Mathématiques discrètes

Automne 2010 [1]

1. Version du 24 novembre 2010

Table des matières

Chapitre 1
Notions de théorie des ensembles

De nombreuses façons, les mathématiques s'intéressent à l'étude des structures et des applications entre elles. Par exemple, l'algèbre linéaire s'occupe des espaces vectoriels et de leurs homeomorphismes ; une grande partie de l'analyse s'intéresse aux espaces vectoriels sur les réels et aux fonctions sur de tels espaces.

La plus simple des structures mathématiques est celle d'un ensemble. Ainsi, la théorie des ensembles est au cœur des mathématiques modernes. Les autres concepts, comme les fonctions ou les relations, peuvent s'obtenir à partir de cette théorie.

Durant la plus grande partie du $19^{\text{ème}}$ siècle, la théorie des ensembles était basée sur la définition intuitive d'un ensemble comme une collection d'objets. Et donc, toute collection d'objets pouvait former un ensemble. Néanmoins, vers la fin du siècle, les mathématiciens ont découvert de sérieuses contradictions dans ce modèle intuitif. L'exemple le plus connu est le paradoxe de Russell : soit un ensemble S dont les éléments sont tous les ensembles qui ne se contiennent pas eux-même. S contient-il S ? Si oui, il contient un ensemble qui se contient lui-même, ce qui contredit la définition de S. Si non, il ne contient pas tous les ensembles qui ne se contiennent pas eux-mêmes, encore une contradiction !

Pour résoudre cette difficulté, Ernst Zermelo a proposé en 1908 la première théorie axiomatique des ensembles, c'est à dire une théorie des ensembles basée sur un petit nombre d'axiomes. L'avantage de cette théorie est qu'à peu près toutes les mathématiques en découlent et qu'elle n'admet pas de contradictions comme le paradoxe de Russell. Cette théorie a ensuite été étoffée par Abraham Frænkel, indépendamment par Thoralf Skolem et aussi par Zermelo lui-même. Aujourd'hui, les axiomes de Zermelo-Fraenkel sont au cœur de la théorie des ensembles.

1.1. Les ensembles

Malgré les problèmes soulevés par une théorie intuitive des ensembles, nous avons choisi dans ces notes cette approche pour sa simplicité, tout en gardant à l'esprit que d'éventuels problèmes peuvent être résolus en utilisant la théorie axiomatique de Zermelo-Fraenkel.

Un ensemble est une collection non ordonnée d'objets, que l'on appelle ses *éléments*. Si un ensemble A contient un élément a, alors on écrit $a \in A$. Si a n'est pas un éléments de A, on écrit $a \notin A$. Un ensemble est *fini* s'il contient un nombre fini d'éléments, sinon on dit qu'il est *infini*.

Exemple 1.1.
- L'ensemble $A = \{1, 0, \text{Pomme}\}$ est fini et $1 \in A$ mais $\text{Table} \notin A$.
- L'ensemble infini de tous les entiers relatifs est noté $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$.
- L'ensemble infini de tous les entiers naturels est noté $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- L'ensemble infini de tous les entiers strictement positifs est noté $\mathbb{N}^\star = \{1, 2, 3, \ldots\}$.
- L'ensemble infini des nombres rationnels est noté $\mathbb{Q}$.
- L'ensemble infini des nombres réels est noté $\mathbb{R}$.
- L'ensemble infini des nombres complexes est noté $\mathbb{C}$.

Un sous-ensemble S d'un ensemble A, noté $S \subseteq A$, est un ensemble avec la propriété suivante :

$$S \subseteq A \iff \forall x\colon (x \in S \implies x \in A).$$

C'est-à-dire qu'un sous-ensemble de A contient certains (peut être tous) éléments de A. L'*ensemble vide*, noté $\emptyset$, est un ensemble ne contenant aucun élément. Pour tout ensemble A, on a $\emptyset \subseteq A$ et $A \subseteq A$. Si S n'est pas un sous-ensemble de A, ou de manière équivalente s'il existe un élément $s \in S$ tel que $s \notin A$, alors on écrit $S \not\subseteq A$.

Il est commode de définir un sous-ensemble d'un ensemble T à l'aide d'une propriété P qui est soit vraie soit fausse pour chacun des éléments de T. On peut alors définir un ensemble $A \subseteq T$ par $A := \{x \mid x \in T, P(x)\text{est vraie}\}$.

Exemple 1.2.
- Les ensembles $\{x \mid x \in \mathbb{N}, x^2 < 12\}$ et $\{0, 1, 2, 3\}$ sont égaux.
- $\mathbb{N} = \{x \mid x \in \mathbb{Z}, x \geq 0\}$.
- Soient $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 4\}$, et $C = \{3, 4, 5\}$. Alors $B \subseteq A$, $C \not\subseteq A$, $B \not\subseteq C$, $C \not\subseteq B$.
- Soient A un ensemble et $B = \{A, \{A\}\}$. Alors $A \in B$, mais quand A est non vide $A \not\subseteq B$. De plus, $\{A\} \in B$, $\{A\} \subseteq B$ et $\{\{A\}\} \subseteq B$.

L'ensemble des parties (*power set* en anglais) $P(A)$ d'un ensemble A est l'ensemble de tous les sous-ensembles de A. Par exemple, si $A = \{1, 2\}$, alors $P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

1.2. Opérations sur les ensembles

Si A et B sont des ensembles, alors leur *produit cartésien* $A \times B$ est défini par

$$A \times B = \{(a, b) \mid a \in A \text{ et } b \in B\}.$$

Le produit cartésien d'un nombre fini d'ensembles $A_1, \ldots, A_n$ est défini récursivement comme :

$$A_1 \times \cdots \times A_n := \begin{cases} A_1 & \text{si } n = 1, \\ A_1 \times A_2 & \text{si } n = 2, \\ (A_1 \times \cdots \times A_{n-1}) \times A_n & \text{si } n > 2. \end{cases}$$

La *différence* de deux ensembles A et B, notée $A \setminus B$, est définie par $A \setminus B := \{x \mid x \in A \text{ et } x \notin B\}$. Ainsi, $A \setminus B$ contient les éléments qui sont dans A mais qui ne sont pas dans B.

Soient A un ensemble et U un autre ensemble qui contient A. Le *complément* de A par rapport à U, noté ${}_U A^c$, ou juste A^c si U est connu d'après le contexte, est défini par $A^c = U \setminus A$. Remarquez que $(A^c)^c = A$ quel que soit l'ensemble U.

L'*intersection* et l'*union* de deux ensembles A et B sont définies comme

$$\begin{aligned} A \cap B &:= \{x \mid x \in A \text{ et } x \in B\}, \\ A \cup B &:= \{x \mid x \in A \text{ ou } x \in B\}. \end{aligned}$$

L'union et l'intersection d'un nombre fini d'ensembles sont définies récursivement de manière analogue à la définition pour le produit cartésien. Le lemme suivant est connu sous le nom de *Loi de De Morgan* en mémoire de Augustus De Morgan, mathématicien britannique du 19ème siècle.

Lemme 1.3. *Soit U un ensemble contenant les ensembles A et B. On a :*

(1) $(A \cup B)^c = A^c \cap B^c$.

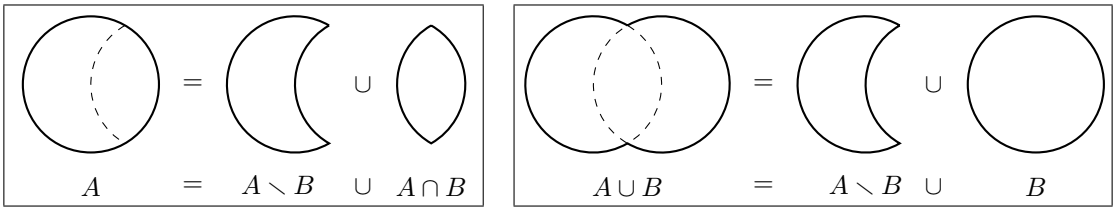
(2) $(A \cap B)^c = A^c \cup B^c$.

Démonstration. Nous ne prouvons que la partie (1), la seconde partie se prouve de manière analogue.

Pour montrer l'égalité de deux ensembles, on doit montrer que tout élément appartenant à l'un des ensembles appartient aussi à l'autre et *vice versa*. Soit $x \in (A \cup B)^c$. Alors $x \notin (A \cup B)$, donc $x \notin A$ et $x \notin B$, donc $x \in A^c$ et $x \in B^c$, donc $x \in A^c \cap B^c$.

Réciproquement, soit $x \in A^c \cap B^c$. Alors $x \in A^c$ et $x \in B^c$, donc $x \notin A$ et $x \notin B$, donc $x \notin A \cup B$, donc $x \in (A \cup B)^c$. □

Les opérations d'intersection et d'union satisfont certaines relations de commutativité et de distributivité indiquées dans la proposition suivante :



(a) (b)

Figure 1.1 – Description graphique de la démonstration du Lemme 1.5

Proposition 1.4. *Soient A, B et C des ensembles.*

(1) $A \cup A = A$, $A \cap A = A$,

(2) $A \cup B = B \cup A$, $A \cap B = B \cap A$.

(3) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$.

(4) $A \cup (B \cap C) = (A \cup C) \cap (A \cup B)$.

(5) $A \cap (B \cup C) = (A \cap C) \cup (A \cap B)$.

Démonstration. Les assertion (1)–(3) sont triviales et les preuves de (4) et (5) sont similaire, on va donc se concentrer sur la démonstration de (4).

Soit $x \in A \cup (B \cap C)$. Alors $x \in A$ ou $x \in B \cap C$. Si $x \in A$, alors $x \in (A \cup C) \cap (A \cup B)$, ce qui montre que $A \cup (B \cap C) \subseteq (A \cup C) \cap (A \cup B)$. Si $x \in B \cap C$, alors $x \in B$ et $x \in C$, donc $x \in (A \cup C) \cap (A \cup B)$, ce qui montre encore que $A \cup (B \cap C) \subseteq (A \cup C) \cap (A \cup B)$.

Réciproquement, soit $x \in (A \cup C) \cap (A \cup B)$. Alors $x \in A \cup C$ et $x \in A \cup B$. Si $x \in A$, alors $x \in A \cup (B \cap C)$, donc $(A \cup C) \cap (A \cup B) \subseteq A \cup (B \cap C)$. Si $x \notin A$, alors $x \in C$ et $x \in B$, donc $x \in B \cap C$ et ainsi $x \in A \cup (B \cap C)$. Cela montre que $(A \cup B) \subseteq A \cup (B \cap C)$ et avec l'autre inclusion on obtient l'égalité des deux ensembles. □

La prochaine opération qui va nous intéresser et celle de l'*union disjointe*. Soient A et B des ensembles. L'*union disjointe* $A \sqcup B$ de A et B est définie comme

$$A \sqcup B = \{(a, 1) \mid a \in A\} \cup \{(b, 2) \mid b \in B\}.$$

De manière similaire, si $A_1, A_2, \ldots$ sont des ensembles, leur union disjointe est définie comme

$$\bigsqcup_{i=1}^{\infty} A_i := \bigcup_{i=1}^{\infty} \{(a, i) \mid a \in A_i\}.$$

On verra plus en détails certaines propriétés de l'union disjointe dans la prochaine section. Pour le moment, montrons juste le résultat suivant :

Lemme 1.5. *Soient A et B des ensembles.*

(a) $A = (A \setminus B) \cup (A \cap B)$.

(b) $A \cup B = (A \setminus B) \cup B$.

Démonstration. (a) L'ensemble à gauche est trivialement contenu dans A, il suffit donc de montrer l'autre inclusion. Soit $x \in A$. Si $x \in A \cap B$, alors x est contenu dans $(A \setminus B) \cup (A \cap B)$ et on a fini, supposons donc que $x \notin A \cap B$. Cela implique que $x \in A$, mais $x \notin B$, donc $x \in A \setminus B$ par définition. Finalement $x \in (A \setminus B) \cup (A \cap B)$ et on a fini.

(b) En utilisant (a), on sait que $A \cup B = (A \setminus B) \cup (A \cap B) \cup B$. Mais $(A \cap B) \cup B = B$ et le résultat en découle. □

Une description graphique de la preuve de ce lemme est donné sur la figure 1.1.

1.3. Fonctions

La notion de fonction, et plus généralement celle de relation, sera vue dans le Chapitre 2. Néanmoins, nous en donnons ici une brève introduction pour pouvoir exposer plus clairement les concepts qui nous intéressent.

Soient A et B des ensembles. Intuitivement, une fonction f de A vers B est une procédure qui assigne à des éléments de A un élément de B. Cette définition n'est malheureusement pas assez précise dans notre contexte. Nous allons plutôt voir f comme un ensemble de paires telle que le premier élément est un argument de la fonction et le deuxième la valeur prise sur cet argument.

Plus précisément, le *graphe* de la fonction $f\colon A \to B$ de A dans B est un sous-ensemble de $G \subseteq A \times B$ tel que pour chaque $a \in A$, si (a, b) et (a, b') sont des éléments de G, alors $b = b'$. Cela revient à imposer qu'une fonction associe au plus une seule valeur pour un argument donné. On identifie une *fonction* avec son graphe et on note $b = f(a)$. On appelle a l'*antécédant* par f de b et b la *valeur* de f sur l'argument a. L'ensemble A est appelé l'*ensemble de départ* de f. L'ensemble des éléments $a \in A$ tels que $f(a)$ est défini est appelé *domaine de définition* de f et est noté $\mathrm{Dom}(f)$. Si le domaine de f est égal à A tout entier, on dit que f est une *application*. L'ensemble B est appelé l'*ensemble d'arrivée* de f. L'ensemble $f(A) := \{f(a) \mid a \in A\}$ est appelé l'*image* $\mathrm{Im}(f)$ de f.

Exemple 1.6. Voici quelques exemples de fonctions et d'objets qui n'en sont pas.
- Soit A un ensemble. L'ensemble $\{(a_1, a_2) \mid a_1, a_2 \in A \text{ et } a_1 = a_2\}$ est le graphe d'une fonction. Il s'agit de *la fonction identité* sur A.
- Soient A un ensemble et $P(A)$ l'ensemble de ses parties. L'ensemble $\{(a, S) \mid a \in S\} \subseteq A \times P(A)$ n'est pas le graphe d'une fonction à moins que A n'ait qu'un élément ou soit vide. Pour voir cela, notez que si a, b sont des éléments distincts de A, alors $(a, \{a\})$ et $(a, \{a, b\})$ sont tous deux dans cet ensemble, ce qui contredit la définition d'un graphe d'une fonction.

Une fonction $f\colon A \to B$ est dite *injective* si $f(a) = f(b)$ implique que $a = b$. Elle est dite *surjective* si pour tout $b \in B$ il existe $a \in A$ tel que $f(a) = b$. Elle est dite *bijective* si elle est à la fois surjective et injective.

Exemple 1.7.
- Soit $f\colon \mathbb{Z} \to \mathbb{Z}$ définie par $f(z) := z + 1$. Alors, f est bijective.
- Soient p un nombre premier, a un entier non divisible par p et $f\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ définie par $f(x) := ax \bmod p$. Alors f est bijective. Pour montrer cela, supposons que $f(x) = f(y)$ Alors $ax \equiv ay \bmod p$, donc $a(x - y) \equiv 0 \bmod p$ ce qui veut dire que $a(x - y)$ est divisible par p. Mais comme p ne divise pas a, il divise nécessairement $x - y$, donc $x \equiv y \bmod p$ ce qui montre l'injectivité de f. La bijectivité s'obtient avec la remarque suivante :
- Soient A un ensemble fini et $f\colon A \to A$. Si f est injective, alors elle est bijective car comme $f(a) \neq f(b)$ pour $a \neq b$, la taille de $\mathrm{Im}(f)$ est égale à la taille de A ce qui montre la surjectivité.
- De manière similaire, si $f\colon A \to A$ est surjective et que A est fini alors f est bijective. Dans le cas contraire, s'il existe des éléments $a, b \in A$ distincts tel que $f(a) = f(b)$, cela montre que $\mathrm{Im}(f)$ a au moins un élément de moins que A ce qui contredit la surjectivité de f.
- Les deux points précédents sont faux si A est infini. La fonction $f\colon \mathbb{Z} \to \mathbb{Z}$ définie par $f(x) = 2x$ est clairement injective, mais elle n'est pas surjective.

Pour un ensemble fini A, le cardinal de A, noté $|A|$ ou $\#A$ est le nombre d'éléments dans A. L'ensemble de toutes les applications de A vers B est noté B^A. Cette notation est très bonne comme le montre le lemme suivant :

Lemme 1.8. *Si A et B sont finis, alors $|B^A| = |B|^{|A|}$.*

Démonstration. Une application $f\colon A \to B$ est déterminée de manière unique par son graphe $\{(a, f(a)) \mid a \in A\}$. Pour tout a, il y a $|B|$ possibilités pour $f(a)$. Comme il est possible de choisir $f(a)$ indépendamment pour chaque a, on voit qu'il y a $|B|^{|A|}$ possibilités pour l'application f. □

Introduisons maintenant quelques notations que l'on va utiliser dans ce cours.
- Pour un nombre naturel n, l'ensemble $\underline{n}$ est défini comme $\{0, \ldots, n-1\}$. On définit également $\underline{0} := \emptyset$.
- Pour un ensemble fini A, on note n^A l'ensemble $\underline{n}^A$, c'est-à-dire l'ensemble de toutes les applications de A dans $\underline{n}$.
- Pour une fonction $f\colon A \to B$ et $b \in B$, on note $f^{-1}(b)$ la *fibre de f en b*, définie par

$$f^{-1}(b) := \{a \in A \mid f(a) = b\}.$$

Remarquez que cet ensemble peut être vide.

– Pour une fonction $f\colon A \to B$ et $S \subseteq A$, la *restriction de f sur S*, notée $f|_S$, est la fonction de S dans B qui associe à $s \in S$ l'élément $f(s)$.

Exemple 1.9. Montrons que pour un ensemble A, il existe une bijection φ de $P(A)$ dans 2^A. Soit $S \subseteq A$. On définit $f\colon A \to \underline{2}$ en posant $f(a) := 1$ ssi $a \in S$. On définit $\varphi(S) := f$. Pour montrer l'injectivité de φ, supposons que $\varphi(S) = \varphi(S') =: f$ pour deux ensembles distincts S, S' et soit $a \in S \smallsetminus S'$. Alors $f(a) = 1$ car $a \in S$ et $f(a) = 0$ car $a \notin S'$, contradiction. Pour montrer que φ est surjective, soit $f \in 2^A$ et soit $S := f^{-1}(1)$. Il est alors trivial que $\varphi(S) = f$.

S'il existe une bijection entre deux ensembles A et B, on écrit $A \leftrightarrow B$. (Une notation plus naturelle serait d'écrire $A \simeq B$, mais elle est usuellement réservé pour des ensembles avec plus de structure, comme les espaces vectoriel, les groupes, les anneaux, etc.) On a le résultat suivant :

Proposition 1.10. *Soient A et B des ensembles.*

(a) *Il existe une application injective de $A \cup B$ dans $A \sqcup B$.*

(b) *Si $A \cap B = \emptyset$, alors $A \sqcup B \leftrightarrow A \cup B$.*

(c) *On a $A \leftrightarrow (A \smallsetminus B) \sqcup (A \cap B)$.*

(d) *On a $A \cup B \leftrightarrow (A \smallsetminus B) \sqcup B$.*

Démonstration. (a) En utilisant le lemme 1.5(b) on a $A \cup B = (A \smallsetminus B) \cup B$. Soit $f\colon A \cup B \to A \sqcup B$ défini de la manière suivante : si $a \in B$, alors $f(a) := (a, 2)$ et si $a \in A \smallsetminus B$ alors $f(a) := (a, 1)$. Cette application est une injection : si $f(a) = f(b)$, alors soit $a, b \in B$, soit $a, b \in A \smallsetminus B$. Dans le premier cas, $(a, 2) = (b, 2)$, donc $a = b$. Dans le second cas, $(a, 1) = (b, 1)$, donc $a = b$.

(b) Dans cette situation, l'application f définie ci-dessus est surjective : pour $(a, 1) \in A \sqcup B$ on doit avoir $a \in A$ et $a \notin B$ (car $A \cap B = \emptyset$). Ainsi $(a, 1) = f(a)$. De manière similaire, $(b, 2) = f(b)$ pour tout $b \in B$, ce qui prouve la surjectivité de f.

(c) D'après le lemme 1.5(a) on sait que $A = (A \smallsetminus B) \cup (A \cap B)$. Mais $(A \smallsetminus B) \cap (A \cap B) = \emptyset$, donc (b) prouve le résultat.

(d) D'après le lemme 1.5(b) on sait que $A \cup B = (A \smallsetminus B) \cup B$. Comme $(A \smallsetminus B) \cap B = \emptyset$, (b) prouve le résultat. □

1.4. Cardinal, ensembles dénombrables et indénombrables

Une bijection existe entre deux ensembles finis ssi ils ont le même cardinal.

Lemme 1.11. *Soient A et B des ensembles finis. Il existe une bijection entre A et B ssi $|A| = |B|$.*

Démonstration. Soit f une bijection entre A et B. Comme f est injective, la cardinal de $f(A)$ est le même que celui de A et par surjectivité $f(A) = B$.

Pour la réciproque, on peut supposer que $A = \{a_1, \ldots, a_m\}$ et $B = \{b_1, \ldots, b_m\}$ et défini l'application f par$f(a_1) = b_1, \ldots, f(a_m) = b_m$. □

Que se passe-t-il si A et B ont un nombre infini d'éléments ? Dans ce cas, il est difficile de donner une définition intuitive de $|A|$ et $|B|$. Une façon de s'en sortir est de ne pas essayer d'associer un nombre à $|A|$, mais de comparer la valeur relative du cardinal de deux ensembles.

Plus précisément, on dit que A et B ont le *même cardinal* ou encore que A et B sont *équipotents* et on note $|A| = |B|$, s'il existe une bijection $f\colon A \to B$.

Exemple 1.12. *L'ensemble des entiers $\mathbb{Z}$ et celui des nombres naturels $\mathbb{N}$ ont le même cardinal.* Pour prouver cela, considérons l'application $f\colon \mathbb{Z} \to \mathbb{N}$ définie par

$$f(z) := \begin{cases} -2z - 1 & \text{si } z < 0 \\ 2z & \text{si } z \geq 0. \end{cases}$$

Pour montrer que f est injective, supposons que $f(z_1) = f(z_2)$. Comme la valeur de f pour un argument négatif est impaire et celle pour un argument positif est pair, z_1 et z_2 sont nécessairement du même signe. Supposons par exemple qu'ils soient tous deux négatifs. Alors $f(z_1) = -2z_1 - 1 = -2z_2 - 1 = f(z_2)$, ce qui implique que $z_1 = z_2$. On arrive à la même conclusion si on les suppose tous deux positifs, ce qui montre l'injectivité de f.

Pour montrer la surjectivité de f, soit $m \in \mathbb{N}$. Si m est impair, il s'écrit $m = 2\ell - 1$ avec $\ell \in \mathbb{N}^\star$ et $m = f(-\ell)$. Si m est pair, il s'écrit $m = 2\ell$ avec $\ell \in \mathbb{N}$ et $m = f(\ell)$. L'application f est donc une bijection ce qui termine la preuve.

On dit que $|A| < |B|$ s'il existe une application injective $f\colon A \to B$, mais qu'il n'existe *pas* de bijection $g\colon A \to B$. Montrer que $|A| < |B|$ est souvent plus difficile que de montrer $|A| = |B|$ car on doit prouver la non-existence d'un objet plutôt que son existence. On dit que $|A| \leq |B|$ s'il existe une application injective $f\colon A \to B$.

Un ensemble A est dit *dénombrable* si $|A| \leq |\mathbb{N}|$, c'est-à-dire s'il existe une injection de A dans $\mathbb{N}$. Une telle application est dite fonction de comptage.

Exemple 1.13. – Tout ensemble fini est dénombrable.
– De l'exemple précédent on en déduit que $\mathbb{Z}$ est dénombrable.

Théorème 1.14. *Les assertions suivantes sont vraies :*

(a) *Un sous-ensemble d'un ensemble dénombrable est dénombrable.*

(b) *Une union finie d'ensembles dénombrables est dénombrable.*

(c) *Si $A_1, A_2, \ldots$ sont dénombrables, alors l'union $\bigcup_{i\in\mathbb{N}} A_i$ est dénombrable.*

(d) *Si A et B sont dénombrable, alors $A \times B$ l'est aussi.*

(e) *L'ensemble $2^{\mathbb{N}}$ n'est pas dénombrable.*

(f) *L'ensemble des réels $\mathbb{R}$ n'est pas dénombrable.*

Démonstration. (a) Soient A dénombrable, $S \subseteq A$ et $f\colon A \to \mathbb{N}$ fonction de comptage pour A. La restriction $f|_S$ est une fonction de comptage pour S.

