

LM226 - Combinatoire et Graphes

Dominique Bernardi

3 juin 2010

Certains paragraphes sont composés en petits caractères. Il ne font pas partie du programme du cours et leur connaissance ne sera pas nécessaire pour l'examen. L'auteur les a inclus parce qu'il estime qu'ils ont leur place logique dans l'exposé et que leur étude serait profitable au lecteur.

0

Chapitre 1

Combinatoire énumérative

1.1 Rappels de théorie des ensembles

Le point de vue adopté est informel. On suppose connue une partie du vocabulaire de base sur les ensembles : appartenance, inclusion, produit cartésien, ensemble des parties.

1.1.1 Applications

Une *application* (ou *fonction*) f d'un ensemble E dans un ensemble F , notée $f : E \rightarrow F$, est la donnée, pour chaque élément x de E d'un élément $f(x)$ de F . L'ensemble E est appelé *ensemble de départ* et l'ensemble F est l'*ensemble d'arrivée*. L'élément $f(x)$ est l'*image* de x par f . On écrit aussi $f : x \mapsto f(x)$. Un exemple trivial d'application est l'*application identique* de E , notée $Id_E : E \rightarrow E$ telle que $\forall x \in E, Id_E(x) = x$. Si $f : E \rightarrow F$ et $g : F \rightarrow G$ sont deux applications, l'*application composée* de f et g est

$$\begin{aligned} g \circ f : E &\rightarrow G \\ x &\mapsto g(f(x)) \end{aligned}$$

Si A est une partie de E , on note $f(A)$ et on nomme *image* de A par f la partie

$$\{y \in F; \exists x \in A, y = f(x)\}$$

de F formée des images dans F des éléments de A . De même, si B est une partie de F , on note $f^{-1}(B)$ et on nomme *image réciproque* de B par f la partie

$$\{x \in E; f(x) \in B\}$$

de E formée des éléments de E dont l'image est dans B . Par extension, si y est un élément de F , on note $f^{-1}(y)$ l'image réciproque du singleton $\{y\}$. C'est

donc l'ensemble des éléments de E dont l'image par f est y . Cet ensemble peut être vide. On dit que l'application f est *surjective*, ou que c'est une *surjection* si elle n'est vide pour aucune valeur de y et qu'elle est *injective*, ou que c'est une *injection* s'il n'a plus d'un élément pour aucune valeur de y :

Définition 1.1.1. Une application $f : E \rightarrow F$ est

– *injective si et seulement si*

$$\forall x, y \in E, \quad f(x) = f(y) \Rightarrow x = y$$

– *surjective si et seulement si*

$$\forall y \in F, \quad \exists x \in E, \quad y = f(x)$$

– *bijective si et seulement si elle est à la fois injective et surjective.*

En résumé, f est bijective si et seulement si pour tout y de F , l'ensemble $f^{-1}(\{y\})$ a un élément et un seul, que l'on note encore $f^{-1}(y)$. On voit facilement que f^{-1} est alors une bijection de F dans E et que l'on a $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$. On dit que f^{-1} est la bijection réciproque de f .

Il existe une autre notation courante pour les applications. La notation $(x_i)_{i \in I}$ désigne une *famille* d'éléments de X *indexée* par l'ensemble I . Il s'agit simplement d'une application de I dans X , où x_i est l'image de i par l'application.

1.1.2 Entiers naturels, récurrence

Nous admettrons l'existence d'un ensemble

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

dit ensemble des *entiers naturels* muni d'une application injective $S : \mathbb{N} \rightarrow \mathbb{N}$ qui à un entier n fait correspondre son *successeur* noté $n + 1$ qui est telle que tout entier autre que 0 a un (unique) *prédécesseur* et qui vérifie le *principe de récurrence* :

$$\forall A \subset \mathbb{N}, \quad [(0 \in A) \text{ et } (\forall n \in \mathbb{N}, n \in A \Rightarrow n + 1 \in A)] \Rightarrow A = \mathbb{N}.$$

Ce principe est en général utilisé de la façon suivante. Soit P un *prédicat* sur \mathbb{N} , c'est-à-dire une propriété qui, pour chaque entier naturel, peut être vraie ou fausse. Si on a établi que $P(0)$ est vrai et si pour n quelconque, en

supposant $P(n)$ on a prouvé $P(n+1)$, alors $P(n)$ est vrai pour tout n . On applique pour cela l'énoncé ci-dessus à la partie A de \mathbb{N} formée des n tels que $P(n)$ est vrai.

On peut déduire de ce principe la

Proposition 1.1.2 (construction par récurrence). *Si $f : X \rightarrow X$ est une application et x un élément de X , il existe une application $g : \mathbb{N} \rightarrow X$ et une seule telle que $g(0) = x$ et $\forall n \in \mathbb{N}, g(n+1) = f(g(n))$.*

Une famille indexée par les entiers naturels s'appelle une *suite*. L'application g ci-dessus est souvent notée sous forme de suite. On pose $x_n = g(n)$ et on dit que la suite $(x_n)_{n \in \mathbb{N}}$ est *définie par récurrence* par les relations $x_0 = x$ et $x_{n+1} = f(x_n)$.

L'ensemble \mathbb{N} est alors muni de trois *lois de composition* c'est-à-dire d'applications de $\mathbb{N} \times \mathbb{N}$ dans \mathbb{N} appelées *addition*, *multiplication* et *exponentiation* et notées respectivement $(a, b) \mapsto a + b$, $(a, b) \mapsto a \cdot b$ ou ab et $(a, b) \mapsto a^b$. La construction se fait en utilisant le principe de récurrence et les relations

- $a + 0 = a$; $a + (b + 1) = (a + b) + 1$
- $a \cdot 0 = 0$; $a \cdot (b + 1) = a \cdot b + a$
- $a^0 = 1$; $a^{b+1} = a^b \cdot a$.

En d'autres termes, l'addition est définie par récurrence à partir de l'application S , la multiplication par récurrence à partir de l'addition et l'exponentiation par récurrence à partir de la multiplication. Retenons en particulier que $0^0 = 1$.

Si m et n sont deux entiers naturels, on dit que m est *inférieur ou égal* à n et on note $m \leq n$ s'il existe $p \in \mathbb{N}$ tel que $m + p = n$. On montre que c'est une *relation d'ordre* c'est-à-dire que l'on a

- $\forall m \in \mathbb{N}, m \leq m$
- $\forall m, n \in \mathbb{N}, (m \leq n \text{ et } n \leq m) \Rightarrow m = n$
- $\forall m, n, p \in \mathbb{N}, (m \leq n \text{ et } n \leq p) \Rightarrow m \leq p$

La relation d'ordre sur \mathbb{N} est un *bon ordre*, c'est-à-dire que l'on a :

Proposition 1.1.3. *Toute partie non vide de \mathbb{N} a un plus petit élément.*

Démonstration. Soit X une partie de \mathbb{N} dont on suppose qu'elle n'a pas de plus petit élément. On pose

$$A = \{n \in \mathbb{N}; \forall m \in X, n < m\}$$

l'ensemble des minorants stricts de X . Comme 0 est le plus petit élément de \mathbb{N} , il ne peut appartenir à X et on a $0 \in A$. D'autre part, si $n \in A$ on a $n < m$ pour tout m dans X . Cela implique $n + 1 \leq m$ mais $n + 1 = m$

impliquerait que $n + 1$ est le plus petit élément de X . On a donc $n + 1 < m$ et $n + 1 \in A$. En application du principe de récurrence, on a $A = \mathbb{N}$, donc $X = \emptyset$, ce qui termine la preuve. **cqfd.**

Si m et n sont deux entiers naturels, on notera

$$[m, n] = \{k \in \mathbb{N}; \quad m \leq k \leq n\}.$$

En particulier, lorsque $m > n$, $[m, n]$ est l'ensemble vide \emptyset .

1.1.3 Le cardinal d'un ensemble

L'existence d'une injection de E dans F peut être interprétée comme “ E est plus petit que F ”. Le résultat suivant permet de donner un sens précis à cette intuition.

Théorème 1.1.4 (de Cantor-Bernstein). *Soient E et F deux ensembles. S'il existe une injection de E dans F et une injection de F dans E , alors il existe une bijection de E dans F .*

Démonstration. On définit par récurrence deux suites de parties de E par $A_0 = E$, $A'_0 = g(F)$, $A_{n+1} = g \circ f(A_n)$ et $A'_{n+1} = g \circ f(A'_n)$. On voit par récurrence que ces parties sont “emboîtées” :

$$A_0 \supset A'_0 \supset A_1 \supset A'_1 \supset A_2 \supset A'_2 \supset \dots$$

On pose

$$A = \bigcap_{n \in \mathbb{N}} A_n.$$

et on définit une application $\varphi : E \rightarrow F$ par

$$\varphi(x) = \begin{cases} g^{-1}(x) & \text{si il existe un entier } n \text{ tel que } x \in A'_n \setminus A_{n+1} \\ f(x) & \text{sinon} \end{cases}$$

Il reste à vérifier que φ est une bijection. **cqfd.**

De même que la couleur bleue est simplement ce qu'ont en commun tous les objets bleus, le *cardinal* d'un ensemble X , noté $|X|$, est ce qu'ont en commun des ensembles qui sont en bijection. En d'autres termes, on dit que X et Y ont même cardinal si et seulement si il existe une bijection de X dans Y . On peut comparer les cardinaux : on dit que le cardinal de X est *inférieur ou égal* à celui de Y , et on note $|X| \leq |Y|$ si et seulement si il existe une injection de X dans Y . Grâce au théorème de Cantor-Bernstein, on a la

Proposition 1.1.5. *Si X et Y sont des ensembles,*

$$|X| \leq |Y| \text{ et } |Y| \leq |X| \Rightarrow |X| = |Y|$$

L'énoncé précédent pourrait paraître évident, sauf que les cardinaux ne sont pas en général des nombres, au sens où on l'entend généralement. Par exemple, un cardinal peut être infini.

Plutôt que d'utiliser les injections pour comparer les ensembles, on aurait pu utiliser les surjections. En fait on a la

Proposition 1.1.6. *Soient X et Y deux ensembles. Les deux propriétés suivantes sont équivalentes*

- *Il existe une injection f de X dans Y .*
- *X est vide ou il existe une surjection g de Y sur X .*

Démonstration. Si X n'est pas vide, choisissons un élément a de X . Si f existe, on définit g par

$$g(y) = \begin{cases} \text{l'unique élément de } f^{-1}(y) & \text{si } y \in f(X) \\ a & \text{sinon.} \end{cases}$$

Si g existe, on définit f en choisissant pour $f(x)$ n'importe quel élément de $g^{-1}(x)$. **cqfd.**

1.1.4 Ensembles finis

Un ensemble E est dit *fini* s'il existe une bijection de E sur un intervalle entier $[1, n]$. S'il n'est pas fini, il est dit *infini*. On va voir que n est alors unique.

Théorème 1.1.7. *Soient n et p deux entiers naturels.*

- i) Il existe une injection de $[1, n]$ dans $[1, p]$ si et seulement si $n \leq p$.*
- ii) Il existe une surjection de $[1, n]$ sur $[1, p]$ si et seulement si $n \geq p > 0$ ou $n = p = 0$.*
- iii) Il existe une bijection de $[1, n]$ sur $[1, p]$ si et seulement si $n = p$.*

En particulier, si X est un ensemble fini, il existe un entier naturel n et un seul tel que X est en bijection avec $[1, n]$. Au lieu de noter $|X| = |[1, n]|$, on notera $|X| = n$ et on dira que le cardinal de X est n .

Démonstration. Démontrons la propriété i) par récurrence sur n et indépendamment de p , c'est-à-dire appelons $P(n)$ la propriété de n qui dit que cette assertion est vraie pour tout p . Comme $[1, 0] = \emptyset$, il y a toujours une injection de $[1, 0]$ dans $[1, p]$ et $0 \leq p$ est toujours vrai. Donc $P(0)$ est vrai. Supposons $P(n)$ et considérons une injection f de $[1, n+1]$ dans $[1, p]$. Supposons d'abord $f(n+1) = p$. On a forcément $p > 0$. Puisque f est injectif, l'image de $[1, n]$ par f est inclus dans $[1, p-1]$. La restriction de f à $[1, n]$, c'est-à-dire l'application

de $[1, n]$ dans $[1, p-1]$ qui coïncide avec f est une injection, et l'hypothèse de récurrence implique $n \leq p-1$ et $n+1 \leq p$.

Dans le cas où $a = f(n+1) < p$, il existe une bijection τ de $[1, p]$ dans lui-même qui échange a et p et laisse fixes tous les autres éléments. La composée $g = \tau \circ f$ est encore une injection de $[1, n+1]$ dans $[1, p]$, et vérifie $g(n+1) = p$. On a donc encore $n+1 \leq p$ et $P(n+1)$ est vrai, ce qui achève de démontrer le i). Mais le ii) est exactement équivalent à i) en échangeant n et p . Enfin i) et ii) donnent iii). **cqfd.**

Le théorème précédent justifie la notation \geq employée en deux sens différents, l'un pour les entiers, l'autres pour les cardinaux. Ces deux acceptations sont compatibles. On peut reformuler le théorème précédent de plusieurs manières.

Théorème 1.1.8 (principe des tiroirs). *Si $f : X \rightarrow Y$ est une application et X et Y sont des ensembles (finis) tels que $|X| > |Y|$, alors f n'est pas injective.*

Si on a plus d'objets que de tiroirs, quel que soit le rangement on est obligé de ranger deux objets dans le même tiroir.

Théorème 1.1.9 (principe d'inclusion). *Si E est un ensemble fini et F une partie de E , alors F est fini et $|F| \leq |E|$. Si, de plus, on a $|E| = |F|$, alors $E = F$.*

1.1.5 Cardinaux infinis

Proposition 1.1.10. *Pour tout ensemble infini E , il existe une injection de \mathbb{N} dans E .*

On dit que E est *dénombrable* s'il a même cardinal que \mathbb{N} . C'est le plus petit infini possible :

Certains ensembles classiques sont dénombrables, comme \mathbb{Z} , $\mathbb{N} \times \mathbb{N}$, l'ensemble \mathbb{Q} des nombres rationnels, ou l'ensemble des parties finies de \mathbb{N} .

Mais il existe des cardinaux infinis plus grands. Par exemple, l'ensemble \mathbb{R} des nombres réels n'est pas dénombrable.

Il est facile de montrer qu'il y a une infinité de cardinaux infinis distincts à l'aide du théorème suivant.

Théorème 1.1.11. *Soit X un ensemble. Il n'y a pas d'application surjective (donc pas de bijection) de X dans l'ensemble $\mathcal{P}(X)$ des parties de X .*

Démonstration. Soit φ une application de X dans $\mathcal{P}(X)$. Posons

$$A = \{x \in X; \quad x \notin \varphi(x)\}$$

Supposons qu'il existe $a \in X$ tel que $\varphi(a) = A$. On peut donc écrire

$$a \in A \Leftrightarrow a \in \varphi(a) \Leftrightarrow a \notin A$$

ce qui est une contradiction. On a donc prouvé que A n'appartient pas à l'image de φ , et φ n'est pas surjective. **cqfd.**

1.1.6 Relations binaires

Une *relation binaire* R sur un ensemble S est un *prédicat* sur $S \times S$, c'est-à-dire une propriété que possède ou ne possède pas chaque couple (s, t) d'éléments de S . S'il possède la propriété, on dit que s est en relation avec t et on note sRt . La relation R est *réflexive* si et seulement si

$$\forall s \in S, \quad sRs.$$

La relation *inverse* ou *opposée* à R est la relation R^{-1} telle que

$$\forall s, t \in S, \quad sR^{-1}t \Leftrightarrow tRs$$

La relation R est *symétrique* si et seulement si

$$\forall s, t \in S, \quad sRt \Leftrightarrow tRs$$

c'est-à-dire $R^{-1} = R$. Elle est *antisymétrique* si et seulement si

$$\forall s, t \in S, \quad (sRt \text{ et } tRs) \Rightarrow s = t.$$

La *clôture symétrique* de la relation R est la relation R^{sym} définie par

$$\forall s, t \in S, \quad sR^{sym}t \Leftrightarrow (sRt \text{ ou } tRs).$$

Elle est évidemment symétrique. La relation R est *transitive* si et seulement si

$$\forall s, t, u \in S, \quad (sRt \text{ et } tRu) \Rightarrow sRu.$$

La *clôture réflexive-transitive* de la relation R est la relation R^{rt} définie par

$$\forall s, t \in S, \quad sR^{rt}t \Leftrightarrow \exists k \in \mathbb{N}, (x_i)_{i \in [0, k]}; s = x_0, t = x_k, \forall i \in [1, k] x_{i-1}Rx_i$$

c'est-à-dire que l'on peut passer de s à t en un nombre fini d'étapes, chaque élément étant en relation avec le suivant le long du chemin. La relation R^{rt} est bien sûr réflexive et transitive.

La relation R est une *relation d'ordre* si et seulement si elle est réflexive, antisymétrique et transitive. C'est une *relation d'équivalence*

si elle est réflexive, symétrique et transitive.

Si $f : S \rightarrow T$ est une application, la relation définie par

$$\forall s, t \in S, \quad sRt \Leftrightarrow f(s) = f(t)$$

est une relation d'équivalence. En fait, toute relation d'équivalence est obtenue de cette manière. Si R est une relation d'équivalence sur S , on associe à chaque s sa *classe d'équivalence* $\pi(s) = \{t \in S; sRt\}$ qui est une partie non vide de S . L'ensemble des classes d'équivalence, noté S/R est une *partition* de S , c'est-à-dire une famille $S_{i \in I}$ de parties non vides de S , disjointes deux à deux et dont la réunion est S . L'application $\pi : S \rightarrow S/R$ redonne R par le procédé décrit au début de ce paragraphe.

1.2 Outils de base

On a vu qu'une des propriétés les plus fondamentales d'un ensemble fini est son cardinal, un entier naturel. L'objet général de la combinatoire énumérative est de "calculer" ce cardinal pour des ensembles particuliers. La plupart du temps, l'ensemble considéré dépend d'un ou plusieurs paramètres, et il s'agit d'exprimer ce cardinal comme fonction de ces paramètres. Nous serons ainsi amenés à définir certaines fonctions de \mathbb{N} ou $\mathbb{N} \times \mathbb{N}$ dans \mathbb{N} , en commençant avec les opérations de base définies plus haut.

Un autre but naturel de cet étude est de montrer que certains ensembles finis ont même cardinal. Une méthode pour prouver que $|A| = |B|$ est de calculer $|A|$ et $|B|$ séparément, puis de comparer les résultats. C'est ce que l'on appelle une preuve par le calcul, ou *calculatoire*. Il est aussi souvent possible de construire explicitement une bijection entre A et B . On a dans ce cas une preuve combinatoire. De manière générale les mathématiciens préfèrent les preuves combinatoires pour deux raisons en fait liées : elles donnent en général une idée de "la raison pour laquelle" $|A| = |B|$ alors que les preuves calculatoires suggèrent rarement des idées nouvelles, et elles sont souvent plus satisfaisantes d'un point de vue esthétique.

1.2.1 Les opérations de base sur les cardinaux

Théorème 1.2.1 (Union disjointe). *Si A et B sont deux ensembles finis disjoints, l'ensemble $A \cup B$ est fini et l'on a*

$$|A \cup B| = |A| + |B|.$$

Démonstration. Par récurrence sur $b = |B|$. Si $b = 0$, B est vide et $A \cup B = A$ a bien pour cardinal $|A| = |A| + 0$. Si $|B| = b + 1$, il existe une bijection f

de $[1, b + 1]$ dans B . Posons $c = f(b + 1)$. La restriction de f à $[1, b]$ est une bijection de $[1, b]$ sur $B' = f([1, b]) = B \setminus \{c\}$. On en déduit que $|B'| = b$, et, par hypothèse de récurrence, $|A \cup B'| = |A| + b$. Il y a donc une bijection g de $[1, n + p]$ dans $A \cup B'$. On pose $g(|A| + b + 1) = c$ et on vérifie que g devient une bijection de $[1, n + p + 1]$ sur $A \cup B$, ce qui achève la récurrence. **cqfd.**

Théorème 1.2.2 (Produit). *Si A et B sont des ensembles finis, leur produit cartésien $A \times B$ est fini, et l'on a*

$$|A \times B| = |A||B|.$$

Démonstration. Par récurrence sur $b = |B|$. Si $b = 0$, B est vide et $A \times B$ aussi. On a donc bien $|A \times B| = 0 = |A|.0$ Si $|B| = b + 1$, on reprend les notations de la démonstration précédente. Comme $A \times B$ est réunion disjointe de $A \times B'$ et de $A \times \{c\}$. Ce dernier ensemble est en bijection avec A par l'application $h : A \rightarrow A \times \{c\}$ qui à $a \in A$ fait correspondre le couple (a, c) . Il est donc de cardinal $|A|$ et en appliquant le théorème précédent on a $|A \times B| = |A \times B'| + |A \times \{c\}| = |A|.b + |A| = |A|. (b + 1) = |A|. |B|$, ce qui achève la démonstration. **cqfd.**

Corollaire 1.2.3 (Principe des bergers). *Soit B un ensemble fini, $f : A \rightarrow B$ une application et n un entier naturel non nul. On suppose que*

$$\forall b \in B, |f^{-1}(b)| = n.$$

Alors A est fini et $|A| = n|B|$.

