{Fonct}}(y,z) &= \exp\left(\sum_{n\geq 1}\frac{y^n\,z^n}{n\,(1-y^n)}\right),\\
&= \prod_{k\geq 0}\frac{1}{1-z\,y^k}. \qquad (6.89)
\end{aligned}$$

6.18 Exercices

6.1. En utilisant le principe des tiroirs, montrer qu'une F-structure sur A admet forcément un autre automorphisme que l'identité, lorsque le cardinal de sa classe d'équivalence selon $\ll \sim \gg$ est plus petit que $n!$ ($n = |A|$). Suggestion : Voir d'abord qu'il y a forcément deux permutations σ et τ de A, telles que $\sigma \cdot s = \tau \cdot s$, pour s dans $F[A]$.

6.2. Montrer que, pour les bijections (6.40), la propriété (6.90) est satisfaite pour toute bijection σ de A vers B, c.-à-d. :

$$\pi_B \circ (\mathsf{E}\cdot\mathsf{E})_\sigma = \mathcal{P}_\sigma \circ \pi_A. \qquad (6.90)$$

6.3. Trouver le nombre

a) d'involutions sans point fixe de $[n]$, c.-à-d. $\sigma : [n] \to [n], \sigma^2 = \mathrm{Id}_{[n]}, \sigma(i) \neq i$ pour tout i,

b) d'involutions de $[n]$, c.-à-d. $\sigma : [n] \to [n]$, $\sigma^2 = id$,

c) de permutations de $[n]$ dont tous les cycles sont de longueur paire,

d) de permutations de $[n]$ dont tous les cycles sont de longueur impaire.

6.4. Soit Gra (resp. Gra^c) l'espèce des graphes simples (resp. des graphes simples connexes).

a) Montrer que

$$|\mathsf{Gra}[n]| = 2^{\binom{n}{2}}$$

b) Montrer que $\mathsf{Gra}^\bullet \simeq (\mathsf{Gra}^c)^\bullet \cdot \mathsf{Gra}$.

c) Soit γ_n le nombre de graphes simples connexes sur $[n]$ (i.e. $\gamma_n = |(\mathsf{Gra}^c)[n]|$).

Déduire une récurrence donnant γ_n en terme de $\gamma_{n-1}, \gamma_{n-2}, \ldots, \gamma_2, \gamma_1$. (On pose $\gamma_0 = 0$.)

6.5. Trouver une expression simple pour $T(z)$ où T est l'espèce des permutations σ telles que $\sigma^4 = \mathrm{Id}$. Même question pour l'espèce $T^{(k)}$ des permutations σ telles que $\sigma^k = \mathrm{Id}$, pour $k \geq 1$.

6.6. Soit $\mathbb{S}$ l'espèce des permutations et $\mathbb{L}$ l'espèce des ordres linéaires. Prouver que

$$\mathbb{S}' \simeq \mathbb{L} \cdot \mathbb{S}. \tag{6.91}$$

6.7. Trouver la série génératrice exponentielle des nombres de dérangements $d_n := \#\mathsf{Der}[n]$, c.-à-d. : la série de l'espèce des dérangements.

6.8. Soit $\mathcal{C}^{(3)}$ l'espèce des permutations cycliques de longueur un multiple de trois et $\mathbb{S}^{(3)}$ celle des permutations à cycles de longueur un multiple de trois. Trouver des expressions simples pour les séries génératrices exponentielles $\mathcal{C}^{(3)}(z)$ et $\mathbb{S}^{(3)}(z)$ de ces espèces.

6.9. Décrire le transport de structures pour les espèces, E, $\mathsf{Élém}$, $\mathcal{P}$, End, $\mathbb{S}$, et Gra.

6.10. Vérifier que la série génératrice de l'espèce $\mathbb{L}$ est la même que celle pour $\mathbb{S}$.

6.11. Montrer que

a) $(F + G)' \simeq F' + G'$,

b) $(F \cdot G)' \simeq F'\,G + F \cdot G'$,

c) $(F \circ G)' \simeq (F' \circ G)\,G'$,

d) $(F + G)^\bullet \simeq F^\bullet + G^\bullet$,

e) $(F \cdot G)^\bullet \simeq F^\bullet\,G + F \cdot G^\bullet$.

6.12. Montrer que (6.65) se déduit de (6.60) en pointant les espèces de chaque membre de l'égalité. Suggestion : Utiliser l'exercice précédent.

6.13. Montrer que le nombre de types de structures d'espèce $\mathbb{L}$ sur n sommets est toujours 1.

6.14. Montrer que le nombre de types de structures d'espèce $\mathbb{S}$ sur n sommets est > 1, si $n > 2$. En conclure que les espèces $\mathbb{S}$ et $\mathbb{L}$ sont différentes.

6.15. Montrer qu'aucune famille de bijections entre $\mathbb{S}[A]$ et $\mathbb{L}[A]$ n'est compatible avec le transport de structures.

6.16. Directement à partir de la définition, calculer $\widetilde{\mathsf{E}}(z)$; et calculer , $\widetilde{\mathbb{S}}(z)$, et $\widetilde{\mathsf{Part}}(z)$, en utilisant les Propositions 5.3 et 5.6. Vérifier aussi qu'on a

$$\widetilde{\mathcal{C}}(z) = \frac{z}{1-z}. \tag{6.92}$$

6.17. le Théorème 6.5 et la Proposition 6.4 pour calculer qu'on a les séries génératrices des types :

$$\widetilde{\mathcal{P}}(z) = \left(\frac{1}{1-z}\right)^2, \tag{6.93}$$

$$\widetilde{\mathcal{P}_k}(z) = \frac{z^k}{1-z}, \tag{6.94}$$

$$\widetilde{\mathsf{Inv}}(z) = \frac{1}{(1-z)(1-z^2)}, \tag{6.95}$$

$$\widetilde{\mathsf{Der}}(z) = \prod_{k\geq 2} \frac{1}{1-z^k}, \tag{6.96}$$

$$\widetilde{\text{Élém}}(z) = \frac{z}{1-z}, \tag{6.97}$$

$$\tag{6.98}$$

6.18. Montrer qu'on a

$$\mathsf{Surj}(y,z) = \exp\big(z\,(\exp(y)-1)\big). \tag{6.99}$$

Programmation mathématique

6.19. Pour chacune des espèces de ce chapitre, concevoir une procédure qui

a) Calcule toutes les structures de cette espèce sur un ensemble A.

b) Effectue le transport de structures correspondant le long d'une bijection $\sigma : A \to B$.