(b) L'assertion est trivialement vrai si l'union ne contient qu'un ensemble. Considérons ensuite le cas de deux ensembles dénombrables A et B, et considérons dans un premier temps le cas où les ensembles sont disjoints. Soient $f\colon A \to \mathbb{N}$ et $g\colon B \to \mathbb{N}$ des fonctions de comptage pour A et B. On définit alors une application $F\colon A \cup B \to \mathbb{N}$ par

$$F(x) := \begin{cases} 2f(x) - 1 & \text{si } x \in A, \\ 2g(x) & \text{si } x \in B. \end{cases}$$

On peut alors vérifier que F est bien définie, et injective (voir la preuve de l'exemple 1.12) et est donc une fonction de comptage pour $A \bigcup B$. Maintenant, pour montrer le cas ou les A et B sont arbitraire, remarquez qu'il existe toujours une injection d'une union d'ensemble dans leur union disjointe (voir 1.10(a)).

On termine ensuite la preuve par récurrence sur le nombre d'ensemble m. Pour $m \geq 3$ et $A_1, \ldots, A_m$ des ensembles dénombrables, par hypothèse de récurrence, $A_1 \cup A_2 \cup \cdots \cup A_{m-1}$ est dénombrable. En utilisant alors la preuve pour deux ensemble, on montre que

$$A_1 \cup A_2 \cup \cdots \cup A_m = (A_1 \cup A_2 \cup \cdots \cup A_{m-1}) \cup A_m$$

est dénombrable.

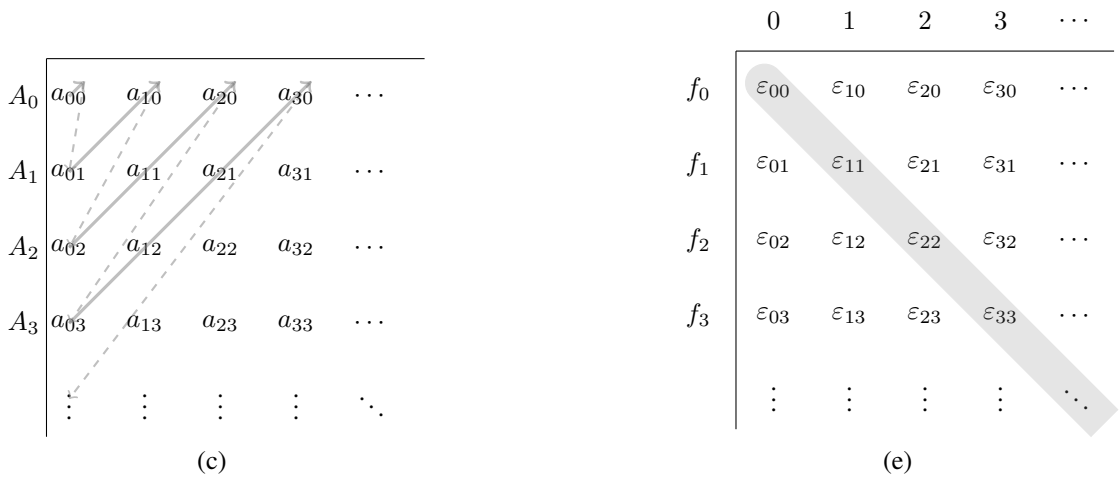
(c) Considérons dans un premier temps le cas où les ensembles sont disjoints. La preuve repose sur une méthode d'*énumération triangulaire*. Notons $f_1, f_2, \ldots$ les fonctions de comptage des ensembles $A_1, A_2, \ldots$. On peut alors ordonner les éléments de A_i comme $\{a_{i1}, a_{i2}, \ldots\}$, où les a_{ij} satisfont $f_i(a_{ij}) < f_i(a_{i,j+1})$ pour tout $j \geq 1$. On définit ensuite une application $F\colon \bigcup_{i\in\mathbb{N}} A_i \to \mathbb{N}$ par

$$F(a_{ij}) := \frac{(i+j-2)(i+j-1)}{2} + j.$$

Remarquez que $F(a_{ij})$ est plus grand que $(i+j-2)(i+j-1)/2$ et inférieur ou égal à $(i+j-1)(i+j)/2$. Pour montrer que F est injective, il suffit de montrer que si $(i,j) \neq (i',j')$, alors $F(a_{ij}) \neq F(a_{i'j'})$. Si $i+j \neq i'+j'$, alors l'assertion est triviale à cause de la borne sur $F(a_{ij})$ mentionnée plus haut. Donc, supposons que $i+j = i'+j'$. On en déduit alors que $j = j'$ et de la que $i = i'$. F est donc injective.

Maintenant, pour montrer le cas ou les A_i sont arbitraire, remarquez qu'il existe toujours une injection d'une union d'ensemble dans leur union disjointe (voir 1.10(a)).

(d) Soit $A = \{a_0, a_1, a_2, \ldots\}$ et $B = \{b_0, b_1, b_2, \ldots\}$. Comme pour (c), on associe à (a_i, b_j) l'entier $(i+j)(i+j+1)/2 + j$. La preuve est alors la même qu'au-dessus.



(c) (e)

Figure 1.2 – Description graphique de la preuve du théorème 1.14(c) et (e).

(e) La preuve est ici beaucoup moins facile car on essaie de montrer qu'une application n'existe pas plutôt que de simplement en construire une. On va utiliser une méthode connue sous le nom de ≪ principe diagonal de Cantor ≫ d'après le mathématicien Allemand Georg Cantor qui l'a utilisée pour montrer que l'ensemble des réels dans l'intervalle $[0, 1)$ est indénombrable.

Pour commencer, supposons que F est une fonction de comptage de l'ensemble $A = 2^{\mathbb{N}}$. On peut alors noter $n_0, n_1, \ldots \in \mathbb{N}$ avec $n_0 < n_1 < \cdots$ les éléments de l'image de F. On considère maintenant les applications $f_0, f_1, f_2 \ldots \in 2^{\mathbb{N}}$ telles que $F(f_i) = n_i$, $i = 0, 1, 2, \ldots$ et l'on pose

$$f_i(j) =: \varepsilon_{ij} \in \{0, 1\}.$$

Définissons alors $g \in 2^{\mathbb{N}}$ par

$$g(j) := \begin{cases} 1 & \text{si } \varepsilon_{jj} = 0, \\ 0 & \text{si } \varepsilon_{jj} = 1. \end{cases}$$

Par définition, on a $g(j) \neq \varepsilon_{jj}$. Comme $g \in 2^{\mathbb{N}}$, elle est nécessairement égale à l'une des f_ℓ pour un certain $\ell \in \mathbb{N}$. Mais alors $g(\ell) = f_\ell(\ell) = \varepsilon_{\ell,\ell}$, ce qui est en contradiction avec la définition de g.

(f) On va montrer que les réels de l'intervalle $[0, 1[$ ne sont pas dénombrables ce qui implique l'assertion en utilisant la partie (a).

A toute suite $\epsilon = (\epsilon_1, \epsilon_2, \ldots)$ où $\epsilon_i \in \{0, 1\}$, on peut associer le réel $z = \sum_{i=1}^{\infty} \epsilon_i 2^{-i}$. Notons S_0 l'ensemble des suites qui deviennent constantes égales à 0 à partir d'un certain rang, S_1 l'ensemble des suites qui deviennent constantes égales à 1 à partir d'un certain rang et T les autres suites. L'ensemble $[0, 1[$ est en bijection avec $S_0 \cup T$. Nous avons déjà vu comment construire un réel à partir d'une suite. Réciproquement, tout réel z admet un développement dyadique que l'on peut construire par divisions euclidiennes successives. Dans cette construction, il est impossible qu'une suite de S_1 survienne car on a pour tout k, $2^{-k} = \sum_{i>k}^{\infty} 2^{-i}$. Comme $2^{\mathbb{N}} = T \cup S_0 \cup S_1$ n'est pas dénombrable et S_1 est dénombrable, $T \cup S_0$ ne peut pas etre dénombrable, cela contredirait (b). Cela montre que $[0, 1[$ n'est pas dénombrable non plus. □

La figure 1.2 donne une description graphique du procédé de comptage utilisé dans la preuve du théorème 1.14(c) et du principe diagonal de la preuve du théorème 1.14(e).

1.5. Le principe d'inclusion et d'exclusion

Comment compter le nombre d'éléments dans une union d'ensembles finis ? Si les ensembles sont disjoints, la solution est facile : le nombre d'éléments de l'union est la somme du nombres d'éléments de chaque ensemble qui apparaît dans l'union. Dans cette section, on développe une technique pour compter le nombre d'éléments dans une union. On ne considérera ici que le cas de 2 ou 3 ensembles, laissant le cas général en exercice.

Commençons par une simple observation.

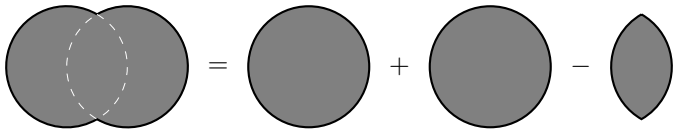


Figure 1.3 – Démonstration graphique de la proposition 1.16

Lemme 1.15. *Soient A et B des ensembles finis. Alors $|A \smallsetminus B| = |A| - |A \cap B|$.*

Démonstration. En utilisant la proposition 1.10(c) on sait que $A \leftrightarrow (A \smallsetminus B) \sqcup (A \cap B)$. Donc $|A| = |A \smallsetminus B| + |A \cap B|$ ce qui montre le résultat. □

Proposition 1.16. *Soient A et B des ensembles finis. Alors $|A \cup B| = |A| + |B| - |A \cap B|$.*

Démonstration. En utilisant la proposition 1.10(d) on a $A \cup B \leftrightarrow (A \smallsetminus B) \sqcup B$. Ainsi $|A \cup B| = |A \smallsetminus B| + |B|$ et le lemme 1.15 nous donne le résultat. □

Cette proposition est connue sous le nom de « principe d'inclusion et d'exclusion ». En voici la raison : on commence par estimer la taille de $A \cup B$ par $|A| + |B|$. Mais de cette manière on a compté les éléments de $A \cap B$ deux fois, donc on doit les exclure de la somme, c'est à dire soustraire $|A \cap B|$.

Que faire pour trois ensembles ?

Proposition 1.17. *Soient A, B et C des ensembles finis. Alors,*

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

Démonstration. D'après la proposition 1.16 et la proposition 1.4(5) on a

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap A \cap C| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap C|. \end{aligned}$$

□

Encore une fois, on peut voir pourquoi la méthode est connue comme principe d'inclusion et d'exclusion : On estime $|A \cup B \cup C|$ par $|A|+|B|+|C|$. Mais on a alors compté les éléments dans les intersections de deux ensembles deux fois, on doit donc les exclure. La nouvelle estimation est $|A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C|$. Mais maintenant on a soustrait les éléments communs aux trois ensembles une fois de trop, on doit donc les inclure à nouveau.

Exemple 1.18. Un sondage a été effectué sur les méthodes de transports pour se rendre à l'EPFL. Les personnes interrogées pouvait choisir « vélo », « Tsol » ou « voiture » et plusieurs réponses étaient possibles. La réponse « vélo » est apparue 30 fois, la réponse « Tsol » 100 fois, la réponse « voiture » 35 fois, les réponses « vélo » et « voiture » 15 fois ensemble, les réponses « Tsol » et « voiture » 15 fois ensemble, les réponses « vélo » et « Tsol » 20 fois ensemble et finalement seulement 5 personnes ont répondu les 3 moyens de transports. Combien de gens ont-ils été interrogés ?

Soient B, T et C les ensembles des questionnaires contenant respectivement les réponse « Vélo », « Tsol » et « voiture ». La solution du problème est alors $|B \cup T \cup C|$. D'après l'énoncé on sait que $|B| = 30, |T| = 100, |C| = 35, |C \cap B| = 15, |T \cap C| = 15, |B \cap T| = 20$ et $|T \cap C \cap B| = 5$. Donc

$$|B \cup T \cup C| = 30 + 100 + 35 - 15 - 15 - 20 + 5 = 120,$$

et la réponse est 120.

Chapitre 2

Relations

Les relations sont l'une des notions les plus fondamentales associées aux ensembles. Tout le monde a une compréhension intuitive d'une relation : par exemple, si A est l'ensemble de tous les êtres vivants, alors la relation C ($\ll$ être le fils de $\gg$) peut être définie sur les éléments de cet ensemble. On dit que deux êtres humains a et b dans A sont liés par cette relation si b est le fils de a, et l'on note $a \sim_C b$. Dans ce cas, l'ordre est important, ainsi $a \sim_C b$ et $b \sim_C a$ sont incompatible. Un autre exemple est donné par l'ensemble des entiers et la relation D (pour $\ll$ divisibilité $\gg$), où $a \sim_D b$ si b divise a.

Notre compréhension intuitive d'une relation est rendue formelle dans ce chapitre. De plus, on discutera des différents types de relations et de leurs représentations comme graphe orienté et matrice booléenne.

2.1. Relations

Définition 2.1. Une relation R entre les ensembles A et B est un sous ensemble de $A \times B$:

$$R \subseteq A \times B.$$

On dit que $a \in A$ et $b \in B$ sont liés par R, ce qui se note $a \sim_R b$, si $(a, b) \in R$. Le *domaine* $\mathrm{Dom}(R)$ est l'ensemble de tous les éléments de A qui sont en relation avec certains éléments de B :

$$\mathrm{Dom}(R) = \{a \in A \mid \exists b \in B \colon a \sim_R b\}.$$

L'*image* (ici *range* en anglais) $\mathrm{Ran}(R)$ est l'ensemble de tous les éléments de B qui sont en relation avec certains éléments de A :

$$\mathrm{Ran}(R) = \{b \in B \mid \exists a \in A \colon a \sim_R b\}.$$

Exemple 2.2.

1. Soient A l'ensemble des professeurs de l'EPFL et B l'ensemble des cours donnés à l'EPFL ce semestre. La relation $R = \{(a, b) \mid a \text{ enseigne le cours } b\}$ décrit le lien entre les cours et les professeurs. $\mathrm{Dom}(R)$ est l'ensemble de tous les professeurs qui donnent un cours ce semestre. L'image $\mathrm{Ran}(R)$ est égale à B.
2. Soient $A = \mathbb{Z}$ et $B = \{0, 1\}$. Soit l'ensemble $R \subseteq A \times B$ défini comme l'ensemble de tous les couples (a, b) tels que $b = 1$ si a est un nombre premier et 0 si a est composé d'exactement deux facteurs premiers distincts. Ainsi, par exemple, $(5, 1) \in R$, mais $(7, 0)$, $(6, 1)$ et $(30, 0)$ ne sont pas dans R. Alors $\mathrm{Dom}(R)$ est l'ensemble des entiers qui ont au plus 2 facteurs premiers et $\mathrm{Ran}(R)$ est $\{0, 1\}$.
3. Soient A l'ensemble de tous les entiers naturels et B l'ensemble de tous les sous-ensembles finis de A. La relation $R = \{(a, b) \in A \times B \mid a = \sum_{x \in b} x\}$ représente les partitions de a comme une somme d'entiers naturels distincts. Alors $\mathrm{Dom}(R) = A$, et $\mathrm{Ran}(R) = B$.

$\diamond$

Très souvent dans ce cours, nous considérerons des relations définies sur un seul ensemble.

Définition 2.3. Soit $R \subseteq A \times A$ une relation

(1) R est dite *symétrique* si $(a, b) \in R$ implique $(b, a) \in R$.

(2) R est dite *réflexive* si $(a, a) \in R$ pour tout $a \in A$.

(3) R est dite *transitive* si

$$\forall a, b, c \in A \colon (a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R.$$

(4) R est une *relation d'équivalence* si elle est symétrique, réflexive et transitive.

Exemple 2.4.

1. Supposons que A est l'ensemble de tous les humains. L'ensemble $R = \{(a, b) \in A \times A \mid a \text{ est marié à b}\}$ décrit la relation "être marié". Il s'agit d'une relation symétrique mais pas réflexive. Que signifie la transitivité pour cette relation ?
2. L'ensemble $\{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \leq b\}$ décrit la relation d'ordre usuelle sur $\mathbb{R}$. Elle n'est pas symétrique, mais elle est réflexive et transitive.
3. Formalisons la relation sur les entiers donnée par $\ll m$ divise $n \gg$. Pour cela, considérons, $A = B = \mathbb{Z}$, et $R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divise } n\}$. Cette relation n'est toujours pas symétrique, mais elle est réflexive et transitive.
4. Prenons encore $A = B = \mathbb{Z}$ l'ensemble des entiers et $m \in \mathbb{Z}$. La relation de $\ll$ congruence $\gg \equiv$ est définie par $R_m = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divise } a - b\}$. On écrit $a \equiv b \bmod m$ si $(a, b) \in R_m$. Cette fois, il s'agit d'une relation d'équivalence. En effet, $(a, a) \in R_m$, car m divise $a - a = 0$. Ensuite, si m divise $a - b$, il divise aussi $b - a$, et donc R_m est réflexive. Finalement, supposons que $(a, b) \in R_m$ et $(b, c) \in R_m$. Alors m divise $a - b$ et divise aussi $b - c$, il doit donc diviser la somme de ces nombres, c'est à dire $a - c$. On en déduit $(a, c) \in R_m$ et la transitivité de R_m.
5. Soit V un espace vectoriel sur un corps K, et soit U un sous-espace vectoriel de V. On peut définir une relation de congruence sur $V \times V$ par $R_U := \{(a, b) \in V \times V \mid a - b \in U\}$. On dit que $a \equiv b \bmod U$ si $(a, b) \in R_U$. Cette relation est aussi une relation d'équivalence. En effet, U est un sous-espace, il contient donc l'élément 0, et pour tout élément a, il contient aussi son opposé $-a$. Ainsi, $(a, a) \in R_U$, et si $(a, b) \in R_U$, alors on a aussi $(b, a) \in R_U$, ce qui montre que R_U est à la fois réflexive et symétrique. Si (a, b) et (b, c) sont dans R_U, alors $a - b$ et $b - c$ sont dans U. Comme U est un sous-espace, il contient $a - b$ et $b - c$ et leur somme, c'est à dire $a - c \in U$ et $(a, c) \in R_U$. Finalement U est bien transitive.
6. Soient $A = \mathbb{R}$, et $R = \{(a, b) \mid b^2 = a\}$. Alors R n'est ni symétrique, ni réflexive, ni transitive.
7. Soit A l'ensemble de tous les polynômes à une variable et à coefficients entiers. On définit la relation R sur A par $(a, b) \in R$ ssi $\deg(a) = \deg(b)$. C'est une relation d'équivalence (preuve laissée en exercice).

◇

Définition 2.5. Soit R une relation sur $A \times B$. Alors, pour tout $a \in A$, l'ensemble

$$[a] := \{b \in B \mid (a, b) \in R\}$$

est appelé la *classe* de a.

Exemple 2.6. Soit A l'ensemble {Lundi, Mardi, Mercredi, Jeudi, Vendredi} et B l'ensemble {Analyse, Mathématiques numériques, Théorie des probabilités, Mathématiques discrètes}. Considérons la table suivante :

	Lundi	Mardi	Mercredi	Jeudi	Vendredi
Analyse	×		×		
Mathématiques numériques		×		×	
Théorie des probabilités		×			×
Mathématiques discrètes				×	

Cette table définit deux relations, l'une, appelons la R, sur $A \times B$, et l'autre, appelons la R', sur $B \times A$. Ces relations sont définies de manière évidente : $(a, b) \in R$ ssi il y a une croix dans la case correspondante à l'intersection de la ligne correspondant à a et de la colonne correspondant à b. Ainsi, [Théorie de probabilité] $= \{$Mardi, Vendredi$\}$. De manière similaire, $(b, a) \in R'$ ssi $(a, b) \in R$. Ainsi, par exemple, [Mercredi] $= \{$Analyse$\}$. $\diamond$

Les classes d'une relation d'équivalence ont des propriétés intéressantes : Deux telles classes sont soit disjointes (c'est à dire d'intersection vide), soit égale. Ce résultat, qui est montré plus bas, n'est en général pas vrai pour les relations. Ainsi, dans l'exemple précédent, [Théorie des probabilité] et [Mathématiques numériques] ont une intersection non vide $\{$Mardi$\}$ et ne sont pas égale.

Exemple 2.7. Considérons la relation de congruence R_m définie dans l'exemple 2.4(4). Alors, pour tout $a \in \mathbb{Z}$, on a $[a] = \{a + mz \mid z \in \mathbb{Z}\}$. Si $a \equiv b \bmod m$, alors $a - b$ est divisible par m, disons $a - b = zm$, et donc $a = b + zm$, de telle manière que $a \in [b]$. Puisque $b = a - zm$, $b \in [a]$ et donc $[a] = [b]$. D'un autre côté, si $a \not\equiv b \bmod m$, alors $[a]$ et $[b]$ sont disjointes : sinon, si $x = a + zm = b + z'm$, alors $a - b = (z' - z)m$, et donc $a \equiv b \bmod m$, une contradiction. Il se trouve que les classes distinctes sont dans ce cas $[0], [1], \ldots, [m-1]$. $\diamond$

Pour prouver le résultat que nous venons de mentionner sur les relations d'équivalences nous avons besoin d'une définition :

Définition 2.8. Soit S un ensemble. Une *partition* de S est un sous-ensemble $\Pi \subseteq P(S)$ d'ensemble des parties de S telle que

(1) Pour tout $A \in \Pi$: $A \neq \emptyset$,

(2) Pour tout $A, B \in \Pi$, si $A \neq B$, alors $A \cap B = \emptyset$.

(3) $S = \cup_{A \in \Pi} A$.

Proposition 2.9. *Soit R une relation d'équivalence sur A.*

(1) *Si $a \sim_R b$, alors $[a] = [b]$.*

(2) *Si $a \not\sim_R b$, alors $[a] \cap [b] = \emptyset$.*

(3) *Les ensembles distincts parmi les classes $[a]$ pour $a \in A$ forment une partition de A.*

Démonstration. (1) Si $a \sim_R b$, alors $b \in [a]$, et par symétrie on a aussi $a \in [b]$. Si $x \in [a]$, alors $x \sim_R a$ et comme $a \sim_R b$, par transitivité, on a $x \sim_R b$. Finalement, $[a] \subseteq [b]$. Par symétrie l'autre inclusion se montre de manière similaire et $[a] = [b]$.

(2) Supposons que $a \not\sim_R b$ et qu'il existe $x \in [a] \cap [b]$. Alors $x \sim_R a$ et $x \sim_R b$. par symétrie, $a \sim_R x$, et par transitivité, $a \sim_R x$ et $x \sim_R b$ impliquent $a \sim_R b$, et donc $[a] = [b]$, ce qui est une contradiction.

(3) Soit $I \subseteq A$ tel que les classes $[a]$, $a \in I$ soient toutes distinctes et représentent toutes les classes de R. (I est appelé un ensemble de représentants de classe.) On prouve d'abord que $A = \cup_{a \in I}[a]$. Soit $x \in A$. Alors, comme $(x, x) \in R$ par symétrie, $x \in [x]$, ce qui montre l'assertion. Comme par (2) les classes $[a]$ et $[b]$ pour $a, b \in I$, $a \neq b$, sont disjointes, on voit que $\{[a] \mid a \in I\}$ forment une partition de A. $\square$

Définition 2.10. Soit R une relation d'équivalence sur un ensemble A. Alors tout sous-ensemble $I \subseteq A$ tel que les classes $[a]$, $a \in I$ forment une partition de A est appelé *un ensemble de représentants de classe* pour R.

Les relations d'équivalence sont les mêmes objets que les partitions comme le montre le théorème suivant.

Théorème 2.11. *Soit A un ensemble. Il y a une bijection entre les relations d'équivalence sur A et les partitions de A.*

Démonstration. Soient L l'ensemble de toutes les relations sur A, et P l'ensemble de toutes les partitions de A. Définissons l'application $f \colon L \to P$ par $f(R) = \{[a] \mid a \in I\}$, où I est un ensemble de représentants des classes de R. Si on peut trouver une application $g \colon P \to L$ telle que $g(f(R)) = R$ pour tout $R \in L$ et $f(g(\Pi)) = \Pi$ pour tout $\Pi \in P$, alors d'après l'exercice **??** on vient de montrer la bijectivité de f.

Soit $\Pi = \{A_1, \ldots, A_t\}$ une partition de A. On définit la relation $g(\Pi) = R_\Pi$ par

$$a \sim_{R_\Pi} b \iff \exists i \colon a \in A_i \wedge b \in A_i.$$

En d'autres mots, a est lié à b si tous deux sont dans le même ensemble de la partition. On affirme que R_Π est une relation d'équivalence. La symétrie et la réflexivité étant facile à voir on va se concentrer sur la transitivité. Supposons que $(a, b) \in R_\Pi$ et $(b, c) \in R_\Pi$. Alors il existe un i tel que $a, b \in A_i$ et il existe un j tel que $b, c \in A_j$.

Puisque $A_i \cap A_j = \emptyset$ pour $i \neq j$ (Cela découle de la définition d'une partition), on en déduit $i = j$, et donc $(a, c) \in R_\Pi$. On définit $g(\Pi) = R_\Pi$.