Démonstration. Pour chaque b dans B , numérotons de 1 à n les éléments de $f^{-1}(b)$. L'application qui à (i, b) fait correspondre le i -ème élément de $f^{-1}(b)$ est alors une bijection de $[1, n] \times B$ sur A . **cqfd.**

Ce principe est souvent appliqué pour calculer le cardinal de B . À chaque élément d'un ensemble A de pattes, on fait correspondre le mouton du troupeau B auquel elle est attachée. Comme chaque mouton a (en principe) 4 pattes, on peut en déduire qu'il y a 4 fois plus de pattes que de moutons, ou 4 fois moins de moutons que de pattes. Cela peut être pratique si l'on voit les pattes mais pas les moutons.

Théorème 1.2.4 (Ensemble puissance). *Si A et B sont des ensembles finis, alors l'ensemble A^B des applications de B dans A est fini et l'on a*

$$|A^B| = |A|^{|B|}.$$

Démonstration. Par récurrence sur $b = |B|$. Si $b = 0$, B est vide et il existe exactement une application de B dans A : à chaque élément de \emptyset est associé un élément de A et ceci ne peut être fait que d'une seule façon. On a donc bien $|A^\emptyset| = 1 = |A|^0$. Si $|B| = b + 1$, on reprend les notations de la démonstration précédente. À chaque application F de B dans A , faisons correspondre le couple $\Phi(F) = (G, a)$, où G est la restriction de F à B' et $a = F(c)$. L'application Φ est une bijection de A^B sur $A^{B'} \times A$. En appliquant successivement le théorème précédent, l'hypothèse de récurrence et la définition de l'exponentiation, on trouve bien

$$|A^B| = |A^{B'} \times A| = |A^{B'}| |A| = |A|^b \cdot |A| = |A|^{b+1} = |A|^{|B|}$$

ce qui achève la démonstration. **cqfd.**

1.2.2 Fonctions caractéristiques

Soit X un ensemble et A une partie de X . On appelle *fonction caractéristique* de A et on note $\mathbf{1}_A$ la fonction de X dans l'ensemble $\{0, 1\}$ définie par

$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon.} \end{cases}$$

Il est clair que l'application qui à A fait correspondre $\mathbf{1}_A$ est une bijection de $\mathcal{P}(X)$ sur $\{0, 1\}^X$, la réciproque étant l'application qui à f fait correspondre $A = \{x \in X; f(x) = 1\}$. On en déduit aussitôt la

Proposition 1.2.5. *Si $|X| = n$, alors $|\mathcal{P}(X)| = 2^n$.*

Les opérations d'intersection, de passage au complémentaire et de réunion se traduisent naturellement en termes de fonctions caractéristiques :

Proposition 1.2.6.

- $\mathbf{1}_{A \cap B} = \mathbf{1}_A \mathbf{1}_B$,
- $\mathbf{1}_{X \setminus A} = 1 - \mathbf{1}_A$,
- $\mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \mathbf{1}_B$.

Nous verrons plus loin une généralisation de cette dernière formule. Le cardinal d'une partie finie peut s'écrire en termes de fonctions caractéristiques :

Proposition 1.2.7. *Pour toute partie A d'un ensemble (fini) X , on a*

$$|A| = \sum_{x \in X} \mathbf{1}_A(x).$$

1.2.3 Sommes et produits dans un anneau commutatif

Soit A un anneau commutatif, c'est-à-dire un ensemble muni de deux lois de composition interne notées $+$ et \cdot (ou sans aucun signe) qui sont associatives et commutatives, admettant chacune un élément neutre noté respectivement 0 et 1 , et dans lequel on a l'existence d'un *opposé* et la relation de *distributivité*. En d'autres termes, pour tout a, b et c dans A , on a

- $a + b = b + a$,
- $(a + b) + c = a + (b + c)$,
- $0 + a = a$,
- $\exists a'; a + a' = 0$,
- $ab = ba$,
- $(ab)c = a(bc)$,
- $1 \cdot a = a$,
- $a(b + c) = ab + ac$.

Dans un anneau commutatif, on peut définir la somme ainsi que le produit d'une famille finie d'éléments : une somme vide vaut 0 et un produit vide vaut 1 , puis, par récurrence, on définit

$$\sum_{i=1}^{n+1} a_i = \left(\sum_{i=1}^n a_i \right) + a_{n+1}$$

et

$$\prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^n a_i \right) a_{n+1}.$$

Comme les opérations sont commutatives, on ne se préoccupe pas de l'ordre des opérands et on peut écrire simplement $\sum_{i \in I} a_i$ ou $\prod_{i \in I} a_i$ dès lors que l'ensemble d'indices I est fini. On peut dans ce cadre "développer un produit" :

Proposition 1.2.8 (Formule du produit). *Soient $(a_i)_{i \in [1, n]}$ et $(b_i)_{i \in [1, n]}$ deux familles finies d'éléments d'un anneau commutatif A . On a*

$$\prod_{i=1}^n (a_i + b_i) = \sum_{I \subset [1, n]} \left(\prod_{i \in I} a_i \right) \left(\prod_{i \in [1, n] \setminus I} b_i \right)$$

la somme étant indexée par les parties de I de $[1, n]$.

L'idée de cette proposition est que si l'on utilise autant de fois que possible la relation de distributivité pour développer le produit, on se retrouve avec une somme de termes. Chacun de ces termes est produit de n facteurs, un facteur provenant de chacune des sommes $(a_i + b_i)$ et valant donc soit a_i soit

b_i . En notant I l'ensemble des indices pour lesquels on a choisi a_i plutôt que b_i , on voit que chaque terme correspond à une partie I de $[1, n]$ et une seule, et que le terme correspondant à I est bien $\left(\prod_{i \in I} a_i\right) \left(\prod_{i \in [1, n] \setminus I} b_i\right)$.

La preuve suivante est là seulement pour respecter le règlement...

Démonstration. Par récurrence sur n . Pour $n = 0$, il suffit de voir que \emptyset est l'unique partie de \emptyset . La somme de droite a donc exactement un terme, qui est un produit vide comme la partie gauche de l'équation. On est donc ramené à $1 = 1$ qui est vrai.

En supposant la relation vraie pour n , on a

$$\begin{aligned}
\prod_{i=1}^{n+1} (a_i + b_i) &= (a_{n+1} + b_{n+1}) \prod_{i=1}^n (a_i + b_i) \\
&= (a_{n+1} + b_{n+1}) \sum_{I \subset [1, n]} \left(\prod_{i \in I} a_i\right) \left(\prod_{i \in [1, n] \setminus I} b_i\right) \\
&= a_{n+1} \sum_{I \subset [1, n]} \left(\prod_{i \in I} a_i\right) \left(\prod_{i \in [1, n] \setminus I} b_i\right) + b_{n+1} \sum_{I \subset [1, n]} \left(\prod_{i \in I} a_i\right) \left(\prod_{i \in [1, n] \setminus I} b_i\right) \\
&= \sum_{I \subset [1, n]} \left(\prod_{i \in I \cup \{n+1\}} a_i\right) \left(\prod_{i \in [1, n] \setminus I} b_i\right) + \sum_{I \subset [1, n]} \left(\prod_{i \in I} a_i\right) \left(\prod_{i \in [1, n+1] \setminus I} b_i\right) \\
&= \sum_{\substack{J \subset [1, n+1] \\ n+1 \in J}} \left(\prod_{i \in J} a_i\right) \left(\prod_{i \in [1, n+1] \setminus J} b_i\right) + \sum_{\substack{J \subset [1, n+1] \\ n+1 \notin J}} \left(\prod_{i \in J} a_i\right) \left(\prod_{i \in [1, n+1] \setminus J} b_i\right) \\
&= \sum_{J \subset [1, n+1]} \left(\prod_{i \in J} a_i\right) \left(\prod_{i \in [1, n+1] \setminus J} b_i\right)
\end{aligned}$$

ce qui constitue la relation pour $n + 1$ et achève la preuve par récurrence. Le passage de la quatrième ligne à la cinquième se fait en posant $J = I \cup \{n + 1\}$ dans la première somme et $J = I$ dans la seconde. **cqfd.**

1.2.4 La formule du binôme

Un cas particulier important de la formule du produit est celui où tous les a_i sont égaux entre eux et tous les b_i de même. la formule devient

$$(a + b)^n = \sum_{I \subset [1, n]} a^{|I|} b^{n-|I|}$$

c'est-à-dire que le terme correspondant à $I \subset [1, n]$ ne dépend que du cardinal $|I|$ qui est un entier k compris entre 0 et n . Il est alors naturel de regrouper

entre eux les termes correspondant à la même valeur de k . Cela amène à définir les *coefficients binômiaux*. Pour tout couple d'entiers naturels n et k , on note $\binom{n}{k}$ et on prononce “ k parmi n ” le nombre de parties à k éléments dans un ensemble à n éléments. On a donc la

Proposition 1.2.9 (formule du binôme).

$$\forall n \in \mathbb{N}, \forall a, b \in A, \quad (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

Il est utile de pouvoir calculer ces coefficients. Pour $n = 0$, il s'agit de compter les parties de l'ensemble vide. Il y en a une seule, et son cardinal est 0. On a donc

$$\binom{0}{k} = \begin{cases} 1 & \text{si } k = 0, \\ 0 & \text{sinon.} \end{cases}$$

De façon générale, il est clair que $\binom{n}{k}$ est nul sauf si $0 \leq k \leq n$. On peut donc convenir que $\binom{n}{k} = 0$ pour $k < 0$. On a alors la

Proposition 1.2.10.

$$\forall n \in \mathbb{N}, \forall k \in \mathbb{Z}, \quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Démonstration. Posons

$$\begin{aligned} A &= \{I \subset [1, n+1]; |I| = k\}, \\ B &= \{I \in A; n+1 \in I\}, \\ C &= \{I \in A; n+1 \notin I\}, \\ B' &= \{J \subset [1, n]; |J| = k-1\}, \\ C' &= \{J \subset [1, n]; |J| = k\}. \end{aligned}$$

L'application $J \mapsto J \cup \{n+1\}$ est une bijection de B' sur B . Les ensembles C et C' coïncident, et A est réunion disjointe de B et C . On a donc

$$\binom{n+1}{k} = |A| = |B| + |C| = |B'| + |C'| = \binom{n}{k-1} + \binom{n}{k},$$

et les coefficients du binôme peuvent se calculer par récurrence. **cqfd.**

En pratique, la méthode ci-dessus est celle qui est employée pour calculer les coefficients du binôme et construire ce qu'on appelle le *triangle de Pascal*, c'est-à-dire une table de ces coefficients, généralement arrangée comme ci-dessous.

	$k = 0$	$k = 1$	$k = 2$	$k = 3$	$k = 4$	$k = 5$	$k = 6$	$k = 7$	$k = 8$
$n = 0$	1								
$n = 1$	1	1							
$n = 2$	1	2	1						
$n = 3$	1	3	3	1					
$n = 4$	1	4	6	4	1				
$n = 5$	1	5	10	10	5	1			
$n = 6$	1	6	15	20	15	6	1		
$n = 7$	1	7	21	35	35	21	7	1	
$n = 8$	1	8	28	56	70	56	28	8	1

chaque terme étant somme de celui qui est immédiatement au dessus et de celui qui est à gauche de celui-là. Les cases vides contiennent la valeur 0.

1.2.5 Arrangements, permutations et combinaisons

La factorielle d'un entier n est définie (par récurrence) par la formule

$$n! = \prod_{i \in [1, n]} i = \begin{cases} 1 & \text{si } n = 0, \\ n \cdot (n-1)! & \text{sinon.} \end{cases}$$

On peut exprimer à l'aide de factorielles le nombre $A(n, k)$ de k -arrangements ou injections de $[1, k]$ dans $[1, n]$:

Proposition 1.2.11.

$$\forall k, n \in \mathbb{N}, \quad A(n, k) = \langle n \rangle_k = \prod_{0 \leq i < k} (n - i) = \begin{cases} \frac{n!}{(n-k)!} & \text{si } k \leq n, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. La deuxième égalité étant évidente, prouvons la première par récurrence sur k . Il y a une seule injection de l'ensemble vide dans $[1, n]$ et le produit vide vaut 1. L'égalité est donc vraie pour $k = 0$. Supposons la relation vraie pour k . À chaque injection f de $[1, k+1]$ dans $[1, n]$ on fait correspondre $g = \varphi(f)$, sa restriction à $[1, k]$ qui est une injection de $[1, k]$ dans $[1, n]$. L'image réciproque $\varphi^{-1}(g)$ est formée des f qui ont même valeur que g sur $[1, k]$. Il y en a autant que de valeurs possibles pour $f(k+1)$,

c'est-à-dire n'importe quel élément de $[1, n]$ différent des k valeurs prises par g . Il y a donc $n - |g([1, k])| = n - k$ éléments dans $\varphi^{-1}(g)$. On déduit donc du principe des bergers que

$$A(n, k+1) = (n-k)A(n, k) = (n-k) \prod_{0 \leq i < k} (n-i) = \prod_{0 \leq i < k+1} (n-i)$$

d'où le résultat.

cqfd.

Le cas particulier $k = n$ mérite d'être considéré à part. On appelle *permutation* d'un ensemble X une bijection de X dans lui-même. Pour tout entier naturel n , on note $\mathfrak{S}(n)$ l'ensemble des permutations de $[1, n]$:

Corollaire 1.2.12.

$$\forall n \in \mathbb{N}, \quad |\mathfrak{S}(n)| = n!.$$

On peut maintenant compter le nombre de *k-combinaisons*, c'est-à-dire de parties de cardinal k , de $[1, n]$:

Proposition 1.2.13.

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } 0 \leq k \leq n \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. Nous allons donner deux preuves distinctes de cette importante relation. La première est une application du principe des bergers. À chaque injection f de $[1, k]$ dans $[1, n]$, faisons correspondre son image $\varphi(f) = A = f([1, k])$. C'est une partie de $[1, n]$ de cardinal k . Si A est une partie de $[1, n]$ de cardinal k , il existe une bijection f de $[1, k]$ sur A . L'ensemble $\varphi^{-1}(A)$ est formé des $f \circ \sigma$, où σ parcourt $\mathfrak{S}(k)$. On a donc

$$|\varphi^{-1}(A)| = |\mathfrak{S}(k)| = k!$$

et le principe des bergers donne

$$A(n, k) = k! \binom{n}{k}$$

d'où la proposition. L'autre démonstration est par récurrence sur n . Le cas

$n = 0$ est immédiat. Un calcul simple donne

$$\begin{aligned}
 \binom{n+1}{k} &= \binom{n}{k} + \binom{n}{k-1} \\
 &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\
 &= \frac{n!}{(k-1)!(n-k)!} \left(\frac{1}{k} + \frac{1}{n-k+1} \right) \\
 &= \frac{n!}{(k-1)!(n-k)!} \cdot \frac{n+1}{k(n-k+1)} \\
 &= \frac{(n+1)!}{k!(n+1-k)!}
 \end{aligned}$$

pour $1 \leq k \leq n$. Il reste les cas $k = 0$ et $k = n + 1$ pour lesquels les deux membres valent 1. **cqfd.**

1.2.6 Les coefficients multinomiaux

Il est facile de généraliser la formule du binôme au cas d'un trinôme, etc. Pour chaque r -uplet d'entiers naturels (k_1, k_2, \dots, k_r) de somme n , on définit le *coefficient multinomial*

$$\binom{n}{k_1, k_2, \dots, k_r}$$

comme le nombre de r -uplets (A_1, A_2, \dots, A_r) de parties disjointes de $[1, n]$ telles que $\forall i, |A_i| = k_i$.

Proposition 1.2.14. *Soit $(a_1, a_2, \dots, a_r) \in \mathcal{A}^r$ un r -uplet d'éléments d'un anneau commutatif et n un entier naturel. On a*

$$(a_1 + a_2 + \dots + a_r)^n = \sum_{k_1+k_2+\dots+k_r=n} \binom{n}{k_1, k_2, \dots, k_r} a_1^{k_1} a_2^{k_2} \dots a_r^{k_r}.$$

On a pour ces coefficients une formule analogue à celle des coefficients binomiaux

$$\binom{n}{k_1, k_2, \dots, k_r} = \frac{n!}{k_1! k_2! \dots k_r!}$$

et dans le cas $r = 2$, on retrouve les coefficients du binôme

Proposition 1.2.15. *Si $k_1 + k_2 = n$, on a*

$$\binom{n}{k_1, k_2} = \binom{n}{k_1} = \binom{n}{k_2}.$$

1.2.7 La formule du crible

Il est relativement simple de prouver que, si A et B sont des parties finies d'un ensemble E , leur réunion est finie et l'on a

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

et de même

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Dans le cas général, on a la *formule du crible*.

Théorème 1.2.16 (Formule du crible). *Si $(A_i)_{i \in [1, n]}$ est une famille de n parties d'un ensemble fini E , leur réunion a pour cardinal*

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \sum_{\substack{I \subset [1, n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right| \\ &= \sum_i |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots \\ &\quad \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n| \end{aligned}$$

Ce théorème est aussi appelé *principe d'inclusion-exclusion*.

Démonstration. Dans l'anneau \mathcal{A} des fonctions de E dans \mathbb{Z} , posons $a_i = -\mathbf{1}_{A_i}$ et $b_i = 1$, de façon que $a_i + b_i = \mathbf{1}_{E \setminus A_i}$, et appliquons la formule du produit :

$$\begin{aligned} 1 - \mathbf{1}_{\bigcup_{i=1}^n A_i} &= \mathbf{1}_{E \setminus \bigcup_{i=1}^n A_i} \\ &= \mathbf{1}_{\bigcap_{i=1}^n E \setminus A_i} \\ &= \prod_{i=1}^n (a_i + b_i) \\ &= \sum_{I \subset [1, n]} \left(\prod_{i \in I} (-\mathbf{1}_{A_i}) \right) \\ &= \sum_{I \subset [1, n]} (-1)^{|I|} \mathbf{1}_{\bigcap_{i \in I} A_i} \\ &= 1 + \sum_{\substack{I \subset [1, n] \\ I \neq \emptyset}} (-1)^{|I|} \mathbf{1}_{\bigcap_{i \in I} A_i}. \end{aligned}$$

En effet, le terme correspondant à $I = \emptyset$ vaut 1. On élimine ce terme et on change de signe pour obtenir

$$\mathbf{1}_{\bigcup_{i=1}^n A_i} = \sum_{\substack{I \subset [1, n] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathbf{1}_{\bigcap_{i \in I} A_i}.$$

Il reste à calculer la somme des valeurs de ces deux fonctions

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \sum_{x \in E} \mathbf{1}_{\bigcup_{i=1}^n A_i}(x) \\ &= \sum_{x \in E} \left(\sum_{\substack{I \subset [1, n] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathbf{1}_{\bigcap_{i \in I} A_i} \right)(x) \\ &= \sum_{\substack{I \subset [1, n] \\ I \neq \emptyset}} (-1)^{|I|+1} \sum_{x \in E} \mathbf{1}_{\bigcap_{i \in I} A_i}(x) \\ &= \sum_{\substack{I \subset [1, n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|. \end{aligned}$$

cqfd.

1.2.8 Surjections

Grâce à la formule du crible, on peut compter le nombre $S(n, k)$ de surjections de $[1, n]$ dans $[1, k]$. Notons $E = [1, k]^{[1, n]}$ l'ensemble des applications de $[1, n]$ dans $[1, k]$. On a vu que $|E| = k^n$. Pour tout $i \in [1, k]$, notons

$$A_i = \{f \in E; i \notin f([1, n])\}$$

l'ensemble des applications de $[1, n]$ dans $[1, k]$. La réunion des A_i est l'ensemble des applications de $[1, n]$ dans $[1, k]$ qui ne sont pas surjectives. Il y en a donc $k^n - S(n, k)$. Pour tout $I \subset [1, k]$, on a

$$A_I = \bigcap_{i \in I} A_i = \{f \in E; f([1, n]) \cap I = \emptyset\} = ([1, k] \setminus I)^{[1, n]}$$

et $|A_I| = (k - |I|)^n$ ne dépend que du cardinal $r = |I|$. La formule du crible donne donc

$$k^n - S(n, k) = \left| \bigcup_{i \in [1, k]} A_i \right| = \sum_{\substack{I \subset [1, k] \\ I \neq \emptyset}} (-1)^{|I|+1} |A_I| = \sum_{r=1}^k \binom{k}{r} (-1)^{r+1} (k-r)^n$$

On a donc montré la

Proposition 1.2.17.

$$\forall n, k \in \mathbb{N}, \quad S(n, k) = \sum_{r=0}^k (-1)^r \binom{k}{r} (k-r)^n.$$

Explicitons le cas $k = 4$. On a

$$S(n, 4) = 4^n - 4 \cdot 3^n + 6 \cdot 2^n - 4 \cdot 1^n + 0^n = \begin{cases} 4^n - 4 \cdot 3^n + 6 \cdot 2^n - 4 & \text{si } n > 0 \\ 1 - 4 + 6 - 4 + 1 = 0 & \text{si } n = 0 \end{cases}$$

n	4^n	3^n	2^n	$4^n - 4 \cdot 3^n + 6 \cdot 2^n - 4 \cdot 1^n + 0^n$	$S(n, k)$
0	1	1	1	$1 - 4 + 6 - 4 + 1$	0
1	4	3	2	$4 - 12 + 12 - 4$	0
2	16	9	4	$16 - 36 + 24 - 4$	0
3	64	27	8	$64 - 108 + 48 - 4$	0
4	256	81	16	$256 - 324 + 96 - 4$	24
5	1024	243	32	$1024 - 972 + 192 - 4$	240

et on vérifie bien que $S(n, 4) = 0$ pour $n < 4$ et $S(4, 4) = 24 = 4!$ puisqu'une surjection de $[1, 4]$ dans lui-même est automatiquement une bijection.