6.20. Étant donné qu'on a des procédures calculant les structures d'espèces F et G, construire des procédures qui calculent les structures d'espèces $F+G$, $F\cdot G$, et $F\cdot G$ sur un ensemble A.

Annexe A

Calcul formel

A.1 Introduction

Les systèmes de calcul formel permettent de manipuler concrètement des objets mathématiques abstraits de façon rigoureuse. Cela va des nombres entiers, rationnels, réels ou complexes (et des calculs sur ceux-ci) ; à des manipulations d'opérateurs sur des espaces de fonctions ; en passant par un vaste spectre de notions mathématiques de l'algèbre, du calcul, de l'analyse complexe, de la théorie des nombres, etc.

Dans les systèmes de calcul formel, une session de travail est habituellement un processus interactif qui consiste à donner au système une instruction de calcul (apparaissant en rouge dans ce qui suit), et on obtient alors comme résultat la valeur du calcul demandé (apparaissant en bleu). Dans notre cas, le système affiche automatiquement le symbole « > » chaque fois qu'il est prêt à effectuer une prochaine instruction. Le « ; » signifie la fin de l'instruction donnée, et la touche « return » (ou « enter ») déclenche le calcul. Ainsi, on peut demander de calculer

$> \gcd(x^{36} - 1, x^{24} - 1)\,;$

$$x^{12} - 1$$

Ici, la fonction Maple « gcd » trouve que $x^{12} - 1$ est un [1] plus grand commun diviseur des polynômes $x^{36} - 1$ et $x^{24} - 1$.

En plus d'effectuer des calculs explicites, il est possible de donner des noms à certains objets au moyen l'assignation « := ». On peut donc poser

$> x := 100\,;$

$$x := 100$$

1. Puisque défini à un multiple scalaire prêt.

Dorénavant, x aura la valeur 100, et l'expression 2^x prendra donc la valeur :

$> \ 2^x$;

$$1267650600228229401496703205376$$

Il faut bien distinguer cette assignation de la relation mathématique usuelle « = » d'égalité.

Aux fins d'une utilisation vraiment efficace des systèmes de calculs formels, la capacité qui est de loin la plus importante est la possibilité de définir de nouvelles fonctions (ou procédures) de calcul, à partir de celles déjà connues. On a ainsi un riche environnement de programmation spécialisée pour les mathématiques. Ces nouvelles fonctions peuvent se définir de nombreuses façons, mais celle qui est la plus naturelle est probablement via la récursivité. Ainsi on peut introduire la fonction :

$> F := n->$
    if $n \leq 1$ then 1
        else $F(n-1) + F(n-2)$
    fi :

Dorénavant, « F » est la fonction d'une variable qui calcule (récursivement) les nombres de Fibonacci. On aura donc :

$> F(20);$

$$10946$$

Les changements de lignes et les espaces supplémentaires n'ont ici aucun effet sur le calcul. Ils ne servent qu'à disposer la description de la fonction « F » de manière plus agréable. Normalement, le résultat d'une telle instruction est d'afficher le texte de la fonction ainsi définie. Le fait d'utiliser le « : », plutôt que le « ; » comme indication de fin de l'instruction, évite cet affichage assez inutile.

Nous allons illustrer dans cette annexe comment il est facile d'utiliser de tels systèmes pour manipuler les objets combinatoires que nous avons rencontrés dans ce texte.

A.2 Théorie des ensembles et calcul formel

Tout système de calcul formel (Sage, Maple, etc.) permet, entre autres, de manipuler des ensembles, des listes, et diverses constructions les concernant (avec les adaptations nécessaires).

Ainsi, on peut donner le nom A à l'ensemble $\{a, b, c\}$ en posant

$> A := \{a, b, a, c, b, b\}$;

$$A := \{a, b, c\}$$

Observons ici (comme le veut la théorie) que la répétition d'un élément n'a aucun effet. Bien entendu, on a aussi les opérations usuelles sur les ensembles

> $\{a, b, c\}$ intersect $\{b, c, d\}$;

$$\{b, c\}$$

> $\{a, b, c\}$ union $\{b, c, d\}$;

$$\{a, b, c, d\}$$

> $\{a, b, c\}$ minus $\{b, c, d\}$;

$$\{a\}$$

En passant, rien n'empêche d'utiliser abstraitement ces opérations sur des ensembles B et C non spécifiés. Ainsi, on obtient

> $(B$ union $D)$ intersect $(C$ union $D)$;

$$(B \cup D) \cap (C \cup D)$$

> B minus B ;

$$\emptyset$$

On peut tester l'égalité d'ensembles, et l'appartenance à un ensemble, en exploitant la fonction « evalb » qui calcule la valeur logique d'une expression. Ainsi, on a

> evalb$(\{a, b, c\} = \{b, c, d\})$;

$$\text{false}$$

> evalb$(\{a, b, c\} = \{b, c, a\})$;

$$\text{true}$$

> b in $\{b, c, a\}$;

$$b \in \{a, b, c\}$$

> evalb$(b$ in $\{b, c, a\})$;

$$\text{true}$$

La fonction « nops » est très générale. Elle permet de compter le nombre d'opérandes dans une expression. En particulier elle donne le nombre d'éléments d'un ensemble. Cependant, pour faciliter la compréhension, il est possible de lui donner un synonyme en posant :

> card := nops :

Par la même occasion, on se permet de mettre en place les autres synonymes :

> '&+' := 'union' :

> '&-' := 'minus' :

L'utilisation du caractère « & », dans « &+ », est nécessaire en Maple lorsqu'on désire considérer de nouveaux opérateurs binaires avec une notation « infixe ». C'est aussi une particularité de la syntaxe de Maple qui forcent l'utilisation des « ‘ » au moment de l'établissement de ces synonymes.