Remarquez que les classes de R_Π sont par définition précisément les ensembles A_i, et donc $f(g(\Pi)) = \Pi$. D'un autre côté, si R est une relation d'équivalence et que $\Pi = f(R)$ est l'ensemble des classe distinctes de R, alors $g(\Pi) = R$, ce dont on peut se convaincre après une courte réflexion. □

Si $R \subseteq A \times A$ est une relation sur l'ensemble A, alors l'ensemble des classes distinctes de R a un nom particulier.

Définition 2.12. Soient A un ensemble et $R \subseteq A \times A$ une relation d'équivalence sur A. Alors l'ensemble des classes de R est noté A/R et est appelé l'ensemble quotient de A par rapport à R.

Exemple 2.13. Soient $A = \mathbb{Z}$, n un entier non nul et R_m la relation de congruence définie dans l'example 2.4 (4). Alors $\mathbb{Z}/R_m$ est formé des m éléments $\{i + m\ell \mid m \in \mathbb{Z}\}$ pour $i = 0, 1, \ldots, m - 1$. L'ensemble $\mathbb{Z}/R_m$ et usuellement noté $\mathbb{Z}/m\mathbb{Z}$ dans la littérature.

2.2. Relations sur les ensembles finis

Supposons que A et B sont des ensembles fini et que $R \subseteq A \times B$ est une relation. Dans cette section on va voir plusieurs façons de représenter R.

La manière la plus simple pour représenter R est simplement de lister ses éléments.

Exemple 2.14. Soit $A = \{0, 1, 2\}$. On définit la relation R sur $A \times A$ telle que $a \sim_R b$ ssi $a + b \equiv 0 \bmod 3$. Alors $R = \{(0, 0), (1, 2), (2, 1)\}$. ◇

Une seconde manière de représenter $R \subseteq A \times B$ est à l'aide d'une matrice d'éléments de l'ensemble $\{0, 1\}$. On considère ainsi une matrice avec $|A|$ lignes et $|B|$ colonnes. Les lignes sont indexées par les éléments de A et les colonnes par ceux de B. Si $(a, b) \in R$, alors on met un 1 à la position indexée par la ligne a et la colonne b. On met sur toute les autres positions un 0.

Exemple 2.15. La matrice de la relation de l'exemple 2.6 est la suivante :

	Lundi	Mardi	Mercredi	Jeudi	Vendredi
Analyse	1	0	1	0	0
Mathématiques Numériques	0	1	0	1	0
Théorie des probabilités	0	1	0	0	1
Mathématiques discrètes	0	0	0	1	0

et la matrice de l'exercice précédent est

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

◇

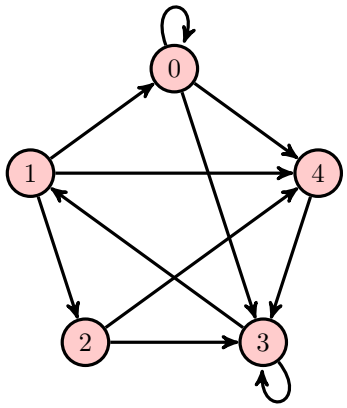
Une troisième façon de représenter une relation est à l'aide d'un graphe orienté.

Définition 2.16. Un *graphe orienté* est une paire $G = (V, E)$ où V est un ensemble fini et $E \subseteq V \times V$. L'ensemble V est appelé l'ensemble des *sommets* de G, et E est appelé l'ensemble des *arêtes* de G. Si E est symétrique, c'est-à-dire que pour tout $a, b \in V$ on a $(a, b) \in E \iff (b, a) \in E$, alors G est appelé un graphe *non-orienté* ou simplement un graphe.

Il est clair qu'une relation sur un ensemble fini est la même chose qu'un graphe orienté et qu'une relation symétrique correspond à un graphe non-orienté. Un des avantages de travailler avec les graphes est que l'on peut les dessiner. Pour cela, on dessine pour chaque élément de l'ensemble de base un *nœud* dans le plan étiqueté par cet élément. Puis, on dessine une arête depuis un nœud d'étiquette a vers un nœud d'étiquette b si $a \sim_R b$.

Exemple 2.17. Soient $A = \{0, 1, 2, 3, 4\}$ et R une relation dont la matrice est donnée sur la partie gauche de la figure ci-dessous. Le graphe orienté correspondant est donné sur la partie droite.

	0	1	2	3	4
0	1	0	0	1	1
1	1	0	1	0	1
2	0	0	0	1	1
3	0	1	0	1	0
4	0	0	0	1	0

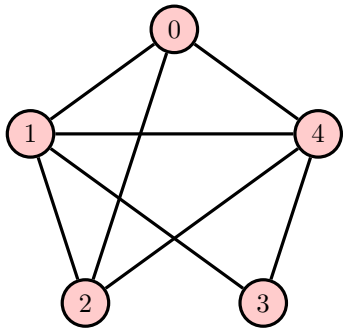


◇

Si une relation est symétrique, alors on omet les flèches sur les arêtes.

Exemple 2.18. Soient $A = \{0, 1, 2, 3, 4\}$ et R une relation dont la matrice est donnée sur la partie gauche de la figure ci-dessous. Le graphe correspondant est donné sur la partie droite.

	0	1	2	3	4
0	0	1	1	0	1
1	1	0	1	1	1
2	1	1	0	0	1
3	0	1	0	0	1
4	1	1	1	1	0

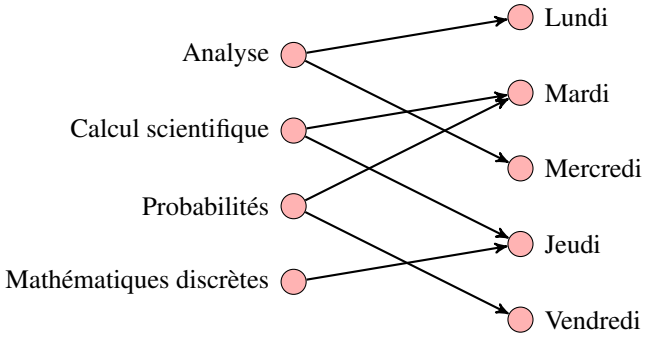


◇

Les relations entre ensembles différents peuvent être aussi représentées par des graphes.

Définition 2.19. Un *graphe biparti* $G = (A \sqcup B, E)$ est un graphe dans lequel l'ensemble des sommets est une union disjointe de deux ensembles A et B, et tel que l'ensemble des arêtes E est un sous-ensemble de $A \times B$. Si E est symétrique, c'est à dire si $(a, b) \in E \iff (b, a) \in E$, alors G est appelé un *graphe biparti non-orienté* ou simplement un graphe biparti.

Exemple 2.20. Le graphe biparti correspondant à la relation de l'exercice 2.14 est donné ci-dessous.



◇

2.3. Opérations sur les relations

La première opération que nous considérons est celle de composition.

Définition 2.21. Soient $R \subseteq A \times B$ et $S \subseteq B \times C$ des relations. La composition $S \circ R$ de R et S est définie comme la relation de $A \times C$ qui vérifie

$$S \circ R := \{(a, c) \mid \exists b \in B \colon (a, b) \in R \wedge (b, c) \in S\}.$$

Voici un exemple.

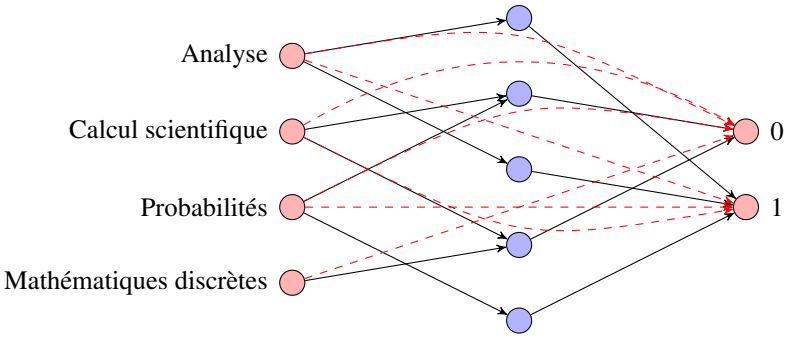
Exemple 2.22. Soient R la relation de l'exemple 2.6 et S la relation sur $B \times C$ où C est l'ensemble $\{0, 1\}$ et la relation est définie par

$$S = \{(\text{Lundi}, 1), (\text{Mardi}, 0), (\text{Mercredi}, 1), (\text{Jeudi}, 0), (\text{Vendredi}, 1)\}.$$

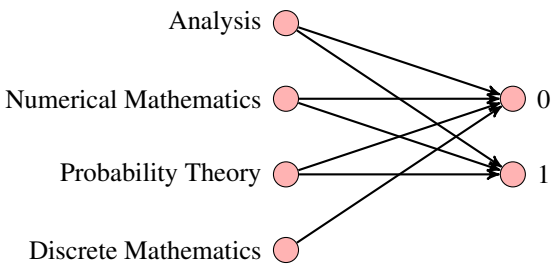
Alors $S \circ R$ est donné sous forme matricielle par

	0	1
Analyse	0	1
Mathématique numériques	1	0
Théorie des probabilités	1	1
Mathématiques discrètes	1	0

La composition de ces deux relations (et en général de n'importe quelle relations) peut être facilement visualisée en terme de graphe biparti. Dans un premier temps, on concatène les deux graphes bipartis de chacune des relations en identifiant les nœuds qui correspondent aux éléments de B. On connecte ensuite les nœuds de A aux nœuds de C pour lequel il y a un chemin entre ces deux sommets passant par un sommet de B :



Cela nous donne à la fin le graphe biparti suivant pour $S \circ R$:



◇

Pour une relation sur un seul ensemble, la notion de composition est légèrement plus simple.

Définition 2.23. Soit $R \subseteq A \times A$ une relation.

– Un chemin de longueur m de la relation R est un ensemble d'éléments $c_0, \ldots, c_m$ tels que $c_0 \sim_R c_1 \sim_R c_2 \sim_R \cdots \sim_R c_m$. On dit qu'il s'agit d'un chemin entre c_0 et c_m.

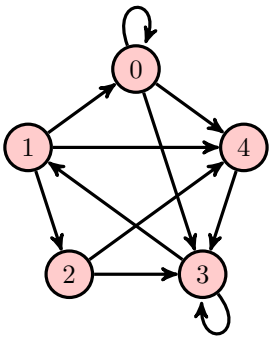
– On définit R^m comme $\underbrace{R \circ R \circ \cdots \circ R}_{m \text{ fois}}$.

La preuve de la remarque suivante est triviale.

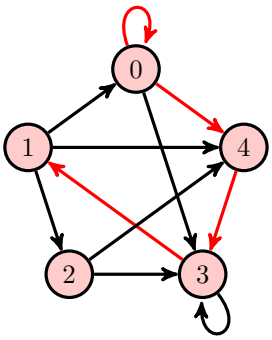
Remarque 2.24. *Soit $R \subseteq A \times A$ une relation et G le graphe orienté correspondant. Alors $(a, b) \in R^m$ ssi il y a un chemin de longueur m entre a et b dans G.*

Exemple 2.25.

(1) Supposons que R est une relation dont le graphe orienté est donné sur la partie gauche de la figure suivante. Alors un chemin de longueur 4 de cette relation est donné sur la partie droite.

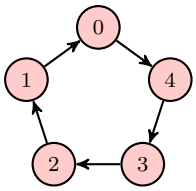


R

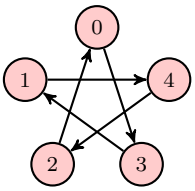


un chemin de longueur 4 dans R

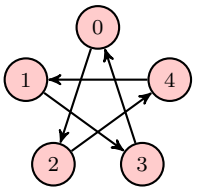
(2) Supposons que R est une relation sur $\{0, 1, 2, 3, 4\}$ donnée par $R = \{(1, 0), (0, 4), (4, 3), (3, 2), (2, 1)\}$. Le graphe orienté pour cette relation et ses puissances $R^2, \ldots, R^5$ est donné ci-dessous :



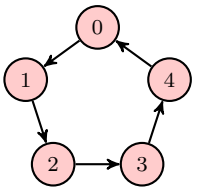
R



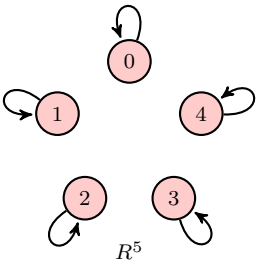
R^2



R^3



R^4



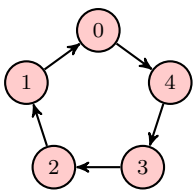
R^5

◇

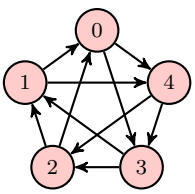
Définition 2.26. Soit $R \subseteq A \times A$ Une relation. La *fermeture transitive* de R, notée $\overline{R}$, est définie par

$$\overline{R} := \bigcup_{i=1}^{\infty} R^i.$$

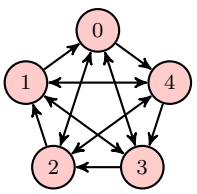
Exemple 2.27. Soit R la relation de l'exemple 2.25 (2). On a alors le résultat suivant :



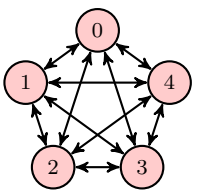
R



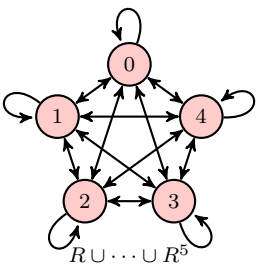
$R \cup R^2$



$R \cup R^2 \cup R^3$



$R \cup \cdots \cup R^4$



$R \cup \cdots \cup R^5$

◇

L'exemple précédent est une illustration typique de ce qui se passe pour les relations sur un ensemble *fini* : La suite $R, R \cup R^2, R \cup R^2 \cup R^3, \ldots$ se stabilise toujours, comme le montre la proposition suivante :

Proposition 2.28. *Si A est un ensemble fini et R est une relation sur A, alors il existe un certain m tel que $\overline{R} = R \cup \ldots \cup R^m$.*

Démonstration. Soient $|A| = n$ et $a, b \in A$. On va montrer que s'il existe un chemin de longueur m entre a et b dans R, alors il existe un chemin de longueur au plus n dans R entre a et b. Cela montre que $\overline{R} = \bigcup_{i=1}^{n} R^i$.

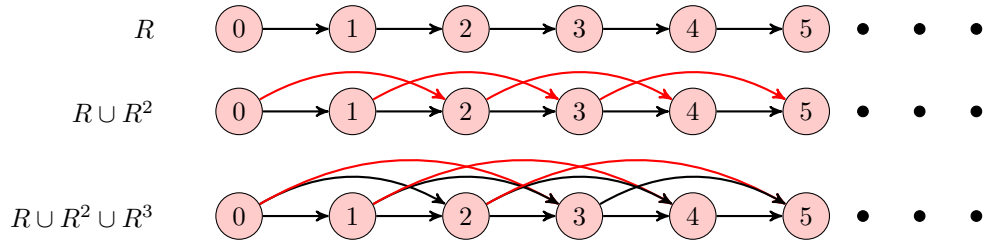
Pour cela, soit $a =: c_0 \sim_R c_1 \sim_R \cdots \sim_R c_{m-1} \sim_R b =: c_m$ un chemin de longueur m entre a et b. Supposons de plus que ce chemin est de longueur minimale. Si $m \geq n+1$, alors, il existe deux indices différents, notons les i et j, tels que $c_i = c_j$, $i < j$, et $(i, j) \neq (0, m)$. En effet, il y a dans ce cas plus de n éléments de A entre $c_0, \ldots, c_{m-1}$ qui participent au chemin et donc tous les éléments du chemin ne peuvent être distincts (principe des tiroirs ou du pigeonnier). On en deduit que il y a $i < j < m$ telle que $c_i = c_j$.

En enlevant les éléments $c_{i+1}, \ldots, c_j$ du chemin, on obtient maintenant un nouveau chemin de a vers b :

$$c_0 \sim_R \cdots \sim_R c_i \sim_R c_{j+1} \sim_R \cdots c_m.$$

Ce chemin est de longueur plus courte que l'original ce qui contredit l'hypothèse de la minimalité de la longueur. Finalement, on en déduit que la longueur d'un chemin minimal est d'au plus n ce qui termine la démonstration. □

Exemple 2.29. L'assertion de la proposition 2.28 n'est pas vraie pour les ensembles infinis. Par exemple, regardons la relation R sur $\mathbb{N}_0$ définie par $R = \{(a, a+1) \mid a \in \mathbb{N}_0\}$. Alors, $R^2 = \{(a, a+2) \mid a \in \mathbb{N}_0\}$, et de manière générale, $R^m = \{(a, a+m) \mid a \in \mathbb{N}_0\}$. Les graphes dirigés correspondant aux relations $R, R \cup R^2$ et $R \cup R^2 \cup R^3$ sont donnés ci-dessous.

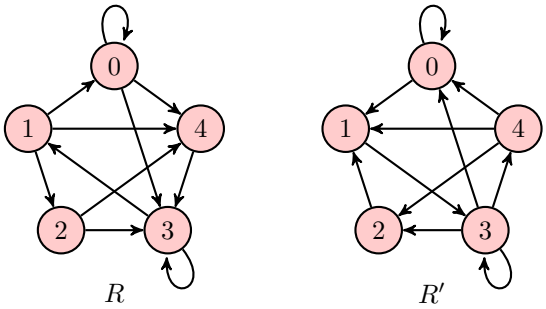


D'un autre côté, $\overline{R} = \{(a, b) \mid a, b \in \mathbb{N}_0 \wedge a < b\}$, et il n'existe pas de m tel que $\overline{R} = \bigcup_{i=1}^{m} R^i$. ◇

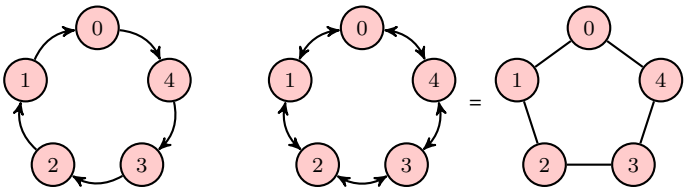
Définition 2.30. Soit $R \subseteq A \times A$ une relation.
- La relation $R' := \{(b, a) \mid (a, b) \in R\}$ est appelée la relation *inverse* de R.
- La relation $\mathrm{Sym}(R) := R \cup R'$ est appelé la relation *symétrisée* de R.

Exemple 2.31.

(1) Supposons que R est une relation sur $\{0, 1, 2, 3, 4\}$ donnée par le graphe de gauche sur le dessin suivant. Le graphe orienté de la relation inverse est donné sur la droite :



(2) Supposons que R est une relation sur $\{0, 1, 2, 3, 4\}$ donnée par $R = \{(1, 0), (0, 4), (4, 3), (3, 2), (2, 1)\}$. La relation R et sa symétrisée sont données ci-dessous :



R $\quad$ $\mathrm{Sym}(R)$

◇

Chapitre 3
Relations d'ordre

Nous allons discuter dans ce chapitre d'un type particulier de relation, les *relations d'ordre*. De telles relations apparaissent dans des domaines variés des mathématiques. Elles ont également un grand nombre de propriétés combinatoires très intéressantes que nous allons voir.

3.1. Ensemble partiellement ordonné (poset)

Définition 3.1. Soient A un ensemble et R une relation sur cet ensemble.

1. R est appelée *une relation d'ordre* ou un *ordre partiel* si les conditions suivantes sont vérifiées
   (a) Pour tout $a \in A$ on a $(a, a) \in R$ (réflexivité).
   (b) Pour tout $a, b \in A$ si $(a, b) \in R$ et $(b, a) \in R$ alors $a = b$ (antisymétrie).
   (c) pour tout $a, b, c \in A$ si $(a, b), (b, c) \in R$, alors $(a, c) \in R$ (transitivité).
2. R est appelé un *ordre total* si c'est un ordre partiel et si pour tous $a, b \in A$ tels que $a \neq b$, soit $(a, b) \in R$, soit $(b, a) \in R$.
3. Si R est un ordre partiel sur A, alors on appelle la paire $\mathcal{P} = (A, R)$ un *ensemble partiellement ordonné* ou un *poset* et on dit que A est un ensemble partiellement ordonné par rapport à R. Si R est un ordre total, alors on appelle $\mathcal{P}$ un *ensemble totalement ordonné* et on dit que A est totalement ordonné par rapport à R.
4. Si $\mathcal{P} = (A, R)$ est un poset, on écrit $a \leq_{\mathcal{P}} b$ pour $(a, b) \in R$, et on écrit $a <_{\mathcal{P}} b$ si $a \leq_{\mathcal{P}} b$ et $a \neq b$. De plus, on écrit $a \in \mathcal{P}$ si $a \in A$.
5. Si a et b sont des éléments d'un poset $\mathcal{P}$ et $a \not\leq_{\mathcal{P}} b$ et $b \not\leq_{\mathcal{P}} a$, alors a et b sont dits *incomparables* ; sinon, il sont dits *comparables*.

Il y a de nombreux exemples d'ensembles partiellement ordonnés que vous connaissez déjà. En voici une petite liste :

Exemple 3.2.
1. L'ensemble $\mathbb{Z}$ muni de l'ordre naturel est totalement ordonné.
2. L'ensemble $\mathbb{N}$ est partiellement ordonné par la relation de divisibilité. On note ce poset par $(\mathbb{N}, |)$.
3. L'ensemble $\mathbb{Z}$ n'est pas partiellement ordonné par rapport à la divisibilité. Soit a un élément non nul. Alors a divise $-a$, et $-a$ divise a. Mais a n'est pas égal à $-a$, et donc la propriété d'antisymétrie n'est pas valide.
4. Si T est un ensemble, l'ensemble de ses parties $P(T)$ est partiellement ordonné par l'inclusion. On note ce poset $(P(T), \subseteq)$.
5. Supposons que A soit un ensemble totalement ordonné par la relation $\leq$, et supposons que n est un entier positif. Alors l'ensemble A^n est totalement ordonné par la relation $\leq_{\text{lex}}$ définie ci-dessous :

$$(a_1, \ldots, a_n) <_{\text{lex}} (b_1, \ldots, b_n) \iff \exists\, i \in [1, n] : \quad a_1 = b_1, b_2 = a_2, \ldots, a_{i-1} = b_{i-1}, a_i < b_i.$$

Cet ordre est appelée l'ordre *lexicographique*.

6. Soit A l'ensemble totalement ordonné de l'exemple précédent. Alors A^n est partiellement ordonné par l'ordre suivant :
$$(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n) \iff \forall i \geq 1 : \quad a_i \leq b_i.$$

◇

Les posets peuvent être représentés par un certain type de graphe.

Définition 3.3. Un cycle dans un graphe $G = (V, E)$ est un chemin qui commence et se termine sur le même sommet. Un graphe $G = (V, E)$ est appelé *un graphe orienté acyclique* ou simplement un *DAG* si G est un graphe orienté qui n'a pas de cycle.

Il se trouve que les DAGs sont essentiellement équivalents aux posets, comme le montre la proposition suivante :

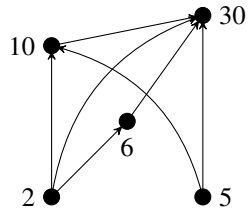
Proposition 3.4. *Soit R un ordre partiel sur un ensemble A. Alors, le graphe de R est l'union d'un DAG clos par transitivité et du graphe $G' = (A, E')$ où $E' = \{(a, a) \mid a \in A\}$. Réciproquement, l'union d'un DAG transitivement clos $G = (V, E)$ et de l'ensemble $\Delta := \{(v, v) \mid v \in V\}$ est un poset.*

Démonstration. Le graphe de R est l'union du graphe $D = (A, E)$ et $G' = (A, E')$, où $E = \{(a, b) \mid (a, b) \in R \wedge a \neq b\}$. On doit montrer que D est un DAG transitivement clos. Pour cela, supposons qu'il existe un cycle $a_0 \sim_R a_1 \sim_R \cdots \sim_R a_m \sim_R a_0$ dans D. Alors la condition d'antisymétrie de R implique que $a_0 = a_1 = \cdots = a_m$, ce qui est une contradiction. Cela nous montre que D ne contient pas de cycles. La cloture de $D \cup G'$ par transitivité découle de la transitivité de R.

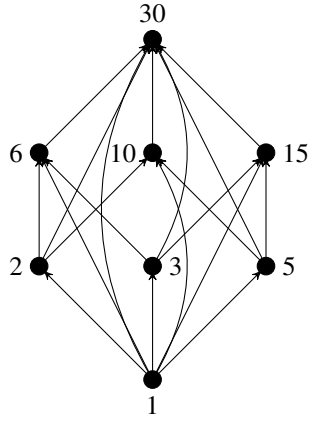
Réciproquement, supposons que $G = (V, E)$ est un DAG transitivement clos et que P est l'union de G et de Δ. On doit montrer que cette union est le graphe d'un ordre partiel. La réflexivité de la relation est claire car le graphe contient Δ. La relation est antisymétrique, car sinon il existerait $v, w \in V$, $v \neq w$, tels que $(v, w) \in V$ et $(w, v) \in V$. Mais cela impliquerait la présence d'un cycle $v \to w \to v$ dans G, une contradiction. Finalement, la transitivité de la relation est équivalente à l'hypothèse que G est transitivement clos. □

Quand on dessine un diagramme d'un poset, on omet usuellement la réflexivité et donc on ne dessine pas des boucles sur tous les sommets du graphe. L'exemple suivant illustre cela.