Chapitre 2

Polynômes et séries formelles

2.1 Séries formelles

2.1.1 L'anneau des séries formelles

Un polynôme $P = \sum_{n=0}^p a_n X^n$ est simplement une façon commode de noter la suite finie $(a_n)_{0 \leq n \leq p}$ de ses coefficients. Si $Q = \sum_{n=0}^q b_n X^n$ est un autre polynôme, on définit leur somme et leur produit par

$$P + Q = \sum_{n=0}^{\max(p,q)} (a_n + b_n) X^n, \quad \text{et} \quad PQ = \sum_{n=0}^{p+q} \left(\sum_{i=0}^n a_i b_{n-i} \right) X^n.$$

mais ces formules ne sont valables qu'à condition d'accepter la convention $a_n = 0$ pour $n > p$. En fait, les coefficients d'un polynôme ne sont pas les éléments d'une suite finie, mais ceux d'une suite infinie $(a_n)_{n \in \mathbb{N}}$ à *support fini* c'est-à-dire que l'on impose que les a_n sont nuls, sauf pour un nombre fini de valeurs de n . Si l'on s'affranchit de cette restriction, on arrive à un objet en un sens encore plus simple qu'un polynôme.

Dans la suite de ce chapitre, nous notons \mathcal{A} un anneau commutatif quelconque, mais nous sommes surtout intéressés par les cas $\mathcal{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou \mathbb{C} .

À toute suite $(a_n)_{n \in \mathbb{N}}$ à valeurs dans un anneau commutatif \mathcal{A} , on associe donc une *série entière formelle*, notée

$$A = \sum_{n=0}^{\infty} a_n X^n$$

et on définit des opérations sur ces objets. Si $B = \sum_{n=0}^{\infty} b_n X^n$ est une autre série entière formelle, leur somme $S = A + B = \sum_{n=0}^{\infty} s_n X^n$ et leur produit

$P = AB = \sum_{n=0}^{\infty} p_n X^n$ sont définis par

$$\forall n \in \mathbb{N}, \quad s_n = a_n + b_n \quad \text{et} \quad p_n = \sum_{i=0}^n a_i b_{n-i} = \sum_{i+j=n} a_i b_j.$$

Pour tout élément a de \mathcal{A} la suite de coefficients $a_0 = a$ et $a_n = 0$ pour $n > 0$ est associée à une série entière formelle que l'on note encore simplement a . On dit que a est une *constante*. On note $\mathcal{A}[[X]]$ l'ensemble des séries entières formelles à coefficients dans \mathcal{A} .

Théorème 2.1.1. *Muni des lois ci-dessus, l'ensemble $\mathcal{A}[[X]]$ des séries entières formelles à coefficients dans l'anneau commutatif \mathcal{A} forme lui-même un anneau commutatif. Les éléments neutres de l'addition et de la multiplication sont les séries constantes 0 et 1, et l'opposé de A est donné par $-A = \sum_{n=0}^{\infty} (-a_n) X^n$.*

Démonstration. Il suffit de vérifier un à un les axiomes des anneaux commutatifs énoncés plus haut. Toutes ces vérifications sont immédiates. Nous traiterons seulement l'associativité de la multiplication et la distributivité. Soit donc $C = \sum_{n=0}^{\infty} c_n X^n$ une troisième série. On a

$$\begin{aligned} (AB)C &= \sum_{n \in \mathbb{N}} \left(\sum_{i+j=n} \left(\sum_{k+l=i} a_k b_l \right) c_j \right) X^n \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{k+l+j=n} a_k b_l c_j \right) X^n \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{k+m=n} a_k \left(\sum_{l+j=m} b_l c_j \right) \right) X^n \\ &= A(BC) \end{aligned}$$

et

$$\begin{aligned} A(B+C) &= \sum_{n \in \mathbb{N}} \left(\sum_{i+j=n} a_i (b_j + c_j) \right) X^n \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{i+j=n} a_i b_j + a_i c_j \right) X^n \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{i+j=n} a_i b_j \right) X^n + \sum_{n \in \mathbb{N}} \left(\sum_{i+j=n} a_i c_j \right) X^n \\ &= AB + AC \end{aligned}$$

cqfd.

Un anneau \mathcal{A} est *intègre* si l'équation $xy = 0$ dans \mathcal{A} implique $x = 0$ ou $y = 0$.

Théorème 2.1.2. *Si \mathcal{A} est intègre, $\mathcal{A}[[X]]$ l'est aussi.*

Démonstration. Supposons $A \neq 0$ et $B \neq 0$. La suite $(a_n)_{n \in \mathbb{N}}$ n'est pas identiquement nulle. Il existe donc un entier i_0 tel que $a_{i_0} \neq 0$ et $\forall i < i_0, a_i = 0$. De même, il existe $j_0 \in \mathbb{N}$ tel que $b_{j_0} \neq 0$ et $\forall j < j_0, b_j = 0$. Posons $n_0 = i_0 + j_0$. On a

$$\sum_{i+j=n_0} a_i b_j = \sum_{\substack{i+j=n_0 \\ i < i_0}} a_i b_j + a_{i_0} b_{j_0} + \sum_{\substack{i+j=n_0 \\ j < j_0}} a_i b_j = a_{i_0} b_{j_0} \neq 0$$

puisque \mathcal{A} est intègre. On en déduit que le coefficient de X^{n_0} dans AB est non nul et $AB \neq 0$. **cqfd.**

2.1.2 Inversion, composition, dérivation

Les séries dont le terme constant est 1 sont *inversibles* :

Proposition 2.1.3. *Si $A = 1 + \sum_{n \geq 1} a_n X^n$ est une série entière formelle dont le coefficient constant est 1, il existe une unique série*

$$B = 1 + \sum_{n \geq 1} b_n X^n$$

telle que $AB = 1$. Cette série sera notée $\frac{1}{A}$.

Démonstration. La condition s'écrit $a_0 b_0 = 1$ et $\sum_{k=0}^n a_k b_{n-k} = 0$ pour $n > 0$. La suite définie par récurrence par

$$\begin{cases} b_0 = 1 \\ b_n = -\sum_{k=1}^n a_k b_{n-k} \quad \text{pour } n > 0 \end{cases}$$

vérifie donc les hypothèses, et c'est la seule. **cqfd.**

Contrairement à ce qui se passe pour les polynômes, il n'est pas possible d'évaluer une série formelle en un point $a \in \mathcal{A}$. Par contre, il est possible de composer les séries A et B , ce qui revient à évaluer A en B , à condition que le coefficient constant de B soit nul.

Proposition 2.1.4. *Si $A = \sum_{n \in \mathbb{N}} a_n X^n$ est une série entière formelle quelconque, et $B = \sum_{n \geq 1} b_n X^n$ est une série entière formelle dont le coefficient constant est nul, il existe une série $C = \sum_{n \in \mathbb{N}} c_n X^n$ et une seule, notée $A(B)$ ou $A \circ B$, telle que pour tout n c_n soit le coefficient de X^n dans l'écriture de la série $\sum_{k=0}^m a_k B^k$ pour tout $m \geq n$. On écrit aussi $C = \sum_{n \in \mathbb{N}} a_n B^n$.*

On peut définir une dérivation. Si $A = \sum_{n \in \mathbb{N}} a_n X^n$ on appelle *dérivée* de A et on note A' la série

$$A' = \sum_{n \in \mathbb{N}} (n+1)a_{n+1}X^n = \sum_{n \geq 1} n a_n X^{n-1}.$$

On a les relations habituelles

$$\begin{aligned} (A+B)' &= A' + B' \\ (AB)' &= A'B + AB' \\ (A \circ B)' &= B' \cdot (A' \circ B). \end{aligned}$$

Démonstration. Démontrons la deuxième égalité. On a

$$\begin{aligned} (AB)' &= \sum_{n \in \mathbb{N}} \left((n+1) \sum_{k=0}^{n+1} a_k b_{n+1-k} \right) X^n \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{k=1}^{n+1} k a_k b_{n+1-k} + \sum_{k=0}^n (n+1-k) a_k b_{n+1-k} \right) X^n \\ &= \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^n (k+1) a_{k+1} b_{n-k} \right) X^n + \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^n a_k (n-k+1) b_{n-k-1} \right) X^n \\ &= A'B + AB' \end{aligned}$$

cqfd.

2.1.3 Quelques exemples

La série $1 - X$ est inversible. Il est facile de voir que son inverse est

$$\frac{1}{1-X} = \sum_{n \in \mathbb{N}} X^n = 1 + X + X^2 + X^3 + \dots$$

plus généralement, si $\alpha \in \mathcal{A}$, on peut écrire

$$\frac{1}{1-\alpha X} = \sum_{n \in \mathbb{N}} \alpha^n X^n = 1 + \alpha X + \alpha^2 X^2 + \alpha^3 X^3 + \dots$$

On peut définir une exponentielle formelle dans $\mathbb{Q}[[X]]$

$$E(X) = \sum_{n \in \mathbb{N}} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \dots$$

et un logarithme formel

$$L(X) = \sum_{n \geq 1} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} + \dots$$

et on a les relations

$$E(L(X)) = 1 + X, \quad L(E(X) - 1) = X.$$

En effet, on voit facilement que $E' = E$ et $L' = \frac{1}{1+X}$. On a donc $(L(E-1))' = E.L'(E-1) = \frac{E}{E} = 1$, ce qui donne $L(E-1) = X$ puisque le coefficient constant est 0. De même, $(E(L))' = L'.E(L)$, donc $(1+X)(E(L))' = E(L)$. Les coefficients de $E(L)$ vérifient donc la récurrence $(n+1)a_{n+1} + na_n = a_n$, ou encore $a_{n+1} = \frac{1-n}{1+n}a_n$ qui, compte tenu de $a_0 = 1$, donne $a_1 = 1$ et $a_n = 0$ pour $n > 1$, donc $E(L) = 1 + X$.

Pour tout $a \in \mathcal{A}$ et tout $n \in \mathbb{N}$, introduisons la *factorielle descendante* $a^n = a(a-1)\dots(a-n+1)$ définie par récurrence par $a^0 = 1$ et $a^{n+1} = (a-n)a^n$. Si $\mathbb{Q} \subset \mathcal{A}$ et $\alpha \in \mathcal{A}$ on peut définir

$$\begin{aligned} (1+X)^\alpha &= E(\alpha L(X)) = \sum_{n \in \mathbb{N}} \frac{\alpha^n}{n!} X^n \\ &= 1 + \alpha X + \frac{\alpha(\alpha-1)}{2} X^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6} X^3 + \dots \end{aligned}$$

En effet, on a $E(\alpha L)' = \alpha L' E(\alpha L)$. Les coefficients de $E(L)$ vérifient donc la récurrence $(n+1)a_{n+1} + na_n = \alpha a_n$, ou encore $a_{n+1} = \frac{\alpha-n}{1+n}a_n$ qui, compte tenu de $a_0 = 1$, donne bien $a_n = \frac{\langle \alpha \rangle_n}{n!}$.

Si $\alpha \in \mathbb{N}$, la série est un polynôme, et on retrouve bien la formule du binôme. On a alors la

Proposition 2.1.5.

$$\forall \alpha, \beta \in \mathcal{A}, \quad (1+X)^{\alpha+\beta} = (1+X)^\alpha \cdot (1+X)^\beta.$$

Démonstration. En utilisant la formule du binôme, on prouve

$$\begin{aligned} E(\alpha X)E(\beta X) &= \sum_{n \in \mathbb{N}} \left(\sum_{k=0}^n \frac{\alpha^k}{k!} \cdot \frac{\beta^{n-k}}{(n-k)!} \right) X^n \\ &= \sum_{n \in \mathbb{N}} \frac{1}{n!} \left(\sum_{k=0}^n \binom{n}{k} \alpha^k \beta^{n-k} \right) X^n \\ &= \sum_{n \in \mathbb{N}} \frac{(\alpha + \beta)^n}{n!} X^n \\ &= E((\alpha + \beta)X) \end{aligned}$$

et on obtient la relation cherchée en substituant L à X .

cqfd.

Explicitons en particulier le cas de la racine carrée

$$\sqrt{1+X} = 1 + \sum_{n \geq 1} \frac{(-1)^{n-1}}{2^{2n-1}n} \binom{2n-2}{n-1} X^n.$$

En effet, le coefficient $\frac{(1/2)^n}{n!}$ peut s'écrire

$$\frac{\frac{1}{2} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdots \frac{3-2n}{2}}{n!} = \frac{(-1)^{n-1} 1 \cdot 3 \cdot 5 \cdots (2n-3)}{2^n n!} = \frac{(-1)^{n-1} (2n-2)!}{2^{2n-1} n! (n-1)!}$$

en "complétant la factorielle" au numérateur par les facteurs impairs manquants $2 \cdot 4 \cdot 6 \cdots (2n-2) = 2^{n-1} (n-1)!$, d'où le résultat.

2.1.4 Récurrences linéaires à coefficients constants.

On peut utiliser les séries génératrices pour retrouver les résultats classiques sur les suites récurrentes linéaires à coefficients constants

Considérons par exemple la suite d'entiers définie par $u_0 = 4$, $u_1 = 13$ et $u_n = 5u_{n-1} - 6u_{n-2}$ pour $n \geq 2$. On forme la série

$$\begin{aligned} U &= \sum_{n \in \mathbb{N}} u_n X^n \\ &= 4 + 13X + \sum_{n \geq 2} u_n X^n \\ &= 4 + 13X + 5 \sum_{n \geq 2} u_{n-1} X^n - 6 \sum_{n \geq 2} u_{n-2} X^n \\ &= 4 + 13X + 5X(U - 4) - 6X^2U \\ &= 4 - 7X + (5X - 6X^2)U \end{aligned}$$

Il s'agit d'une équation de degré 1 en U , que l'on résout :

$$U = \frac{4 - 7X}{1 - 5X + 6X^2} = \frac{4 - 7X}{(1 - 2X)(1 - 3X)}$$

en décomposant la fraction rationnelle en éléments simples, on obtient

$$U = \frac{5}{1 - 3X} - \frac{1}{1 - 2X} = \sum_{n \in \mathbb{N}} (5 \cdot 3^n - 2^n) X^n$$

et la formule finale $\forall n \in \mathbb{N}, u_n = 5 \cdot 3^n - 2^n$.

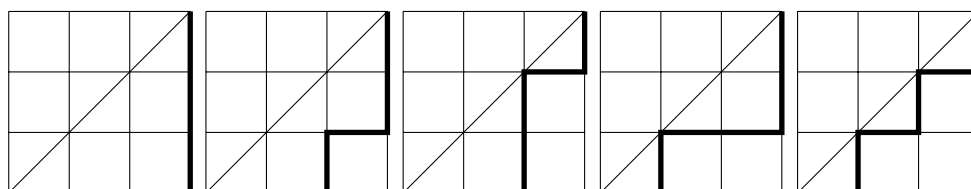
Dans ce cas, le *polynôme caractéristique* $1 - 5X + 6X^2$ avait deux racines distinctes, $\frac{1}{2}$ et $\frac{1}{3}$. Voyons ce qui se passe s'il a une racine double. Définissons la suite v par $v_0 = 1$, $v_1 = 6$ et $v_n = 6v_{n-1} - 9v_{n-2}$. Un calcul similaire donne

$$V = \frac{1}{1 - 6X + 9X^2} = \frac{1}{(1 - 3X)^2} = \sum_{n \in \mathbb{N}} (n + 1)3^n X^n$$

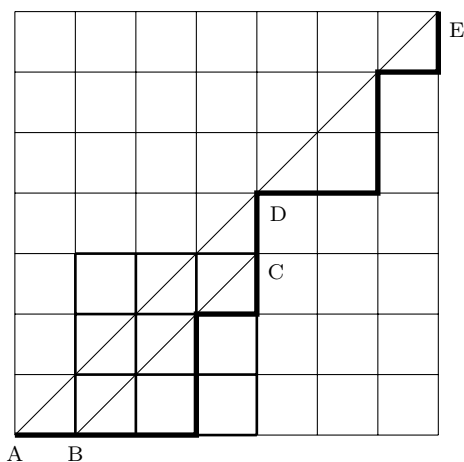
Cette dernière formule peut s'obtenir soit à partir de la formule générale pour $(1 + X)^\alpha$ avec $\alpha = -2$, soit en remarquant que $\frac{1}{(1-X)^2}$ est la dérivée de $\frac{1}{1-X} = \sum_{n \in \mathbb{N}} X^n$.

2.1.5 Les nombres de Catalan

Nous concluons cette section par un théorème célèbre dû à Euler (1707-1783). Nous allons calculer le nombre C_n de chemins qui mènent du coin en bas à gauche d'un carré de côté n au coin en haut à droite en suivant les côtés des carrés de côté 1, en allant toujours vers le haut ou vers la droite et sans jamais monter au dessus de la diagonale principale du carré. La figure ci-dessous illustre les chemins acceptables pour $n = 3$ et prouve que $C_3 = 5$. On voit facilement que $C_0 = C_1 = 1$ et $C_2 = 2$, mais comment obtenir une formule générale ?



On voit que tout chemin acceptable commence par aller de $A = (0, 0)$ à $B = (1, 0)$. Il refera contact avec la diagonale pour la première fois au point $D = (k, k)$. L'entier k est compris entre 1 et n . Combien y a-t-il de chemins acceptables pour une valeur donnée de k ? Juste avant d'atteindre (k, k) , le chemin venait forcément de $C = (k, k - 1)$ et entre les points $(1, 0)$ et $(k, k - 1)$, il parcourt un chemin acceptable dans le carré de sommets $(1, 0)$ et $(k, k - 1)$ qui est de côté $k - 1$. La figure représente un cas avec $n = 7$ et $k = 4$.



Il y a donc C_{k-1} possibilités pour cette première étape. Entre $D = (k, k)$ et $E = (n, n)$, il parcourt un chemin acceptable dans le carré de sommets (k, k) et (n, n) qui est de côté $n - k$. Il y a donc C_{n-k} possibilités pour cette deuxième étape. Le nombre de chemins possibles à k fixé est donc $C_{k-1}C_{n-k}$ et on a établi la formule

$$\forall n \geq 1, \quad C_n = \sum_{k=1}^n C_{k-1}C_{n-k} = \sum_{k=0}^{n-1} C_k C_{n-1-k}$$

qui permet de calculer les C_n par récurrence. On a donc $C_4 = 1.5 + 1.2 + 2.1 + 5.1 = 14$, $C_5 = 1.14 + 1.5 + 2.2 + 5.1 + 14.1 = 42$, etc. Formons la série génératrice $F = \sum_{n \in \mathbb{N}} C_n X^n$. On a donc

$$F = 1 + \sum_{n \geq 1} \left(\sum_{k=0}^{n-1} C_k C_{n-1-k} \right) X^n = 1 + X \sum_{m \in \mathbb{N}} \left(\sum_{k=0}^m C_k C_{m-k} \right) X^m$$

en posant $m = n - 1$. On reconnaît sur la droite le développement de F^2 . On a donc prouvé

$$F = 1 + XF^2$$

ce qui est une équation du second degré en F . La résolution habituelle de l'équation $XF^2 - F + 1 = 0$, de discriminant $\Delta = 1 - 4X$ donnerait

$$F = \frac{1 \pm \sqrt{1 - 4X}}{2X}$$

Le choix du signe $+$ ne donne pas une série entière formelle. En utilisant la formule ci dessus pour $\sqrt{1 + X}$, on trouve

$$\sqrt{1 - 4X} = 1 - \sum_{n \geq 1} \frac{2}{n} \binom{2n-2}{n-1} X^n.$$

On a donc

$$F = \frac{1 - \sqrt{1 - 4X}}{2X} = \sum_{n \geq 1} \frac{1}{n} \binom{2n-2}{n-1} X^{n-1} = \sum_{n \in \mathbb{N}} \frac{1}{n+1} \binom{2n}{n} X^n$$

et la formule

$$\forall n \in \mathbb{N}, \quad C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{2n!}{n!(n+1)!}.$$

On pourrait objecter que la formule pour la résolution des équations du second degré n'a pas été démontrée dans le cadre des séries entières formelles. Pour compléter le raisonnement, on peut partir de la solution proposée : la série

$$G = \frac{1 - \sqrt{1 - 4X}}{2X} = \sum_{n \in \mathbb{N}} \frac{1}{n+1} \binom{2n}{n} X^n$$

vérifie bien $G = 1 + XG^2$. En soustrayant cette équation à $F = 1 + XF^2$, on trouve $(F - G)(1 - X(F + G)) = 0$. Comme le facteur $1 - X(F + G)$ n'est pas nul et $\mathbb{Q}[[X]]$ est intègre, on en déduit bien $F = G$.