Pour décrire un ensemble de la forme $\{g(x) \mid x \in A\}$, on peut utiliser la fonction Maple « seq » qui permet de construire des séquences de valeurs $g(x)$ pour x variant dans A. Puisque l'ensemble A a déjà été défini (mais pas g), on obtient :

```
> {seq(g(x), x in A)});
```

$$\{g(a), g(b), g(c)\}$$

ou encore, avec la fonction de Fibonacci F :

```
> {seq(F(x), x in {1,2,3,4,5,6,7,8,9})});
```

$$\{1, 2, 3, 5, 8, 13, 21, 34, 55\}$$

Autres opérations. On peut définir d'autres opérations usuelles sur les ensembles comme ci-dessous. Si $A = \{x\} + B$, le calcul de l'ensemble $\mathcal{P}[A]$ des parties de A est basé sur la récurrence :

$$\mathcal{P}[A] = \mathcal{P}[B] \ + \ \{C + \{x\} \mid C \in \mathcal{P}[B]\}. \tag{A.1}$$

Avec une syntaxe légèrement différente de celle déjà utilisée, on exploite cette récurrence pour obtenir la nouvelle fonction

```
> P := proc(A) local x, B :
    if A = {} then {{}}
        else x := op(1, A) :                    (x est le premier élément dans A)
            B := A &- {x} :
            P(B) &+ {seq( C &+ {x}, C in P(B)}
    fi
end :
```

Après avoir considéré le cas spécial $A = \emptyset$, on choisit x comme étant le premier élément de A, et la cinquième ligne reproduit (presque fidèlement) le membre de droite de (A.1). On obtient ainsi une fonction calculant l'ensemble $P(A)$ des parties de A :

```
> P({a, b, c});
```

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Avant de construire le produit cartésien comme opération binaire, on rappelle qu'en Maple un couple, normalement dénoté (x, y) dans des contextes mathématiques, est plutôt dénoté $[x, y]$. Ceci est du au fait que les parenthèses usuelles sont réservées à d'autres fins syntaxiques. On pose donc

```
> '&X' := proc(A, B) local x, y :
      {seq(seq([x, y] , x in A), y in B)}
 end :
```

Alors, on obtient

```
> {a, b, c} &X {a, b} ;
```

$$\{[1,a],[1,b],[2,a],[2,b],[3,a],[3,b]\}$$

et aussi

```
> {a, b, c} &X {} ;
```

$$\emptyset$$

comme il se doit. On peut maintenant obtenir la fonction qui calcule l'ensemble des relations entre A et B, simplement en posant :

```
> Relations := (A, B)-> P(A &X B) :
```

et donc on peut ensuite calculer que

```
> Relations({a, b}, {x, y}) ;
```

$$\{\emptyset,\{[a,x]\},\{[a,y]\},\{[b,x]\},\{[b,y]\},\{[a,x],[a,y]\},\{[a,x],[b,x]\},\{[a,x],[b,y]\},\{[a,y],[b,x]\},$$
$$\{[a,y],[b,y]\},\{[b,x],[b,y]\},\{[a,x],[a,y],[b,x]\},\{[a,x],[a,y],[b,y]\},\{[a,x],[b,x],[b,y]\},$$
$$\{[a,y],[b,x],[b,y]\},\{[a,x],[a,y],[b,x],[b,y]\}\}$$

Pour calculer récursivement l'ensemble des fonctions entre A et B, il suffit de poser

```
> Fonct := (A, B)->
      if A = {} then {{}}
           else x := A[1] :
                {seq(seq(f &+ {x, y} , y in B), f in Fonct(A &- {x}, B))}
      fi :
```

et alors

```
> Fonct({a, b}, {0, 1}) ;
```

$$\{\{[a,0],[b,0]\},\{[a,0],[b,1]\},\{[a,1],[b,0]\},\{[a,1],[b,1]\}\}$$

Une construction similaire permet d'obtenir l'ensemble des mots de longueur k, sur un alphabet A, au moyen de la fonction Maple « cat » qui concatène deux mots.

```
> Mots := (A, k)->
      if k = 1 then A
```

```
        else {seq(seq(cat(w, x) , x in A), w in Mots(A, k - 1))}
    fi :
> Mots({a, b, c}, 3) ;
```

$$\{aaa, aab, aac, aba, abb, abc, aca, acb, acc,$$
$$baa, bab, bac, bba, bbb, bbc, bca, bcb, bcc,$$
$$caa, cab, cac, cba, cbb, cbc, cca, ccb, ccc\}$$

A.3 Le package GFUN

Le package « GFUN » (pour « Generating FUNction ») à été développé par Bruno Salvy et Paul Zimmermann de l'INRIA (un des centres de recherche en informatique les plus importants de France), à partir d'un prototype développé par l'auteur et Simon Plouffe (dans le cadre de son mémoire de Maîtrise). Il consiste en un ensemble d'outils pour la manipulation de récurrences et de fonctions génératrices, et il permet de « deviner » la fonction génératrice d'une suite à partir des premiers termes de celle-ci. Il existe maintenant pour plusieurs systèmes de calcul formels.

On l'ajoute aux fonctionnalités de Maple par la commande :

```
> with(gfun) :
```

Le résultat étant la liste des nouvelles fonctions maintenant disponibles. On peut demander des informations sur chacune d'entre elles avec, par exemple

```
> ?gfun,guessgf
```

Comme premier exemple de son utilisation, considérons le calcul d'une formule pour les coefficients d'une fonction génératrice rationnelle :

$$\frac{P(x)}{Q(x)}.$$

On a

```
> ratpolytocoeff((1 + a x)/(1 - 4 x + 4 x^2), x, n) ;
```

$$4\left(\frac{1}{4}+\frac{1}{8}a\right)\left(\frac{1}{2}\right)^{-n}(n+1)-\frac{1}{2}a\left(\frac{1}{2}\right)^{-n}$$

Plusieurs autres fonctions de ce genre (certaines très puissantes) sont disponibles. On peut utiliser ces fonctions pour découvrir des identités profondes. Cependant, une des utilisations les plus amusantes de « gfun » consiste à deviner des formules.

On suppose ici qu'on a calculé (péniblement) les premières valeurs d'une suite, par exemple en énumérant des objets combinatoires. On connaît donc

$$a_0, a_1, a_2, \ldots, a_N,$$

et c'est tout. Pour l'instant les autres termes de la suite nous sont inconnus. La fonction « guessgf » de « gfun » permet (souvent, mais pas toujours) de deviner le reste de la suite. En fait elle découvre [2] (dans les bons cas) une fonction génératrice pour la suite en question.

Par exemple,

```
> liste_de_nombres:= [1, 1, 3, 19, 145, 1401, 16051, 213403, 3223809, 54514225, 1019601091,
20890209891, 465156779473, 11181638663209, 288536019179955] :
> guessgf(liste_de_nombres,x) ;
```

$$[e^{-x/(x^2+x-1)}, \text{egf}]$$

où « egf » signifie que le résultat est une série génératrice exponentielle. La suite ci-dessus correspond donc aux a_n apparaissant dans développement en série de

$$e^{-x/(x^2+x-1)} = \sum_{n\geq 0} a_n \frac{x^n}{n!}$$

pour $0 \leq n \leq 14$. En effet, on a :

```
> series(exp(x/(1 − x − x^2)), x, 15) ;
```

$$1 + x + \frac{3}{2}x^2 + \frac{19}{6}x^3 + \frac{145}{24}x^4 + \frac{467}{40}x^5 + \frac{16051}{720}x^6 + \frac{213403}{5040}x^7 + \frac{358201}{4480}x^8 + \frac{10902845}{72576}x^9 + \frac{1019601091}{3628800}x^{10} + \frac{6963403297}{13305600}x^{11} + \frac{465156779473}{479001600}x^{12} + \frac{1597376951887}{889574400}x^{13} + \frac{19235734611997}{5811886080}x^{14} + O\left(x^{15}\right)$$

et, on a bien comme coefficients

```
> [seq(liste_de_nombres[i]/(i − 1)!, i = 1..15)] ;
```

$$\left[1, 1, \frac{3}{2}, \frac{19}{6}, \frac{145}{24}, \frac{467}{40}, \frac{16051}{720}, \frac{213403}{5040}, \frac{358201}{4480}, \frac{10902845}{72576}, \frac{1019601091}{3628800}, \frac{6963403297}{13305600}, \frac{465156779473}{479001600}, \frac{1597376951887}{889574400}, \frac{19235734611997}{5811886080}\right]$$