Exemple 3.5. (1) Soient $A = \{2, 5, 6, 10, 30\}$ et R la relation de divisibilité sur A. son DAG est donné ci-dessous :



(2) Soient $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ et R la relation de divisibilité sur A. La représentation par DAG de ce poset est donné ci-dessous :



(3) En général, soit n un entier positif. On note $(\mathrm{Div}(n), |)$ le poset dont les éléments sont tous les diviseurs de n, et la relation est celle de divisibilité. La partie (2) de cet exemple est le DAG de $(\mathrm{Div}(30), |)$.

◇

Le lecteur s'est peut-être déjà aperçu que la représentation par un DAG d'un poset contient un grand nombre de redondance. Par exemple, dans le DAG de la première partie de l'exemple précédent, l'arête de 2 à 30 est redondante puisqu'il y a déjà une arête de 6 à 30 et une entre 2 et 6. L'arête entre 2 et 30 est implicite. La définition suivante rend cela plus précis :

Définition 3.6. Soit $\mathcal{P}$ un poset.

1. Pour $a, b \in \mathcal{P}$ tel que $a \leq_{\mathcal{P}} b$ on appelle b un *successeur* de a et a un *prédécesseur* de b.
2. Un élément de $a \in \mathcal{P}$ est dit *minimal* s'il n'a aucun prédécesseur. Un élément de $b \in \mathcal{P}$ est dit *maximal* s'il n'a aucun successeur.
3. Un *prédécesseur immédiat* de $a \in \mathcal{P}$ est un élément $b \in \mathcal{P}$ tel que $b \leq_{\mathcal{P}} a$ et tel qu'il n'existe pas de $c \neq b$ distinct de a tel que $b \leq_{\mathcal{P}} c \leq_{\mathcal{P}} a$.

Exemple 3.7. (1) Dans l'exemple 3.5 (1), les éléments 2 et 5 n'ont pas de prédécesseur, ils sont donc minimaux. L'élément 30 n'a pas de successeur, il s'agit donc d'un élément maximal. Les éléments 6 et 10 sont des prédécesseurs immédiats de l'élément 30.

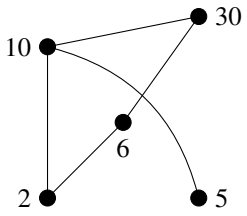
(2) Dans l'exemple 3.5 (2), le poset a exactement un élément minimal 1 et exactement un élément maximal 30.

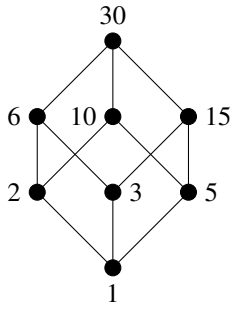
◇

Les prédécesseurs immédiats n'existent pas dans tous les posets. Par exemple, aucun des éléments du poset $\mathcal{P} = (\mathbb{R}, \leq)$ formé des nombres réels muni de l'ordre naturel n'admet de prédécesseur immédiat.

Les prédécesseurs immédiats existent de manière évidente pour les posets finis. Pour de tel posets, il y a une représentation très pratique qui utilise les *diagrammes de Hasse*. Comme pour la représentation par DAG, on dessine les éléments du poset comme les sommets d'un graphe, mais on ne connecte l'élément a à l'élément b que si a est un prédécesseur immédiat de b. On oublie également l'orientation des arêtes ; à la place, si $a \leq_{\mathcal{P}} b$, alors on dessine le sommet correspondant à a sous le sommet correspondant à b. Le diagramme final est alors équivalent à tout le poset.

Exemple 3.8. Les diagrammes de Hasse des posets des exemples 3.5 (1) et (2) sont donnés ci-dessous :





◇

Précisons à présent le sens de certaines notions que vous avez déjà dû utiliser par ailleurs.

Définition 3.9. Soient $\mathcal{P} = (A, \leq)$ un poset et $C \subseteq A$ une partie de A.

1. On appelle *minorant* de C tout élément m de A tel que pour tout $c \in C$, $m \leq_{\mathcal{P}} c$.
2. On appelle *majorant* de C tout élément M de A tel que pour tout $c \in C$, $c \leq_{\mathcal{P}} M$.
3. On dit d'un élément x de C qu'il est *minimal* dans C s'il n'a pas de prédécesseur dans C, i.e. si pour tout $c \in C$, $c \leq x$ implique $c = x$.
4. On dit d'un élément y de C qu'il est *maximal* dans C s'il n'a pas de successeur dans C, i.e. si pour tout $c \in C$, $c \geq x$ implique $c = x$.
5. On appelle *plus petit élément* ou *minimum* de C tout élément m de C tel que pour tout $c \in C$, $m \leq_{\mathcal{P}} c$.

6. On appelle *plus grand élément* ou *maximum* de C tout élément M de C tel que pour tout $c \in C$, $c \leq_{\mathcal{P}} M$.
7. On appelle *borne inférieure* ou *infimum* de C le plus grand des minorants.
8. On appelle *borne supérieure* ou *supremum* de C le plus petit des majorants.

Remarque 3.10. *Lorsqu'ils existent, le minimum, le maximum, la borne inférieure et la borne supérieure sont uniques. Par contre, un ensemble peut contenir plusieurs éléments minimaux et plusieurs éléments maximaux distincts. Lorsqu'il existe, le minimum de C est aussi un minorant de C et la borne inférieure de C ; de même, lorsqu'il existe, le maximum de C est aussi un majorant de C et la borne supérieure de C.*

3.2. Chaînes et lemme de Zorn

Définition 3.11. Soit $\mathcal{P}$ un poset. Une *chaîne* de $\mathcal{P}$ est un sous-ensemble qui est totalement ordonné par $\leq_{\mathcal{P}}$. Un élément $x \in \mathcal{P}$ est appelé un *majorant* pour une chaîne C si pour tout $a \in C$ on a $a \leq_{\mathcal{P}} x$.

Le lemme de Zorn, donné ci-dessous, garantit l'existence d'éléments maximaux et minimaux d'un poset qui a certaines propriétés. Malgré son nom de « lemme », il s'agit en fait d'un axiome qui est équivalent à l'axiome de bon ordre et à l'axiome du choix (axiomes dont on ne discutera pas ici).

Théorème 3.12 (Lemme de Zorn)**.** *Un poset pour lequel chaque chaîne admet un majorant contient au moins un élément maximal. De manière équivalente, un poset pour lequel chaque chaîne admet un minorant contient au moins un élément minimal.*

Le lemme de Zorn est un outil puissant pour prouver un bon nombre d'assertions que nous considérons usuellement comme données. Par exemple, on montre que tout espace vectoriel admet une base.

Exemple 3.13. Soit K un corps (par exemple $\mathbb{R}$) et soit V un espace vectoriel sur K. Un ensemble $S \subset V$ est dit *linéairement indépendant* si pour tout nombre $n \in \mathbb{N}$, tous $a_1, \ldots, a_n \in K$ non tous nuls et tous $s_1, \ldots, s_n \in S$ distincts deux à deux, on a $\sum_{i=1}^{n} a_i s_i \neq 0$. Une *base* de V est un sous-ensemble B linéairement indépendant tel que

$$V = \left\{ a \;\middle|\; \exists n \in \mathbb{N}, a_1, \ldots, a_n \in K, b_1, \ldots, b_n \in B : \quad a = \sum_{i=1}^{n} a_i b_i \right\}.$$

Soit L un sous-ensemble indépendant de V (par exemple $\emptyset$). L'ensemble de tous les sous-ensembles indépendants de V contenant L est un poset G par rapport à l'inclusion. (C'est un sous-poset de $(P(V), \subseteq)$.) Supposons que C est une chaîne dans G. Soit alors $T = \cup_{c \in C} c$. Notez que T est un majorant de C (c'est clair) et que $T \in G$ (pourquoi ?). Ainsi, en utilisant le lemme de Zorn, le poset G admet au moins un élément maximal B. Par définition, B est linéairement indépendant. On affirme, qu'il s'agit également d'un ensemble de générateurs pour V et donc d'une base. Supposons le contraire et supposons que W est l'espace vectoriel généré par B. Soit alors x un élément de $V \setminus W$. Par maximalité de B, l'ensemble $B \cup \{x\}$ n'est pas linéairement indépendant, donc il existe $n \in \mathbb{N}$, $b_1, \ldots, b_n \in B$ et $a_1, \ldots, a_n, a \in K$ non tous nuls tels que

$$a_1 b_1 + \cdots + a_n b_n + ax = 0.$$

Clairement, $a \neq 0$ car les b_i sont linéairement indépendants. Ainsi, x est une combinaison linéaire des b_i et appartient à W, une contradiction.

3.3. Treillis

Définition 3.14. Soient $\mathcal{P}$ un poset et a, b des éléments de $\mathcal{P}$.

1. Une *borne supérieure* ou *plus petit majorant* ou encore *supremum* de a et b, notée $a \vee b$ est un élément c tel que $a \leq_{\mathcal{P}} c$ et $b \leq_{\mathcal{P}} c$ et tel que si d est un autre élément de $\mathcal{P}$ qui vérifie $a \leq_{\mathcal{P}} d$ et $b \leq_{\mathcal{P}} d$, alors $c \leq_{\mathcal{P}} d$.
2. Une *borne inférieure* ou *plus grand minorant* ou *infimum* de a et b, notée $a \wedge b$ est un élément c tel que $c \leq_{\mathcal{P}} a$ et $c \leq_{\mathcal{P}} b$ et tel que si d est un autre élément de $\mathcal{P}$ qui vérifie $d \leq_{\mathcal{P}} a$ et $d \leq_{\mathcal{P}} b$, alors $d \leq_{\mathcal{P}} c$.
3. Un *Treillis* est un poset pour lequel chaque paire d'éléments admet un infimum et un supremum.

La preuve de la remarque suivante est laissé au lecteur.

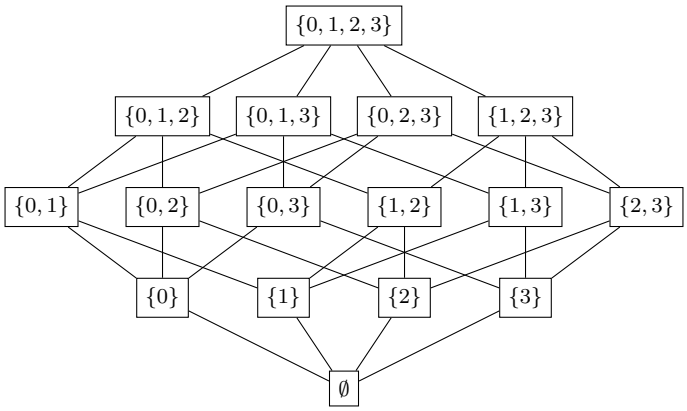


Figure 3.1 – Diagramme de Hasse de $\mathcal{B}_4$.

Remarque 3.15. *Soit $\mathfrak{L}$ un treillis. Alors la borne supérieure et la borne inférieure de n'importe quelle paire d'éléments est unique.*

Un treillis n'a pas nécessairement un élément maximal ou minimal, mais si c'est le cas alors ces éléments sont uniques :

Proposition 3.16. *Soit $\mathfrak{L}$ un treillis. Alors $\mathfrak{L}$ a au plus un élément minimal et un élément maximal.*

Démonstration. Supposons que $\mathfrak{L}$ a deux éléments minimaux a et b. Il s'ensuit que si $c \in \mathfrak{L}$ est tel que $c \leq_{\mathfrak{L}} a$ alors $c = a$, il en est de même pour b. Soit alors $c = a \wedge b$ la borne inférieure de a et b. Par définition $c \leq_{\mathfrak{L}} a$ et $c \leq_{\mathfrak{L}} b$, ce qui implique $c = a = b$.

La preuve pour l'unicité d'un élément maximal est analogue. □

Exemple 3.17. (1) Considérons l'ensemble totalement ordonné $\mathbb{R}$ avec l'ordre naturel. Alors $\mathbb{R}$ est un treillis. La borne inférieure de a et b est $\min(a, b)$, et la borne supérieure de a et b est $\max(a, b)$. Néanmoins $\mathbb{R}$ n'admet ni d'élément maximal, ni d'élément minimal.

(2) Considérons le poset $(\mathbb{N}, |)$. Il n'est pas totalement ordonné mais c'est un treillis : La borne inférieure de a et b est $\text{pgcd}(a, b)$, et la borne supérieure de a et b est $\text{ppcm}(a, b)$. Ce treillis possède un unique élément minimal 1, mais n'admet pas d'élément maximal.

(3) Soit le poset $(\mathbb{N}_0, |)$. C'est un treillis et il admet un unique élément maximal, 0. Même si ce treillis a un élément maximal, il contient des chaînes de longueur arbitraire.

(4) Considérons maintenant le poset $(\text{Div}(n), |)$ introduit dans l'exemple 3.5 (3). C'est aussi un treillis avec $a \wedge b = \text{pgcd}(a, b)$ et $a \vee b = \text{ppcm}(a, b)$. Il admet un unique élément minimal 1, et un unique élément maximal n. Le diagramme de droite de l'exemple 3.8 est le diagramme de Hasse de $(\text{Div}(30), |)$.

(5) Le treillis $(P(\underline{n}), \subseteq)$ est appelé le *treillis booléen d'ordre n*, et est usuellement noté $\mathcal{B}_n$. Il admet un unique élément maximal, $\underline{n}$, et un unique élément minimal, $\emptyset$. La figure 3.1 montre le diagramme de Hasse de $\mathcal{B}_4$. ◇

3.4. La fonction de Möbius

Soit $\mathfrak{L}$ un treillis fini et soit g une fonction $\mathfrak{L} \to \mathbb{R}$. On définit la fonction $f \colon \mathfrak{L} \to \mathbb{R}$ par

$$\forall a \in \mathfrak{L} \colon \quad f(a) := \sum_{\mathfrak{L} \ni b \leq_{\mathfrak{L}} a} g(b).$$

Le but de cette section est de trouver une expression pour g en terme de f.

Définition 3.18. Soit $\mathfrak{L}$ un treillis fini. La *fonction de Möbius bivariée* sur $\mathfrak{L}$ est la fonction $\mu_{\mathfrak{L}} \colon \mathfrak{L} \times \mathfrak{L} \to \mathbb{Z}$ caractérisée par les propriétés suivantes :

1. Si $a \not\leq_{\mathcal{L}} b$ alors $\mu_{\mathcal{L}}(a,b) = 0$.
2. Pour tout $a, b \in \mathcal{L}$ avec $a \leq_{\mathcal{L}} b$ on a

$$\sum_{a \leq_{\mathcal{L}} x \leq_{\mathcal{L}} b} \mu_{\mathcal{L}}(x,b) = \begin{cases} 1 & \text{si } a = b \\ 0 & \text{sinon.} \end{cases}$$

On note que cette propriété implique $\mu_{\mathcal{L}}(a,a) = 1$ pour $a \in \mathcal{L}$.

Si $\mathcal{L}$ admet un élément minimal t (et c'est toujours le cas pour un treillis fini), alors la *fonction de Möbius univariée*, noté encore $\mu_{\mathcal{L}}$ est définie par $\mu_{\mathcal{L}}(a) := \mu_{\mathcal{L}}(t,a)$, pour tout $a \in \mathcal{L}$.

Commençons par voir pourquoi les propriétés définies plus haut définissent de façon unique la fonction de Möbius.

Proposition 3.19. *La fonction de Möbius d'un treillis fini $\mathcal{L}$ est définie de manière unique par les propriétés de la définition précédente.*

Démonstration. Supposons qu'il existe deux telles fonctions de Möbius μ_1 et μ_2, et que $a, b \in \mathcal{L}$ sont tels que $\mu_1(a,b) \neq \mu_2(a,b)$. Soit S l'ensemble de tous les $x \leq_{\mathcal{L}} b$ tels que $\mu_1(x,b) \neq \mu_2(x,b)$. S est un poset, il est fini, non vide ($a \in S$) et admet donc un élément maximal. Appelons le c. Notez que $c <_{\mathcal{L}} b$ puisque $\mu_1(b,b) = \mu_2(b,b) = 1$. On sait par définition de μ que pour $i = 1, 2$

$$\mu_i(c,b) = -\sum_{c <_{\mathcal{L}} x \leq_{\mathcal{L}} b} \mu_i(x,b).$$

Le terme de droite de cette équation est le même pour les deux valeurs de i, car c est un élément maximal de S. Ainsi, le terme de gauche doit être le même aussi, une contradiction. □

On peut maintenant énoncé le théorème principal de cette partie :

Théorème 3.20 (Inversion de Möbius sur les treillis)**.** *Soient $\mathcal{L}$ un treillis fini et $g, f : \mathcal{L} \to \mathbb{R}$ des fonctions telles que pour tout $a \in \mathcal{L}$ on a $f(a) = \sum_{b \leq_{\mathcal{L}} a} g(b)$. Alors pour tout $a \in \mathcal{L}$:*

$$g(a) = \sum_{b \leq_{\mathcal{L}} a} \mu_{\mathcal{L}}(b,a) f(b).$$

Dans une maniere similaire, si $f(a) = \sum_{a \leq_{\mathcal{L}} b} g(b)$ pour chaque $a \in \mathcal{L}$, alors pour tout $a \in \mathcal{L}$:

$$g(a) = \sum_{a \leq_{\mathcal{L}} b} \mu_{\mathcal{L}}(a,b) f(b).$$

Démonstration. On a

$$\begin{aligned} \sum_{b \leq_{\mathcal{L}} a} \mu_{\mathcal{L}}(b,a) f(b) &= \sum_{b \leq_{\mathcal{L}} a} \mu_{\mathcal{L}}(b,a) \sum_{c \leq_{\mathcal{L}} b} g(c) \\ &= \sum_{c \leq_{\mathcal{L}} a} \left(\sum_{\substack{b \\ c \leq_{\mathcal{L}} b \leq_{\mathcal{L}} a}} \mu_{\mathcal{L}}(b,a) \right) g(c) \\ &= g(a), \end{aligned}$$

ce qui prouve le théorème. La démonstration de la deuxieme forme est similaire. □

Des fois, il est utile de considérer une description « duale » de la fonction de Möbius. La définition plus haut utilise que la somme de tous les $\mu_{\mathcal{L}}(x,b)$ entre a et b de $\mathcal{L}$ vaut 0. Dans la formulation duale, on montre que la somme de tous les $\mu_{\mathcal{L}}(a,x)$ pour x entre a et b vaut également 0.

Proposition 3.21. *Supposons que $\mathcal{L}$ est un treillis fini avec comme fonction de Möbius $\mu_{\mathcal{L}}$. Soient a et b des éléments de $\mathcal{L}$ avec $a \leq_{\mathcal{L}} b$. On a alors*

$$\sum_{a \leq_{\mathcal{L}} x \leq_{\mathcal{L}} b} \mu_{\mathcal{L}}(a,x) = \begin{cases} 1 & \textit{si } a = b \\ 0 & \textit{sinon.} \end{cases}$$

De plus, si une fonction $\mu_{\mathcal{L}}$ satisfait cette condition et vérifie de plus $\mu_{\mathcal{L}}(a,b) = 0$ pour tout $a, b \in \mathcal{L}$ telle que $a \not\leq_{\mathcal{L}} b$, alors $\mu_{\mathcal{L}}$ est la fonction de Möbius de $\mathcal{L}$.

Démonstration. (Idée.) Considérons une matrice M dont les lignes et les colonnes sont indexées par les éléments de $\mathcal{L}$, et telle que $M_{a,b} = \mu_{\mathcal{L}}(a,b)$. De plus, considérons la matrice Z dont les lignes et les colonnes sont aussi indexées par $\mathcal{L}$, et telle que $Z_{a,b}$ est à 1 si $a \leq_{\mathcal{L}} b$, et est à 0 sinon. (Ainsi, Z est la matrice des relations du treillis sous-jacent.) On laisse en exercice la preuve que l'énoncé de l'inversion de Möbius est équivalent à dire que ZM est la matrice identité. C'est-à-dire que M est l'inverse de Z, mais alors MZ est aussi la matrice identité. Le coefficient (a,b) de ce produit est nul si $a \neq b$ et vaut 1 si $a = b$. Ce coefficient égale

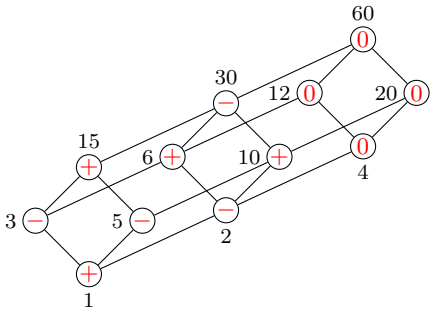
$$\sum_{x \in \mathcal{L}} M_{a,x} Z_{x,b} = \sum_{x \leq_{\mathcal{L}} b} \mu_{\mathcal{L}}(a,x) = \sum_{a \leq_{\mathcal{L}} x \leq_{\mathcal{L}} b} \mu_{\mathcal{L}}(a,x).$$

Ce qui termine (l'idée de) la preuve. □

L'existence de la fonction de Möbius sur tout treillis fini peut être facilement obtenue par récurrence en utilisant cette forme duale. Pour calculer $\mu_{\mathcal{L}}(a,b)$, on commence par $\mu_{\mathcal{L}}(a,a) = 1$. Ensuite, si on connaît tout les $\mu_{\mathcal{L}}(a,c)$ pour $a \leq_{\mathcal{L}} c <_{\mathcal{L}} b$, on définit $\mu_{\mathcal{L}}(a,b)$ par $-\sum_{a \leq_{\mathcal{L}} c <_{\mathcal{L}} b} \mu_{\mathcal{L}}(a,c)$.

Exemple 3.22. Soit $\mathcal{L}$ le treillis $(\mathrm{Div}(60), |)$. Dans cet exemple on va calculer la valeur de $\mu_{\mathcal{L}}(1,x)$ pour plusieurs éléments x dans ce treillis et pour cela on va utiliser la proposition précédente. Premièrement il est clair que $\mu_{\mathcal{L}}(1,1) = 1$. Ensuite, supposons que x est un nombre premier (Dans ce cas, soit 2, 3, ou 5). Alors en utilisant la proposition 3.21 On a $0 = \sum_{y|x} \mu_{\mathcal{L}}(1,y) = \mu_{\mathcal{L}}(1,1) + \mu_{\mathcal{L}}(1,x)$, et donc $\mu_{\mathcal{L}}(1,x) = -1$. Ensuite, on calcule $\mu_{\mathcal{L}}(1,4)$: on a $0 = \mu_{\mathcal{L}}(1,1) + \mu_{\mathcal{L}}(1,2) + \mu_{\mathcal{L}}(1,4)$, et donc $\mu_{\mathcal{L}}(1,4) = 0$.

Le dessin suivant montre le diagramme de Hasse de ce treillis et les valeurs de $\mu_{\mathcal{L}}(1,x)$ Pour tous les éléments du treillis :



Ici, « + » veut dire 1, et « − » veut dire -1. ◇

De manière similaire, on peut calculer la valeur de la fonction de Möbius sur nos deux treillis favoris :

Théorème 3.23. (1) *Soit $\mathcal{L}$ le treillis $(Div(n), |)$. Alors on a pour des nombres naturels a, b avec $a \mid b \mid n$:*

$$\mu(a,b) = \begin{cases} (-1)^t & \text{si } b/a \text{ est le produit de } t \text{ nombres premiers distincts,} \\ 0 & \text{sinon.} \end{cases}$$

(2) *Soient S un ensemble fini et $\mathcal{L}$ le treillis $(P(S), \subseteq)$. Alors on a pour des sous-ensembles $X \subseteq Y \subseteq S$:*

$$\mu_{\mathcal{L}}(X,Y) = (-1)^{|Y \setminus X|}.$$

Démonstration. (1)

Pour prouver le théorème, on utilise l'unicité de la fonction de Möbius (cf proposition 3.19). Il nous suffit donc de montrer que la fonction donnée dans l'énoncé satisfait les deux propriétés de la définition 3.21. La première est trivialement vérifiée donc on se concentre sur la deuxième. On doit donc montrer que

$$\sum_{\substack{d \\ a \mid d \mid b}} \mu_{\mathcal{L}}(d,b) = \begin{cases} 1 & \text{si } a = b, \\ 0 & \text{sinon.} \end{cases}$$

Les nombres d tels que $a \mid d \mid b$ sont en bijection avec les diviseurs δ de b/a en écrivant $a\delta = d$. Il faut donc montrer que pour $m \in \mathbb{N}$ (qui correspond à b/a) on a

$$\sum_{\delta \mid m} \mu_{\mathcal{L}}(1,\delta) = 0\,.$$

Pour cela, supposons que $m = \prod_{i=1}^{t} p_i^{e_i}$ où les p_i sont des nombres premiers et $e_i \geq 1$ pour tout i. Ainsi tout $\delta \mid m$ est de la forme $\prod_{i=1}^{t} p_i^{\varepsilon_i}$, avec $0 \leq \varepsilon_i \leq e_i$. En utilisant la formule du théorème, $\mu_{\mathcal{L}}(1, \delta) = 0$ s'il existe un $\varepsilon_i > 1$. On doit donc monter que

$$\sum_{0 \leq \varepsilon_1 \leq 1, \ldots, 0 \leq \varepsilon_t \leq 1} \mu_{\mathcal{L}} \left(1, \prod_{i=1}^{t} p_i^{\varepsilon_i} \right) = 0 \, .$$

En utilisant encore une fois la définiton de μ du théorème, on voit que dans cette somme, $\mu_{\mathcal{L}}(1, \prod_{i=1}^{t} p_i^{\varepsilon_i}) = (-1)^s$ où s est le nombre de ε_i non nuls. L'ensemble des vecteurs $(\varepsilon_1, \ldots, \varepsilon_t)$ qui ont s composantes non nulles est de cardinal $\binom{t}{s}$. On en déduit

$$\sum_{0 \leq \varepsilon_1 \leq 1, \ldots, 0 \leq \varepsilon_t \leq 1} \mu_{\mathcal{L}} \left(1, \prod_{i=1}^{t} p_i^{\varepsilon_i} \right) = \sum_{s=0}^{t} \binom{t}{s} (-1)^s = (1-1)^t = \begin{cases} 1 & \text{si } t = 0, \\ 0 & \text{sinon,} \end{cases}$$

et on a terminé.