Les nombres de Catalan ne comptent pas seulement des trajets dans un carré. On peut montrer que C_n est le nombre de façons de diviser en triangles un polygone convexe à $n+2$ côtés, le nombre de façons correctes d'imbriquer n parenthèses ouvrantes et n parenthèses fermantes, le nombre d'arbres binaires pleins à n nœuds intérieurs, etc.

2.2 Polynômes

2.2.1 Relations entre racines et coefficients

Soit $(\alpha_1, \alpha_2, \dots, \alpha_n)$ un n -uplet d'éléments d'un anneau commutatif A . On définit le polynôme unitaire

$$P = \prod_{i=1}^n (X - \alpha_i).$$

On peut encore utiliser la formule du produit en posant $a_i = -\alpha_i$ et $b_i = X$. On trouve

$$P = \sum_{I \subset [1, n]} (-1)^{|I|} \left(\prod_{i \in I} \alpha_i \right) X^{n-|I|}$$

ce qui suggère de regrouper les I de même cardinal k :

$$P = \sum_{k=0}^n (-1)^k \sum_{\substack{I \subset [1, n] \\ |I|=k}} \left(\prod_{i \in I} \alpha_i \right) X^{n-k} = \sum_{k=0}^n (-1)^k \sigma_k X^{n-k}.$$

où

$$\sigma_k = \sum_{\substack{I \subset [1,n] \\ |I|=k}} \left(\prod_{i \in I} \alpha_i \right)$$

est le k -ième *polynôme symétrique élémentaire* des $(\alpha_i)_{i \in [1,n]}$. Par exemple, pour $n = 4$, en notant a, b, c et d plutôt que $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, on trouve

$$\begin{aligned} \sigma_0 &= 1 \\ \sigma_1 &= a + b + c + d \\ \sigma_2 &= ab + ac + ad + bc + bd + cd \\ \sigma_3 &= abc + abd + acd + bcd \\ \sigma_4 &= abcd \\ \sigma_k &= 0 \quad \text{pour } k > 4. \end{aligned}$$

2.2.2 Polynômes symétriques

Un polynôme de plusieurs variables est dit *symétrique* s'il ne dépend pas de l'ordre des variables. Par exemple chaque σ_k est une fonction symétrique des α_i . En fait tous les polynômes symétriques s'obtiennent à partir de ces derniers, ce qui justifie leur nom.

Théorème 2.2.1. *Pour tout polynôme $f \in A[\alpha_1, \dots, \alpha_n]$ symétrique en les indéterminées $(\alpha_i)_{1 \leq i \leq n}$, il existe un polynôme $g \in A[S_1, \dots, S_n]$ (et un seul) tel que $f(\alpha_1, \dots, \alpha_n) = g(\sigma_1, \dots, \sigma_n)$.*

Démonstration. Nous allons prouver l'existence de g en énonçant un algorithme permettant de le calculer. On peut ordonner les monômes $\alpha_1^{k_1} \dots \alpha_n^{k_n}$ de la façon suivante : $\alpha_1^{k_1} \dots \alpha_n^{k_n}$ vient avant $\alpha_1^{k'_1} \dots \alpha_n^{k'_n}$ si et seulement si $k_1 > k'_1$, ou $k_1 = k'_1$ et $k_2 > k'_2$, ou $k_1 = k'_1$ et $k_2 = k'_2$ et $k_3 > k'_3$, etc. Tout polynôme f non nul a un *terme dominant* $d(f) = c \alpha_1^{k_1} \dots \alpha_n^{k_n}$ qui est le premier qui intervient avec un coefficient c non nul. Si f est symétrique, on voit que ce terme vérifie $k_1 \geq k_2 \geq \dots \geq k_n$. On définit alors

$$s(f) = c S_1^{k_1 - k_2} S_2^{k_2 - k_3} \dots S_{n-1}^{k_{n-1} - k_n} S_n^{k_n}$$

Substituons $\sigma_1, \dots, \sigma_n$ à S_1, \dots, S_n , puis développons en les α_i . On obtient un polynôme $t(f)$ symétrique en les α_i et un examen attentif montre que le terme dominant du polynôme $t(f)$ est le même que celui de f . Cela justifie l'algorithme suivant

Donnée: un polynôme f symétrique en n indéterminées
 Sortie: un polynôme g satisfaisant à la condition du théorème

```
g <- 0
tant que f n'est pas nul faire
  g <- g + s(f)
  f <- f - t(f)
fin tant que
```

Il reste à voir que l'algorithme s'arrête. Cela est dû au fait que la suite des termes dominants est strictement décroissante au sens de l'ordre défini plus haut et que cet *ordre lexicographique* est un *bon ordre* dans lequel, comme dans \mathbb{N} , toute suite strictement décroissante est finie. **cqfd.**

Donnons un exemple du procédé. Nous prenons $n = 3$ et les variables a , b et c plutôt que α_1 , α_2 et α_3 . On part du polynôme symétrique

$$f = a^3b + a^3c + ab^3 + ac^3 + bc^3 + b^3c$$

présenté en ordre lexicographique décroissant. On a donc $d(f) = a^3c$ et $s(f) = S_1^2S_2$, donc

$$\begin{aligned} t(f) &= (a + b + c)^2(ab + ac + bc) \\ &= a^3b + a^3c + 2a^2b^2 + 5a^2bc + 2a^2c^2 + ab^3 \\ &\quad + 5ab^2c + 5abc^2 + ac^3 + b^3c + 2b^2c^2 + bc^3. \end{aligned}$$

On recommence donc avec une nouvelle valeur de

$$f = -2a^2b^2 - 5a^2bc - 2a^2c^2 - 5ab^2c - 5abc^2 - 2b^2c^2$$

Le terme dominant est $d(f) = -2a^2b^2$ et $s(f) = -2S_2^2$, donc

$$t(f) = -2(ab + ac + bc)^2 = -2a^2b^2 - 4a^2bc - 2a^2c^2 - 4ab^2c - 4abc^2 - 2b^2c^2$$

On recommence donc avec une nouvelle valeur de

$$f = -a^2bc - ab^2c - abc^2$$

Le terme dominant est $d(f) = -a^2bc$ et $s(f) = -S_1S_3$ donc

$$t(f) = -(a + b + c)(abc) = f$$

ce qui achève l'algorithme. Le polynôme obtenu est donc $g = S_1^2S_2 - 2S_2^2 - S_1S_3$ et on obtient l'identité

$$a^3b + a^3c + ab^3 + ac^3 + bc^3 + b^3c = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3.$$

2.2.3 Les formules de Newton

Nous allons donner une version explicite du théorème précédent dans un cas particulier. Notons

$$s_k = \sum_{i=1}^n \alpha_i^k$$

la somme des puissances k -ièmes des α_i . C'est une fonction symétrique des α_i , que l'on peut donc exprimer en fonction des σ_k . Il est en fait possible de calculer les s_k par récurrence grâce aux *formules de Newton* :

Théorème 2.2.2. *Pour $k \leq n$, on a*

$$s_k = \sum_{i=1}^{k-1} (-1)^{i-1} \sigma_i s_{k-i} + (-1)^{k-1} k \sigma_k$$

et pour $k \geq n$

$$s_k = \sum_{i=1}^n (-1)^{i-1} \sigma_i s_{k-i}.$$

Démonstration. Partons de la relation de définition

$$\prod_{i=1}^n (X - \alpha_i) = \sum_{i=0}^n (-1)^i \sigma_i X^{n-i} = X^n - \sigma_1 X^{n-1} + \dots,$$

dérivons-la

$$\sum_{i=1}^n \prod_{j \neq i} (X - \alpha_j) = \sum_{i=0}^{n-1} (-1)^i (n-i) \sigma_i X^{n-i-1} = nX^{n-1} - (n-1)\sigma_1 X^{n-1} + \dots,$$

divisons membre à membre ces deux égalités

$$\sum_{i=1}^n \frac{1}{X - \alpha_i} = \frac{\sum_{i=0}^{n-1} (-1)^i (n-i) \sigma_i X^{n-i-1}}{\sum_{i=0}^n (-1)^i \sigma_i X^{n-i}} = \frac{nX^{n-1} - (n-1)\sigma_1 X^{n-1} + \dots}{X^n - \sigma_1 X^{n-1} + \dots},$$

substituons $\frac{1}{T}$ à X et chassons les dénominateurs en T

$$\sum_{i=1}^n \frac{1}{1 - \alpha_i T} = \frac{\sum_{i=0}^{n-1} (-1)^i (n-i) \sigma_i T^i}{\sum_{i=0}^n (-1)^i \sigma_i T^i} = \frac{n - (n-1)\sigma_1 T + \dots}{1 - \sigma_1 T + \dots}.$$

Écrivons le développement en série formelle du premier membre :

$$L = \sum_{i=1}^n \frac{1}{1 - \alpha_i T} = \sum_{i=1}^n \left(\sum_{j \in \mathbb{N}} \sigma_i^j T^j \right) = \sum_{j \in \mathbb{N}} s_j T^j.$$

L'identité ci-dessus peut donc s'écrire

$$\left(\sum_{i=0}^n (-1)^i \sigma_i T^i \right) \left(\sum_{j \in \mathbb{N}} s_j T^j \right) = \sum_{i=0}^{n-1} (-1)^i (n-i) \sigma_i T^i$$

ou encore

$$\begin{aligned} (s_0 + s_1 T + s_2 T^2 \dots) (1 - \sigma_1 T + \dots + (-1)^n \sigma_n T^n) \\ = n - (n-1) \sigma_1 T + \dots + (-1)^{n-1} \sigma_{n-1} T^{n-1}. \end{aligned}$$

Le coefficient de T^k dans le premier membre est

$$\sum_{i=0}^{\min(k,n)} (-1)^i \sigma_i s_{k-i}.$$

La comparaison avec le second membre donne les formules de Newton. **cqfd.**

On déduit de ces formules l'expression des s_k en fonction polynômiale des σ_i :

$$\begin{aligned} s_1 &= \sigma_1 \\ s_2 &= \sigma_1^2 - 2\sigma_2 \\ s_3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \\ s_4 &= \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 - 4\sigma_4 \end{aligned}$$

mais cette expression explicite devient vite compliquée.

2.2.4 Un exemple

Le polynôme $X^4 - X^3 - 2X^2 + 5X - 1$ a quatre racines dans \mathbb{C} : $\alpha_1 \simeq -1.8072$, $\alpha_2 \simeq 0.2213$, $\alpha_3 \simeq 1.2929 - 0.9105i$ et $\alpha_4 = \overline{\alpha_3} \simeq 1.2929 + 0.9105i$. On a

$$\begin{aligned} \sigma_1 &= 1 \\ \sigma_2 &= -2 \\ \sigma_3 &= -5 \\ \sigma_4 &= -1 \end{aligned}$$

On en déduit les sommes de puissances successives

$$\begin{array}{llll}
 s_1 & = & \sigma_1 & = & \sigma_1 & = & 1 \\
 s_2 & = & \sigma_1 s_1 - 2\sigma_2 & = & s_1 + 4 & = & 5 \\
 s_3 & = & \sigma_1 s_2 - \sigma_2 s_1 + 3\sigma_3 & = & s_2 + 2s_1 - 15 & = & -8 \\
 s_4 & = & \sigma_1 s_3 - \sigma_2 s_2 + \sigma_3 s_1 - 4\sigma_4 & = & s_3 + 2s_2 - 5s_1 + 4 & = & 1 \\
 s_5 & = & \sigma_1 s_4 - \sigma_2 s_3 + \sigma_3 s_2 - \sigma_4 s_1 & = & s_4 + 2s_3 - 5s_2 + s_1 & = & -39 \\
 s_6 & = & \sigma_1 s_5 - \sigma_2 s_4 + \sigma_3 s_3 - \sigma_4 s_2 & = & s_5 + 2s_4 - 5s_3 + s_2 & = & 8
 \end{array}$$

et ainsi de suite. On remarque que cette procédure est en quelque sorte l'inverse de celle concernant les récurrences linéaires à coefficients constants : au lieu de partir d'une suite s_k qui satisfait une récurrence linéaire et de trouver des α_i qui permettent d'exprimer s_k comme combinaison linéaire des puissances k -ièmes des α_i , on part des α_i et on trouve une récurrence linéaire satisfaite par la suite s_k .

Chapitre 3

Graphes

3.1 Graphes simples

3.1.1 Définitions

Un *graphe simple* est un couple $G = (S, A)$ d'ensembles finis. L'ensemble S des *sommets* est supposé non vide. Son cardinal, le nombre n de sommets est appelé l'*ordre* du graphe G . L'ensemble A des *arêtes* est un sous-ensemble quelconque de l'ensemble des parties à deux éléments ou *paires* de sommets. Les deux éléments d'une arête a sont ses *extrémités*. Comme il y a $\binom{n}{2} = \frac{n(n-1)}{2}$ paires de sommets, il y a entre 0 et $\frac{n(n-1)}{2}$ arêtes.

On dit que deux sommets s et s' sont *voisins* si $\{s, s'\}$ est une arête. Le nombre de voisins du sommet s est appelé son *degré* et est souvent noté $d(s)$. Un *sommet isolé* est un sommet de degré 0, c'est-à-dire sans voisin.

Donnons tout de suite un résultat fondamental

Théorème 3.1.1. *Le nombre d'arêtes d'un graphe simple est égal à la demi-somme des degrés de ses sommets :*

$$\sum_{s \in S} d(s) = 2|A|.$$

Démonstration. Notons B l'ensemble des *bouts*, couples $(s, a) \in S \times A$ tels que $s \in a$. Comme chaque arête a deux bouts, on a $|B| = 2|A|$ par le principe des bergers. D'autre part, chaque sommet s appartient à $d(s)$ arêtes. On a donc $|B| = \sum_{s \in S} d(s)$, d'où le résultat. **cqfd.**

En conséquence,

Corollaire 3.1.2. *le nombre de sommets de degré impair d'un graphe simple est pair.*

On utilise souvent des raccourcis, parlant du graphe plutôt que de ses sommets ou de ses arêtes. Par exemple, le *degré minimum*, respectivement *maximum*, du graphe G est défini comme

$$\delta(G) = \min_{s \in S} d(s)$$

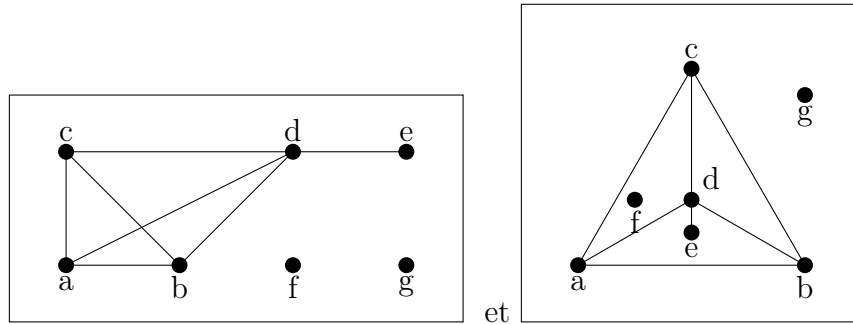
respectivement

$$\Delta(G) = \max_{s \in S} d(s).$$

Si ces deux nombres sont égaux, c'est-à-dire si tous les sommets ont le même degré k , on dit que le graphe est *k-régulier*.

Une *représentation plane* du graphe $G = (S, A)$ est un dessin plan, comportant $n = |S|$ points étiquetés par les éléments de S et pour chaque arête $\{s, s'\} \in A$, une courbe simple, par exemple un segment de droite, joignant les sommets étiquetés s et s' . Les croisements entre ces représentations des arêtes ne sont pas significatifs. Toutefois, il est souvent préférable de les éviter si possible. Un *graphe planaire* est un graphe qui admet une représentation plane sans croisement, mais cette notion ne jouera pas un rôle central dans ce cours. Voici deux représentations du graphe

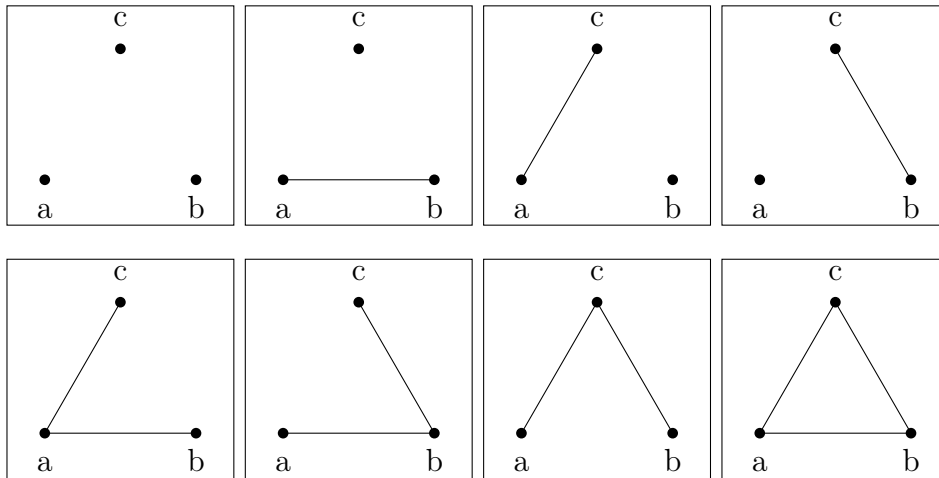
$$G = (\{a, b, c, d, e, f, g\}, \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{d, e\}\}).$$



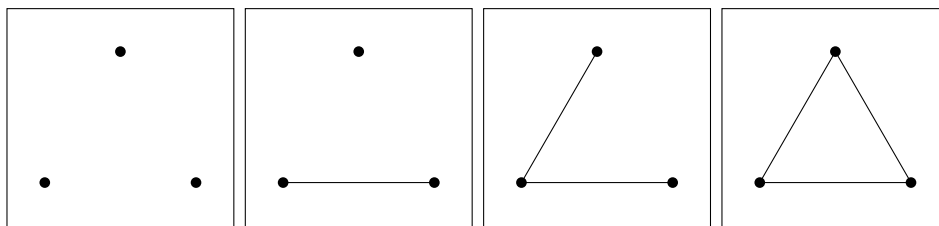
Un *isomorphisme* du graphe simple $G = (S, A)$ sur le graphe simple $G' = (S', A')$ est une bijection $\varphi : S \rightarrow S'$ telle que

$$\forall s, t \in S, \quad \{s, t\} \in A \Leftrightarrow \{\varphi(s), \varphi(t)\} \in A'.$$

Il est facile de voir que cela définit une relation d'équivalence sur les graphes. Par exemple, il y a 8 graphes distincts dont l'ensemble des sommets est $S = \{a, b, c\}$:



Ils se répartissent en quatre classes d'isomorphisme. On dit qu'il y a, à *isomorphisme près*, 4 graphes simples d'ordre 3 distincts :

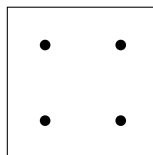


En effaçant les étiquettes des sommets, on obtient une représentation plane d'un graphe à isomorphisme près.

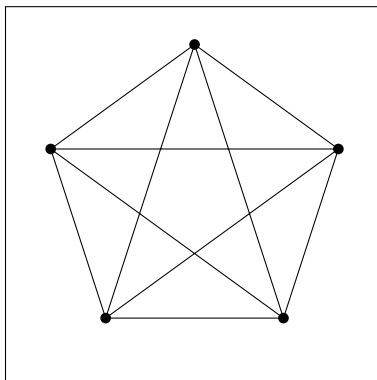
3.1.2 Bestiaire

Nous allons donner des exemples de (classes d'isomorphismes de) graphes simples naturels.