Ceci fonctionne même pour une liste de polynômes (énumération pondérée) :

```
> liste_de_polynomes:= [1, t, t^2 + 2 t, t^3 + 6 t^2 + 6 t, t^4 + 12 t^3 + 36 t^2 + 24 t, t^5 + 20 t^4 + 120 t^3 + 240 t^2 +
120 t, t^6 + 30 t^5 + 300 t^4 + 1200 t^3 + 1800 t^2 + 720 t, t^7 + 42 t^6 + 630 t^5 + 4200 t^4 + 12600 t^3 + 15120 t^2 +
5040 t, t^8 + 56 t^7 + 1176 t^6 + 11760 t^5 + 58800 t^4 + 141120 t^3 + 141120 t^2 + 40320 t, t^9 + 72 t^8 + 2016 t^7 +
28224 t^6 + 211680 t^5 + 846720 t^4 + 1693440 t^3 + 1451520 t^2 + 362880 t] :
```

2. Cela se fait de façon assez simple. On commence par trouver, par une méthode de paramètres indéterminés, une équation différentielle pour la fonction génératrice, puis on utilise Maple pour résoudre cette équation.

> guessgf(liste_de_polynomes,x) ;

$$\left[\frac{e^{-\frac{t}{x-1}}}{e^t}, \text{egf}\right]$$

Cela suggère donc que la suite de polynômes considérés a

$$e^{t\,\frac{x}{1-x}}$$

comme fonction génératrice exponentielle.

A.4 q-analogues

L'utilisation de système de calcul formel permet de faciliter la compréhension d'objets mathématiques nouveaux. En guise d'illustration, on considère ici un peu plus en profondeur la notion de **q-analogues** qui nous avons déjà entrevues à la Section 3.6. En gros, l'idée est de « remplacer » les entiers par des polynômes en la variable q, dont la valeur en 1 redonne les entiers originaux. On dégage alors des identités polynomiales qui généralisent des formules pour les entiers.

On commence par considérer n_q le **q-analogue de l'entier** n :

$$n_q := \frac{q^n - 1}{q - 1} = q^{n-1} + \ldots + q + 1. \tag{A.2}$$

On a donc bien $n_q = n$, lorsque $q = 1$. Désirant définir un opérateur infixe dans notre système de façon à ce que n &. q donne le polynôme n_q, on pose simplement

> '&.' := (n, q)-> normal($(q^n - 1)/(q - 1)$) :

On définit ensuite $n_q!$ le **q-analogue de** $n!$, en posant

$$n_q! := \begin{cases} 1 & \text{si } n = 0, \\ (n-1)_q!\, n_q & \text{si } n > 1. \end{cases} \tag{A.3}$$

Par exemple,

$$\begin{aligned} 5_q! &= 1_q \cdot 2_q \cdot 3_q \cdot 4_q \cdot 5_q \\ &= 1\,(1+q)\,(1+q+q^2)\,(1+q+q^2+q^3)\,(1+q+q^2+q^3+q^4). \end{aligned}$$

Clairement, le polynôme $n_q!$ prend la valeur $n!$ lorsqu'on pose $q = 1$. En fait c'est polynômes coïncidents avec les polynômes indicateurs d'inversion de la Proposition 5.4. Ces polynômes peuvent se calculer comme suit, avec notre système :

```
> '&!' := (n, q)->
      if n = 0 then 1
      else ((n − 1) &! q) * (n &. q) fi :
```

ou encore comme

```
> '&!' := (n, q)->
      if n = 0 then 1
      else mul(k &. q, k = 1..n) fi :
```

Comme le degré k_q est $k-1$ (voir A.2), le degré de $n_q!$ est manifestement égal à

$$\begin{aligned} \deg(n_q!) &= \sum_{k=1}^{n} \deg(k_q) \\ &= \binom{n}{2}, \end{aligned} \tag{A.4}$$

et on a

```
> for n from 0 to 5 do sort(expand(n &! q)) od ;
```

$$1$$
$$1$$
$$q+1$$
$$q^3+2\,q^2+2\,q+1$$
$$q^6+3\,q^5+5\,q^4+6\,q^3+5\,q^2+3\,q+1$$
$$q^{10}+4\,q^9+9\,q^8+15\,q^7+20\,q^6+22\,q^5+20\,q^4+15\,q^3+9\,q^2+4\,q+1$$

Pour calculer à la main avec les polynômes n_q et $n_q!$, il est utile d'apprendre à les factoriser en polynômes irréductibles, à coefficients dans $\mathbb{Z}$. Un système de calcul formel aide à développer une familiarité avec cette factorisation. On calcule d'abord que :

> for k to 9 do n_q=factor(q^k-1) od;

$$
\begin{aligned}
1_q &= 1\\
2_q &= q+1\\
3_q &= q^2+q+1\\
4_q &= (q+1)(q^2+1)\\
5_q &= q^4+q^3+q^2+q+1,\\
6_q &= (q^2+q+1)(q^2-q+1)\\
7_q &= q^6+q^5+q^4+q^3+q^2+q+1\\
8_q &= (q+1)(q^2+1)(q^4+1)\\
9_q &= (q^2+q+1)(q^6+q^3+1)
\end{aligned}
$$

et on observe qu'il y a exactement un facteur « nouveau » dans chaque décomposition. Ceci permet de redécouvrir les **polynômes cyclotomiques**, dénotés $\varphi_n(q)$:

$$
\begin{array}{lllllllll}
\varphi_1(q) &=& q-1, & \varphi_2(q) &=& q+1, & \varphi_3(q) &=& q^2+q+1,\\
\varphi_4(q) &=& q^2+1, & \varphi_5(q) &=& q^4+q^3+q^2+q+1, & \varphi_6(q) &=& q^2-q+1,\\
\varphi_7(q) &=& q^6+\ldots+q+1, & \varphi_8(q) &=& q^4+1, & \varphi_9(q) &=& q^6+q^3+1.
\end{array}
$$