(2) On raisonne par récurrence sur $n = |Y \setminus X|$. On commence avec $n = 0$, ce qui est trivial. Supposons maintenant que $|Y \setminus X| = n + 1$, et que l'assertion est vraie pour tous les couples Y, Z avec $|Y \setminus Z| \leq n$. On utilise maintenant le fait que

$$\sum_{X \subseteq Z \subseteq Y} \mu_{\mathcal{L}}(Z, Y) = 0.$$

Mais

$$\begin{aligned} \sum_{X \subseteq Z \subseteq Y} \mu_{\mathcal{L}}(Z, Y) &= \mu_{\mathcal{L}}(X, Y) + \sum_{X \subset Z \subseteq Y} \mu_{\mathcal{L}}(Z, Y) \\ &= \mu_{\mathcal{L}}(X, Y) + \sum_{i=1}^{n+1} \binom{n+1}{i} (-1)^{n+1-i}. \end{aligned}$$

Pour voir cela, supposons que $Y \setminus X = \{b_1, \ldots, b_{n+1}\}$. Alors tous les ensembles possibles Z sont obtenus comme $Z = X \cup T$ où T est un sous-ensemble non-vide de $Y - X$. Le nombre de tels sous-ensembles à i éléments est $\binom{n+1}{i}$, et si Z est un tel sous-ensemble, on a $\mu_{\mathcal{L}}(Z, Y) = (-1)^{n+1-i}$ par hypothèse de récurrence.

En continuant avec la dernière expression, notez que

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

ainsi $\mu_{\mathcal{L}}(X, Y) = (-1)^{n+1}$, et le résultat en découle. □

Définition 3.24. Comme la fonction de Möbius sur le treillis $(\mathrm{Div}(n), |)$ ne dépend que du quotient de ses arguments et en particulier ne dépend pas de n, on définit la fonction de Möbius à une variable (c'est la fonction originale) μ de $\mathbb{N}$ dans $\{-1, 0, 1\}$ par

$$\mu(x) := \begin{cases} (-1)^t & \text{si } x \text{ est le produit de } t \text{ nombres premiers distincts,} \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, $\mu(x) = \mu_{\mathcal{L}}(1, x)$ où $\mu_{\mathcal{L}}$ est la fonction de Möbius de $(\mathrm{Div}(n), |)$, pour un n multiple de x.

La preuve de la remarque suivante est laissé en exercice.

Remarque 3.25. *La fonction de Möbius μ est* faiblement multiplicative *: si n et m sont des entiers tels que $pgcd(n, m) = 1$, alors $\mu(nm) = \mu(n)\mu(m)$.*

Corollaire 3.26 (Inversion de Möbius originelle)**.** *Soient $f, g \colon \mathbb{N} \to \mathbb{R}$ des fonctions telles que pour tout $n \in \mathbb{N}$ on a $g(n) = \sum_{d \mid n} f(d)$. Alors on a pour tout $n \in \mathbb{N}$:*

$$f(n) = \sum_{d \mid n} \mu \left(\frac{n}{d} \right) g(d).$$

Démonstration. Soit $\mu_{\mathcal{L}}$ la fonction de Möbius du treillis $(\mathrm{Div}(n), |)$. On a $f(n) = \sum_{d \mid n} \mu_{\mathcal{L}}(d, n) g(d)$. Notez que $\mu_{\mathcal{L}}(d, n) = \mu_{\mathcal{L}}(1, n/d) = \mu(n/d)$. □

3.5. Exemple : la fonction φ d'Euler

On donne dans cette section une application de la formule d'inversion de Möbius. Pour un entier $n \in \mathbb{N}$ on note $\varphi(n)$ le nombre d'entiers d, $1 \leq d \leq n$, tels que $\text{pgcd}(d, n) = 1$. Cette fonction est appelé la *fonction d'Euler*. Par exemple, $\varphi(10) = 4$, car les seuls entiers plus petits que 10 qui sont premiers avec 10 sont $1, 3, 7, 9$.

On commence par montrer que

$$n = \sum_{d|n} \varphi(d). \tag{3.1}$$

Pour cela, on définit pour chaque diviseur d de n l'ensemble $F_d := \{x \mid 0 \leq x < n, \text{pgcd}(x, n) = d\}$. Il est clair que les ensembles F_d sont disjoints. De plus l'ensemble $\{0, 1, \ldots, n-1\}$ est égal à l'union des F_d : si x est un élément de l'ensemble précédent, alors $x \in F_d$ avec $d = \text{pgcd}(x, n)$. On en déduit que $n = \sum_{d|n} |F_d|$. On montre maintenant que $|F_d| = \varphi(n/d)$. Pour cela, remarquez que $x \in F_d$ ssi $\gcd(x/d, n/d) = 1$. Ce qui prouve (3.1).

En appliquant la formule d'inversion de Möbius du corollaire 3.26 a (3.1), on voit que

$$\varphi(n) = \sum_{d|n} \mu(n/d)d.$$

De cette formule, on peut facilement en déduire les faits suivants :

1. si n est un nombre premier, alors $\varphi(n) = n - 1$: Dans ce cas les seuls diviseur sont n et 1, et comme $\mu(n) = -1$, le résultat en découle.
2. Si $n = p^t$ pour un nombre premier p, alors $\varphi(n) = (p-1)p^{t-1}$: dans ce cas les diviseurs de n sont $1, p, \ldots, p^t$, et $\mu(n/d) \neq 0$ seulement si $d = p^{t-1}$ ou $d = p^t$; dans le premier cas $\mu(n/d) = -1$, est dans le second cas c'est 1.
3. Si $n = PQ$ où $\text{pgcd}(P, Q) = 1$, alors $\varphi(n) = \varphi(P)\varphi(Q)$: dans ce cas, tout diviseur d de n peut s'écrire de manière unique comme $d = d_1 d_2$ avec d_1 un diviseur de P et d_2 un diviseur de Q (preuve ?). Ainsi

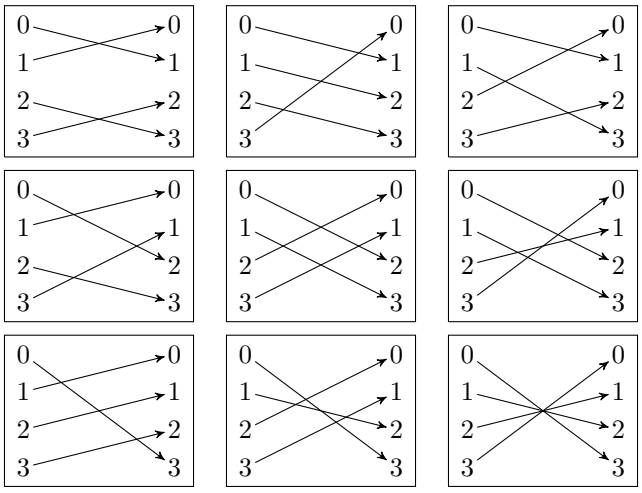
$$\varphi(n) = \sum_{d_1|P, d_2|Q} \mu\left(\frac{PQ}{d_1 d_2}\right) d_1 d_2.$$

Comme P/d_1 et Q/d_2 sont premiers entre eux et que μ est une fonction faiblement multiplicative d'après la remarque 3.25, la dernière expression est égale à

$$\left(\sum_{d_1|P} \mu\left(\frac{P}{d_1}\right) d_1\right)\left(\sum_{d_2|Q} \mu\left(\frac{Q}{d_2}\right) d_2\right) = \varphi(P)\varphi(Q).$$

3.6. Exemple : nombre de dérangements

Un *dérangement* sur $\underline{n}$ est une application bijective de $\underline{n}$ sur lui-même qui ne fixe aucun élément de $\underline{n}$. Par exemple les applications suivantes sont toutes des dérangements de $\underline{4}$:



Dans cette section, on va calculer le nombre de dérangements de $\underline{n}$ en utilisant la formule d'inversion de Möbius sur $\mathcal{B}_n$. Soit S un sous-ensemble de $\underline{n}$, et soit $p_n(S)$ le nombre de bijections qui fixent tous les éléments de S et aucun des éléments hors de S. De plus, soit $q_n(S)$ le nombre d'applications qui fixent tous les éléments de S sans contrainte sur les éléments hors de S. Clairement, $q_n(S) = (n - |S|)!$, puisqu'une application fixant les éléments de S est une permutation quelconque hors de S. De plus, on a

$$q_n(S) = \sum_{S \subseteq T} p_n(T),$$

car les applications fixant S peuvent être partitionnées en celles fixant T et ne fixant aucun élément hors de T, pour tout T contenant S. Par application de la deuxieme forme de formule d'inversion de Möbius, on obtient

$$\begin{aligned} p_n(S) &= \sum_{S \subseteq T} \mu_{\mathcal{B}_n}(S,T) q_n(T) \\ &= \sum_{S \subseteq T} (-1)^{|T \setminus S|} (n - |T|)! \qquad \text{(par le théorème 3.23 (2))} \\ &= \sum_{\ell=|S|}^{n} (-1)^{\ell - |S|} \binom{n-|S|}{\ell-|S|} (n-\ell)!. \end{aligned}$$

La dernière étape est obtenue en choisissant $\ell := |T|$ et en remarquant que le nombre d'ensemble contenant S est $\binom{n-|S|}{\ell-|S|}$. On est intéressé dans la valeur de cette expression pour $S = \emptyset$, puisque dans ce cas $p_n(\emptyset)$ nous donne le nombre de dérangements. On obtient

$$p_n(\emptyset) = n! \left(\frac{1}{2!} - \frac{1}{3!} \pm \cdots + (-1)^n \frac{1}{n!} \right).$$

Avec $\mathrm{e} \simeq 2.7182818\cdots$ qui est le nombre d'Euler on a encore selon la parité de n

$$p_n(\emptyset) = \left\lceil \frac{n!}{\mathrm{e}} \right\rceil \text{ si } n \text{ est pair} \qquad p_n(\emptyset) = \left\lfloor \frac{n!}{\mathrm{e}} \right\rfloor \text{ si } n \text{ est impair,}$$

parce que $\sum_{k=0}^{\infty} \frac{(-1)^k}{k!}$ est une série alternée qui converge vers e^{-1}. Comme la série est alternée, son terme de reste $\sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}$ est compris entre 0 et $\frac{1}{(n+1)!}$ quand n est impair et $\frac{1}{(n+1)!}$ et 0 quand n est pair. Comme l'intervalle $[0, \frac{1}{n+1}]$ est de longueur inférieure à 1 et $p_n(\emptyset)$ est entier, on peut se contenter d'arrondir $\frac{n!}{\mathrm{e}}$ vers le bas, respectivement vers le haut, pour retrouver sa valeur quand n est impair, respectivement quand n est pair. En particulier, quand $n = 4$, on obtient

$$p_4(\emptyset) = \frac{4!}{2!} - \frac{4!}{3!} + \frac{4!}{4!} = 12 - 4 + 1 = 9.$$

3.7. Décomposition en chaînes, antichaînes et largeur

Définition 3.27. Soit $\mathcal{P}$ un poset. Une *antichaîne* de $\mathcal{P}$ est une suite $c_1, c_2, \ldots, c_m$ d'éléments de $\mathcal{P}$ telle que pour tout i, j, $i \neq j$, c_i et c_j ne sont pas comparables dans $\mathcal{P}$. La *largeur* d'un poset fini $\mathcal{P}$ est la longueur maximale d'une antichaîne de $\mathcal{P}$.

Exemple 3.28.

1. Considérons le poset $(\underline{10}, |)$. (Notez que $\underline{n}$ n'est pas egal à $(\mathrm{Div}(10), |)$. Les suites $(1,2,4,8)$, $(3,6)$, $(5,10)$, (7), et (9) forment des chaînes disjointes de ce poset. L'ensemble $\{5,6,7,8,9\}$ est une antichaîne de ce poset.
2. Considérons le treillis $\mathcal{B}_4$. Voici une liste des chaînes disjointes de ce poset :

$$\begin{gathered} (\emptyset, \{0\}, \{0,1\}, \{0,1,2\}, \{0,1,2,3\}) \\ (\{1\}, \{1,2\}, \{1,2,3\}) \\ (\{2\}, \{2,3\}, \{0,2,3\}) \\ (\{3\}, \{1,3\}, \{0,1,3\}) \\ (\{0,2\}) \\ (\{0,3\}). \end{gathered}$$

L'ensemble suivant est une antichaîne :

$$\{\{0,1\},\{0,2\},\{0,3\},\{1,2\},\{1,3\},\{2,3\}\}.$$

◇

Soit $\mathcal{P}$ un poset. Un ensemble $\{C_1,\dots,C_m\}$ de chaînes disjointes de $\mathcal{P}$ tel que $\mathcal{P} = \cup_{i=1}^{m} C_i$ est appelé *une décomposition en chaînes* de $\mathcal{P}$. Une *décomposition minimale en chaînes* de $\mathcal{P}$ est une décomposition pour laquelle le nombre de chaîne est minimal.

Lemme 3.29. *Soit $\mathcal{P}$ un poset.*

(1) *Alors le cardinal de la décomposition minimale en chaînes de $\mathcal{P}$ est au moins égal à la largeur de $\mathcal{P}$.*

(2) *Si w est la largeur de $\mathcal{P}$, $C_1,\dots,C_w$ est une décomposition en chaînes de $\mathcal{P}$, et A est une antichaîne qui comporte w éléments, alors $|A \cap C_i| = 1$ pour tout $i = 1,\dots,w$.*

Démonstration. (1) Soient A une antichaîne de $\mathcal{P}$, et $C_1,\dots,C_t$ des chaînes disjointes couvrant $\mathcal{P}$. Alors pour tout i on a $|A \cap C_i| \leq 1$. Sinon, s'il existe $x, y \in A \cap C_i$ avec $x \neq y$, x et y sont comparables et donc ne peuvent appartenir tous deux à A, une contradiction. Comme les C_i sont disjoints, on a $|A| = \sum_{i=1}^{t} |A \cap C_i|$ et ce dernier nombre est au plus t.

(2) Si $t = w$, alors $w = |A| = \sum_{i=1}^{w} |A \cap C_i| \leq w$, et nous avons une égalité des deux côtés. De plus, $|A \cap C_i| = 1$ pour tout i. □

En fait, le théorème de Dilworth montre que le cardinal d'une décomposition minimale en chaînes et la largeur d'un poset sont les mêmes. La preuve, donnée ci-dessous, construit une décomposition en chaînes du poset et une antichaîne qui sont toutes deux de même taille. En utilisant le lemme précédent, il est alors possible de conclure à l'égalité de la largeur du poset avec le cardinal d'une décomposition minimale en chaînes.

Théorème 3.30 (Théorème de Dilworth)**.** *Soit $\mathcal{P}$ un poset fini. La largeur de $\mathcal{P}$ est égale au cardinal d'une décomposition minimale en chaînes de $\mathcal{P}$.*

Démonstration. La preuve utilise un raisonnement par récurrence sur les éléments du poset $\mathcal{P}$. Si le nombre d'éléments est 1, l'assertion est triviale.

Supposons maintenant que l'assertion soit vraie pour tout poset de n éléments. On aimerait montrer qu'elle est également satisfaite par un poset à $n+1$ éléments. Pour cela, soit $\mathcal{P}$ un poset à $n+1$ éléments. Soit y un élément maximal de $\mathcal{P}$, et considérons le poset $\mathcal{P}' := \mathcal{P} \setminus \{y\}$ avec n éléments. Par hypothèse de récurrence, le cardinal d'une décomposition minimale en chaînes et la largeur de $\mathcal{P}'$ sont les mêmes, disons w.

Soient $C_1,\dots,C_w$ des chaînes disjointes couvrant $\mathcal{P}'$. On va construire une antichaîne A de $\mathcal{P}'$ avec w éléments de la manière suivante : pour tout i, on choisit dans C_i un élément maximal x_i qui appartient à une antichaîne de longueur w.

Commençons par nous convaincre que les x_i sont deux à deux incomparables. Supposons que i et j sont deux à deux différents et que $x_i \geq x_j$. Soit B une antichaîne de longueur w qui contient x_i. D'après le lemme 3.29 (2) on a $B \cap C_j = \{y_j\}$ pour un certain y_j. On a $y_j \leq x_j$, car y_j appartient à une antichaîne de longueur w, et que x_j est un élément maximal par rapport à cette condition. Comme y_j est dans l'antichaîne B, x_i et y_j ne sont pas comparable, on ne peut donc avoir $x_i \geq x_j$. Comme i et j ont été choisis arbitrairement, on vient de montrer que pour tous i et j les éléments x_i et x_j ne sont pas comparables donc que A est une antichaîne.

On va maintenant utiliser A pour construire une antichaîne et une décomposition en chaînes de $\mathcal{P}$ de la même taille, ce qui terminera le raisonnement par récurrence. On va distinguer 2 cas.

(1) Supposons d'abord que $y \geq x_i$ pour un certain i. Dans ce cas, on va trouver une décomposition en chaînes de $\mathcal{P}$ avec w éléments et une antichaîne de $\mathcal{P}$ avec w éléments. Le lemme 3.29 (1) nous montre alors que le cardinal d'une décomposition minimale de $\mathcal{P}$ est le même que sa largeur. Soit $C := \{y\} \cup \{z \in C_i \mid z \leq x_i\}$. C est une chaîne. Considérons le poset $\mathcal{P}'' := \mathcal{P} - C$.

On va montrer que $\mathcal{P}''$ n'a pas d'antichaîne de longueur w. Supposons d'abord que x_i est l'élément maximal de C_i. Alors, enlever C de $\mathcal{P}$ est la même chose qu'enlever C_i de $\mathcal{P}'$, de telle manière que $\mathcal{P}''$ admet une décomposition en $w-1$ chaînes, ce qui implique que la largeur de $\mathcal{P}''$ ne peut dépasser $w-1$. Ensuite, supposons que x_i n'est pas l'élément maximal de C_i. Alors, les autres éléments de C_i qui sont plus grand que x_i ne peuvent être dans une antichaîne de longueur w par définition de x_i. Il s'ensuit que la largeur de $\mathcal{P}''$ est d'au plus $w-1$.

On en déduit que $\mathcal{P}''$ peut être couvert par au plus $w-1$ chaînes disjointes et que donc $\mathcal{P}$ peut être couvert par au plus w chaînes disjointes (celles de $\mathcal{P}''$ et C), ainsi la largeur de $\mathcal{P}$ est d'au plus w. Comme A est une antichaîne de $\mathcal{P}$ de taille w, on vient de montrer qu'il y a une décomposition en chaînes de $\mathcal{P}$ de la même taille qu'une antichaîne, ce qui prouve le théorème.

(2) Supposons maintenant que $y \not\geq x_i$ pour tout i. Comme y est un élément maximal de $\mathcal{P}$, y est incomparable avec tous les x_i, et donc $A' := \{y, x_1, \ldots, x_w\}$ est une antichaîne. D'un autre côté, $\{y\}, C_1, \ldots, C_w$ est une décomposition en chaînes de $\mathcal{P}$ de taille $w+1 = |A'|$, on en déduit donc que dans ce cas également le cardinal d'une décomposition minimale en chaînes de $\mathcal{P}$ est le même que sa largeur.

En regroupant ces deux cas, la preuve est terminée. □

Théorème 3.31 (Théorème de Sperner)**.** *La largeur de $\mathcal{B}_n$ est $\binom{n}{\lfloor n/2 \rfloor}$.*

Démonstration. Premièrement, remarquez que l'ensemble de tous les ensembles de taille $\lfloor n/2 \rfloor$ forme une antichaîne de $\underline{n}$. Il reste donc à prouver qu'il n'existe pas d'antichaîne qui a plus d'éléments. Soit $A = \{S_1, \ldots, S_w\}$ une antichaîne maximale de $\mathcal{B}_n$. Une chaîne maximale de $\mathcal{B}_n$ est une chaîne qu'on ne peut augmenter. Remarquez que $\mathcal{B}_n$ a $n!$ chaînes maximales, une pour chaque permutation de $\underline{n}$. Chacune de ces chaînes intersecte l'ensemble A en au plus un élément. (Sinon A contiendrait au moins deux éléments comparables ce qui n'est pas possible.) Si la taille de S_i est n_i, alors le nombre de chaînes maximales contenant S_i est $n_i!(n-n_i)!$ ce qui correspond au nombre de toutes les permutations de $\underline{n}$ qui laissent l'ensemble S_i invariant. On a alors

$$\sum_{i=1}^{w} n_i!(n-n_i)! \leq n!,$$

car on a à gauche le nombre de chaînes maximales qui contiennent un des éléments de A, et on a à droite le nombre de toutes les chaînes maximales. En divisant les deux côtés par $n!$, on obtient l'inégalité LYM

$$\sum_{i=1}^{w} \frac{1}{\binom{n}{n_i}} \leq 1.$$

Remarquez que $\binom{n}{n_i} \leq \binom{n}{\lfloor n/2 \rfloor}$, et donc

$$w\frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \leq \sum_{i=1}^{w} \frac{1}{\binom{n}{n_i}} \leq 1.$$

On en déduit

$$w \leq \binom{n}{\lfloor n/2 \rfloor},$$

ce qui prouve le théorème. □

Chapitre 4

Théorie élémentaire des graphes

4.1. Les sept ponts de Königsberg

Au $18^{\text{ème}}$ siècle, la ville de Königsberg en Prusse (maintenant Kaliningrad en Russie) qui se situe sur la rivière Pregel (Pregolya en Russe), contenait deux îles qui étaient connectées entre elles et aux berges par sept ponts comme indiqué sur la figure 1 : A et B correspondent aux îles alors que C et D correspondent aux deux berges. Un problème fut posé dont la solution échappait aux mathématiciens de l'époque : est-il possible de trouver un chemin dans la ville qui passe par chacun de ces sept ponts exactement une fois ? Malgré de nombreux essais, aucune solution de ce problème n'a pu être trouvée. Serait-il possible qu'il n'y ait pas de solution et si oui, comment quelqu'un pourrait-il le prouver ? Il est facile de convaincre quelqu'un de l'existence d'une solution juste en la lui donnant. Mais comment convaincre des mathématiciens qu'une solution n'existe pas ?

Le mathématicien Suisse Léonard Euler fut parmi ceux qui s'intéressèrent au problème et trouva une méthode ingénieuse pour prouver qu'il n'y avait pas de solutions. De plus, la preuve qu'il publia en 1735 à l'académie de St.Petersbourg marque la naissance d'un domaine important des mathématiques, celui de la théorie des graphes et de la topologie.

Une des clefs de la preuve d'Euler est l'abstraction du problème : la taille des îles n'est pas importante ; ce qui est important c'est comment elles sont reliées entres elles et aux berges. Dans la terminologie d'aujourd'hui, Euler a introduit le concept de graphe avec des arêtes multiples.