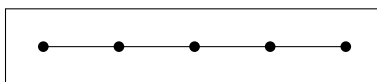
- Le *n-stable* S_n , ou *stable d'ordre n* est un graphe d'ordre n sans arête.
Voici S_4 :



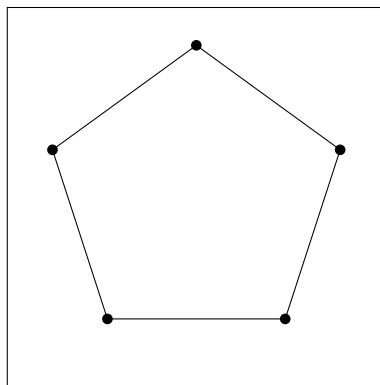
- La n -*clique*, ou *graphe complet* d'ordre n est un graphe d'ordre n dans lequel deux sommets distincts sont toujours voisins. Voici K_5 :



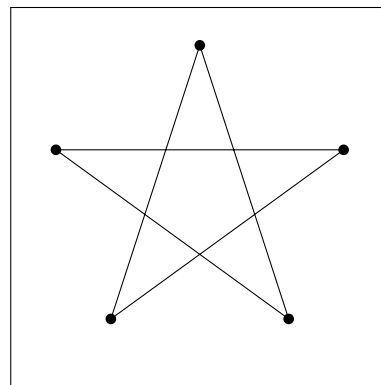
- La n -*chaîne* P_n ou chaîne de longueur n a pour ensemble de sommets $[0, n]$ (c'est donc un graphe d'ordre $n + 1$), avec i voisin de j si et seulement si $|i - j| = 1$. Voici P_4 :



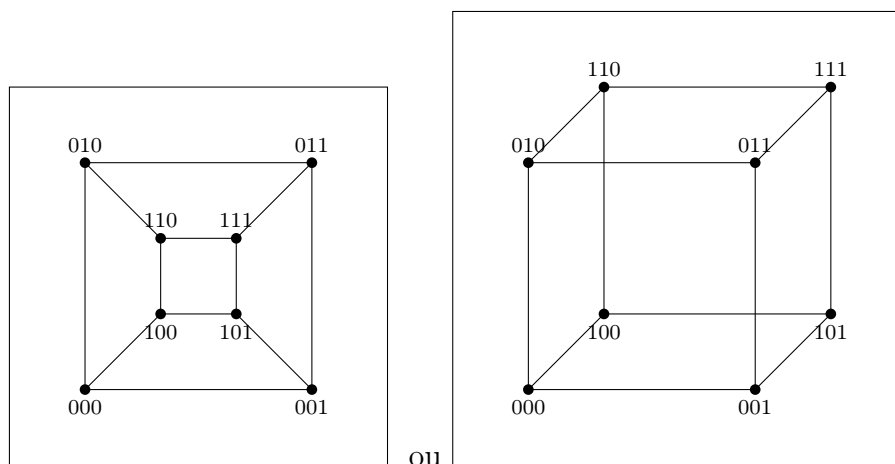
- Le n -*cycle* C_n ou cycle de longueur n a pour ensemble de sommets $[1, n]$ (c'est donc un graphe d'ordre n), avec i voisin de j si et seulement si $|i - j| = 1$ ou $|i - j| = n - 1$. Voici C_5 :



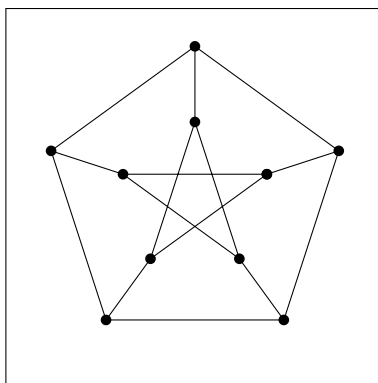
ou encore



- Soit $d \geq 0$ un entier. Le d -*cube* Q_d , ou *cube de dimension* d est un graphe dont les sommets sont les chaînes de caractères de longueur d sur l'alphabet $\{0, 1\}$. Deux sommets sont voisins dans le graphe si et seulement si les chaînes correspondantes diffèrent en une seule position. Voici Q_3 :



– Le *graphe de Petersen* est le graphe suivant, étudié en exercice :



3.1.3 Sous-graphes, le théorème de Turán

Le *graphe complémentaire* du graphe simple $G = (S, A)$ est un graphe $\overline{G} = (S, \overline{A})$ qui a les mêmes sommets que G , mais dans lequel deux sommets distincts sont voisins si et seulement si ils ne le sont pas dans G . En d'autres termes, on a $\overline{A} = \mathcal{P}_2(S) \setminus A$. Un graphe est *auto-complémentaire* si et seulement si il est isomorphe à son complémentaire. Les deux figures plus haut pour C_5 et K_5 montrent que C_5 est auto-complémentaire.

Un *sous-graphe* d'un graphe simple $G = (S, A)$ est un graphe $G' = (S', A')$ tel que $S' \subset S$ et $A' \subset A$. On dit que c'est un sous-graphe *couvrant* si $S' = S$. Pour toute partie S' de S , on définit le *sous-graphe de G induit par S'* et on note $G(S')$ le graphe $G(S') = (S', A')$, où $A' = A \cap \mathcal{P}_2(S')$ est l'ensemble des arêtes de A dont les deux extrémités sont dans S' .

On dit que G *contient* le graphe G' s'il existe un sous-graphe de G isomorphe à G' . Nous allons prouver le

Théorème 3.1.3 (de Turán). *Soit $n \geq 1$ et $p \geq 2$ des entiers. Si le graphe simple $G = (S, A)$ d'ordre n ne contient pas de p -clique, alors*

$$|A| \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}.$$

Démonstration. Par récurrence sur n et p . Pour $n = 1$ ou $p = 2$, il n'y a rien à démontrer. Soit donc $n > 1$ et $p > 2$ deux entiers, et supposons le résultat vrai pour $p' < p$ ou $n' < n$. On considère un graphe simple $G = (S, A)$ d'ordre n qui ne contient pas de p -clique.

Si G ne contient pas de $(p-1)$ -clique, on peut appliquer l'hypothèse de récurrence avec $p' = p-1$. On a donc

$$|A| \leq \left(1 - \frac{1}{p-2}\right) \frac{n^2}{2} \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}.$$

Nous pouvons donc supposer que G contient une $(p-1)$ -clique, c'est-à-dire qu'il existe une partie S' de S de cardinal $p-1$ telle que tous les éléments de S' sont voisins entre eux. Notons $S'' = S \setminus S'$. Si S'' est vide, le graphe G est la clique K_{p-1} , on a $n = p-1$ et

$$|A| = \frac{(p-1)(p-2)}{2} = \left(\frac{p-2}{p-1}\right) \frac{(p-1)^2}{2} = \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}.$$

Sinon, le graphe induit $G'' = G(S'')$ ne contient pas non plus de p -clique et a un ordre $n'' = n - p + 1 < n$. On peut lui appliquer l'hypothèse de récurrence et on a

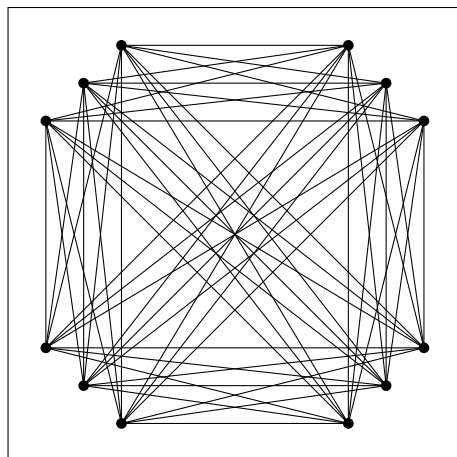
$$|A''| \leq \left(1 - \frac{1}{p-1}\right) \frac{n''^2}{2}.$$

Les arêtes de G sont de trois sortes : celles qui ont leurs deux extrémités dans S' , au nombre de $\frac{(p-1)(p-2)}{2}$, celles dont les deux extrémités sont dans S'' , au nombre de $|A''|$ majoré ci dessus, et celles dont une extrémité est dans S' et l'autre dans S'' . Pour chaque sommet s de S'' , il y a au moins un sommet t de S' qui n'est pas voisin de s , puisque autrement $G(S' \cup \{s\})$ serait une p -clique de G . Il y a donc au plus $p-2$ arêtes de la troisième espèce qui ont s pour extrémité, et il y a au plus $(p-2)n''$ arêtes de troisième espèce en tout. Au total, on a

$$\begin{aligned} |A| &\leq \frac{(p-1)(p-2)}{2} + \left(1 - \frac{1}{p-1}\right) \frac{n''^2}{2} + (p-2)n'' \\ &= \frac{p-2}{2(p-1)} \left((p-1)^2 + n''^2 + 2(p-1)n'' \right) = \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}. \end{aligned}$$

cqfd.

On remarque que si $n = q(p-1)$ est un multiple de $p-1$, on peut construire un graphe d'ordre n de la façon suivante : on répartit les sommets en $p-1$ groupes de q éléments et deux sommets quelconques sont voisins si et seulement si ils n'appartiennent pas au même groupe. Voici l'exemple $p = 5, q = 3$:



Il est clair que ce graphe ne contient pas de p -clique puisque d'après le principe des tiroirs toute partie de S de cardinal p contient deux sommets de même groupe, donc non voisins. Comptons les arêtes du graphe. Il y a $\binom{p-1}{2} = \frac{(p-1)(p-2)}{2}$ paires de groupes et q^2 arêtes entre éléments de cette paire de groupes. On a donc

$$|A| = \frac{(p-1)(p-2)}{2} q^2 = \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}$$

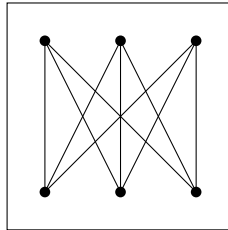
et la borne donnée par le théorème de Turán est atteinte.

3.1.4 Colorations

Une application $f : S \rightarrow C$ de l'ensemble des sommets d'un graphe simple $G = (S, A)$ est une *coloration* du graphe si l'image par f d'une arête est toujours un ensemble à 2 éléments. On appelle *couleur* du sommet s l'élément $f(s)$ de C et la condition s'exprime sous la forme "Si deux sommets sont voisins, ils sont de couleurs différentes".

Le plus souvent, on ne s'intéresse pas aux couleurs, mais seulement à la répartition des sommets en couleurs distinctes. Les sommets d'une couleur donnée forment un *stable* de G , c'est-à-dire une partie de S qui ne contient aucune paire de sommets voisins. Si $|f(S)| = k$, on dit que la coloration utilise k couleurs. Les ensembles de sommets des différentes couleurs forment une *partition* de S en k stables. On dit que le graphe G est *k-parti* (*biparti* pour $k = 2$, *triparti* si $k = 3$, etc.) s'il existe une telle partition, ou encore s'il existe une coloration de G qui utilise exactement k couleurs. Nous verrons plus loin une caractérisation simple des graphes bipartis.

Nous ajoutons ici un spécimen dans notre bestiaire. Soit $k \geq 2$ un entier et $(n_i)_{i \in [1,k]}$ une famille d'entiers non nuls. On définit le *graphe multiparti complet* K_{n_1, n_2, \dots, n_k} de la manière suivante. L'ensemble S des sommets a $n = \sum_i n_i$ éléments. Il est partitionné en k parties $(S_i)_{i \in [1,k]}$, avec $|S_i| = n_i$ pour tout i . Deux sommets sont voisins si et seulement si ils n'appartiennent pas à la même partie. C'est, bien sûr, un graphe k -parti. Le graphe $K_{3,3,3,3}$ est représenté plus haut dans la discussion du théorème de Turán. Voici une représentation de $K_{3,3}$



Il est clair que l'application identique I_S est une coloration de G qui utilise n couleurs. Il est alors naturel de se demander combien de couleurs sont nécessaires pour colorier un graphe G . Le *nombre chromatique* $\chi(G)$ du graphe G est le plus petit entier k pour lequel il existe une coloration de G utilisant k couleurs. La proposition suivante donne les nombres chromatiques associés aux graphes vus plus haut.

Proposition 3.1.4.

- $\chi(G) = 1$ si et seulement si G est un n -stable,
- $\chi(G) = n$ si et seulement si G est une n -clique,
- $\chi(P_n) = 2$ pour $n \geq 1$,
- $\chi(C_n) = \begin{cases} 2 & \text{si } n \geq 4 \text{ est pair} \\ 3 & \text{si } n \geq 3 \text{ est impair.} \end{cases}$,
- $\chi(Q_d) = 2$ pour $d \geq 1$,
- $\chi(\text{Petersen}) = 3$,
- $\chi(K_{n_1, \dots, n_k}) = k$.

La preuve de cette proposition sera faite en exercice.

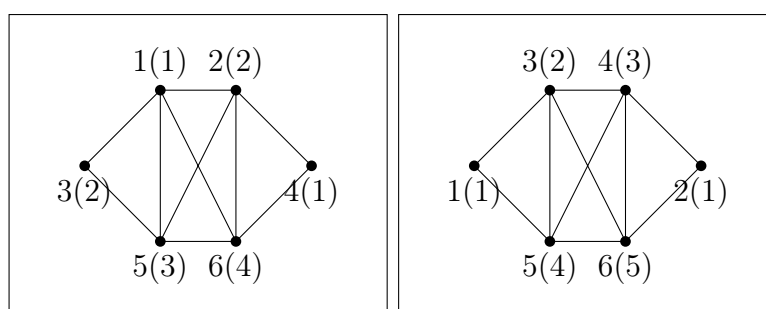
À chaque numérotation $[1, n] \rightarrow S$ des sommets, on fait naturellement correspondre une coloration par des entiers naturels non nuls grâce à l'*algorithme glouton* :

```

pour i allant de 1 à n faire
  colorier le sommet i avec la première couleur parmi 1,2,3...
  qui n'est pas déjà utilisée par un voisin du sommet i
fin faire

```

Ainsi, le sommet s_1 est colorié avec la couleur 1, le sommet s_2 est colorié avec la couleur 2 s'il est voisin de s_1 et avec c_1 sinon, etc. Dans la figure suivante, nous avons appliqué cet algorithme deux fois au même graphe, mais avec des numérotations différentes des sommets. Entre parenthèses les numéros des couleurs sont indiqués. On voit que la première numérotation utilise 4 couleurs en tout alors que la deuxième en utilise 5. On peut montrer qu'il existe toujours une numérotation des sommets telle que l'algorithme glouton utilise $\chi(G)$ couleurs, mais cela n'a rien d'évident.



Rappelons que nous avons défini le *degré maximum* $\Delta(G)$ d'un graphe G comme le maximum des degrés des sommets de G . On a la

Proposition 3.1.5. *Le nombre chromatique d'un graphe simple vérifie*

$$\chi(G) \leq \Delta(G) + 1$$

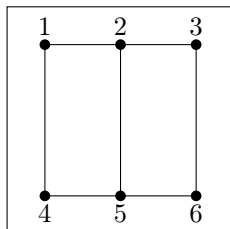
Démonstration. En fait, quel que soit l'ordre choisi sur les sommets, l'algorithme glouton utilise au maximum $\Delta(G) + 1$ couleurs distinctes. Soit en effet k le numéro de la plus haute couleur utilisée, et s un sommet qui a cette couleur. L'algorithme glouton attribue la couleur k à s parce que les voisins de s déjà coloriés occupent toutes les couleurs de 1 à $k-1$. Donc s a au moins $k-1$ voisins distincts, et $k-1 \leq \Delta(G)$, d'où $\chi(G) \leq k \leq \Delta(G) + 1$. **cqfd.**

3.1.5 Graphes planaires

On rappelle qu'un graphe est *planaire* s'il admet une représentation plane dans laquelle les courbes qui représentent les arêtes ne se croisent pas. On dit que le graphe K est un *mineur* du graphe G si on peut obtenir un graphe isomorphe à K à partir de G en effectuant une suite d'opérations dont chacune est de l'un des trois types suivants :

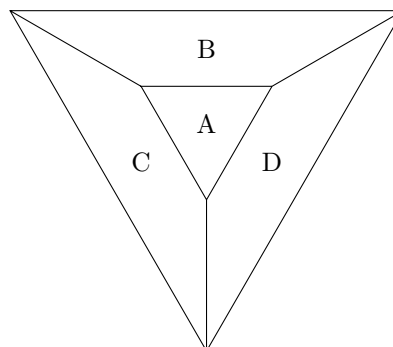
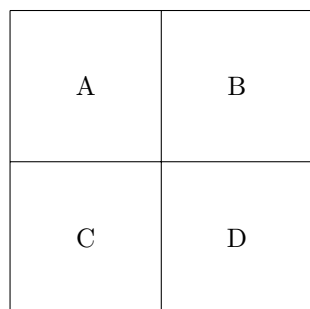
- *ablation* d'une arête
- *ablation d'un sommet* et de toutes les arêtes dont ce sommet est une extrémité.
- *suture* d'une arête : On identifie les deux extrémités de l'arête, et on efface la boucle et les arêtes multiples qui découleraient de cette identification.

Par exemple, par ablation des sommets 3 et 6 et suture de l'arête $\{4, 5\}$, on voit que le graphe K_3 est un mineur du graphe suivant.

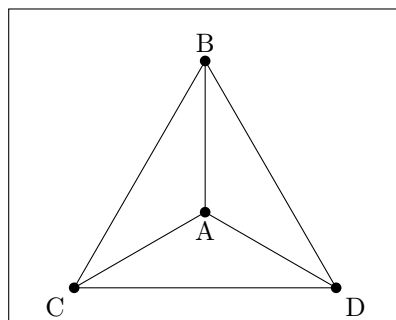
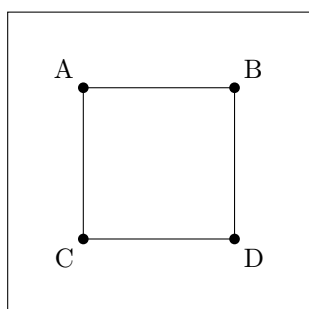


On peut montrer qu'un graphe G est planaire si et seulement si ni K_5 ni $K_{3,3}$ ne sont des mineurs de G .

Considérons une carte de géographie, divisée en un certain nombre de pays d'un seul tenant. On lui associe un graphe de la manière suivante : dans chaque pays, on met un sommet, et les sommets associés à deux pays sont voisins si ces pays ont une frontière commune — pas seulement un point commun, une certaine longueur de frontière. Aux deux cartes suivantes,



on associe donc les deux graphes suivants :



Le graphe obtenu est planaire, et à une coloration de ce graphe on associe un coloriage de la carte dans lequel deux pays limitrophes ont des couleurs différentes.

En 1976, Appel et Haken ont démontré le

Théorème 3.1.6 (des quatre couleurs). *Toute carte de géographie plane peut être coloriée avec quatre couleurs de façon que deux pays limitrophes aient toujours des couleurs différentes.*

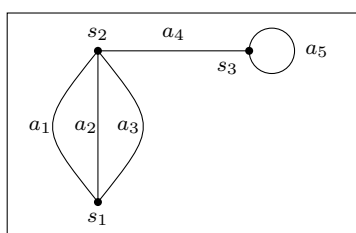
Les considérations ci-dessus montrent que cet énoncé est équivalent au suivant :

Théorème 3.1.7. *Si G est un graphe simple plane, $\chi(G) \leq 4$.*

La démonstration a fait sensation à l'époque, non seulement parce que le problème datait de plus d'un siècle, mais aussi parce qu'elle se décomposait en environ 1500 cas, ce qui avait rendu nécessaire d'en faire écrire et vérifier une partie essentielle par des machines.

3.2 Multigraphes

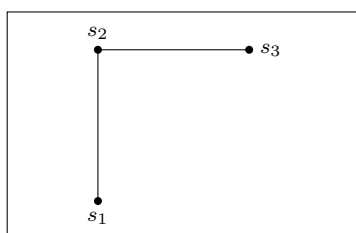
Un *multigraphe* est la donnée d'un couple $G = (S, A)$ d'ensembles finis, avec S non vide, ainsi que d'une application $\varphi : A \rightarrow \mathcal{P}_1(S) \cup \mathcal{P}_2(S)$ qui à chaque *arête* fait correspondre un ensemble de 1 ou 2 *sommets*, ses *extrémités*. Si $\varphi(a) = s$ est un singleton, on dit que l'arête a est une *boucle* de base s . On parlera en général du multigraphe $G = (S, A)$, en oubliant la fonction φ . Les *représentations* des multigraphes utilisent des lignes courbes. Voici un exemple de multigraphe



À tout multigraphe $G = (S, A)$, on fait correspondre le graphe simple *sous-jacent* $G' = (S, A')$, où

$$A' = \{a' \in \mathcal{P}_2(S); \exists a \in A, \varphi(a) = a'\},$$

en d'autres termes, on efface les boucles et on consolide les *arêtes multiples* en une seule. Le graphe simple sous-jacent au multigraphe ci-dessus est donc



Dans toute la suite, nous utiliserons le terme *graphe* pour désigner un multigraphe, pour signifier qu'en réalité la situation ne concerne que le graphe simple sous-jacent.

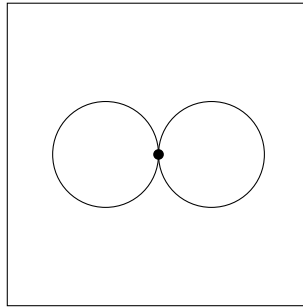
On définit de façon naturelle un isomorphisme entre $G = (S, A)$ et $G' = (S', A')$ comme un couple (f, g) , où f est une bijection de S sur S' , g est une bijection de A sur A' telle que

$$\forall a \in A, \quad \varphi'(g(a)) = f(\varphi(a)).$$

Un *sous-graphe* d'un multigraphe (S, A) est un multigraphe (S', A') tel que $S' \subset S$, $A' \subset A$ et $\forall a \in A', \quad \varphi'(a) = \varphi(a)$. Un tel sous-graphe est *couvrant* si $S' = S$. Le *sous-graphe induit* par $S' \subset S$ est le multigraphe (S', A') , avec

$$A' = \{a \in A; \varphi(a) \subset S'\}.$$

On peut encore dire qu'un multigraphe en *contient* un autre s'il admet un sous-graphe isomorphe à cet autre. Par exemple, le multigraphe G contient



si et seulement si il existe dans G deux boucles de même base.