Les factorisations obtenues plus tôt s'écrivent donc maintenant comme

$$
\begin{array}{lllllllll}
2_q &=& \varphi_2(q), & 3_q &=& \varphi_3(q), & & & \\
4_q &=& \varphi_2(q)\varphi_4(q), & 5_q &=& \varphi_5(q), & 6_q &=& \varphi_2(q)\varphi_3(q)\varphi_6(q),\\
7_q &=& \varphi_7(q), & 8_q &=& \varphi_2(q)\varphi_4(q)\varphi_8(q), & 9_q &=& \varphi_3(q)\varphi_9(q).
\end{array}
$$

Un peu plus d'observation permet de redécouvrir qu'on a en fait la formule

$$q^n-1=\prod_{d\,|\,n}\varphi_d(q), \tag{A.5}$$

où $d\,|\,n$ signifie que d divise n. À son tour, cette formule fournit une définition récursive pour les polynômes cyclothymiques :

$$\varphi_n(q)=\frac{q^n-1}{\prod_{\substack{d\,|\,n\\ d\neq n}}\varphi_d(q)}, \tag{A.6}$$

si $n>1$, avec $\varphi_1(q)=q-1$. Ceci peut s'écrire avec notre système comme :

```
> φ := (q, n)->
      if n = 1 then q - 1
      else factor((q^n - 1)/mul(φ(q, d), d = 1..n - 1)) fi :
```

si $\varphi(q,d)$ dénote le polynôme $\varphi_d(q)$.

Comme il est illustré ci-dessous, on peut apprendre à mieux connaître les **coefficients q-binomiaux**, défini par la formule

$$\binom{n}{k}_q := \frac{n_q!}{k_q!\,(n-k)_q!}. \tag{A.7}$$

Ce n'est pas directement évident, mais cette définition redonne les polynômes que nous définit en (3.43). Pour le voir, on vérifie par calcul que la formule (A.7) satisfait la récurrence (3.44). De l'une ou l'autre de ces définitions, on déduit que le coefficient q-binomial est un polynôme de degré $n\,(n-k)$:

$$\deg \binom{n}{k}_q = n\,(n-k). \tag{A.8}$$

On peut calculer ces polynômes au moyen de la procédure :

```
> qbinomial :=proc(n, k) option remember :
    if k = 0 then 1
    elif k > iquo(n + 1, 2) then qbinomial(n, n − k)
    else factor((qbinomial(n, k − 1)((n − k + 1) &. q))/(k &. q)) fi
    end :
```

qui exploite l'identité

$$\binom{n}{k}_q = \left(\binom{n}{k-1}_q (n-k+1)_q\right) k_q, \tag{A.9}$$

pour éviter de construire des polynômes de trop grand degré dans des calculs intermédiaires. On peut alors reformuler la description du q-triangle de pascal en terme des polynômes cyclotomique. Dans ce qui suit, la fonction « en_phi » transforme un polynôme en produit de polynômes cyclotomiques.

```
> for n to 7 do seq(en_phi(qbinomial(n, k)),k = 0..n) od ;
```

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & \varphi_2 & & 1 & & & & \\
 & & & 1 & & \varphi_3 & & \varphi_3 & & 1 & & & \\
 & & 1 & & \varphi_2\varphi_4 & & \varphi_3\varphi_4 & & \varphi_2\varphi_4 & & 1 & & \\
 & 1 & & \varphi_5 & & \varphi_4\varphi_5 & & \varphi_4\varphi_5 & & \varphi_5 & & 1 & \\
1 & & \varphi_2\varphi_3\varphi_6 & & \varphi_3\varphi_5\varphi_6 & & \varphi_2\varphi_4\varphi_5\varphi_6 & & \varphi_3\varphi_5\varphi_6 & & \varphi_2\varphi_3\varphi_6 & & 1
\end{array}$$

Chacune de ces expressions peut se calculer facilement, « à la main » , en utilisant la formule (A.5), et on constate la polynomialité des résultats. Reste alors (au lecteur) à donner une explication générale.

Annexe B

Séries génératrices pour des nombres bien connus

$n!$ **: Nombres factoriel** (1.67)

$$\frac{1}{1-y} = \sum_{n=0}^{\infty} n! \frac{y^n}{n!}, \tag{B.1}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	...
$n!$	1	1	2	6	24	120	720	5040	40320	362880	3628800	39916800	...

F_n **: Nombres de Fibonacci** (2.50)

$$\frac{1}{1-y-y^2} = \sum_{n=0}^{\infty} F_n \frac{y^n}{n!}, \tag{B.2}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	...

C_n **: Nombres de Catalan** (3.27)

$$\frac{1-\sqrt{1-4\,y}}{2\,y} = \sum_{n=0}^{\infty} C_n \frac{y^n}{n!}, \tag{B.3}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	...
C_n	1	1	2	5	14	42	132	429	1430	4862	16796	58786	208012	...

B_n : **Nombres de Bell** (2.16)

$$\exp(\exp(y)-1) = \sum_{n=0}^{\infty} B_n \frac{y^n}{n!}, \tag{B.4}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	...
B_n	1	1	2	5	15	52	203	877	4140	21147	115975	678570	4213597	...

$p(n)$: **Nombres de partages de** n, Section 5.3

$$\prod_{k=1}^{\infty} \frac{1}{1-y^k} = \sum_{n=0}^{\infty} p(n) \frac{y^n}{n!}, \tag{B.5}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$p(n)$	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176	231	...