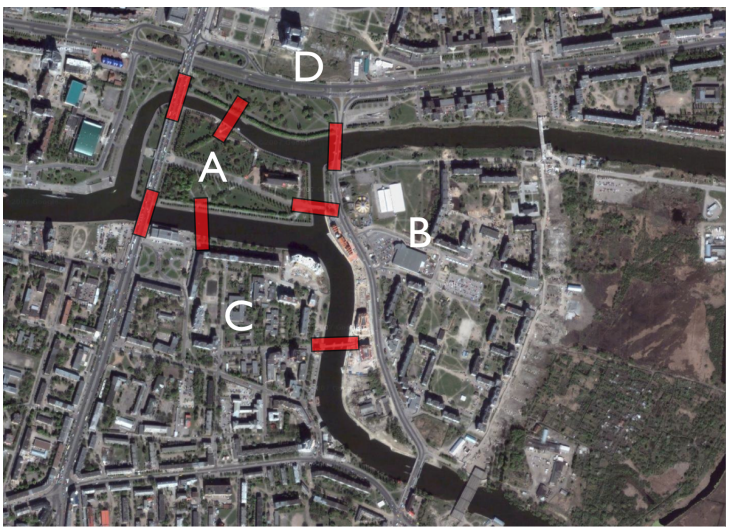
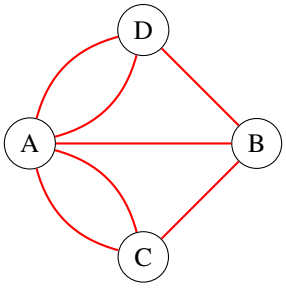


Figure 4.1 – Photographie satellite de la ville de Kaliningrad en Russie, autrefois Königsberg en Prusse. Les ponts sont dessinés en rouge. Notez que deux de ces ponts n'existent plus aujourd'hui et que parmi les 5 autres, seulement deux ont survécu depuis 1736. (image extraite de Google maps.)

Définition 4.1. Un *multigraphe* est un graphe $G = (V, E)$ avec une application $E \to \mathbb{N}$ appelée *fonction de multiplicité* qui associe à chaque arête un entier positif, sa *multiplicité*. Ce nombre représente le *nombre d'arêtes* entre les deux sommets ainsi reliés. Dans cette terminologie, un graphe est un multigraphe pour lequel la multiplicité de chaque arête vaut 1. Un graphe est parfois appelé un *graphe simple*.

Avec cette définition, le multigraphe associé avec le problème des ponts est le *graphe de Königsberg* donné ci-dessous :

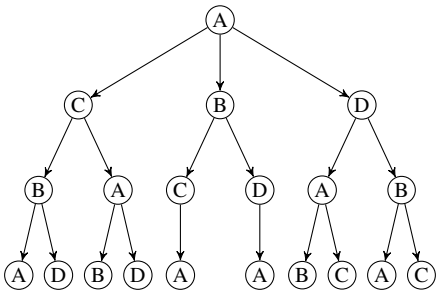


Dans la formulation en terme de multigraphes, le problème est le suivant : trouver un chemin dans le graphe de Königsberg tel que chaque arête est traversée seulement une seule fois. En honneur de Léonard Euler, un tel chemin est appelé un *chemin eulérien*.

Définition 4.2. Soient $G = (V, E)$ un multigraphe et $f : E \to \mathbb{N}$ sa fonction de multiplicité. Un *chemin eulérien* dans G est un chemin $a_0 - a_1 - \cdots - a_m$ tel que pour tout i, (a_i, a_{i+1}) est une arête et chaque arête apparaît dans ce chemin exactement autant de fois que sa multiplicité. Si $a_0 = a_m$, alors le chemin est appelé un *tour eulérien*. Un graphe est dit *eulérien* s'il admet un tour eulérien.

Avec cette définition, le problème devient de trouver un chemin eulérien du graphe précédent, ou montrer qu'il n'en existe pas.

Cette formulation nous permet déjà de résoudre le problème par une attaque par force brute : on peut énumérer tous les chemins possibles qui n'utilisent pas deux fois la même arête et voir s'il n'en existe pas un de longueur 7. Par exemple, voici une liste des chemins de longueur 3 qui partent du sommet A et n'utilisent pas deux fois la même arête :



En principe, il est possible de résoudre le problème avec une telle approche. Néanmoins cette approche n'apporte rien sur la compréhension du phénomène. De plus, le mécanisme d'abstraction qui a rendu cette approche possible la rend également inefficace. En effet, maintenant que le problème est formulé en terme de multigraphe, pourquoi se restreindre au cas du graphe de Königsberg ? On peut maintenant se demander si un multigraphe arbitraire admet un chemin eulérien et si oui, comment le trouver. L'approche d'énumération exhaustive devient alors impraticable quand la taille du graphe augmente.

La solution d'Euler nous donne en fait une caractérisation simple des multigraphes qui contiennent un chemin eulérien. Son idée principale est qu'en fait seul le degré des sommets a une importance.

Définition 4.3. Dans un multigraphe G le degré d'un sommet v est la somme de la multiplicité des arêtes qui le touchent.

Ainsi, pour le graphe de Königsberg, $\deg(A) = 5$, alors que $\deg(B) = \deg(C) = \deg(D) = 3$. Le résultat d'Euler est donné dans le théorème suivant, qui montre que le graphe de Königsberg n'admet pas de chemin eulérien.

Théorème 4.4 (Euler)**.** *Si un multigraphe admet un chemin eulérien alors il ne contient pas plus de deux sommets de degré impair.*

Démonstration. Supposons qu'on ait un chemin eulérien qui part de a et arrive en b. Appelons les sommets de $V - \{a, b\}$ des *sommets internes* du chemin. Le point important est que si l'on arrive dans un sommet interne

en suivant une arête, il faut en sortir par une autre. Ainsi, le nombre d'arêtes (comptées avec multiplicité) qui touche un sommet interne doit être pair. En effet un chemin eulérien doit parcourir toutes les arêtes. Ainsi, les seuls sommets de degré impair peuvent être le départ du chemin a et l'arrivée b. □

La preuve nous montre également que dans un multigraphe avec deux sommets de degré impair, tout chemin eulérien doit commencer par l'un d'entre eux et finir par l'autre.

En fait, Euler affirmait (sans preuve) que la réciproque du théorème précédent est également vraie. La première preuve de la réciproque est due au mathématicien Allemand German Hierholzer dans un article intitulé « Über die Möglichkeit, einen Linienzug ohne Wiederholung und ohne Unterbrechung zu umfahren, » publié dans le journal « Mathematische Annalen, » Volume 6, pages 30–32. Dans ce théorème, on utilise la notion de graphe connexe que l'on donnera plus loin dans la définition 4.13.

Théorème 4.5 (Hierholzer)**.** *Si un multigraphe connexe a au plus deux sommets de degré impair, il admet un chemin eulérien.*

Nous donnerons une preuve de ce théorème pour les graphes dans la section suivante.

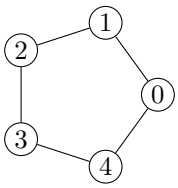
4.2. Concepts élémentaires

Dans toute cette section, on travaille avec des graphes simples et non-orientés, sauf mention contraire. On commence notre discussion sur la théorie des graphes en formalisant l'égalité entre deux graphes.

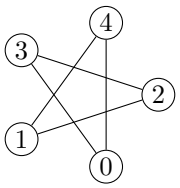
Définition 4.6. Deux graphes $G = (V, E)$ et $G' = (V', E')$ sont dit *isomorphes* si et seulement s'il existe une bijection $\pi : V \to V'$ telle que pour tout $a, b \in V$ on a : $(a, b) \in E \iff (\pi(a), \pi(b)) \in E'$.

En d'autres mots, deux graphes sont isomorphes si on peut passer de l'un à l'autre en renommant leur sommets.

Exemple 4.7. Les graphes G et G' sont isomorphes par l'application π donnée sur la droite.



G



G'

x	0	1	2	3	4
$\pi(x)$	4	1	2	3	0

◇

On continue maintenant en donnant des relations numériques entre les divers nombres associés à un graphe. Souvent, de telles formules sont plus simples si l'on n'autorise pas de boucle sur les sommets du graphe (c'est-à-dire une arête de la forme (a, a)).

Le premier résultat de ce type est le suivant :

Proposition 4.8. *Soit $G = (V, E)$ un graphe sans boucles, alors $2|E| = \sum_{v \in V} \deg(v)$.*

Démonstration. Quand on compte $\sum_{v \in V} \deg(v)$ chaque arête est comptée deux fois, une pour chacun des sommets qu'elle relie. Ainsi, cette somme est le double de $\sum_{e \in E} f(e)$. □

On en déduit immédiatement le corollaire suivant :

Corollaire 4.9. *Le nombre de sommets de degré impair d'un graphe est pair.*

Démonstration. La somme des degrés est paire d'après la proposition précédente. Un nombre impair de sommets de degré impair rendrait la somme impaire, ce qui n'est pas le cas. □

En général, excepté cette égalité, on ne peut pas dire grand chose de plus sur la relation entre le nombre d'arêtes et de sommets d'un graphe. La seule affirmation générale est la suivante :

Proposition 4.10. *Soit n un entier positif. Alors pour tout e avec $0 \leq e \leq n(n-1)/2$ il existe un graphe sans boucle avec n sommets et e arêtes. Si $e > n(n-1)/2$ il n'existe pas de graphe sans boucles avec n sommets et e arêtes.*

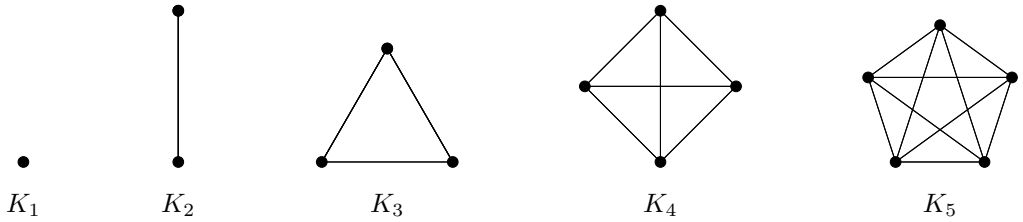
Démonstration. Comme le degré de n'importe quel sommet d'un graphe avec n sommets et sans boucle ne peut dépasser $n-1$, la somme des degrés est d'au plus $n(n-1)$. Ainsi, le nombre d'arêtes est d'au plus $n(n-1)/2$. En construisant un graphe K_n pour lequel chaque sommet est relié à tous les autres et en supprimant des arêtes, on peut obtenir pour tout $e \leq n(n-1)/2$ un graphe avec e arêtes et n sommets. □

Le graphe que nous avons construit dans la preuve précédente a un nom. Il s'agit du *graphe complet* à n sommets.

Définition 4.11. Soient n et m des entiers positifs.

1. Le graphe $G = (\underline{n}, E)$ avec $E = \{(i,j) \mid i,j \in \underline{n}\}$ est appelé le *graphe complet sur n sommets* et il est noté K_n.
2. Le graphe biparti $G = (\underline{m} \sqcup \underline{n}, E)$ avec $E = \{(i,j) \mid i \in \underline{m}, j \in \underline{n}\} \cup \{(j,i) \mid i \in \underline{m}, j \in \underline{n}\}$ est appelé le *graphe biparti complet entre m et n sommets*. On le note $K_{m,n}$.

Exemple 4.12. Voici quelques exemples de graphes complets :



K_1 K_2 K_3 K_4 K_5

Voici quelques exemples de graphe bipartis complets

$K_{1,2}$ $K_{2,2}$ $K_{2,3}$ $K_{3,3}$ $K_{3,4}$

◇

Une autre propriété des graphes qui va beaucoup nous intéresser est celle de connexité.

Définition 4.13. Un graphe $G = (V, E)$ est dit *déconnecté* si V peut être partitionné en deux ensembles disjoints et non vides T et S tels que $E \subseteq T \times T \cup S \times S$. Un graphe est dit *connecté* ou *connexe* s'il n'est pas déconnecté.

Une autre définition de la connexité utilise le concept de chemin :

Définition 4.14. Un *chemin* de longueur t dans le graphe $G = (V, E)$ est une suite de sommets $v_0 - v_1 - \cdots - v_t$ telle que $(v_i, v_{i+1}) \in E$ pour $i = 0, \ldots, t-1$ et telle que les ensembles $\{v_i, v_{i+1}\}$ sont tous distincts. Un chemin est dit *simple* si de plus tous les sommets sont distincts. Un chemin est un *cycle* si $v_t = v_0$.

La remarque suivante est immédiate.

Remarque 4.15. *Un graphe est connexe ssi pour chaque paire de sommets v et w il existe un chemin connectant v et w.*

Démonstration. Supposons que le graphe $G = (V, E)$ est déconnecté, on peut alors écrire $V = T \sqcup S$ et $E \subseteq T \times T \cup S \times S$. Alors il n'existe pas de chemin entre les sommets de T et ceux de S : sinon, s'il existe $t \in T$ et $s \in S$ tels que $(t, s) \in E$, alors $E \not\subseteq T \times T \cup S \times S$.

Maintenant, supposons qu'il existe des sommets v et w entre lesquels il n'existe pas de chemin dans G. Soit T l'ensemble de tous les sommets atteignables par un chemin partant de v, et soit $S := V - T$. Alors $E \subseteq T \times T \cup S \times S$, ce qui montre que le graphe est déconnecté. □

Remarque 4.16. *Tout graphe non vide est une union disjointe de graphe connexes.*

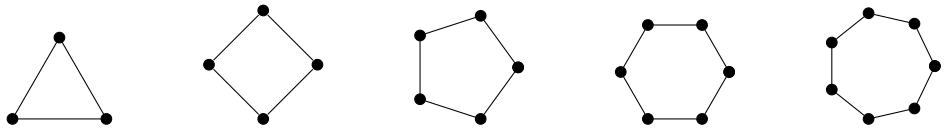
Démonstration. On fait une preuve par récurrence sur le nombre de sommets du graphe. Si le graphe ne contient qu'un sommet, il est trivialement connecté. Supposons maintenant que $G = (V, E)$ a $n > 1$ sommets et que l'affirmation est vraie pour tous les graphes avec moins de n sommets. Choisissons $v \in V$. Soit T l'ensemble de tous les sommets atteignables depuis v. Alors T est connexe puisque pour chaque sommet de T il existe un chemin connectant ce sommet à v. Il existe alors un chemin entre n'importe quel couple de sommets (u, w) dans T. En effet, u est relié à v selon un certain chemin $u - u_1 - \cdots - v$ et w est relié à v selon un certain chemin $w - w_1 - \cdots - v$. On considère alors le plus petit indice i tel que u_i appartient au chemin $v - w$ et j le plus grand indice tel que $v_j = u_i$. La suite $u - \cdots u_{i-1} - u_i = v_j - \cdots - w$ est un chemin qui relie u à w. De plus, il n'existe pas d'arêtes entre les sommets de T et ceux de $S = V - T$ (voir la preuve de la remarque précédente). L'ensemble E est une union disjointe des ensembles $E_1 \subseteq T \times T$ et $E_2 \subseteq S \times S$, et G est une union disjointe de (T, E_1) et (S, E_2). Par hypothèse de récurrence, (S, E_2) est une union disjointe de graphes connexes et il en est de même pour G. □

Définition 4.17. Si un graphe est une union disjointe de graphes connexes, alors les sous-graphes sont appelés les *composantes connexes* de G.

Un autre type de graphes joue un rôle important dans la preuve du théorème de Hierholzer. Ce sont les cycles.

Définition 4.18. Un graphe est un *cycle simple* ou un *cycle* si et seulement s'il est isomorphe au graphe $G = (V, E)$ avec $V = \{v_0, v_1, \ldots, v_m\}$ et $(v_i, v_j) \in E$ si et seulement si $|i - j| = 1$ ou $|i - j| = m$. Un cycle de m sommets est noté C_m. Un graphe $G = (V, E)$ est dit *décomposable en cycles* si c'est une union de cycles simples d'arêtes disjointes, c'est-à-dire si $V = V_1 \cup V_2 \cup \cdots \cup V_t$ et $E = E_1 \cup E_2 \cup \cdots \cup E_t$ ou les (V_i, E_i) sont des cycles simples pour $i = 1, \ldots, t$, et $E_i \cap E_j = \emptyset$ si $i \neq j$.

Exemple 4.19. Voici quelques exemple de cycle simple.



C_3 C_4 C_5 C_6 C_7

Voici quelques exemples de graphes décomposables en cycles qui ne sont pas des cycles simples.

G_1 G_2 G_3 G_4

Les graphes G_1 et G_4 sont connexes, alors que G_2 et G_3 ne le sont pas. ◇

Les cycles et les graphes décomposables en cycles se caractérisent facilement. Mais nous avons d'abord besoin du lemme suivant :

Lemme 4.20. *Soit $G = (V, E)$ un graphe et soit d le degré minimum des sommets de G.*

(1) *G admet un chemin simple de longueur d.*

(2) *Si $d \geq 2$, alors G admet un cycle simple de longueur au moins $d + 1$.*

Démonstration. (1) Soit un chemin simple maximal $v_0 - \cdots - v_l$ de G, c'est-à-dire un chemin que l'on ne peut prolonger à droite ou a gauche. Alors, tous les voisins de v_0 doivent être dans le chemin, sinon on pourrait le prolonger à gauche. On en déduit que $l \geq \deg(v_0) \geq d$.

(2) Dans le chemin simple précédent, soit $k := \max\{i \mid (v_0, v_i) \in E\}$ l'index maximal d'un voisin de v_0. L'arête (v_k, v_0) ne peut pas avoir été employée au cours du chemin. Considérons alors le cycle $v_0 - v_1 - \cdots - v_k - v_0$ de longueur $k + 1$. Comme $k \geq \deg(v_0) \geq d$, la taille de ce cycle est d'au moins $d + 1$. □

Voici maintenant la caractérisation des cycles et des graphes décomposables en cycles.

Théorème 4.21. *Soit $G = (V, E)$ un graphe.*

(1) *G est un cycle ssi il est connexe et tout sommet est de degré 2.*

(2) *G est décomposable en cycles ssi tout sommet est de degré pair.*

Démonstration. (1) Si G est un cycle, alors il est connecté et tous les sommets sont de degré 2. Pour prouver l'autre sens, en utilisant le lemme 4.20(2) on sait que G contient un cycle $C = (V_1, E_1)$ de longueur au moins 3. Supposons que G n'est pas égal à C. Comme G est connexe, il existe donc au moins une arête $(a, b) \notin E_1$ avec $a \in V_1$. Mais c'est impossible, car a est de degré 2 et a uniquement des arêtes qui vont dans C.

(2) Si G est décomposable en cycles, alors chaque sommet de G a un degré pair : chaque sommet est dans un nombre m de cycles simples avec $m \geq 0$ et chacun de ces cycles contribue de 2 au degré du sommet qui est donc de $2m$.

Pour montrer l'autre sens on utilise une récurrence sur le nombre d'arêtes du graphe. Si tous les sommets du graphe sont de degré zéro, alors l'ensemble des arêtes du graphe est vide et le graphe est décomposable en cycles de manière triviale. Cela termine le début de la récurrence. Pour la suite, supposons que G a un certain nombre $m > 1$ d'arêtes. Soit alors Z l'ensemble des sommets de degré 0 et T l'ensemble des autres sommets qui sont donc de degré pair et ≥ 2. Il est suffisant de montrer que T est un graphe décomposable en cycle. Comme le degré minimal d'un sommet de T est 2, d'après le lemme 4.20 il existe un cycle C dans T de longueur au moins 3.

Supprimons maintenant toutes les arêtes de ce chemin de G. Dans le graphe résultant, G', tous les sommets sont encore de degré pair car chaque sommet qui participait au chemin précédent a perdu 2 arêtes et tous les autres aucune. Ainsi G' est décomposable en cycles. Comme G est l'union de G' et C, il est aussi une union de cycles d'arêtes disjointes et est donc décomposable en cycles. □

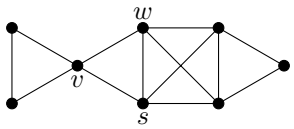
On est maintenant capable de prouver une version plus faible du théorème de Hierholzer :

Théorème 4.22. *Un graphe est eulérien ssi il est connexe et tous ses sommets sont de degré pair. De plus, si G est un graphe connexe dont tous les sommets sont de degré pair, alors pour tout sommet v de G il existe un circuit eulérien qui commence et termine en v.*

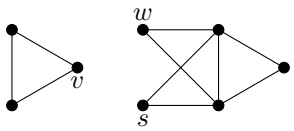
Démonstration. On montre d'abord que si un graphe G est eulérien, alors il est connexe et tous ses sommets sont de degré pair. Pour cela, soit $v_0 - v_1 - v_2 - \cdots - v_{m-1} - v_0$ un circuit eulérien. Le nombre d'arêtes du graphe est donc m. Comme chaque sommet de ce cycle a 2 arêtes incidentes (une entrante, une sortante), le degré de chaque sommet est pair. De plus le graphe est connexe car cette propriété est nécessaire pour l'existence du circuit eulérien.

On montre maintenant la réciproque : si tous les sommets du graphe sont de degré pair et si le graphe est connexe, alors il existe un circuit eulérien dans le graphe. En fait on va montrer que pour chaque sommet v du graphe, il existe un circuit eulérien qui commence et termine en v. On va montrer cela par récurrence sur le nombre d'arêtes de G. L'affirmation est évidente si G n'a que trois arêtes ; ce qui permet de commencer la récurrence. Pour la suite, choisissons un sommet v, son degré est forcément non nul car G est connexe. Par le théorème 4.21, on sait que G est un graphe décomposable en cycles, v appartient donc à un cycle C. Enlevons les arêtes de C du graphe G pour obtenir un graphe G'. Soient $G_1, \ldots, G_t$ les composantes connexes de G', et $v_1, \ldots, v_t$ les sommets respectifs de C dans $G_1, \ldots, G_t$. Chaque G_i est un graphe connexe pour lequel le degré des sommets est pair. Soit P_i un tour eulérien dans G_i qui commence et termine en v_i (ce tour existe par hypothèse de récurrence). On va maintenant construire un tour eulérien dans G : On part de v et on avance sur le cycle C jusqu'à v_1, puis on suit le tour P_1 qui nous ramène à v_1, on continue ensuite sur C jusqu'à v_2, puis on suit P_2 et ainsi de suite. □

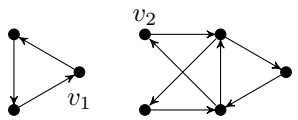
Exemple 4.23. Appliquons le procédé de la preuve précédente sur le graphe suivant :



Comme cycle C on choisit celui formé par les sommets v, w, et s. En l'enlevant du graphe, on obtient deux composantes connexes :

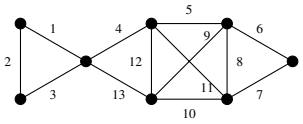


On choisit $v_1 := v$ et $v_2 := w$ (on aurait aussi pu choisir $v_2 = s$). Ensuite, on trouve un tour eulérien pour chacune des deux composantes :



Les flèches indiquent dans quelle direction on doit suivre le chemin. Ainsi, dans la composante connexe de gauche le chemin commence en v_1, puis va sur le sommet du haut et descend sur le sommet du bas avant de revenir sur v_1.

Maintenant, on remet le cycle C, on va de v_1 à v_2 puis on suit le tour eulérien sur la composante connexe de droite, on retourne en v_2 et on finit le tour en retournant en v_1 par le cycle C.



Pour éviter toute confusion, les nombres sur les arêtes du dessin précédent donne leur ordre dans le tour eulérien de G. ◇

On peut maintenant prouver le théorème de Hierholzer pour les graphes :

Démonstration. On raisonne par récurrence sur le nombre d'arêtes de G. Pour commencer, prenons un graphe avec une arête : un tel graphe peut avoir seulement 2 sommets (car il est connexe), chacun de degré 1 et le théorème est vrai.

Pour la suite de la récurrence, on remarque d'abord que G peut soit avoir deux sommets de degré impair soit aucun d'après le corollaire 4.9. Supposons que G n'ait pas de sommet de degré impair. Alors G possède un tour eulérien d'après le théorème 4.22, ce qui fini ce cas. Supposons maintenant que G ait deux sommets de degré impair notés v et w.

On va distinguer deux cas : Commençons par supposer que v et w sont connectés par une arête e. On enlève e pour obtenir un nouveau graphe G'. Ce graphe a au plus deux composantes connexes et tous ses sommets sont de degré pair. S'il a deux composantes, G_1 et G_2, qui contiennent respectivement v et w, alors on trouve un tour eulérien P_1 dans G_1 qui commence et termine par v, et un autre tour P_2 dans G_2 qui commence et termine par w, ce qu'on peut faire d'après le théorème 4.22. En suivant le tour P_1, puis l'arête e, et le tour P_2 on obtient un chemin eulérien dans G. Si G' est connexe, on trouve un tour eulérien P_1 de ce graphe et on lui ajoute e pour obtenir un chemin eulérien de G.

Dans le deuxième cas, on suppose que v et w ne sont pas connectés. Alors v est connecté à un sommet z de degré pair par une arête e. On l'enlève du graphe pour obtenir un graphe G'. Comme précédemment, G' peut avoir au plus deux composantes connexes. S'il en a deux G_1 et G_2, alors v et z ne sont pas dans la même, disons que v est dans G_1 et que z est dans G_2. Le degré de v dans G_1 est pair et celui de z dans G_2 est impair. On en déduit que w doit forcément être dans G_2 aussi (car le nombre de sommets de degré impair est impair d'après le corollaire 4.9). De plus, tous les sommets de G_1 sont de degré pair. Donc G_1 admet un tour eulérien P_1. De plus, par hypothèse de récurrence G_2 admet un chemin eulérien P_2 qui commence en z et fini en w. En suivant P_1, puis l'arête e de v à z et ensuite le chemin eulérien P_2 de z à w nous donne un chemin eulérien de v a w dans G.