3.2.1 Matrices d'incidence et d'adjacence

On numérote les sommets et arêtes d'un multigraphe $G = (S, A)$:

$$S = \{s_1, s_2, \dots, s_n\}, \quad A = \{a_1, a_2, \dots, a_m\}.$$

La *matrice d'incidence* M du graphe est une matrice $n \times m$ définie par

$$m_{i,j} = \begin{cases} 2 & \text{si } a_j \text{ est une boucle de base } s_i \\ 1 & \text{si } s_i \text{ est une des deux extrémités distinctes de } a_j \\ 0 & \text{si } s_i \text{ n'est pas une extrémité de } a_j. \end{cases}$$

La somme des éléments de la colonne d'indice j vaut 2. La somme des éléments de la ligne i est, par définition, le *degré* de s_i : les boucles de base s_i comptent pour 2, les autres arêtes d'extrémité s_i pour 1. On peut alors énoncer la même relation fondamentale que pour les graphes simples :

Théorème 3.2.1. *Le nombre d'arêtes d'un multigraphe est égal à la demi-somme des degrés de ses sommets :*

$$\sum_{s \in S} d(s) = 2|A|.$$

Démonstration. Ce nombre est égal à la somme de tous les éléments de la matrice M :

$$\sum_{s \in S} d(s) = \sum_{i=1}^n d(s_i) = \sum_{i=1}^n \left(\sum_{j=1}^m m_{ij} \right) = \sum_{j=1}^m \left(\sum_{i=1}^n m_{ij} \right) = \sum_{j=1}^m 2 = 2|A|.$$

cqfd.

Et on a encore le

Corollaire 3.2.2. *Le nombre de sommets de degré impair d'un multigraphe est pair.*

La *matrice d'adjacence* A_G du graphe G est une matrice $n \times n$ définie par

$$\begin{aligned} a_{ij} &= |\{a \in A; \varphi(a) = \{s_i, s_j\}\}| \\ &= \begin{cases} \text{Nombre de boucles de base } s_i & \text{si } i = j \\ \text{Nombre d'arêtes d'extrémités } s_i \text{ et } s_j & \text{si } i \neq j. \end{cases} \end{aligned}$$

On voit que cette matrice est symétrique. La somme des éléments d'une ligne (ou colonne) n'est pas le degré du sommet correspondant puisque les boucles ne sont ici comptées qu'une fois.

Voici les matrices d'incidence et d'adjacence du multigraphe dessiné plus haut.

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 3 & 0 \\ 3 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

3.2.2 Chaînes dans un multigraphe

Soit $k \in \mathbb{N}$ un entier naturel. Une k -chaîne, ou *chaîne de longueur k* d'un multigraphe est la donnée d'une famille $(v_i)_{i \in [0, k]}$ de $k + 1$ sommets et d'une famille $(e_i)_{i \in [1, k]}$ de k arêtes telles que pour tout $i \in [1, k]$, on ait $\varphi(e_i) = \{v_{i-1}, v_i\}$. On note

$$\gamma = (v_0, e_1, v_1, e_2, \dots, e_k, v_k).$$

On dit que la chaîne γ *visite* chacun des v_i et des e_i . Le sommet v_0 est l'*origine* de la chaîne γ et v_k est son *extrémité*. En particulier, si $s \in S$ est un sommet, (s) est une 0-chaîne, d'origine s et extrémité s . Une chaîne est *fermée* si $v_0 = v_k$. Elle est *simple* si les arêtes e_1, \dots, e_k sont distinctes. Elle est *élémentaire* si les sommets v_0, \dots, v_k sont distincts.

Dans un graphe simple, on a forcément $e_i = \{v_{i-1}, v_i\}$. On se contente donc de noter les sommets et on écrit $\gamma = (v_0, v_1, \dots, v_k)$.

Il y a des opérations naturelles sur les chaînes : Si l'extrémité de $\gamma = (v_0, e_1, v_1, e_2, \dots, e_k, v_k)$ est égale à l'origine de $\delta = (w_0, f_1, w_1, f_2, \dots, f_l, w_l)$, c'est-à-dire si $v_k = w_0$, on peut définir la *concaténation*

$$\gamma \cdot \delta = (v_0, e_1, v_1, e_2, \dots, e_{k+l}, v_{k+l})$$

en posant $e_i = f_{i-k}$ et $v_i = w_{i-k}$ pour $k < i \leq k+l$. On peut aussi définir la chaîne

$$\tilde{\gamma} = (v'_0, e'_1, v'_1, e'_2, \dots, e'_k, v'_k) = (v_k, e_k, \dots, e_1, v_0)$$

qui est “ γ parcourue dans l'autre sens” en posant $e'_i = e_{k+1-i}$ et $v'_i = v_{k-i}$.

Théorème 3.2.3. *Soit $G = (S, A)$ un multigraphe, et A_G sa matrice d'incidence. Pour tout $k \in \mathbb{N}$ et tout couple $(i, j) \in [1, n]^2$, le coefficient $(A_G^k)_{ij}$ de la puissance k -ième de A_G est égal au nombre de k -chaînes d'origine s_i et extrémité s_j .*

Démonstration. Par récurrence sur k . La matrice A_G^0 est la matrice identité I_n , et il est clair que le nombre de 0-chaînes d'origine s_i et extrémité s_j vaut 1 si $i = j$ et 0 sinon. La propriété est donc vraie pour $k = 0$. Supposons-la vraie pour k . Une $k+1$ -chaîne d'origine s_i et extrémité s_j s'écrit $(v_0, \dots, v_k, e_{k+1}, v_{k+1})$, avec $v_0 = s_i$ et $v_{k+1} = s_j$. Si $v_k = s_l$, (v_0, \dots, v_k) est une k -chaîne d'origine s_i et extrémité s_l et e_{k+1} vérifie $\varphi(e_{k+1}) = \{s_l, s_j\}$. L'hypothèse de récurrence dit qu'il y a $(A_G^k)_{il}$ possibilités pour la première partie et la définition de A_G dit qu'il y a $(A_G)_{lj}$ possibilités pour la seconde. Le nombre de $k+1$ -chaînes d'origine s_i , extrémité s_j et telles que le sommet v_k soit s_l vaut donc $(A_G^k)_{il}(A_G)_{lj}$. le nombre total de $k+1$ -chaînes d'origine s_i et extrémité s_j est donc

$$\sum_{l=1}^n (A_G^k)_{il}(A_G)_{lj} = (A_G^{k+1})_{ij}.$$

cqfd.

3.2.3 Algorithmes de Moore et de Dijkstra

On définit une fonction $D : S \times S \rightarrow \mathbb{N} \cup \{\infty\}$ appelée *distance* sur G de la façon suivante. S'il existe une chaîne d'origine s et extrémité t , $D(s, t)$ est la longueur minimale d'une telle chaîne. S'il n'en existe pas, on pose $D(s, t) = \infty$.

Cette fonction n'est pas une distance au sens usuel puisque elle peut prendre la valeur ∞ . Mais il est facile de voir que la fonction

$$\tilde{D}(s, t) = \begin{cases} \frac{D(s, t)}{1 + D(s, t)} & \text{si } D(s, t) \neq \infty \\ 1 & \text{si } D(s, t) = \infty \end{cases}$$

est une distance sur S . Dans la pratique, on préfère utiliser D , qui prend des valeurs entières.

Donnons un algorithme classique de calcul de $D(s, t)$, pour un sommet fixé et tout sommet t , l'*algorithme de Moore* :

Données: Un sommet s d'un graphe (S, A)

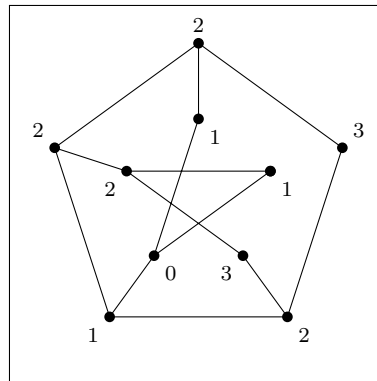
Sortie: Pour tout t dans S , $D[t]$ contient $D(s, t)$

```

D[s] <- 0
Pour tout t dans S faire
  D[t] <- infini
fin pour
k <- 0
V <- {s} (V est un ensemble de sommets, au départ un singleton)
tant que V n'est pas vide faire
  k <- k+1
  W <- {} (ensemble vide)
  pour tout x dans V faire
    pour tout y voisin de x et tel que D[y] = infini faire
      D[y] <- k
      W <- W union {y} (on ajoute y à l'ensemble W)
    fin pour
  fin pour
  V <- W
fin tant que

```

En d'autres termes, s est étiqueté 0, les voisins de s étiquetés 1, les voisins des voisins de s sauf s lui-même sont étiquetés 2, et si t est étiqueté k , ses voisins non encore étiquetés seront étiquetés $k + 1$, etc. Voici un exemple d'exécution de l'algorithme de Moore



Il existe une généralisation naturelle de cette notion de distance sur un graphe. Un *graphe valué* (S, A, μ) est la donnée d'un multigraphe $G = (S, A)$ et d'une fonction $\mu : A \rightarrow \mathbb{R}^{*+}$ appelée *coût* ou *poids* ou *longueur*... Le coût d'une chaîne $\gamma = (v_0, e_1, v_1, e_2, \dots, e_k, v_k)$ est alors défini par $\mu(\gamma) = \sum_{i \in [1, k]} \mu(e_i)$. On définit la distance $C(s, t)$ entre deux sommets d'un graphe valué comme le minimum des coûts des chaînes d'origine s et extrémité t s'il en existe, et ∞ s'il n'en existe pas. Pour déterminer $C(s, t)$ pour un sommet fixé s et chaque sommet t , on peut utiliser l'*algorithme de Dijkstra* :

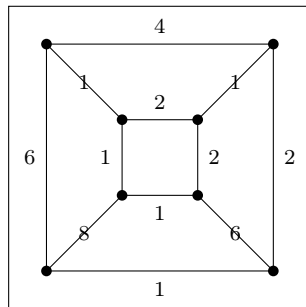
Données: Un sommet s d'un graphe valué (S, A, m) ,
 Sortie: Pour tout t dans S , $C[t]$ contient $C(s, t)$
 Si $0 < C[t] < \text{infini}$, $T[t]$ contient la première étape
 dans une chaîne de coût minimal menant de t à s .

```

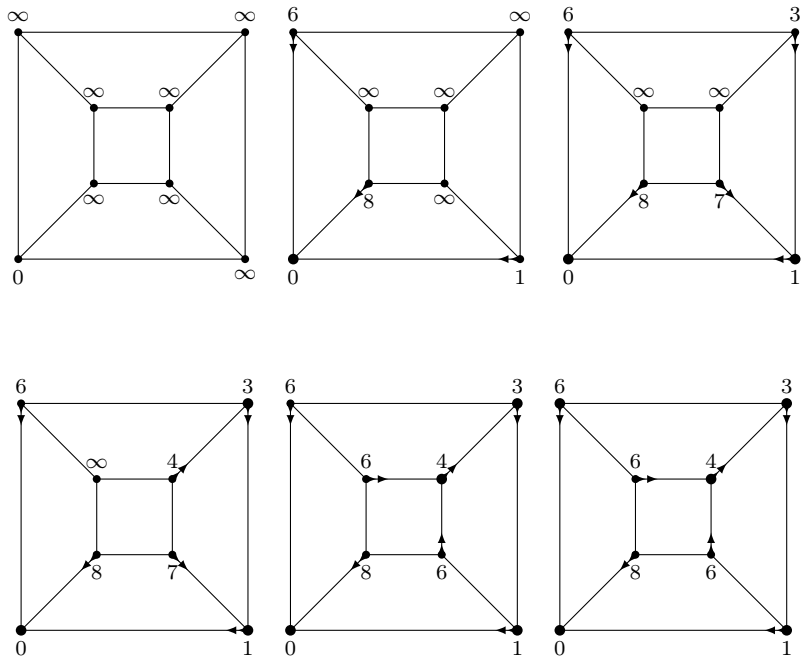
Pour tout t dans S faire
  C[t] <- infini
fin pour
C[s] <- 0
V <- {} (ensemble vide)
W <- S (tous les sommets)
tant qu'il y a dans W un sommet t tel que C[t] est fini faire
  u <- un sommet de W tel que C[u] soit minimal
  V <- V union {u}
  W <- W \ {u} (On transfère u de W vers V)
  pour chaque voisin x de u faire
    si C[u] + m({u, x}) < C[x] faire
      C[x] <- C[u] + m({u, x})
      T[x] <- u
    fin si
  fin pour
fin tant que
  
```

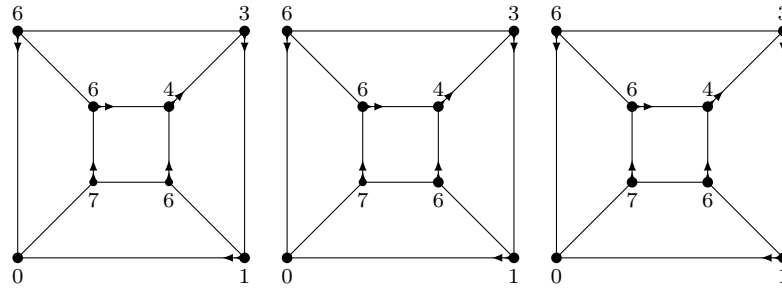
Pour montrer que cet algorithme est correct, il suffit de vérifier que l'*invariant de boucle* suivant est maintenu : si $t \neq s$ est dans V , un chemin de moindre coût de t à s commence par $T[t]$ est reste dans V . On peut montrer que la complexité de cet algorithme est en $\mathcal{O}((n + m) \log(n))$, où n est le nombre de sommets et m le nombre d'arêtes.

Voici par exemple les étapes de l'algorithme sur une valuation du cube Q_3 .



Les étiquettes des sommets représentent le tableau C et le tableau T est représenté par des flèches qui pointent de t vers $T[t]$. Si un sommet est dans V , le point qui le marque est plus gros.





Pour trouver comment rejoindre le coin en bas à gauche à moindre coût, suivre les flèches.

3.3 Chaînes et cycles

3.3.1 Connexité

Si s et t sont deux sommets d'un graphe $G = (S, A)$, on dira que s est *relié* à t et on écrira $s \sim_G t$ s'il existe une chaîne de G dont l'origine est s et l'extrémité t . Cela revient à dire que $D(s, t)$ est fini.

Théorème 3.3.1. *La relation \sim_G est une relation d'équivalence sur S .*

Démonstration. Elle est

- *réflexive* puisque (s) est une 0-chaîne d'origine s et extrémité s .
- *symétrique* puisque si γ a pour origine s et extrémité t , alors $\tilde{\gamma}$ a pour origine t et extrémité s .
- *transitive* puisque si γ a pour origine s et extrémité t , et δ a pour origine t et extrémité u , alors $\gamma \cdot \delta$ a pour origine s et extrémité u .

cqfd.

Un graphe sera dit *connexe* si deux sommets quelconques sont toujours reliés. Il revient au même de dire que D ne prend que des valeurs finies, ou encore que le *diamètre* $D(G) = \max\{D(s, t); s, t \in S\}$ du graphe G est fini.

À toute relation d'équivalence sur un ensemble S , on associe une *partition* de S en *classes d'équivalence*. On a donc une partition $S = \cup_{i \in [1, p]} S_i$. Si deux sommets sont voisins, ils sont reliés. Toute arête de G relie donc deux sommets qui appartiennent à la même classe. En posant $A_i = \{a \in A; \varphi(a) \subset S_i\}$, on a donc montré que A est réunion disjointe des A_i . Les multigraphes $G_i = (S_i, A_i)$ ont la propriété que deux sommets quelconques de G_i sont reliés dans G_i . Ils sont donc connexes, et on a montré le

Théorème 3.3.2. *Pour tout graphe $G = (S, A)$, il existe une partition unique de S en $p \geq 1$ parties non vides telle que les sous-graphes induits $G_i = G(S_i)$ soient connexes et que toute arête de G appartienne à un des G_i .*

Les G_i sont appelés les *composantes connexes* de G et p est le *nombre des composantes connexes* de G . La fonction D induit une distance sur chaque composante connexe de G . Il est facile de voir que tous les graphes du bestiaire sont connexes, sauf le stable S_n pour $n > 1$, qui a n composantes connexes.

Théorème 3.3.3. *Un graphe $G = (S, A)$ est connexe si et seulement si pour toute partition de S en 2 parties (non vides) S' et S'' , il existe une arête $a \in A$ dont une extrémité est dans S' et l'autre dans S'' .*

Démonstration. Supposons d'abord G connexe. Considérons une partition S en 2 parties (non vides) S' et S'' . Comme S' et S'' sont non vides, on peut choisir $s \in S'$ et $t \in S''$. Comme G est connexe, il existe une chaîne $\gamma = (v_0, e_1, \dots, v_k)$ d'origine s et extrémité t . L'ensemble $I = \{i \in [0, k]; v_i \in S''\}$ n'est pas vide puisque $v_k = t \in S''$, et ne contient pas 0 puisque $v_0 = s \in S'$. Notons $r > 0$ son plus petit élément. On a $v_{r-1} \notin S''$, donc $v_{r-1} \in S'$ et $v_r \in S''$. L'arête e_r a une extrémité dans S' et une autre dans S'' .

Réciproquement, supposons que pour toute partition de S en 2 parties (non vides) S' et S'' , il existe une arête $a \in A$ dont une extrémité est dans S' et l'autre dans S'' . Considérons deux sommets s et t de S . Notons S' l'ensemble des extrémités des chaînes d'origine s , et S'' le complémentaire de S' dans S . Supposons que $t \in S''$. Ni S' ni S'' ne sont alors vides. On applique l'hypothèse sur G : il existe une arête $e = u, v$, avec u dans S' et $v \in S''$. Il existe une chaîne $\gamma = (v_0, e_1, \dots, v_k)$ d'origine s et extrémité u , alors, l'existence de $\gamma \cdot (u, e, v) = (v_0, e_1, \dots, v_k, e, v)$, d'origine s et extrémité v montre que $v \in S'$, une contradiction. On a donc montré que $t \in S'$, il y a une chaîne d'origine s et extrémité t . On en déduit que G est connexe. **cqfd.**

3.3.2 Cycles

Pour $k \geq 1$ un *k-cycle* ou *cycle de longueur k* d'un multigraphe G est une *k-chaîne simple fermée* de G . Un *k-cycle* est dit *élémentaire* si les sommets (v_1, \dots, v_k) sont tous distincts. L'origine (et extrémité) du cycle est plutôt appelée sa *base*. Remarquons qu'un 1-cycle est associé à une boucle et qu'un 2-cycle est associé à une arête double. On en déduit que dans un graphe simple, la longueur d'un cycle est au moins 3.

Proposition 3.3.4. *De tout cycle, on peut extraire un cycle élémentaire.*

Démonstration. Si $\gamma = (v_0, e_1, v_1, \dots, e_k, v_k)$ est un k -cycle, l'ensemble des couples d'entiers (i, j) tels que $0 \leq i < j \leq k$ et $v_i = v_j$ n'est pas vide, puisqu'il contient $(0, k)$. Il existe donc un tel couple (i, j) avec $j - i$ minimal. On voit que $(v_i, e_{i+1}, v_{i+1}, \dots, v_j)$ est un cycle élémentaire. **cqfd.**

Proposition 3.3.5. *De toute chaîne fermée de longueur impaire, on peut extraire un cycle de longueur impaire.*

Démonstration. Par récurrence sur la longueur k de la chaîne fermée. Si $k = 1$, la 1-chaîne fermée (s, a, s) est un 1-cycle. Supposons la propriété vraie pour toute k' -chaîne fermée, avec $k' < k$ impair. Si la k -chaîne fermée $\gamma = (v_0, e_1, v_1, \dots, e_k, v_k)$ est simple, c'est un cycle. Sinon, il existe (i, j) , avec $1 \leq i < j \leq k$ tel que $e_i = e_j$. On en déduit que les ensembles $\{v_{i-1}, v_i\}$ et $\{v_{j-1}, v_j\}$ sont égaux. Il y a deux possibilités :

1. $v_{i-1} = v_{j-1}$ et $v_i = v_j$. Posons alors

$$\gamma_1 = (v_{i-1}, e_i, v_i, e_{i+1}, v_{i+1}, \dots, e_{j-1}, v_{j-1})$$

et

$$\gamma_2 = (v_{j-1}, e_j, v_j, \dots, e_k, v_k, e_1, v_1, \dots, e_{i-1}, v_{i-1}).$$

Ce sont deux chaînes fermées extraites de γ . La première a pour longueur $k_1 = j - i > 0$ et la seconde $k_2 = (k - j + 1) + (i - 1) > 0$. On a $k_1 + k_2 = k$ impair, donc l'un des deux est impair, strictement plus petit que k . On peut appliquer l'hypothèse de récurrence à γ_1 ou γ_2 pour obtenir un cycle impair extrait de γ .

2. $v_{i-1} = v_j$ et $v_i = v_{j-1}$. Posons alors

$$\gamma_1 = (v_i, e_{i+1}, v_{i+1}, \dots, e_{j-1}, v_{j-1})$$

et

$$\gamma_2 = (v_j, \dots, e_k, v_k, e_1, v_1, \dots, e_{i-1}, v_{i-1}).$$

Ce sont deux chaînes fermées extraites de γ . La première a pour longueur $k_1 = j - i - 1$ et la seconde $k_2 = (k - j) + (i - 1)$. On a $k_1 + k_2 = k - 2$ impair, donc l'un des deux est impair, strictement plus petit que k . On peut appliquer l'hypothèse de récurrence à γ_1 ou γ_2 pour obtenir un cycle impair extrait de γ .

cqfd.