$\binom{n}{k}$: **Coefficients binomiaux** (1.70)

$$\exp((1+z)\,y) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k} z^k \frac{y^n}{n!}, \tag{B.6}$$

$n \setminus k$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	1												
1	1	1											
2	1	2	1										
3	1	3	3	1									
4	1	4	6	4	1								
5	1	5	10	10	5	1							
6	1	6	15	20	15	6	1						
7	1	7	21	35	35	21	7	1					
8	1	8	28	56	70	56	28	8	1				
9	1	9	36	84	126	126	84	36	9	1			
10	1	10	45	120	210	252	210	120	45	10	1		
11	1	11	55	165	330	462	462	330	165	55	11	1	
12	1	12	66	220	495	792	924	792	495	220	66	12	1

$\left(\!\binom{n}{k}\!\right)$: **Coefficients binomiaux de 2-ième sorte** (1.90)

$$\exp\left(\frac{y}{1-z}\right)-1=\sum_{n=1}^{\infty}\sum_{k=0}^{\infty}\left(\!\binom{n}{k}\!\right)z^k\,\frac{y^n}{n!}, \tag{B.7}$$

$n\setminus k$	0	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10
3	1	3	6	10	15	21	28	36	45	55
4	1	4	10	20	35	56	84	120	165	220
5	1	5	15	35	70	126	210	330	495	715
6	1	6	21	56	126	252	462	792	1287	2002
7	1	7	28	84	210	462	924	1716	3003	5005
8	1	8	36	120	330	792	1716	3432	6435	11440
9	1	9	45	165	495	1287	3003	6435	12870	24310
10	1	10	55	220	715	2002	5005	11440	24310	48620

$\begin{bmatrix}n\\k\end{bmatrix}$: **Nombres de Stirling de 1-ère sorte** (5.11)

$$\left(\frac{1}{1-y}\right)^{z}=\sum_{n=0}^{\infty}\sum_{k=1}^{n}\begin{bmatrix}n\\k\end{bmatrix}z^k\,\frac{y^n}{n!}, \tag{B.8}$$

$n\setminus k$	1	2	3	4	5	6	7	8	9	10
1	1									
2	1	1								
3	2	3	1							
4	6	11	6	1						
5	24	50	35	10	1					
6	120	274	225	85	15	1				
7	720	1764	1624	735	175	21	1			
8	5040	13068	13132	6769	1960	322	28	1		
9	40320	109584	118124	67284	22449	4536	546	36	1	
10	62880	1026576	1172700	723680	269325	63273	9450	870	45	1

$\begin{Bmatrix}n\\k\end{Bmatrix}$: **Nombres de Stirling de 2-ième sorte** (2.15)

$$\exp(z\,(\exp(y)-1))=\sum_{n=0}^{\infty}\sum_{k=1}^{n}\begin{Bmatrix}n\\k\end{Bmatrix}z^k\,\frac{y^n}{n!}, \tag{B.9}$$

$n \setminus k$	1	2	3	4	5	6	7	8	9	10
1	1									
2	1	1								
3	1	3	1							
4	1	7	6	1						
5	1	15	25	10	1					
6	1	31	90	65	15	1				
7	1	63	301	350	140	21	1			
8	1	127	966	1701	1050	266	28	1		
9	1	255	3025	7770	6951	2646	462	36	1	
10	1	511	9330	34105	42525	22827	5880	750	45	1

Annexe C

Notations

O **:** l'espèce vide, Section 6.4.

$\mathbb{1}$ **:** l'espèce caractéristique de l'ensemble vide, Section 6.4.

$\sim$ **ou** $\equiv$ **:** une relation d'équivalence, Section 2.3.

$\sim_f$ **:** partition en fibre selon la fonction f, Section 2.3.

$\left\{ {n \atop k} \right\}$ **:** les nombres de Stirling de 2-ième sorte, (2.15).

$\left[{n \atop k} \right]$ **:** les nombres de Stirling de 1-ère sorte, (5.11).

$\preceq$ **ou** $\leq$ **:** une relation d'ordre, Section 2.5.

$|A|$ **:** le cardinal d'un ensemble A, Section 1.2.

$|w|$ **et** $|w|_x$ **:** la longueur du mot w, le nombre d'occurrences de la lettre x dans le mot w, Section 3.2.

$[n]$ **:** l'ensemble usuel de cardinal n, Section 1.2.

$\{A_i\}_{i\in I}$ **:** famille d'ensembles indexés par les éléments de I, Chapitre 1.

$(A_i)_{i\in I}$ **:** suite d'ensembles indexés par les éléments de I, Chapitre 1.

$\prod_{i\in I} A_i$ **et** $A \times B$ **:** produits cartésiens d'ensembles, Chapitre 1.

$\sum_{i\in I} A_i$ **et** $A + B$ **:** unions disjointes d'ensembles, Chapitre 1.

$\binom{t}{k}$ **:** le coefficient (polynôme) binomial, (1.70).

$\binom{n}{k}_q$ **:** coefficients q-binomiaux, (3.44).

$\left(\!\!\binom{t}{k}\!\!\right)$ **:** le coefficient (polynôme) binomial de 2-ième sorte, (1.90).

$\mathrm{aire}(\gamma)$ **:** aire d'un chemin, (3.40).

$\mathcal{A}$: l'espèce des arborescences, (2.58) et Section 6.12.

$A/\sim$ **ou** $A/\equiv$: l'ensemble quotient par une relation d'équivalence, (2.7).

$A \overrightarrow{+} B$: la somme ordonnée de deux ensembles ordonnés A et B, Section 2.5.

$A \times_\ell B$: le produit lexicographique de deux ensembles ordonnés A et B, Section 2.5.

Abc : l'espèce des arbres binaires croissants, (4.5).

A^n **et** A^* : les mots de longueur n sur A, le monoïde des mots sur A, (3.2). L'espèce des mots de longueur n, et l'espèce des mots, Section 6.42.

Arb : L'espèce des arbres, Section 2.7 et (6.63).

B_n : les nombres de Bell, (2.16).

$B_n(t)$: les polynômes de Bell, (2.17).

Bij$[A, B]$: l'ensemble des fonctions bijectives de A vers B, (1.49).

$\mathcal{B}$: l'espèce des arbres binaires, Section 4.2 et (6.55).

$\mathcal{C}(q)$: polynôme énumérateur d'aire, (3.41).

C_n : les nombres de Catalan, (3.27).

Con : l'espèce des endofonctions connexes, Exercice 2.19 et Section 6.12.

Croi$[A, B]$: l'ensemble des fonctions croissantes entre deux ensembles ordonnés A et B, (2.34).

$\mathcal{C}$: l'espèce des permutations cyclique sur A. Sections 5.2 et 6.11.

$\delta(\ell)$: déployé d'un ordre total, (4.7).

$\mathcal{D}$: le langage des mots de Dyck, (3.23).

Der : l'espèce des dérangements, (5.12) et Section 6.9.

Dyck$[n]$: ensemble des chemins de Dyck, Section 3.7.

$\Delta[n]$: ensemble des triangulations d'un polygone à n cotés, (4.12).

ε **ou** 1 : le mot vide, Section 3.2.

$\eta(\gamma)$: le normalisé d'un chemin γ, (3.33).

Élém : l'espèce élément de A, Section 6.4.

Equiv$[A]$: l'ensemble des relations d'équivalence sur A, Section 2.3.

End : l'espèce des endofonctions, Sections 2.8 et 6.12.

E : l'espèce ensemble, Section 6.4.