Si G' est connexe, alors il existe un chemin eulérien P de z à w par hypothèse de récurrence. En suivant l'arête e, puis le chemin P on obtient un chemin eulérien de v a w et on a fini. □

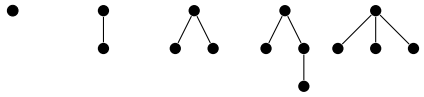
4.3. Graphes planaires et formule d'Euler

Quel est le nombre minimum d'arêtes que peut avoir un graphe connexe ? De manière évidente, un tel graphe ne peut avoir de cycle, car on pourrait enlever l'une des arêtes d'un tel cycle sans rompre la connexité.

Définition 4.24. Un graphe est dit *acyclique* s'il ne contient pas de cycle. Un graphe acyclique et connexe est un *arbre*.

Ainsi, un graphe connexe avec un nombre d'arêtes minimal est nécessairement un arbre.

Exemple 4.25. Voici une liste exhaustive des arbres sur 1, 2, 3 et 4 sommets :



◇

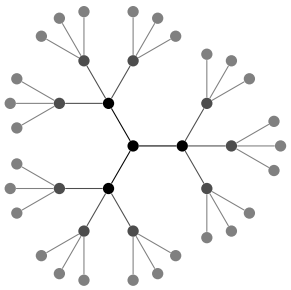
Un point commun de tous ces exemples est que le nombre d'arêtes est toujours égal au nombre de sommets moins un. En fait, c'est toujours le cas comme le montre le résultat suivant. Le nombre d'arêtes minimal qu'un graphe connexe sur n sommets peut avoir est $n - 1$.

Théorème 4.26. *Le nombre d'arêtes d'un arbre sur n sommets est $n - 1$.*

Démonstration. On fait un raisonnement par récurrence sur le nombre de sommets de l'arbre. Si $n = 1$, alors l'affirmation est triviale. Supposons maintenant que $n > 1$ et que l'affirmation est vraie pour tout $i < n$, c'est-à-dire que pour tout $i < n$ on sait que le nombre d'arêtes d'un arbre sur i sommets est $i - 1$.

Prenons un arbre sur n sommets, choisissons une de ses arêtes e et supprimons-la. Le graphe résultant n'est plus connexe : sinon rajouter l'arête e provoquerait un cycle. De plus, chacune des parties du graphe est connexe : sinon l'arbre original ne serait pas connexe non plus. Supposons que ces parties contiennent respectivement m et $n - m$ sommets. Par hypothèse de récurrence, elles ont $m - 1$ et $n - m - 1$ arêtes. Ainsi le nombre total d'arêtes de l'arbre original est $1 + (m - 1) + (n - m - 1) = n - 1$. □

Les arbres peuvent être dessinés dans le plan de telle manière que deux arêtes ne se touchent que sur les sommets. Voici un algorithme possible pour cela : on commence par placer un sommet arbitraire, on dessine ses voisins en cercle autour de lui est avec des angles identiques et ainsi de suite. Un exemple est donné sur la figure de droite.



Définition 4.27. Un *graphe planaire* est un graphe qui peut être dessiné dans le plan de telle manière que ses arêtes ne se touchent qu'en leurs extrémités.

Comme l'on a vu plus haut, les arbres sont des graphes planaires. Néanmoins, l'ensemble des graphes planaires est beaucoup plus large que juste les arbres. Par exemple, une union disjointe de graphes planaires est un graphe planaire, ce qui peut se voir facilement en les dessinant suffisamment loin les un des autres dans le plan.

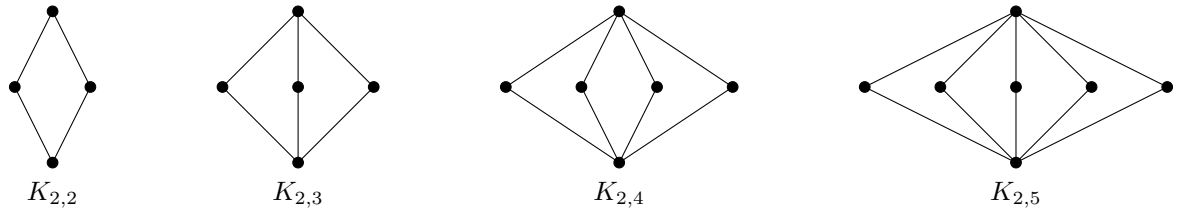
On en déduit que tout graphe acyclique est planaire : si le graphe est connexe c'est un arbre. Sinon, ses composantes connexes sont des arbres et donc planaires. Et c'est encore le cas du graphe original vu que c'est une union disjointe de graphes planaires.

Un ingrédients clef pour montrer qu'un arbre n'est pas planaire réside dans l'étude de ses sous-graphes. Si $G = (V, E)$ est un graphe, alors tout graphe de la forme (V', E') avec $V' \subseteq V$ et $E' \subseteq E \cap (V' \times V')$ est appelé un *sous-graphe* de G. Clairement, si un graphe est planaire, alors c'est le cas de tous ses sous-graphes. En particulier, un graphe n'est pas planaire s'il contient un sous-graphe non planaire. Mais la réciproque est-elle également vraie ? C'est-à-dire, un graphe est-il planaire si et seulement si tout ses sous-graphes propres (différents de lui-même) sont planaire ? Il se trouve que ce n'est pas le cas, comme on le verra plus loin.

Exemple 4.28. Les graphes complets K_1, K_2, K_3 sont planaires. K_4 est également planaire.

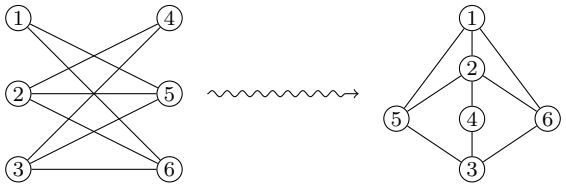
On montrera plus loin que K_5 n'est pas planaire. On en déduit que K_n n'est pas planaire pour tout $n \geq 5$ car un tel K_n admet K_5 comme sous-graphe.

Les graphes bipartis complets $K_{1,n}$ sont planaires pour tout n (ce sont des arbres). $K_{2,n}$ est aussi planaire pour tout n comme le montre la figure suivante :



On montrera plus loin que $K_{3,3}$ n'est pas planaire. On en déduit que $K_{m,n}$ n'est pas planaire si m et n sont tous les deux plus grands ou égaux à 3 car un tel graphe contient $K_{3,3}$ comme sous-graphe. ◇

Le fait que $K_{3,3}$ n'est pas planaire est très intéressant : en fait, tous les sous-graphes propres de $K_{3,3}$ sont planaires. Pour voir cela, il suffit de montrer que la suppression de n'importe quelle arête de $K_{3,3}$ le rend planaire. Comme $K_{3,3}$ est symétrique par rapport aux sommets de chacun des ses côtés, on peut choisir l'arête que l'on veut. Dans la figure ci-dessous, on supprime l'arête entre les sommets 4 et 1 :

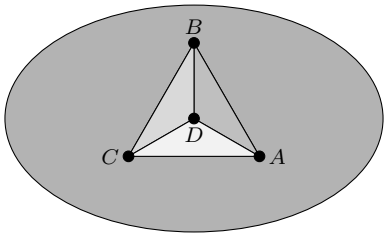


Un autre ingrédient clef dans l'étude des graphes planaires est la subdivision du plan donnée par le graphe. Cette notion est rendue plus précise dans la définition suivante.

Définition 4.29. Soit G un graphe planaire dessiné dans le plan. Une *face* du graphe est une région du plan telle que n'importe quel couple de points peut être relié par un chemin continu qui ne coupe aucune des arêtes du graphe. Par « coupe » on veut dire que le chemin admet deux points de part et d'autre de l'arête.

Exemple 4.30. Un arbre n'admet qu'une face : le plan en entier. En fait, il est possible de trouver un chemin continu de n'importe quel point du plan à un autre sans couper une arête de l'arbre. C'est possible car l'arbre n'a pas de cycles.

Le graphe planaire K_4 a 4 faces dessinées ci-dessous :



Une des faces est donnée par le triangle $\langle A, D, B\rangle$, une autre par le triangle $\langle C, D, A\rangle$, une autre par le triangle $\langle C, D, B\rangle$, et la dernière par la région autour du graphe. ◇

Pour les graphes planaires, le nombre de faces, de sommets et d'arêtes satisfait une égalité fondamentale connue sous le nom de formule d'Euler.

Théorème 4.31 (Formule d'Euler)**.** *Supposons que G est un graphe connexe avec f faces, e arêtes et v sommets. Alors $v - e + f = 2$.*

Démonstration. On montre le théorème par récurrence sur le nombre e d'arêtes de G. Si $e = 1$, alors G est un arbre sur 2 sommets et possède une seule face, le théorème est donc valide.

Supposons maintenant que G a e arêtes et supposons que le théorème est vrai pour tous les graphes avec au plus $e - 1$ arêtes. Si G est acyclique, alors $f = 1$ et $e = v - 1$ d'après le théorème 4.26, et donc $v - e + f = 2$. Si G n'est pas acyclique, prenons alors une arête (a, b) qui participe à un cycle de G et supprimons la du graphe G. Le graphe résultant est encore connexe et par hypothèse de récurrence, la formule d'Euler est valide pour ce graphe. Si f et e sont le nombre de faces et d'arêtes du graphe original, alors le graphe résultant a $f - 1$ faces et $e - 1$ arêtes. On sait que pour ce graphe $v - (e - 1) + (f - 1) = 2$, ce qui termine la preuve du théorème. □

Le théorème précédent est une généralisation du théorème 4.26 : si G est un arbre, alors il admet une face, donc $v - e = 1$. ce qui nous donne l'affirmation du théorème 4.26.

De manière intuitive, un graphe planaire ne peut avoir trop d'arêtes : plus il y en a, plus il est difficile de dessiner le graphe dans un plan sans intersection. Le théorème suivant est essentiel pour prouver cette affirmation intuitive. Pour la preuve, on a besoin des concepts suivants :

Définition 4.32. Soit $G = (V, E)$ un graphe connexe.

1. La *circonférence* de G est la taille du plus petit cycle dans G, s'il existe.
2. Un *pont* dans G est une arête de G qui sépare G en deux composantes connexes si on l'enlève.

Exemple 4.33. Le graphe dans l'exemple de la figure 4.2 a une circonférence de 3 et il a un pont. ◇

La preuve de la proposition suivante est laissée en exercice.

Proposition 4.34. *Soit G un graphe planaire.*

(1) *Chaque arête de G est contenue dans au plus 2 faces.*

(2) *Une arête de G est un pont ssi elle est contenue dans exactement une face.*

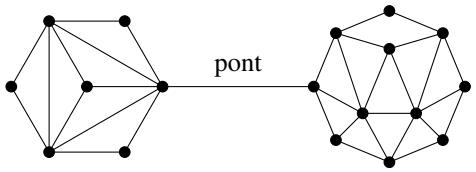


Figure 4.2 – Exemple de pont

Théorème 4.35. *Soit G une composante connexe de n sommets d'un graphe planaire. Si G n'a pas de cycle, alors G a $n-1$ arêtes. Si G a une circonférence g, alors G a au plus $g(n-2)/(g-2)$ arêtes.*

Démonstration. Si G est un arbre, alors l'affirmation en découle d'après le théorème 4.31. Supposons donc que G a un cycle. Comme la circonférence de G est ≥ 3 par hypothèse, il s'ensuit que le nombre de sommets n de G est au moins 3. On va faire une récurrence sur le nombre de sommets de G.

Pour $n = 3$ l'affirmation est triviale. Supposons maintenant que l'affirmation du théorème est vraie pour tous les graphes avec n sommets. On va prouver que l'affirmation est aussi vraie pour les graphes sur $n + 1$ sommets.

Soit G un graphe avec $n + 1$ sommets. On va distinguer 2 cas :

Cas 1 Commençons par supposer que G admet un pont b. Enlever b coupe G en deux composantes connexes G_1 et G_2. Notons respectivement leur nombre de sommets n_1 et n_2 et leur nombre d'arêtes e_1 et e_2. Ainsi $n + 1 = n_1 + n_2$ et le nombre e d'arêtes de G est $e_1 + e_2 + 1$. Comme G a un cycle, il se trouve que G_1 et G_2 ne peuvent être tous deux acycliques, supposons par exemple que G_1 a un cycle. Si G_2 a également un cycle, alors par hypothèse de récurrence on a

$$e_1 + e_2 + 1 \leq \frac{g(n_1 - 2 + n_2 - 2)}{g-2} + 1 \leq \frac{g(n+1-3)-2}{g-2} \leq \frac{g(n-1)}{g-2},$$

ce qui montre l'affirmation. (Notez qu'il est possible que la circonférence de G_1 ou de G_2 soit plus grande que g ; mais comme la fonction $g/(g-2)$ est décroissante, on peut toujours remplacer la circonférence réelle de G_1 ou de G_2 par g)

Si G_2 est un arbre, alors $e_2 = n_2 - 1$, et on a

$$e_1 + e_2 + 1 = e_1 + n_2 \leq \frac{g(n_1 - 2)}{g-2} + n_2 < \frac{g(n_1 + n_2 - 1)}{g-2},$$

car $g/(g-2) > 1$.

Cas 2 Supposons maintenant que G n'a pas de pont. Alors par la proposition 4.34 toutes les arêtes de G sont contenues dans deux faces. Si f_i représente le nombre de faces de G dont les bords sont formés de i arêtes, alors on a

$$2e = \sum_{i=1}^{n+1} i f_i \geq \sum_{i=1}^{n+1} g f_i = gf,$$

avec f le nombre de faces de G. En effet, $f_i = 0$ pour $i < g$, puisque g est la circonférence de G. D'un autre coté, en appliquant la formule d'Euler, on a

$$e + 2 = (n+1) + f \leq (n+1) + \frac{2e}{g}.$$

Cela montre que $e \leq g(n-1)/(g-2)$, ce qui termine la preuve.

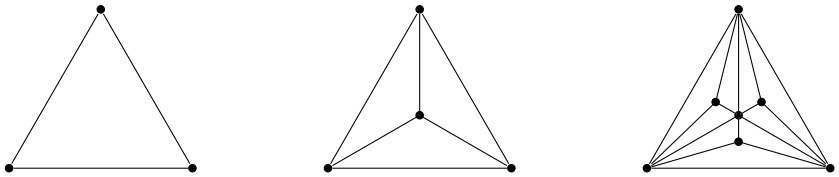
□

Exemple 4.36. La borne du théorème précédent est exacte : considérons les graphes $K_{2,n}$, On voit que $g = 4$, le nombre de sommets est $n + 2$, et le nombre d'arêtes est $2n = 4n/2$. ◇

Corollaire 4.37. *Soit G un graphe planaire et connexe avec $n \geq 3$ sommets. Alors G contient au plus $3n - 6$ arêtes.*

Démonstration. Tout graphe G est soit acyclique, ou a une circonférence d'au moins 3. S'il est acyclique, alors le nombre d'arêtes est $n - 1 < 3n - 6$. Sinon, un graphe de circonférence 3 a au plus $3(n - 2) = 3n - 6$ arêtes d'après le théorème ci-dessus. De plus, si la circonférence du graphe est plus grande que 3, on peut toujours lui rajouter des arêtes pour obtenir un triangle et se ramener au cas précédent. □

Exemple 4.38. La borne du corollaire précédent est exacte pour une suite infinie de graphes planaires, les trois premiers étant donnés ci-dessous :



$m = 0$ $m = 1$ $m = 2$

Ainsi, on commence avec un triangle et à chaque étape, on choisit un sommet dans chaque triangle du graphe et on le connecte aux sommets voisins. Si m correspond au numéro de l'étape, on peut montrer par récurrence que le graphe numéro m est formé de 3^m triangles. Si e_m et n_m correspondent respectivement au nombre d'arêtes et de sommet du graphe numéro m, alors on a les formules :

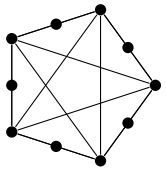
$$e_0 = 3, n_0 = 3, e_{m+1} = e_m + 3^{m+1}, n_{m+1} = n_m + 3^m, \quad m \geq 0.$$

En effet, au passage de l'étape m à l'étape $m + 1$ on va prendre autant de nouveaux sommets que de triangles à l'étape m, c'est-à-dire 3^m. D'où la formule pour n_{m+1}. De plus, chacun des ces nouveaux sommets conduit à trois nouvelles arêtes, une pour chaque sommets du triangle précédent. D'où la formule pour e_{m+1}.

On utilise encore un récurrence pour montrer que $e_m = 3(n_m - 2)$ pour tout m. L'affirmation est claire pour $m = 1$. et pour $m \geq 2$, on a $3(n_{m+1} - 2) = 3(n_m - 2 + 3^m) = 3(n_m - 2) + 3^{m+1} = e_{m+1}$, ce qui termine la démonstration. Remarquez que comme e_m et n_m sont des séries géométriques, on peut calculer que $e_m = (3^{m+1} + 3)/2$ et $n_m = (3^m + 5)/2$. ◇

Corollaire 4.39. *Le graphe complet K_5 n'est pas planaire. Le graphe biparti complet $K_{3,3}$ n'est pas planaire.*

Démonstration. K_5 a 5 sommets, mais son nombre d'arêtes est 10 ce qui est plus grand que $3 \cdot 5 - 6 = 9$. $K_{3,3}$ a une circonférence de 4, donc son nombre d'arêtes devrait être d'au plus $2 \cdot (6 - 2) = 8$, mais il est de 9. □



Comment pouvons-nous cependant tester en général si un graphe est planaire ou pas ? Si un graphe contient K_5 ou $K_{3,3}$, il n'est certainement pas planaire, mais ce critère n'est pas suffisant. Par exemple, le graphe sur la droite ne contient aucun de ces deux graphes mais il n'est pas planaire. Ce graphe est obtenu depuis K_5 par un procédé appelé *subdivision* dans lequel un nouveau sommet est placé sur une arête qui existe déjà. Un théorème du mathématicien Polonais Kazimierz Kuratowski des années 1930 montre qu'un graphe est planaire ssi il ne contient pas une subdivision de K_5 ou une subdivision de $K_{3,3}$.

Ce théorème ne conduit pas à une méthode très efficace pour tester si un graphe est planaire ou non. Une telle méthode fut trouvée en 1967 par les mathématiciens israéliens Lempel, Even et Cederbaum (Il s'agit d'ailleurs du même Lempel que celui de l'algorithme de compression de Lempel-Ziv). La méthode fut rendue encore plus efficace en 1974 par Even et Tarjan. Ces méthodes et le résultat de Kuratowski dépassent le cadre de ce cours.

On mentionne encore un résultat sur les graphes planaires qui montre que de tels graphes ont énormément de sommets de faible degré.

Proposition 4.40. *Soit G un graphe planaire avec n sommets et soit n_d le nombre de sommets de degré inférieur à d dans G. Alors pour tout $d \geq 1$ on a*

$$n_d \geq \frac{n(d-5) + 12}{d+1}.$$

Ainsi G a au moins 2 sommets de degré inférieur à 5 et pour des n grands, au moins $1/7$ des sommets de G sont de degré inférieur à 6.

Démonstration. $n - n_d$ est le nombre de sommets de degré au moins $d+1$, ainsi $(n-n_d)(d+1)/2$ est inférieur au nombre d'arêtes de G. En appliquant le corollaire 4.37, on a

$$(n - n_d)(d+1) \leq 6n - 12.$$

Un simple manipulation conduit au résultat. □

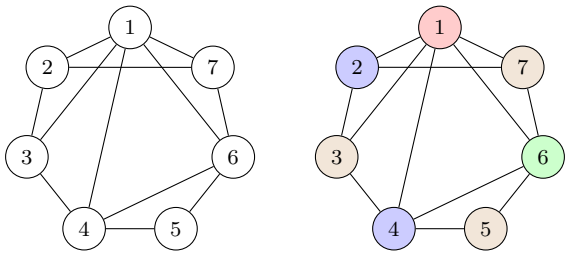
4.4. Coloriage de graphe

Supposez que vous vouliez planifier les dates d'examens et que, par gentillesse, vous voulez éviter que les étudiants aient plus d'un examen par jour. Notons les différents cours 1,2,3,4,5,6,7. La table ci-dessous contient une étoile dans la case (i, j) si au moins un étudiant suit les cours i et j, cours dont les examens ne peuvent donc avoir lieu le même jour.

	1	2	3	4	5	6	7
1		*	*	*		*	*
2	*		*				*
3	*	*		*			
4	*		*		*	*	
5				*		*	
6	*			*	*		*
7	*	*				*	

Quel est le nombre minimal de jours requis pour la période d'examens ?

Ce problème peut être posé en terme de théorie des graphes. On interprète la table précédente comme un graphe sur l'ensemble $\{1, 2, \ldots, 7\}$: ce que l'on veut faire, c'est associer à chaque sommet un nombre d'un ensemble S (de jours) tel que deux sommets adjacents n'aient pas le même nombre. La plus petite taille de S qui nous permet de faire cela est donc le nombre minimal de jours nécessaires. Il est d'usage de voir l'ensemble S comme un ensemble de « couleurs ». On appelle ainsi une telle association de couleurs à chaque sommet un coloriage du graphe. Pour notre exemple, la figure suivante nous montre le graphe et un coloriage possible avec 4 couleurs.



Dans ce cas, on peut voir qu'un coloriage avec seulement 3 couleurs n'est pas possible : Si c'était le cas, les arêtes 1, 2 et 7 obtiendraient chacune une de ces couleurs, par exemple rouge, bleu et vert. Mais comme les sommets 1 et 2 touchent 3, 3 serait également vert. De même 1, 7 et 6 sont connectés, la couleur de 6 est donc bleue. Enfin 1, 3 et 4 étant connectés, la couleur de 4 serait aussi bleue, une contradiction car 4 et 6 sont connectés.

Définition 4.41. Soit $G = (V, E)$ un graphe.

1. Un *coloriage* de G avec k couleurs est une application $f\colon V \to \{1, 2, \ldots, k\}$ telle que pour $(a, b) \in E$ on a $f(a) \neq f(b)$.
2. G est dit *k-coloriable* s'il existe un coloriage de G avec k couleurs.
3. Le *nombre chromatique* de G, noté $\chi(G)$, est le plus petit k tel que G soit k-coloriable.

Voici quelques résultats élémentaires sur le nombre chromatique :

Proposition 4.42. *Soit $G = (V, E)$ un graphe.*

(1) $\chi(G) = 1$ *ssi G n'a pas d'arête.*

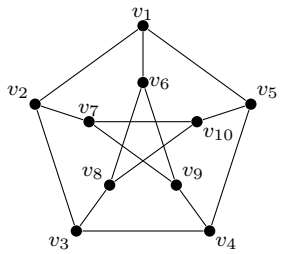


Figure 4.3 – Le graphe de Petersen et une numérotation de ses sommets

(2) $\chi(G) \leq |V|$.

(3) $\chi(K_n) = n$ *pour tout* $n \geq 1$.

(4) $\chi(C_n) = 2$ *si* n *est pair et* 3 *si* n *est impair.*

Démonstration. (1) Facile.

(2) Facile aussi, il suffit de colorier chaque sommet d'une couleur différente.

(3) N'importe quel coloriage de K_n avec moins de n couleurs implique que deux sommets sont de la même couleur, ce qui est une contradiction car tous les sommets sont adjacents entre eux.

(4) Par (1), $\chi(C_n) \geq 2$. Associons l'ensemble des sommets de C_n à $\underline{n}$. Si n est pair, alors on colorie tous les sommets d'indice pairs avec une couleur et tous les autres avec l'autre.

Si n est impair, on montre que C_n n'est pas 2-coloriable. Supposons qu'il le soit et qu'on colorie ses sommets en bleu ou rouge. On suppose que 0 est bleu. Alors 1 et $n-1$ doivent être rouge, 2 et $n-2$ doivent être bleu et de façon générale k et $n-k$ sont de la même couleur pour tout $1 \leq k < n/2$. Si $n = 2m+1$, alors avec $k = m$, on voit que m et $m+1$ sont de la même couleur, une contradiction.

Il est aussi facile de voir que C_n est 3-coloriable, dans la preuve ci-dessus, il suffit de colorier le sommet d'indice m avec la troisième couleur. □

Trouver la valeur exacte de $\chi(G)$ est souvent très difficile. Une des méthodes qui peut aider à borner $\chi(G)$ est donnée dans la remarque suivante.

Remarque 4.43. *Supposons que* H *est un sous-graphe de* G*. Alors* $\chi(H) \leq \chi(G)$.

Comment pouvons nous trouver un coloriage d'un graphe ? Dans la suite, on donne un algorithme simple qui permet de trouver un coloriage avec peu de couleurs d'un graphe (mais pas nécessairement celui avec le moins de couleurs). On suppose que les couleurs sont des nombres $1, 2, \ldots$, et que les sommets du graphe sont ordonnés (de manière arbitraire) et notés $v_1, v_2, \ldots, v_n$. On va colorier les sommets un par un, en utilisant toujours la couleur de plus petit indice qui convient. Donnons une description plus précise de l'algorithme. Il associe à chaque sommet v une couleur $c(v)$. E est l'ensemble des arêtes de G.