Théorème 3.3.6. *Si le degré minimum $\delta(G)$ d'un multigraphe G vaut au moins 2, alors il existe un cycle dans G .*

Démonstration. Soit $\gamma = (v_0, e_1, v_1, \dots, e_k, v_k)$ une chaîne simple de longueur k maximale. Comme il y a au moins un sommet, et que son degré n'est pas nul, il y a au moins une arête, et $k \geq 1$. Si e_k est une boucle, (v_k, e_k, v_k) est un cycle. Sinon, comme $d(v_k) > 1$, il existe une arête e d'origine v_k et différente de e_k . Notons u le sommet tel que $\varphi(e) = \{v_k, u\}$. La chaîne $\gamma' = (v_0, e_1, v_1, \dots, e_k, v_k, e, u)$ a pour longueur $k + 1$. Elle n'est donc pas simple. On en déduit qu'il existe i , avec $1 \leq i < k$ tel que $e_i = e$. Il existe donc j , avec $j = i$ ou $j = i - 1$ tel que $j < k$ et $v_j = v_k$. On a donc un cycle $(v_j, e_{j+1}, \dots, e_k, v_k)$. **cqfd.**

Théorème 3.3.7. *Si le degré minimum $\delta(G)$ d'un graphe simple G vaut au moins 2, alors il existe dans G un cycle élémentaire de longueur au moins égale à $\delta(G) + 1$.*

Démonstration. Soit $\gamma = (v_0, \dots, v_k)$ une chaîne élémentaire de longueur k maximale. Comme il y a au moins un sommet, et que son degré n'est pas nul, il y a au moins une arête, et $k \geq 1$. Soit u un voisin de v_0 . La chaîne $(u, v_0, v_1, \dots, v_k)$ a pour longueur $k + 1$, et n'est donc pas élémentaire. On en déduit que u est égal à l'un des v_i , pour un $i \in [1, k]$, que nous appellerons l'indice du voisin u . Chacun des voisins de v_0 a un indice différent. L'un d'eux au moins a donc un indice $i \geq \delta(G)$. Puisque v_i est voisin de v_0 , $(v_0, v_1, \dots, v_i, v_0)$ est un cycle élémentaire, et sa longueur vaut au moins $\delta(G) + 1$. **cqfd.**

Donnons enfin la caractérisation des graphes bipartis en termes de cycles :

Théorème 3.3.8. *Un multigraphe $G = (S, A)$ différent du 1-stable est biparti si et seulement si il n'existe pas dans G de cycle de longueur impaire. En particulier, il ne doit pas avoir de boucle.*

Remarquons que le nombre chromatique $\chi(G)$ est inférieur ou égal ou égal à 2 si et seulement si G est biparti ou 1-stable.

Démonstration. Si G est biparti, il existe une partition $S = S' \cup S''$ telle que toute arête ait une extrémité dans S' et une autre dans S'' . Si $\gamma = (v_0, e_1, v_1, \dots, e_k, v_k)$ est un k -cycle et si $v_0 \in S'$, on voit, par récurrence sur i , que $v_i \in S'$ pour i pair et $v_i \in S''$ pour i impair. On sait que $v_k \in S'$. Donc k est pair.

Réciproquement, supposons que G n'admette pas de cycle impair. Commençons par supposer que G est connexe et $A \neq \emptyset$. Choisissons un sommet $s \in S$. Notons

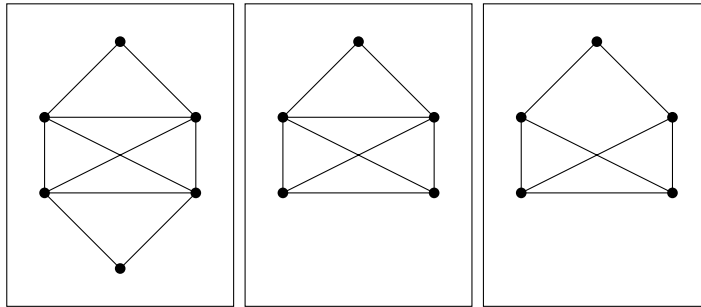
$$\begin{aligned} S' &= \{\text{extrémités des } k\text{-chaînes d'origine } s, \text{ avec } k \text{ pair}\} \\ S'' &= \{\text{extrémités des } k\text{-chaînes d'origine } s, \text{ avec } k \text{ impair}\} \end{aligned}$$

Comme G est connexe, il est clair que $S = S' \cup S''$. D'autre part, tout voisin d'un élément de S' est dans S'' et tout voisin d'un élément de S'' est dans S' . Comme $A \neq \emptyset$, on voit que ni S' ni S'' ne sont vides. Il reste donc à prouver que $S' \cap S'' = \emptyset$. Si $t \in S' \cap S''$ il existe une chaîne paire γ et une chaîne impaire δ d'origine s et extrémité t . La concaténation $\gamma.\delta$ de ces deux chaînes est une chaîne fermée de longueur impaire. On peut donc en extraire un cycle impair, une contradiction. Dans le cas où G n'est pas connexe, on voit que chacune des composantes connexes de G est bipartie ou 1-stable et G lui-même est donc biparti ou 1-stable. **cqfd.**

3.3.3 Graphes eulériens

Un *cycle eulérien* d'un multigraphe G est un cycle qui visite toutes les arêtes et tous les sommets de G . Un *graphe eulérien* est un multigraphe qui admet un cycle eulérien. Une *chaîne eulérienne* est une chaîne simple qui visite toutes les arêtes et tous les sommets de G . Un *graphe semi-eulérien* est un multigraphe qui admet une chaîne eulérienne.

Notons que ces chaînes passent une fois et une seule par chaque arête, et au moins une fois par chaque sommet, mais qu'elles peuvent passer plusieurs fois par le même sommet. Des trois graphes suivants, le premier est eulérien, le second est semi-eulérien sans être eulérien, et le troisième n'est pas semi-eulérien.



Théorème 3.3.9. *Soit G un multigraphe d'ordre au moins 2. Le multigraphe G est eulérien si et seulement si il est connexe et tous ses sommets sont de degré pair.*

Démonstration. Remarquons d'abord qu'en ajoutant ou effaçant une boucle, on ne change pas la connexité, ni la parité du degré des sommets, ni l'existence d'un cycle eulérien. Nous pouvons donc supposer que G n'a pas de boucle. Si G est eulérien, soit $\gamma = (v_0, e_1, v_1, \dots, e_k, v_k)$ une chaîne eulérienne. Elle visite tous les sommets, donc pour tout couple (s, t) de sommets, elle induit une chaîne d'extrémités s et t . Le graphe G est donc connexe. Soit s un sommet

de G , A_s l'ensemble des arêtes incidentes à s et $I_s = \{i \in [1, k]; v_i = s\}$. L'application $f_s : A_s \rightarrow I_s$ qui à une arête a incidente à s fait correspondre l'unique entier $i \in [1, k]$ tel que $s = v_i$ et ($a = e_i$ ou $a = e_{i+1}$) vérifie

$$f_s^{-1}(i) = \begin{cases} \{e_i, e_{i+1}\} & \text{si } i < k \\ \{e_k, e_1\} & \text{si } i = k. \end{cases}$$

On déduit alors du principe des bergers que $d(s) = |A_s| = 2|I_s|$ est pair.

Réciproquement, supposons que G est connexe et que tous les sommets de G sont de degré pair. Considérons une chaîne simple de longueur k maximale $\gamma = (v_0, e_1, v_1, \dots, e_k, v_k)$. Nous allons montrer que γ est un cycle eulérien.

Supposons d'abord que γ ne soit pas fermée, c'est-à-dire que $v_k \neq v_0$. Posons $s = v_k$ et définissons A_s l'ensemble des arêtes incidentes à s visitées par γ , I_s et f_s comme ci-dessus. On voit que $f_s^{-1}(k) = \{e_k\}$ est un singleton et $|f_s^{-1}(i)|$ vaut 2 pour $i < k$. On en déduit que $|A_s|$ est impair. Comme s est de degré pair, il existe une arête a incidente à $s = v_k$ qui n'est pas visitée par γ et $\gamma \cdot a$ est une $k + 1$ -chaîne simple, une contradiction. On a donc montré que γ est un cycle.

Supposons maintenant qu'il existe une arête a non visitée par γ , et posons $\{u, v\} = \varphi(a)$. Comme G est connexe, il existe une chaîne

$$\delta = (w_0, f_1, \dots, f_l, w_l)$$

d'origine $w_0 = v_0$ et extrémité $w_l = u$. Posons $f_{l+1} = a$ et $w_{l+1} = v$. Notons i le plus petit élément de $[1, l + 1]$ tel que f_i ne soit pas visité par γ . Il est clair que w_{i-1} est visité par γ . Il existe donc $j \in [0, k]$ tel que $v_j = w_{i-1}$. On voit que

$$(v_j, \dots, v_k = v_0, \dots, v_j = w_{i-1}, f_i, w_i)$$

est une $k + 1$ -chaîne simple, une contradiction.

Supposons enfin qu'il existe un sommet s non visité par γ . Comme G est connexe, il existe une arête e incidente à s , et cette arête n'est pas visitée par γ , ce qui est impossible comme on vient de le voir. **cqfd.**

Corollaire 3.3.10. *Soit G un multigraphe d'ordre au moins 2. Le multigraphe G est semi-eulérien si et seulement si il est connexe et le nombre de ses sommets de degré impair est 0 ou 2.*

Démonstration. Si γ est une chaîne eulérienne de $G = (S, A)$ dont les extrémités sont u et v , considérons le graphe G' obtenu en ajoutant à G une arête e d'extrémités u et v . La chaîne $\gamma \cdot e$ est un cycle eulérien de G' . On en déduit que les degrés de tous les sommets de G (autres que u et v si

$u \neq v$) sont pairs. La connexité de G est évidente exactement comme dans la démonstration du théorème.

Réciproquement, si G a deux sommets distincts de degré impair, u et v , le graphe G' défini comme ci-dessus a tous ses sommets de degré pair. Si G est connexe, G' l'est aussi et on peut appliquer le théorème à G' . Si γ est un cycle eulérien de G' , il visite forcément e et, en retirant e de γ , on obtient une chaîne eulérienne de G . **cqfd.**

3.3.4 Graphes hamiltoniens

Un *cycle hamiltonien* est un cycle élémentaire qui visite tous les sommets d'un graphe. Sa longueur est donc l'ordre n du graphe. Une *chaîne hamiltonienne* est une chaîne élémentaire qui visite tous les sommets d'un graphe. Sa longueur est donc $n - 1$. Un *graphe hamiltonien* est un multigraphe qui admet un cycle hamiltonien.

Proposition 3.3.11. *Les graphes simples C_n et K_n sont hamiltoniens si et seulement si $n \geq 3$.*

En effet, dans un graphe simple, la longueur d'un cycle est au moins 3.

Théorème 3.3.12. *Si $G = (S, A)$ est un graphe simple d'ordre $n \geq 3$ tel que pour toute paire (u, v) de sommets non voisins, on a $d(u) + d(v) \geq n$, alors G est hamiltonien.*

Démonstration. Considérons dans G une chaîne élémentaire de longueur maximale $\gamma = (v_0, \dots, v_k)$. On voit facilement que $1 < k < n$ et que les voisins de v_0 et ceux de v_k sont tous visités par γ . Deux cas se présentent :

- Si v_0 et v_k sont voisins, posons

$$\delta = (v_0, \dots, v_k, v_0).$$

- Si v_0 et v_k ne sont pas voisins, posons

$$I = \{i \in [1, k]; v_0 \text{ et } v_i \text{ sont voisins}\}$$

et

$$J = \{i \in [1, k]; v_k \text{ et } v_{i-1} \text{ sont voisins}\}.$$

On a $|I| = d(v_0)$ et $|J| = d(v_k)$. D'après l'hypothèse sur G , on a $|I| + |J| \geq n > k$, donc I et J ont un élément commun i , avec $1 < i < k$. Posons alors

$$\delta = (v_0, \dots, v_{i-1}, v_k, v_{k-1}, \dots, v_i, v_0).$$

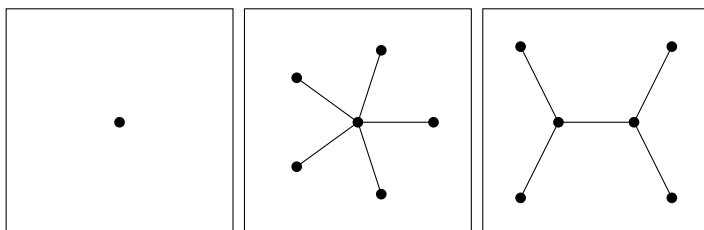
Dans tous les cas, δ est un cycle élémentaire de longueur $k + 1$, que nous réécrivons $\delta = (w_0, \dots, w_{k+1})$, avec $w_{k+1} = w_0$. Nous allons montrer que δ est un cycle hamiltonien.

Soit s un sommet qui n'est pas visité par δ . S'il est voisin d'un des w_i , alors $(s, w_i, \dots, w_k, w_0, \dots, w_{i-1})$ est une chaîne élémentaire de longueur $k + 1$, une contradiction. On en déduit que les voisins de s ne rencontrent pas les $k + 1$ sommets visités par δ , donc $d(s) \leq n - k - 1$. De même, les voisins de w_0 sont parmi les k sommets visités par δ autres que w_0 , et $d(w_0) \leq k$. On a donc $d(s) + d(w_0) < n$, ce qui mène à une contradiction avec le fait que s et w_0 ne sont pas voisins. **cqfd.**

Corollaire 3.3.13. *Si G est un graphe simple d'ordre $n \geq 3$ tel que $\delta(G) \geq \frac{n}{2}$, alors G est hamiltonien.*

3.4 Arbres

Une *forêt* est un multigraphe sans cycle. En particulier, c'est un graphe simple. Un *arbre* est un graphe connexe sans cycle. Voici quelques arbres.



Le théorème suivant montre que les arbres ont une position centrale. Nous aurons besoin de quelques propositions préliminaires.

3.4.1 Préliminaires

Un *sommet pendant* d'un graphe est un sommet de degré 1. Si s est un sommet pendant, il existe une arête e incidente à s et une seule.

Proposition 3.4.1. *Si $G = (S, A)$ est une forêt, et si A n'est pas vide, alors il y a au moins deux sommets pendants dans G .*

Démonstration. On rappelle que G est un graphe simple. Soit

$$\gamma = (v_0, v_1, \dots, v_k)$$

une chaîne élémentaire de longueur k maximale. Comme A n'est pas vide, il y a au moins une arête, donc $k > 0$. Le seul voisin de v_0 est v_1 . En effet, si u

est un autre voisin de v_0 , soit u est l'un des v_i , avec $i > 1$ et $(v_0, v_1, \dots, v_i, u)$ est un cycle, une contradiction, soit non, auquel cas (u, v_0, \dots, v_k) est une chaîne élémentaire de longueur $k + 1$, encore une contradiction. On en déduit $d(v_0) = 1$, et de même $d(v_k) = 1$. **cqfd.**

Corollaire 3.4.2. *Si $G = (S, A)$ est un arbre d'ordre $|S| = n$, il y a dans A exactement $n - 1$ arêtes.*

Démonstration. Par récurrence sur n . Pour $n = 1$, il n'y a pas de boucle, donc $A = \emptyset$ et $|A| = 0$. Si $n > 1$, il y a au moins deux sommets. Comme G est connexe, il y a au moins une chaîne qui les joint, donc A n'est pas vide. Il y a donc au moins un sommet pendant s . Soit e l'unique arête adjacente à s . Le graphe $G' = G \setminus \{s\} = (S \setminus \{s\}, A \setminus \{e\})$ est un arbre d'ordre $n - 1$. On peut lui appliquer l'hypothèse de récurrence. On a donc

$$m - 1 = |A \setminus \{e\}| = |G \setminus \{s\}| - 1 = n - 2,$$

donc $m = n - 1$. **cqfd.**

Proposition 3.4.3. *Soit*

$$\gamma = (u = v_0, e_1, v_1, \dots, v_k = v)$$

et

$$\delta = (u = w_0, f_1, w_1, \dots, w_l = v)$$

deux chaînes simples distinctes d'origine u et extrémité v dans un multigraphe G . De la chaîne fermée $\gamma \cdot \tilde{\delta}$, on peut extraire un cycle.

Démonstration. Par récurrence sur $p = k + l$. Si $p = 0$, il n'est pas possible que $\gamma \neq \delta$, il n'y a donc rien à démontrer. Supposons la propriété vraie si la somme des longueurs est strictement plus petite que $p > 0$. Si $\gamma \cdot \tilde{\delta}$ est simple, c'est un cycle. Sinon, il existe une arête visitée deux fois par $\gamma \cdot \tilde{\delta}$. Comme γ et δ sont simples, une des visites est dans γ et l'autre dans $\tilde{\delta}$: il existe $i \in [1, k]$ et $j \in [1, l]$ tels que $e_i = f_j$. Il y a deux possibilités :

1. $v_{i-1} = w_{j-1}$ et $v_i = w_j$. On a alors soit $(v_0, \dots, v_{i-1}) \neq (w_0, \dots, w_{j-1})$ soit $(v_i, \dots, v_k) \neq (w_j, \dots, w_l)$. Dans les deux cas on peut appliquer l'hypothèse de récurrence pour obtenir un cycle extrait de $\gamma \cdot \tilde{\delta}$.
2. $v_{i-1} = w_j$ et $v_i = w_{j-1}$. On a alors soit $(v_0, \dots, v_i) \neq (w_0, \dots, w_{j-1})$ soit $(v_{i-1}, \dots, v_k) \neq (w_j, \dots, w_l)$. Dans les deux cas on peut appliquer l'hypothèse de récurrence pour obtenir un cycle extrait de $\gamma \cdot \tilde{\delta}$.

cqfd.

Corollaire 3.4.4. *Dans un multigraphe $G = (S, A)$, il existe un cycle si et seulement si il existe deux chaînes simples distinctes qui ont même origine et même extrémité.*

Enfin, dans un graphe connexe $G = (S, A)$, un *isthme* est une arête e telle que le graphe $G \setminus \{e\} = (S, A \setminus \{e\})$ ne soit pas connexe.

Proposition 3.4.5. *Dans un graphe connexe, une arête est un isthme si et seulement si elle n'est visitée par aucun cycle.*

Démonstration. Supposons d'abord que e est visité par un cycle. On peut écrire $\gamma = (v_0, e = e_1, v_1, \dots, v_k)$, avec $v_k = v_0$. Soit u et v deux sommets de G . Comme G est connexe, il existe une chaîne simple

$$\delta = (u = w_0, f_1, \dots, w_l = v).$$

Si δ ne visite pas e , on pose $\delta' = \delta$. Dans le cas contraire, il existe un unique $i \in [1, l]$ tel que $f_i = e$. On "remplace e dans δ par le grand arc de γ ", c'est-à-dire qu'on pose

$$\delta' = (u = w_0, \dots, w_{i-1} = v_1, \dots, v_k = w_i, \dots, w_l = v)$$

si $w_{i-1} = v_1$ et $w_i = v = 0$, et

$$\delta' = (u = w_0, \dots, w_{i-1} = v_k, e_k, v_{k-1} \dots, v_1 = w_i, \dots, w_l = v)$$

si $w_{i-1} = v_0$ et $w_i = v_1$. Il existe dans tous les cas une chaîne δ' de $G \setminus \{e\}$, d'origine u et extrémité v . On en déduit que $G \setminus \{e\}$ est connexe et e n'est pas un isthme. Réciproquement, si e n'est pas un isthme, notons u et v les extrémités de e . Comme $G \setminus \{e\}$ est connexe, il existe une chaîne simple γ de $G \setminus \{e\}$ d'origine v et extrémité u . La chaîne $\delta \cdot (u, e, v)$ est fermée et simple : c'est un cycle qui visite e . **cqfd.**

Corollaire 3.4.6. *Soit $G_1 = (S_1, A_1)$ et $G_2 = (S_2, A_2)$ deux arbres, composantes connexes distinctes d'une forêt $G = (S, A)$. Soit $s_1 \in S_1$ et $s_2 \in S_2$. Posons $e = \{s_1, s_2\}$. Le graphe simple $G' = (S, A \cup \{e\})$ est encore une forêt.*

En effet, e est un isthme du graphe connexe $G'' = (S_1 \cup S_2, A_1 \cup A_2 \cup \{e\})$. Un cycle de G' doit visiter e donc rester dans G'' , une contradiction.

3.4.2 Caractérisation des arbres

Théorème 3.4.7. *Soit $G = (S, A)$ un multigraphe. On note $n = |S|$ son ordre et $m = |A|$ le nombre de ses arêtes. Les propriétés suivantes sont équivalentes :*

1. G est un arbre.
2. Pour tout couple (u, v) de sommets, il existe une chaîne simple d'origine u et extrémité v et une seule.
3. G est connexe, et toute arête de G est un isthme (G est connexe minimal).
4. G est une forêt, et pour toute arête $e \notin A$, $(S, A \cup \{e\})$ admet un cycle (G est une forêt maximale).
5. G est connexe et $m = n - 1$.
6. G est une forêt, et $m = n - 1$.