$f^+ = \mathcal{P}[f]$: la fonction image de sous-ensemble par une fonction f, (1.42).

f^- : la fonction image inverse de sous-ensemble par une fonction f, (1.44).

$f\big|_C$: la fonction f restreinte au sous-ensemble C, (1.35).

f^k : k-ième itéré pour la composition de f, (2.63).

f_μ : nombre tableaux de Young de forme μ, (5.60).

$F[A]$: ensemble des F-structures sur A, Section 6.2.

F_σ : transport de F-structures le long de la bijection σ, Section 6.2.

$F(y)$: la série génératrice de l'espèce F, Section 6.8.

F_n : les nombres de Fibonacci, (2.50).

$\widetilde{F}(y)$: la série génératrice des types de F-structures, (6.67).

$F + G$: somme des espèces F et G, Section 6.6.

$F \cdot G$: produit des espèces F et G, Section 6.6.

F^m : puissance m-ième de l'espèce F, Section 6.6.

$F \circ G$ **ou** $F(G)$: substitution de l'espèce G dans l'espèce F, l'espèce des F de G-structures, Section 6.10.

F' : l'espèce dérivée de l'espèce F, Section 6.13.

$F^\bullet$: l'espèce des F-structures pointées, Section 6.13.

$\mathsf{Fonct}[A, B]$: l'ensemble des fonctions de A vers B, (1.31).

$g \circ f$: composé de fonctions g et de f, (1.37).

$\gamma_1 \cdot \gamma_2$: composé de chemins, Section 2.6.

Gro : l'espèce des graphes orientés, (2.1) et Section 6.4.

Gra : l'espèce des graphes simples, (2.4) et Section 6.4.

$\Gamma(\sigma)$: décomposition cyclique de σ, (5.3).

$\Gamma_g^\ell(x, y)$: l'ensemble des chemins de longueur ℓ allant de x à y dans le graphe g, Section 2.6.

$h_c = h_c(\mu)$: longueur de l'équerre de la case c dans le partage μ, (5.62).

$\mathsf{Inv}_n(q)$: polynôme énumérateur d'inversions, (5.27).

Inv : l'espèce des involutions, (5.24) et Section 6.4.

Id_A : la fonction identité sur A, Chapitre 1.

$\mathrm{Im}(f)$: l'image d'une fonction f, (1.43).

$\mathsf{Inj}[A, B]$: l'ensemble des fonctions injectives de A vers B, (1.55).

$\ell(\sigma)$: le nombre d'inversions (ou la longueur) d'une permutation σ, (5.26).

$\lambda(\sigma)$: forme de la permutation σ, (5.4).

$\lambda \vdash n$: λ partage de n, Section 5.3.

$\mathbb{L}(F)$: l'espèce des liste de F-structures, Section 6.6.

$\mathcal{L} + \mathcal{L}'$: union de langages, Section 3.3.

$\mathcal{L} \cdot \mathcal{L}'$: produit de langages, Section 3.3.

$\mathcal{L}^*$: étoile de langages, Section 3.3.

$\Lambda[n]$: ensemble des partages de n, Section 5.3.

$\Lambda_I[n]$: ensemble des partages de n en parts impaires, Section 5.5.

$\Lambda_K[n]$: ensemble des partages de n en parts dans $K \subseteq \mathbb{N}$, Section 5.5.

$\Lambda_{\neq}[n]$: ensemble des partages de n en parts distinctes, Section 5.5.

$\Lambda_{K;\neq}[n]$: ensemble des partages de n en parts distinctes dans K, Section 5.5.

$\Lambda_{\leq k}(n)$: ensemble des partages de n en parts $\leq k$, Section 5.5.

$\mathcal{M}_k[A]$: l'ensemble des multi-sous-ensembles de cardinal k de A, Chapitre 1.

$p(n)$: nombre de partages de n, Section 5.3.

$p_{\neq}(n)$: nombre de partages de n en parts distinctes, Section 5.5.

$p_I(n)$: nombre de partages de n en parts impaires, Section 5.5.

$p_K(n)$: nombre de partages de n en parts dans $K \subseteq \mathbb{N}$, Section 5.5.

$p_{K;\neq}(n)$: nombre de partages de n en parts distinctes dans K, Section 5.5.

$\pi(\alpha)$: projection d'un arbre binaire croissant, (4.7).

$\pi_{\gamma\gamma'}$: polyomino parallélograme contenu entre deux chemins de Dyck γ et γ', (4.20).

$P(\sigma)$: P-tableau de σ selon la correspondance RSK, Section 5.9.

$\mathsf{Pal}[A]$ **et** $\mathsf{Pal}_k[A]$: ensembles de palindromes sur A, Section 3.2.

Part : l'espèce des partitions, Sections 2.3 et 6.11.

Part_k : l'espèce des partitions en parts de taille k, Sections 2.3 et 6.11.

Plan : l'espèce des arbres plans, (4.10) et Section 6.15.

$\mathsf{Pol}_{/\!/}[n]$: ensemble des polyominos parallélogrames de périmètre $2\,n$, (4.20).

$\mathcal{P}$: l'espèce des parties, (1.9) et Section 6.4.

$\mathcal{P}_k$: l'espèce des parties à k-éléments, Section 6.4.

$Q(\sigma)$: Q-tableau de σ selon la correspondance RSK, Section 5.9.

$\widehat{R}$: la fermeture transitive d'une relation R, (2.2).

$\mathsf{Rel}[A, B]$: l'ensemble des relations de A vers B, (1.26).

s_i : transposition adjacente dans $\mathbb{S}[n]$, (5.20).

$\sigma^*(x)$: orbite de x selon σ, (5.2).

$\mathbb{S}$: l'espèce des permutations, (1.49) et Sections 5.2 et 6.4.

$\mathsf{Sta}[n]$: ensemble des fonctions de stationnement, (4.13).

Sta_γ : ensemble des fonctions de stationnement de type γ, (4.17).

$\mathsf{Strict}[A, B]$: l'ensemble des fonctions strictement croissantes (injectives) entre deux ensembles ordonnés A et B, (2.34).

$\mathsf{Surj}[A, B]$: l'ensemble des fonctions surjectives de A vers B, (1.58).

$t_{(k)}$: la k^e puissance factorielle décroissante de t, (1.68).

$t^{(k)}$: la k^e puissance factorielle croissante de t, (1.69).

$\mathcal{T}$: l'espèce des transpositions, (5.19).

$u \cdot v$: concatenation des mots u et v, Section 3.2.

w^k : puissance k-ième d'un mot w, (3.7).

$\widetilde{w}$: image miroir d'un mot w, (3.8).

$\omega(n)$: nombre pentagonaux, Section 5.6.

$x \to_\preceq y$ **ou** $x \to y$: x est couvert par y (ou y couvre x) dans l'ordre $\preceq$, Section 2.5.

$[x, y]_\preceq$ **ou** $[x, y]$: l'interval des éléments entre x et y dans l'ordre $\preceq$, (2.28).

$x \vee y$ **et** $x \wedge y$: supremum et infimum de x et y, Section 2.5.

χ_B : la fonction caractéristique d'un sous-ensemble B, (1.38).

Y : l'espèce caractéristique des singletons de sorte Y, Section 6.4.

$\mathsf{Young}[\mu]$: ensemble des tableaux de Young de forme μ, (5.59).

Z : l'espèce caractéristique des singletons de sorte Z, Section 6.4.

Bibliographie

[1] M. Aigner, *A Course in Enumeration*, Graduate Texts in Mathematics, Springer-Verlag, 2007.

[2] G. Andrews et K. Eriksson, *Integer Partitions*, Cambridge University Press, 2004.

[3] E.A. Bender and S.G. Williamson, *Foundations of Applied Combinatorics*, Addison-Wesley, 1991.

[4] C. Berge, *Principes de Combinatoire*, Dunod, 1968.

[5] F. Bergeron, *Algebraic Combinatorics and Coinvariant Spaces*, CMS Treatise in Mathematics, CMS et A.K. Peters, 2009.

[6] F. Bergeron, G. Labelle & P. Leroux, *Espèces de structures et combinatoire des structures aborescentes*, Publications du LACIM **19**, UQAM, Montréal, 1994.

[7] F. Bergeron, G. Labelle & P. Leroux, *Combinatorial Species and Tree-Like Structures*, Encyclopedia of Mathematics and its Applications **67**, Cambridge University Press, 1998.

[8] F. Bergeron and S. Plouffe, *Computing the Generating Function of a Series Given its First Few Terms*, Experimental Mathematics **1**, 1992, 307–312.

[9] M. Bona, *A Walk Through Combinatorics : An Introduction to Enumeration and Graph Theory*, World Scientific, 2006.

[10] L. Comtet, *Analyse combinatoire*, Presses Universitaires de France, 2 tomes, 1970.

[11] A. Cayley, *A theorem on trees*, Quart. J. Pure Appl. Math. **23** (1889).

[12] N.G. de Bruijn, *Asymptotic Methods in Analysis*, Dover, 1981.

[13] S. Eilenberg, *Automata, Languages and Machines*, Academic Press **Vol. A**, 1974 ; et **Vol. B**, 1976.

[14] Ph. Flajolet et R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, 2009. Aussi disponible gratuitement sur le site :

http://algo.inria.fr/flajolet/Publications/book.pdf

[15] J.S. Frame, G. de B. Robinson and R.M. Thrall, *The Hook Graphs of the Symmetric Groups*, Canadian J. Math. **6** (1954), 316–324.

[16] I.P. Goulden and D.M. Jackson, *Combinatorial Enumeration*, Wiley, 1983.

[17] R.L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.

[18] F. Harary, *Graph Theory*, Addison-Wesley, 1972.

[19] F. Harary and E. Palmer, *Graphical Enumeration*, Academic Press, 1973.

[20] A. Joyal, *Une théorie combinatoire des séries formelles*, Advances in Mathematics **42** (1981), 1–82.

[21] V. Kac and P. Cheung, *Quantum Calculus*, Springer, 2001.

[22] Donald Knuth, *The Art of Computer Programming*, Addison-Wesley, 3-ième édition, 1997.

[23] G. Konheim et B. Weiss, *An occupancy discipline and applications*, SIAM J. Applied Math. 14 (1966), 1266–1274.

[24] C. Kostka, *Über den Zusammenhang zwischen einigen Formen von symmetrischen Funktionen*, Crele's Journal, **93**, (1882) 89-123.

[25] J. Kung, G.C. Rota, et C. Yan, *Combinatorics : The Rota Way*, Cambridge University Press, 2009.

[26] J. Labelle, *Théorie des graphes*, Modulo éditeur, Montréal, 1981.

[27] M. Lothaire, *Combinatorics on Words*, Encyclopedia of Mathematics **Vol. 17**, Addison-Wesley, 1983.

bibitemmoon J.W. Moon, *Counting Labelled Trees*, Canadian Mathematical Monographs **1**, CMS, 1970.

[28] M. Petkovsek, H. Wilf, et D.Zeilberger, *A=B*, A.K. Peters, 1996. Aussi disponible gratuitement sur le site :

http://www.math.upenn.edu/∼wilf/Downld.html

[29] G. Pólya and R.C. Read, *Combinatorial Enumeration of Groups, Graphs and Chemical Compounds*, Springer-Verlag, 1987.

[30] R. Pyke, *The supremum and infimum of the Poisson process*, Ann. Math. Statistics **30** (1959), 568–576.

[31] C. Reutenauer, *Free Lie Algebras*, Oxford University Press, 1983.

[32] J. Riordan, *Ballots and trees*, J. Comb. Th. 6 (1969), 408–411.

[33] J. Riordan, *An Introduction to Combinatorial Analysis*, Princeton University Press, 1980.

[34] G. de B. Robinson, *On the Representations of the Symmetric Group*, Amer. J. Math **60** (1938), 745–760.

[35] B. Sagan, *The Symmetric Group*, Wadsworth and Brooks, 1991.

[36] C. Schensted, *Longest increasing and decreasing subsequences*, Canad. J. Math. 13 (1961), 179–191.

[37] N. Sloane et S. Plouffe, *Encyclopedia of Integer Sequences*, Academic Press, 1995.

[38] R.P. Stanley, *Enumerative Combinatorics*, Cambridge University Press, 1999.

[39] R.P. Stanley, *Acyclic orientations of graphs*, Discrete Math., 5 (1973), 171–178.

[40] D. Stanton & D. White, *Constructive Combinatorics*, UTM, Springer Verlag, 1986.

[41] J. H. van Lint & R. M.Wilson, *A course in Combinatorics*, Cambridge University Press, 1992.

[42] X.G. Viennot, *Une forme géométrique de la correspondance de Robinson-Schensted*, in*Combinatoire et Représentation du Groupe Symétrique*, Lecture Notes in Math. **579** (1977), Springer-Verlag, 29–58.

[43] K. Wehrhahn, *Introductory Combinatorics*, Carslaw, 1992.

[44] H. Wilf, *generatingfunctionology*, Academic Press, 1993. Aussi disponible gratuitement sur le site :

http://www.math.upenn.edu/∼wilf/DownldGF.html