On rappelle sans démonstration un théorème tout-à-fait analogue à celui-ci :

Théorème 3.4.8. Soit E un K -espace vectoriel de dimension n , et $B = (b_i)_{1 \leq i \leq m}$ une famille finie d'éléments de E . Les propriétés suivantes sont équivalentes :

1. B est une base de E .
2. Pour tout vecteur $x \in E$, il existe une famille $(\lambda_i)_{1 \leq i \leq m}$ de scalaires telle que $\sum_{i=1}^m \lambda_i b_i = x$ et une seule.
3. B est une famille génératrice de E et pour tout $i \leq m$ la famille obtenue en enlevant b_i à B ne l'est pas (B est génératrice minimale).
4. B est libre et quelle que soit la valeur de b_{m+1} , la famille $(b_i)_{1 \leq i \leq m+1}$ ne l'est pas (B est libre maximale).
5. B est une famille génératrice de E et $m = n$.
6. B est une famille libre et $m = n$.

Démonstration. $1 \Leftrightarrow 2$ La connexité est équivalente à l'existence de chaînes simples de u à v pour tous sommets u et v . D'autre part, grâce au lemme aller-retour, on voit que l'existence d'un cycle équivaut à celle de deux chaînes simples ayant même origine et même extrémité.

$1 \Leftrightarrow 3$ D'après la proposition 3.4.5, dans un graphe connexe, l'existence d'un isthme est équivalente à la non-existence d'un cycle.

$1 \Leftrightarrow 4$ D'après le corollaire 3.4.6, si une forêt n'est pas connexe, on peut lui ajouter une arête sans créer de cycle. Réciproquement, si G est un arbre et $e = \{u, v\} \notin A$, alors il existe une chaîne simple d'origine u et extrémité v dans G , (u, e, v) en est une autre dans $G \cup \{e\}$, ce qui, grâce à la proposition 3.4.3 montre que $G \cup \{e\}$ n'est pas une forêt.

$1 \Rightarrow 5$ et 6 C'est une conséquence du corollaire 3.4.2.

$5 \Rightarrow 3$ Parmi les sous-graphes couvrants de G qui sont connexes, il y en a au moins un $G' = (S, A')$ qui est minimal. C'est un arbre. D'après $1 \Rightarrow 5$, on a $|A'| = n - 1 = |A|$. Or $A' \subset A$. On en déduit $A' = A$.

$5 \Rightarrow 3$ Une forêt est un graphe simple. On en déduit que parmi les forêts sur S dont G est un graphe couvrant, il en existe une $G' = (S, A')$ qui est maximale. C'est un arbre. D'après $1 \Rightarrow 5$, on a $|A'| = n - 1 = |A|$. Or $A' \subset A$. On en déduit $A' = A$.

cqfd.

3.4.3 Arbres couvrants

Un *arbre couvrant* d'un multigraphe G est un sous-graphe couvrant de G qui est un arbre. Si un graphe a un arbre couvrant, il est connexe. Le théorème précédent montre que la réciproque est vraie. Nous présentons deux algorithmes naturels pour trouver un arbre couvrant d'un multigraphe G connexe.

Données: Un multigraphe connexe $G = (S, A)$

Sortie: Une partie A' de A telle que $G' = (S, A')$ est un arbre.

```
A' <- {}
tant que $G'$ n'est pas connexe
  choisir une composante connexes C de G'
  choisir une arête e de A liant C et S \ C
  faire A' <- A' union {e}
fin tant que
```

L'existence de l'arête e est due au fait que G est connexe. L'adjonction de e à A' ne change pas le fait que G' est une forêt. L'algorithme s'arrête donc bien quand G' est un arbre.

Cet algorithme a une variante adaptée aux graphes valués : on définit le poids d'un sous-graphe comme la somme des coûts de toutes les arêtes de ce sous-graphe, et on cherche un arbre couvrant de poids minimal.

Données: Un multigraphe valué connexe $G = (S, A, c)$

Sortie: Une partie A' de A telle que $G' = (S, A')$ est un arbre et le poids total de A' est minimal.

numéroter les éléments de A par poids croissant:

```
c(e_1) <= ... <= c(e_m)
A' <- {}
pour i allant de 1 à m faire
  si (e_i n'est pas une boucle et si) les extrémités de e_i
    sont sur des composantes connexes différentes de G' faire
```

```

    A' <- A' union {e_i}
  fin si
fin tant que

```

Cet algorithme, qui prend en priorité les arêtes de poids faible, est appelé *glouton* pour la même raison qui fait qu'en informatique les arbres sont représentés avec leurs racines en haut et les feuilles en bas.

Il existe une méthode duale pour extraire un arbre couvrant, qui consiste à couper les cycles tant qu'il y en a. Nous allons l'énoncer pour un multigraphe quelconque.

Données: Un multigraphe $G = (S, A)$ à e composantes connexes.
 Sortie: A' est une partie de A telle que $G' = (S, A')$
 est une forêt à e composantes connexes.

```

A' <- A
tant qu'il existe un cycle dans G'
  choisir un cycle C dans G'
  choisir un arête e visitée par C
  faire A' <- A' \ {e}
fin tant que

```

Comme on l'a vu plus haut, le fait d'enlever un arête visitée par un cycle ne change rien à la connexité. Le nombre de composantes connexes de G' est donc le même que celui de G . En particulier, si G est connexe, G' est un arbre couvrant de G . En général, combien de fois la boucle interne de l'algorithme s'exécute-t'elle? Appelons p ce nombre. On voit que $p = |A| - |A'|$ est le nombre d'arêtes qu'on a enlevées. La proposition suivante montre que p ne dépend pas des choix faits dans l'algorithme, mais seulement du multigraphe G . Nous appellerons p le *nombre de cycles indépendants* de G .

Proposition 3.4.9. *Dans l'algorithme précédent, la boucle interne s'exécute p fois, avec*

$$p = m - n + e$$

où n est l'ordre de G , m son nombre d'arêtes, et e son nombre de composantes connexes.

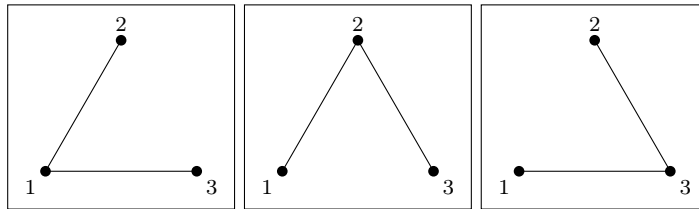
Démonstration. Notons $G_i = (S_i, A_i)$ les e composantes connexes d'une forêt $G = (S, A)$ à n sommets et m arêtes. Chaque G_i est un arbre, on a donc $|A_i| = |S_i| - 1$. Comme S est réunion disjointe des S_i et A réunion disjointe des A_i , on a

$$m = |A| = \sum_{i=1}^e |A_i| = \sum_{i=1}^e (|S_i| - 1) = \sum_{i=1}^e |S_i| - e = |S| - e = n - e.$$

Si maintenant $G = (S, A)$ est un multigraphe quelconque et qu'on exécute l'algorithme, le résultat est une forêt (S, A') qui a le même nombre n de sommets et le même nombre e de composantes connexes que G . Son nombre d'arêtes est $m' = m - p$. Or on vient de montrer que $m' = n - e$, d'où le résultat. **cqfd.**

3.4.4 Théorème de Cayley

On s'intéresse ici aux arbres couvrants de la clique K_n , ou plutôt à leur nombre. On voit facilement que K_1 et K_2 sont des arbres et que K_3 a trois arbres couvrants.



Il est plus difficile d'établir que les arbres couvrants de K_4 sont au nombre de 16, mais il n'y en a que deux à isomorphisme près. Supposons désormais $n \geq 3$. Nous allons décrire une opération de codage qui à tout arbre T dont l'ensemble des sommets est $[1, n]$ fait correspondre une famille (b_1, \dots, b_{n-2}) de $n - 2$ éléments de $[1, n]$ de la façon suivante.

Données: Un arbre $T = (S, A)$ d'ensemble de sommets $S = [1, n]$

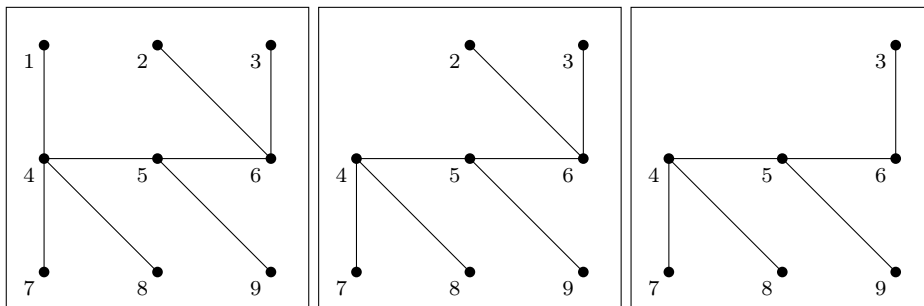
Sortie: le tableau b contient $n-2$ entiers de $[1, n]$

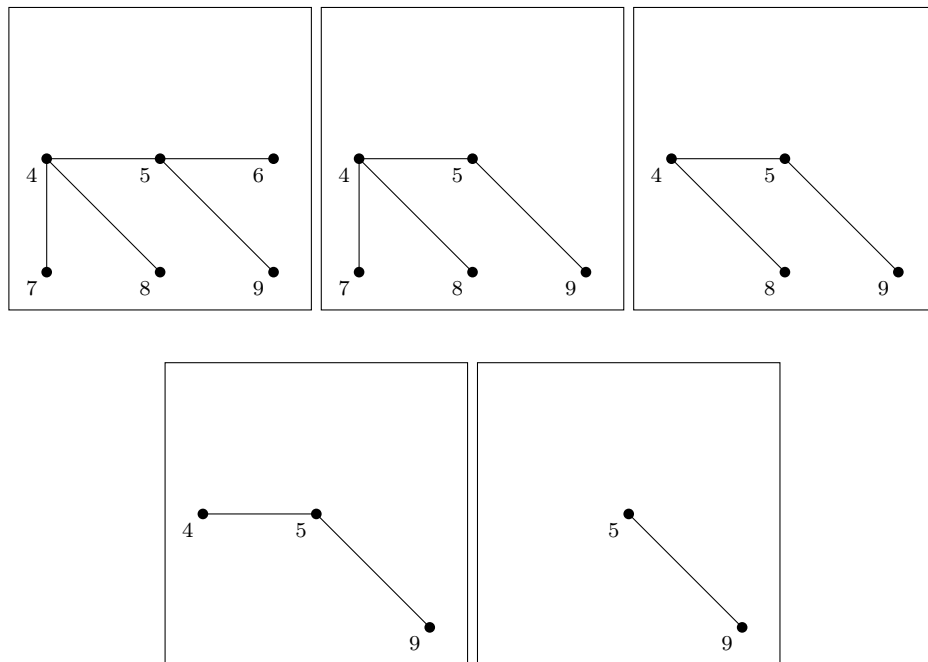
```

pour i de 1 à n-2 faire
  s <- le plus petit sommet pendent de T
  e <- l'arête incidente à s
  b[i] <- le voisin de s dans T
  S <- S \ {s}
  A <- A \ {e}
fin pour

```

Voici la suite des opérations qui donne l'encodage d'un certain arbre couvrant de K_9 .





Le résultat final est donc la famille $(4, 6, 6, 5, 4, 4, 5)$. L'opération de décodage se décrit de la même façon :

Données: Un tableau b de $n-2$ entiers de $[1, n]$
 Sortie: $T = ([1, n], A)$ est un arbre

$A \leftarrow \{\}$

$S \leftarrow [1, n]$

pour i de 1 à $n-2$ faire

$s \leftarrow$ le plus petit élément de S qui n'est égal
 à aucun $b[j]$ avec $i \leq j \leq n-2$.

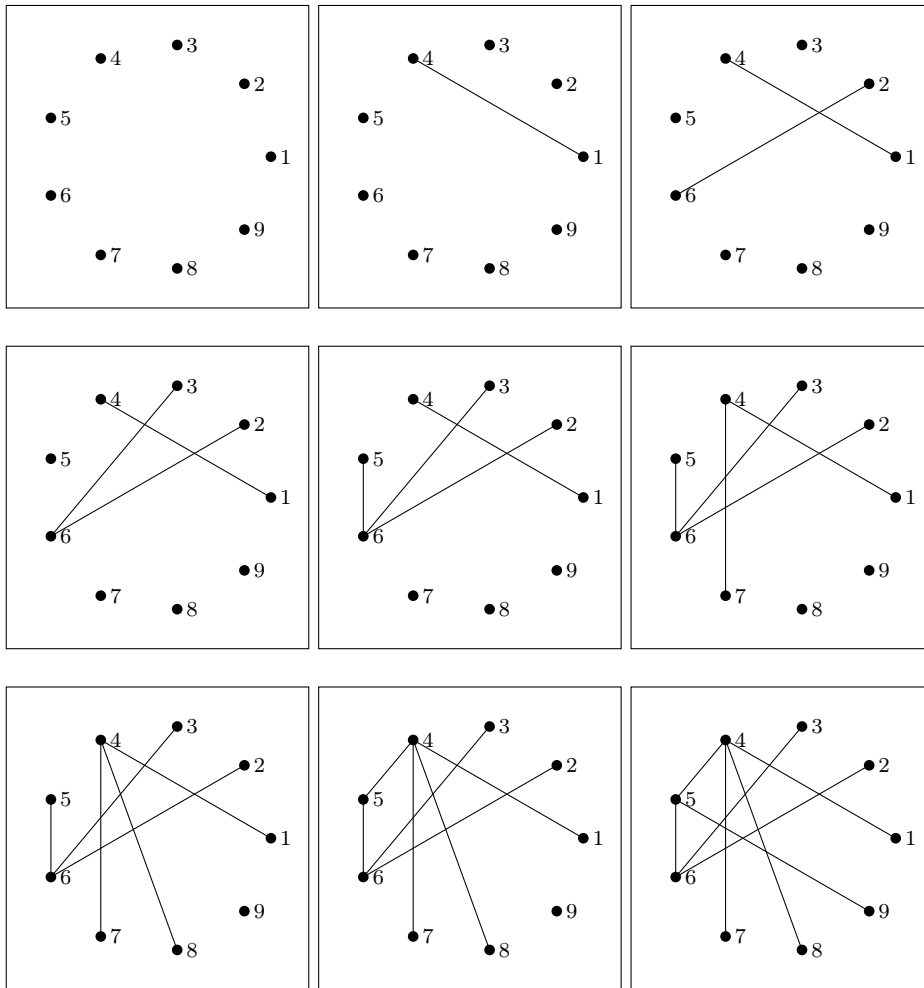
$A \leftarrow A \cup \{s, b[i]\}$

$S \leftarrow S \setminus \{s\}$

fin pour

$A \leftarrow A \cup \{S\}$

Comme S a $n - i + 1$ éléments et j ne prend que $n - i - 1$ valeurs, on peut toujours trouver s . Pour prouver que le graphe obtenu est un arbre, il suffit de remarquer qu'à tout moment S contient un sommet et un seul dans chaque composante connexe de T . Comme $b[i]$ n'a pas pu être enlevé de S aux tours précédents, il est encore dans S et l'arête $\{s, b[i]\}$ réunit deux composantes connexes différentes : il ne peut se créer de cycle. Après la fin de la boucle, S ne contient que deux éléments, appartenant aux deux composantes connexes de $([1, n], A)$. Enfin, T est une forêt à $n - 1$ arêtes, c'est donc bien un arbre. Voici la suite d'opérations décrivant le décodage de $(4, 6, 6, 5, 4, 4, 5)$:



On voit que les opérations de codage et de décodage sont inverses l'une de l'autre. On a donc une bijection entre l'ensemble T_n des arbres couvrants de K_n et $[1, n]^{n-2}$. On a donc prouvé le

Théorème 3.4.10 (de Cayley). *Pour tout $n \geq 1$, une n -clique a exactement n^{n-2} arbres couvrants.*

Index

- Addition, 5
- Algorithme de Dijkstra, 52
- Algorithme de Moore, 51
- Algorithme glouton, 44
- Antisymétrie, 9
- Application, 3
- Application composée, 3
- Application identique, 3
- Arête, 37, 47
- Arête multiple, 47
- Arbre, 61
- Arbre couvrant, 65
- Arrangement, 16
- Auto-complémentaire, 41

- Base, 55
- Biparti, 43
- Bon ordre, 5
- Boucle, 47

- Cardinal, 6
- Chaîne, 40, 49
- Chaîne élémentaire, 50
- Chaîne eulérienne, 58
- Chaîne fermée, 50
- Chaîne hamiltonienne, 60
- Chaîne simple, 50
- Clôture réflexive-transitive, 9
- Clôture symétrique, 9
- Clique, 40
- Coût, 52
- Coefficient binomial, 15
- Coefficient multinomial, 18
- Coloration, 43

- Combinaison, 17
- Composante connexe, 55
- Concaténation, 50
- Constante, 24
- Couleur, 43
- Cube, 40
- Cycle, 40, 55
- Cycle élémentaire, 55
- Cycle eulérien, 58
- Cycle hamiltonien, 60

- Dénombrable, 8
- Dérivée, 26
- Degré, 37, 48
- Diamètre, 54
- Distance, 51
- Distributivité, 13

- Ensemble d'arrivée, 3
- Ensemble de départ, 3
- Entier naturel, 4
- Exponentiation, 5
- Extrémité, 37, 47, 50

- Factorielle descendante, 27
- Famille, 4
- Fini, 7
- Fonction, 3
- Fonction caractéristique, 12
- Forêt, 61
- Formules de Newton, 34

- Graphe, 48
- Graphe complémentaire, 41
- Graphe complet, 40

- Graphe connexe, 54
- Graphe de Petersen, 41
- Graphe eulérien, 58
- Graphe hamiltonien, 60
- Graphe mineur, 45
- Graphe multiparti complet, 44
- Graphe planaire, 38, 45
- Graphe semi-eulérien, 58
- Graphe simple, 37
- Graphe simple sous-jacent, 47
- Graphe valué, 52

- Image, 3
- Image réciproque, 3
- Infini, 7
- Injection, 4
- Intègre, 25
- Invariant de boucle, 53
- Isomorphisme, 38
- Isthme, 63

- Loi de composition, 5

- Matrice d'adjacence, 49
- Matrice d'incidence, 48
- Multigraphe, 47
- Multiplication, 5

- Nombre chromatique, 44

- Ordre, 37
- Origine, 50

- Paire, 37
- Parmi, 15
- Partition, 10, 43, 54
- Permutation, 17
- Poids, 52
- Polynôme caractéristique, 29
- Polynôme symétrique élémentaire, 32
- Prédicat, 4, 9
- Principe de récurrence, 4

- Réflexivité, 9
- Régulier, 38
- Relation binaire, 9
- Relation d'équivalence, 9
- Relation d'ordre, 5, 9
- Représentation plane, 38

- Série entière formelle, 23
- Sommet, 37, 47
- Sommet isolé, 37
- Sommet pendant, 61
- Sous-graphe, 41, 48
- Sous-graphe couvrant, 41, 48
- Sous-graphe induit, 48
- Stable, 39
- Successeur, 4
- Suite, 5
- Support fini, 23
- Surjection, 4
- Symétrie, 9

- Transitivité, 9
- Triangle de Pascal, 16

- Visiter, 50
- Voisin, 37

Table des matières

1	Combinatoire énumérative	1
1.1	Rappels de théorie des ensembles	1
1.1.1	Applications	1
1.1.2	Entiers naturels, récurrence	2
1.1.3	Le cardinal d'un ensemble	4
1.1.4	Ensembles finis	5
1.1.5	Cardinaux infinis	6
1.1.6	Relations binaires	7
1.2	Outils de base	8
1.2.1	Les opérations de base sur les cardinaux	8
1.2.2	Fonctions caractéristiques	10
1.2.3	Sommes et produits dans un anneau commutatif	11
1.2.4	La formule du binôme	12
1.2.5	Arrangements, permutations et combinaisons	14
1.2.6	Les coefficients multinomiaux	16
1.2.7	La formule du crible	17
1.2.8	Surjections	18
2	Polynômes et séries formelles	21
2.1	Séries formelles	21
2.1.1	L'anneau des séries formelles	21
2.1.2	Inversion, composition, dérivation	23
2.1.3	Quelques exemples	24
2.1.4	Réurrences linéaires à coefficients constants.	26
2.1.5	Les nombres de Catalan	27
2.2	Polynômes	29
2.2.1	Relations entre racines et coefficients	29
2.2.2	Polynômes symétriques	30
2.2.3	Les formules de Newton	32
2.2.4	Un exemple	33

3	Graphes	35
3.1	Graphes simples	35
3.1.1	Définitions	35
3.1.2	Bestiaire	37
3.1.3	Sous-graphes, le théorème de Turán	39
3.1.4	Colorations	41
3.1.5	Graphes planaires	43
3.2	Multigraphes	45
3.2.1	Matrices d'incidence et d'adjacence	46
3.2.2	Chaînes dans un multigraphe	47
3.2.3	Algorithmes de Moore et de Dijkstra	49
3.3	Chaînes et cycles	52
3.3.1	Connexité	52
3.3.2	Cycles	53
3.3.3	Graphes eulériens	56
3.3.4	Graphes hamiltoniens	58
3.4	Arbres	59
3.4.1	Préliminaires	59
3.4.2	Caractérisation des arbres	61
3.4.3	Arbres couvrants	63
3.4.4	Théorème de Cayley	65