(1) Poser $c(v_1) := 1$.

(2) Pour $i = 2$ jusqu'à n faire

  (2a) Poser $A := \{c(v_j) \mid j < i \wedge (v_i, v_j) \in E\}$.

  (2b) Poser $j := \min(\mathbb{N} - A)$.

  (2c) Poser $c(v_i) := j$.

Exemple 4.44. Appliquons l'algorithme précédent pour colorier le *graphe de Petersen* donné sur la figure 4.3.

On part du sommet v_1 et on pose $c(v_1) = 1$. Ensuite, on prend le sommet v_2 ; et comme il est connecté à v_1, on obtient $c(v_2) = 2$. Pour calculer $c(v_3)$, on remarque que l'ensemble A de l'étape (2a) vaut $\{2\}$, et donc $c(v_3) = 1$. De même on a $c(v_4) = 2$. Pour calculer $c(v_5)$, on remarque que v_5 est relié à v_1 et v_4, donc $A = \{1, 2\}$ et $c(v_5) = 3$.

Passons maintenant aux sommets intérieurs. v_6 est connecté uniquement à v_1 parmi les sommets déjà coloriés, donc $c(v_6) = 2$. De même, $c(v_7) = 1$. v_8 est connecté à v_6 et v_3 parmi les sommets déjà coloriés ; comme $c(v_6) = 2$ et $c(v_3) = 1$, on obtient $c(v_8) = 3$. Le sommet v_9 est connecté à v_6, v_7 et v_4. Ici, l'ensemble A vaut

$\{1, 2\}$ et donc $c(v_9) = 3$. Finalement, v_{10} est connecté à v_5, v_7, et v_8, donc $A = \{c(v_5), c(v_7), c(v_8)\} = \{3, 1\}$ et $c(v_{10}) = 2$. Pour résumer, on a la liste suivante :

v	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}
$c(v)$	1	2	1	2	3	2	1	3	3	2

Ce qui montre que $\chi(P) \leq 3$. D'un autre côté, P contient C_5 et donc $\chi(P) \geq \chi(C_5) = 3$, d'après la proposition 4.42(4). On en conclu que $\chi(P) = 3$. ◇

Même s'il peut sembler que l'algorithme précédent utilise toujours le moins de couleur possible, ce n'est pas le cas. En fait, trouver le nombre chromatique d'un graphe est vraiment très difficile, avec un sens que l'on peut préciser.

Proposition 4.45. *Soit $\Delta(G)$ le degré maximum d'un sommet du graphe G. Alors $\chi(G) \leq \Delta(G) + 1$.*

Démonstration. On raisonne par récurrence sur le nombre de sommets de G. L'affirmation est claire si G n'a qu'un sommet. Supposons que G a n sommets, avec $n \geq 1$. Choisissons un sommet v de G de degré $\Delta(G)$ et supprimons le du graphe avec toutes les arêtes qui lui sont reliées. Cela nous donne un nouveau graphe G', avec $n-1$ sommets et $\Delta(G') \leq \Delta(G)$. Par hypothèse de récurrence, G' est coloriable avec au plus $\Delta(G') + 1 \leq \Delta(G) + 1$ couleurs. Ce qui veut dire que parmi les voisins de v une de ces couleurs n'apparaît pas et donc v peut être colorié avec cette couleur. □

La proposition ci-dessus peut être rendu plus forte, mais nous n'allons pas le faire ici. On mentionne seulement le théorème suivant du à Brooks :

Théorème 4.46. *Soit G un graphe connexe qui n'est pas complet et n'admet pas de cycle de longueur paire. Alors $\chi(G) \leq \Delta(G)$.*

Une grande partie de la recherche sur le nombre chromatique des graphes s'est centrée autour d'un effort monumental pour trouver le nombre chromatique des graphes planaires.

Imaginons un plan qui est découpé par un ensemble de courbes de telle manière qu'aucun point ne peut appartenir à plus de trois des régions délimitées par les courbes. On parle de *carte admissible*, de *frontières* et d'*états*. Ainsi, on exclut le cas de plus de quatre états qui ont un point commun sur leur frontière, comme c'est par exemple le cas pour les états Utah, Nouveau Mexique, Arizona et Colorado de la carte des États Unis (voir figure 4.4). Un coloriage admissible d'une carte est un coloriage tel qu'il n'existe pas d'états voisins avec la même couleur. Quel est le nombre minimal de couleurs requises pour colorier n'importe quelle carte admissible de cette façon ?

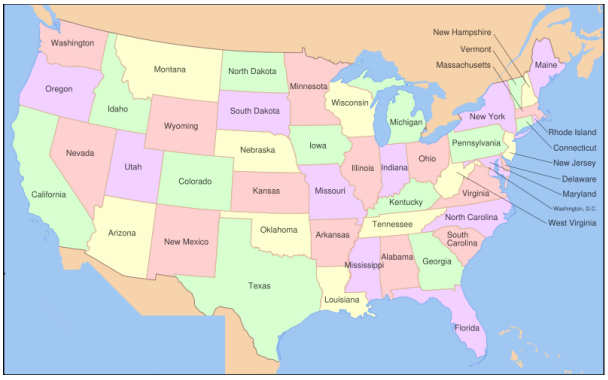


Figure 4.4 – 4-coloriage d'une carte des États Unis. Remarquez que cette carte peut être coloriée avec 4 couleurs même si elle ne satisfait pas complètement les conditions requises car les états Utah, Nouveau Mexique, Arizona et Colorado n'ont pas une relation de voisinage convenable.

Ce problème de coloriage de carte peut être traduit dans le langage des graphes. Pour cela, définissons le graphe $G = (V, E)$ comme un graphe dont les états sont les sommets et pour lequel deux sommets sont reliés s'ils sont frontaliers. Il est facile de voir que ce graphe est planaire : en fait, choisir un point arbitraire de chaque état et les relier produit un graphe planaire. Un coloriage de cette carte correspond alors à un coloriage de G. La question est donc de savoir si on peut borner le nombre chromatique des graphes planaires.

Pendant plus de 100 ans, le problème ouvert le plus connu de la théorie des graphes était de savoir si 4 couleurs suffisent à colorier n'importe quel graphe planaire. C'est-à-dire si $\chi(G) \leq 4$ pour tout graphe planaire G. Ce problème a été posé pour la première fois en 1852 par Francis Gutherie. Plus de 100 ans de recherche ont produit un grand nombre de preuves erronées, mais également un grand nombre d'approches prometteuses. Le sommet de tous ces efforts fut le travail d'Appel et d'Haken, qui en 1976 ont prouvé le « théorème des quatre couleurs » en utilisant un ensemble de réductions théoriques et de nombreuses heures de calculs sur des ordinateurs.

Théorème 4.47 (Théorème des quatres couleurs)**.** *Le nombre chromatique d'un graphe planaire est au plus* 4*.*

La preuve de ce théorème dépasse largement le cadre de ce cours. A la place, on va se contenter d'un peu moins. Dans la suite de cette section on va montrer que 5 couleurs suffisent toujours. En d'autres termes, on va montrer le théorème suivant :

Théorème 4.48 (Théorème des cinq couleurs)**.** *Soit G un graphe planaire. Alors $\chi(G) \leq 5$.*

Bien sûr, ce théorème est un corollaire du théorème des quatre couleurs. Mais en raison de la complexité de la preuve de ce dernier, un preuve simple du théorème des cinq couleurs est la bienvenue. Une telle preuve fut donnée par Heawood en 1990. Dans ce cours, on suit une preuve encore plus simple donnée par Thomassen en 1994 qui prouve en fait beaucoup plus que le théorème des cinq couleurs.

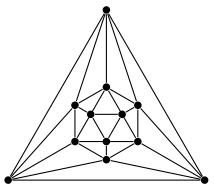
Pour nous échauffer, prouvons le théorème des six couleurs.

Proposition 4.49. *Soit G un graphe planaire, alors $\chi(G) \leq 6$.*

Démonstration. La preuve est très similaire à celle de la proposition 4.45, et utilise une récurrence sur le nombre de sommets de G. Si G n'a qu'un sommet, c'est trivial.

Supposons que G a n sommets, avec $n \geq 2$. En utilisant la proposition 4.40, G a un sommet v de degré au plus 5. On enlève v et toutes les arêtes qui le touchent de G pour obtenir un graphe planaire G' sur $n-1$ sommets. Par hypothèse de récurrence G' est 6-coloriable. Ce qui nous laisse le choix d'au moins une couleur qui n'apparaît pas dans les voisins de v. On peut la choisir pour v et on obtient un coloriage admissible de G. □

Si l'on est capable de montrer que tout graphe planaire a au moins un sommet de degré au plus 4, alors on peut utiliser exactement le même argument pour montrer le théorème des cinq couleurs. Malheureusement, ce n'est pas vrai. Le graphe sur la droite nous donne un contre exemple. Ce graphe est le graphe d'incidence des sommets de l'icosaèdre, qui est l'un des cinq solides de Platon. L'icosaèdre a 20 faces et 12 sommets. Pour cette raison ce graphe est simplement appelé l'icosaèdre.



Théorème 4.50 (Thomassen)**.** *Si G est un graphe planaire, alors* $\mathrm{ch}(G) \leq 5$*.*

Démonstration. On associe à chaque sommet v de G un ensemble $S_v \subseteq \{1, 2, \ldots, 5\}$ de couleurs admissibles et on cherche à construire un coloriage $f\colon V \to \{1, \ldots, 5\}$ tel que pour chaque sommet v, la couleur $f(v)$ appartienne à S_v. On peut supposer que G est dessiné dans le plan. Soit

$$C\colon v_1 - v_2 - \cdots - v_{p-1} - v_p - v_1$$

le « cycle extérieur » du graphe, c'est-à-dire le bord de l'unique face infinie qui entoure le dessin de G. Il est possible que le bord de la face infinie ne forme pas un cycle (penser à un arbre par exemple), dans ce cas pour obtenir un cycle, on complète le graphe par de nouvelles arêtes qui délimitent l'enveloppe convexe du dessin de G. On rajoute également de nouvelles arêtes à G de telle manière que le graphe soit complètement triangulaire. Ainsi on peut supposer que toutes les faces finies de G sont triangulaires. Clairement, il suffit de démontrer le résultat pour ce cas qui est potentiellement plus dur. On rend le problème encore plus difficile en supposant que

$$\begin{aligned} &|S_{v_1}| = |S_{v_2}| = 1 \\ &\forall i,\ 3 \leq i \leq p, \quad |S_{v_i}| \geq 3. \end{aligned}$$

Cette astuce va nous permettre de montrer le résultat par récurrence sur $n = |V|$. Un tel coloriage est dit *admissible*.

Le cas de base avec $p = n = 3$ (et donc $G = C$) est trivial puisqu'au moins l'une des couleurs dans $f(v_3)$ n'a pas encore été utilisée pour v_1 et v_2.

Soit à présent $n \geq 4$. On distingue deux cas.

Cas 1. On suppose que C admet une corde $e = (v, w)$, c'est-à-dire qu'il existe deux sommets v et w du cycle extérieur C qui sont connectés par une arête e dans le graphe. Alors $C \cup \{e\}$ est la réunion de deux cycles C_1 et C_2 qui possèdent l'arête e en commun. De plus, le graphe G peut se diviser en deux sous-graphe G_1 et G_2 délimit'es par C_1 et C_2 respectivement. On peut supposer sans perte de généralité que les sommets v_1 et v_2 appartiennent au cycle C_1. Une illustration de ce cas est donnée sur la figure 4.5. On applique maintenant l'hypothèse de récurrence à C_1 et on obtient un coloriage f_1 du G_1 tel que $f_1(u) \in S_u$ pour

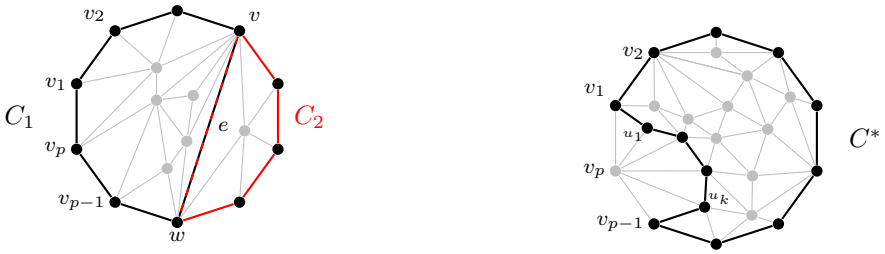


Figure 4.5 – Illustration des deux cas de la démonstration du théorème 4.50.

chaque sommet u du G_1. On définit $S'_v := \{f_1(v)\}$ et $S'_w := \{f_1(w)\}$ et pour tous les autres sommets u de G_2, on pose $S'_u := S_u$. En utilisant d'hypothèse de récurrence, on obtient un coloriage f_2 de G_2 tel que $f_2(u) \in S'_u$ pour chaque sommet u de G_2. Maintenant, on définit

$$f(u) := \begin{cases} f_1(u) & \text{si } u \text{ est un sommet du } G_1 \\ f_2(u) & \text{si } u \text{ est un sommet du } G_2. \end{cases}$$

Comme $f_1(v) = f_2(v)$ et $f_1(w) = f_2(w)$, la fonction f est bien définie. De plus, $f(u) \in S_u$ pour tout u, donc, f est un coloriage admissible parce que f_1 et f_2 sont tous les deux admissibles.

Cas 2. Supposons maintenant que C n'admet pas de corde. Étiquetons les voisins de v_p selon leur ordre naturel (par exemple dans le sens des aiguilles d'une montre) par $v_1, u_1, \ldots, u_k, v_{p-1}$. Alors les u_i appartiennent à l'intérieur de C et comme G est triangulé,

$$P\colon v_1 - u_1 - u_2 - \cdots - u_k - v_{p-1}$$

est un chemin dans G. Comme C n'a pas de corde, $C^* := P \cup (C - \{v_p\})$ est le cycle du bord du sous-graphe $G' := G \setminus \{v_p\}$. La situation est illustrée sur la figure 4.5. Puisque $|S_{v_p}| \geq 3$, il existe au moins deux éléments distincts i, j de l'ensemble $S_{v_p} \setminus S_{v_1}$ (noter que $|S_{v_1}| = 1$). On définit $S'_{u_\ell} := S_{u_\ell} \setminus \{i, j\}$ pour $\ell = 1, \ldots, k$ et $S'_u := S_u$ pour tous les sommets u de G distincts de $u_1, \ldots, u_k, v_p$. D'après l'hypothèse de récurrence, il existe un coloriage f de G' tel que $f(u) \in S_u$ pour tous les sommets u de G'. On étend f à un coloriage admissible de G : soit $a \in \{i, j\}$ un élément tel que $a \neq f(v_{p-1})$. On pose $f(v_p) := a$. Alors, $f(v_p) \in S_{v_p}$, grâce au fait que $\{i, j\} \subseteq S_{v_p}$, $f(v_p) \neq f(v_1)$, $f(v_p) \neq f(v_{p-1})$ grâce à la manière dont on a choisi a, et $f(v_p) \neq f(u_\ell)$ pour $\ell = 1, \ldots, k$ parce que S'_{u_ℓ} et $\{i, j\}$ sont disjoints par construction. Nous avons bien construit un coloriage admissible.

□

La preuve du théorème 4.48 est maintenant triviale compte tenu de la remarque **??**.

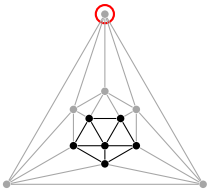
4.5. Ensemble indépendant, clique et partition en clique

Définition 4.51. Soit $G = (V, E)$ un graphe. Un *ensemble indépendant* de G est un ensemble $I \subseteq V$ tel que $I \times I \cap E = \emptyset$. Autrement dit, il n'existe pas d'arête entre deux éléments de I. Un *ensemble indépendant maximal* de G est un ensemble indépendant de cardinalité maximale. Le *nombre d'indépendance*, noté $\alpha(G)$ est la taille d'un ensemble indépendant maximal de G.

Exemple 4.52.

1. $\alpha(K_n) = 1$ pour tout n : comme tous les sommets sont connectés, le nombre d'indépendance est strictement plus petit que 2 et vaut donc 1.
2. $\alpha(C_n) = \lfloor n/2 \rfloor$ pour tout n. On va le prouver dans le cas n pair. Supposons que les sommets de C_n soient indexés dans le sens des aiguilles d'une montre par $0, 1, \ldots, n-1$. Ainsi, le sommet d'index i est connecté avec celui d'index $i-1$ et celui d'index $i+1$, le tout modulo n. Supposons que l'on a un ensemble indépendant de taille t et d'indices $i_1 < i_2 < \cdots < i_t$. Comme il est indépendant, on a $i_{j+1} - i_j \geq 2$ pour $j = 1, \ldots, t-1$. Donc, $n - 2 \geq i_t - i_1 \geq 2t - 2$, ce qui nous montre que $t \leq n/2$. De plus, il est facile de voir que c'est une égalité en prenant l'ensemble des sommets d'indice pair par exemple.

3. Le nombre d'indépendance de $K_{n,m}$ est $\max\{n, m\}$. Clairement, on peut trouver un ensemble indépendant de cette taille car on peut prendre tous les sommets du côté le plus large du graphe biparti. De plus, il ne peut être plus grand car un ensemble indépendant ne peut contenir deux sommets qui ne sont pas du même côté car ils seraient connectés.
4. Le nombre d'indépendance du graphe de Petersen de la figure 4.3 est 4 : clairement, les sommets v_2, v_5, v_8 et v_9 sont indépendant. Prouvons maintenant qu'il n'y a pas d'ensemble indépendant de taille 5. Soit S un ensemble indépendant. Clairement, S ne peut avoir plus de deux sommets sur le cycle extérieur car le nombre d'indépendance de C_5 est 2. De manière similaire, S ne peut avoir plus de deux sommets sur l'étoile intérieure (également isomorphe à C_5). Finalement, S ne peut avoir plus de 4 éléments.
5. Le nombre d'indépendance de l'icosahèdre est 3. Pour voir cela, remarquez que chaque sommet joue un rôle symétrique (en terme de voisinage), on peut donc fixer le premier sommet d'un ensemble indépendant. Par exemple, le sommet du haut du triangle extérieur. On peut alors exclure ses 5 voisins et il nous reste un graphe plus petit pour lequel on doit trouver un ensemble indépendant. Ce graphe correspond aux arêtes en gras de la figure de droite. Il s'agit d'un 5-cycle avec en plus un sommet central connecté à tous les autres. Si ce sommet central appartient à l'ensemble indépendant, aucun des autres sommets du cycle ne peut y appartenir et on obtient un ensemble indépendant de taille 2. Sinon, on est ramené à trouver un ensemble indépendant d'un 5-cycle qui est de cardinal 2. On peut donc conclure que le nombre d'indépendance de l'icosahèdre est 3.



6. Le graphe sur la droite de la figure 4.6 est appelé le *dodécahèdre*. Comme pour l'icosahèdre, c'est le graphe d'incidence des arêtes d'un dodécahèdre, un autre des 5 solides de Platon. On va montrer que le nombre d'indépendance de ce graphe est 8. On peut facilement trouver un ensemble indépendant de taille 8 : R, P, B, X, F ,J, M, T. Montrons qu'on ne peut pas faire mieux. Tout ensemble indépendant ne peut avoir plus de 2 sommets sur le pentagone extérieur, 5 sommets sur le polygone à 10 sommets internes et 2 sommets sur le pentagone intérieur. Le nombre d'indépendance est donc d'au plus 9. Supposons qu'il soit égal à 9. Alors le polygone à 10 sommets internes contiendrait 5 sommets de cet ensemble indépendant. Il n'y a que 2 possibilités, l'ensembe {N,Q,X,J,L}, ou l'ensemble {P,Z,H,K,M}. Dans le premier cas, aucun des sommets du pentagone extérieur ne peut appartenir à cet ensemble indépendant. Dans le second cas, aucun des sommets du pentagone intérieur ne peut appartenir à cet ensemble indépendant. On en conclut que le nombre d'indépendance du dodécahèdre est bien 8.

A partir de ces exemples, il semblerait que trouver le nombre d'indépendance d'un graphe soit une tâche difficile : chaque graphe a besoin d'un raisonnement particulier et il n'y a pas d'algorithme général qui se détache. Cette impression n'est pas loin de la vérité. En fait, la théorie de la complexité montre qu'il s'agit en général d'une tâche très difficile et qu'il est improbable qu'il existe un critère simple qui marche pour tous les graphes.

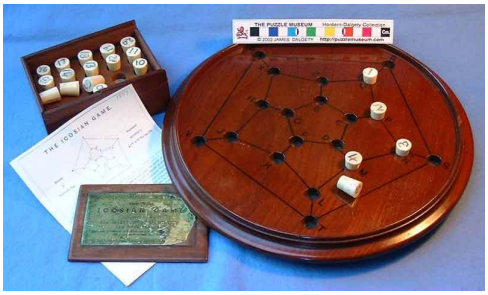
On va maintenant introduire deux autres notions liées au nombre d'indépendance.

Définition 4.53. Soit G un graphe. Une *clique* de taille n dans G est un sous-graphe de G isomorphe à K_n. La taille maximale d'une clique de G est notée $\omega(G)$. La *taille minimale d'une partition en cliques* de G est notée $\theta(G)$.

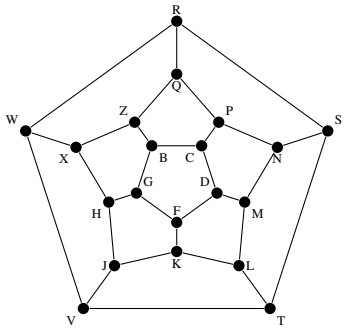
Théorème 4.54. *Soient $G = (V, E)$ un graphe et $\overline{G} = (V, V \times V - E)$ son graphe complémentaire. On a les résultats suivants :*

(1) $\chi(G) \geq \omega(G)$.
(2) $\alpha(G) \leq \theta(G)$.
(3) $\alpha(G) = \omega(\overline{G})$.
(4) $\theta(G) = \chi(\overline{G})$.
(5) $\alpha(G) \leq \chi(\overline{G})$.

Démonstration. (1) Les arêtes d'une clique doivent avoir des couleurs différentes.
(2) Les sommets d'un ensemble indépendant doivent être dans des cliques distinctes.
(3) Les ensembles indépendants de G sont des cliques dans $\overline{G}$.
(4) Un coloriage de $\overline{G}$ est équivalent à une partition de V en clique.
(5) Découle de (2) et (4). □



(a)



(b)

Figure 4.6 – (a) Une version originale du jeu de Sir William Rowan Hamilton « Icosian Game, » avec une description, la plaque qui indique que le jeu était breveté et (b) le graphe qui lui corrrespond.

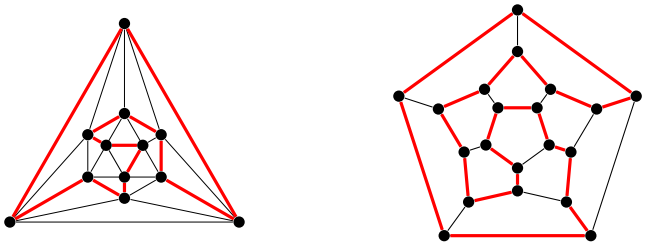
4.6. Cycle hamiltonien

En 1857, le mathématicien et astronome britanique William Rowan Hamilton invente un jeu appelé l'« Icosian Game ». Une image de ce jeu est donné sur la figure 4.6. La description originale du jeu, en anglais, est donné ci-dessous :

> *In this new Game (invented by Sir WILLIAM ROWAN HAMILTON, LL.D., &c., of Dublin, and by him named Icosian from a Greek word signifying 'twenty') a player is to place the whole or part of a set of twenty numbered pieces or men upon the points or in the holes of a board, represented by the diagram above drawn, in such a manner as always to proceed along the lines of the figure, and also to fulfill certain other conditions, which may in various ways be assigned by another player. Ingenuity and skill may thus be exercised in proposing as well as in resolving problems of the game. For example, the first of the two players may place the first five pieces in any five consecutive holes, and then require the second player to place the remaining fifteen men consecutively in such a manner that the succession may be cyclical, that is, so that No. 20 may be adjacent to No. 1 ; and it is always possible to answer any question of this kind. Thus, if B C D F G be the five given initial points, it is allowed to complete the succession by following the alphabetical order of the twenty consonants, as suggested by the diagram itself ; but after placing the piece No. 6 in hole H, as before, it is also allowed (by the supposed conditions) to put No. 7 in X instead of J, and then to conclude with the succession, W R S T V J K L M N P Q Z. Other Examples of Icosian Problems, with solutions of some of them, will be found in the following page.*

Définition 4.55. Un *chemin hamiltonien* sur un graphe G est un chemin $a_0 - a_1 - \cdots - a_m$ avec $V = \{a_0, a_1, \ldots, a_m\}$. En d'autres mots, un chemin hamiltonien visite chaque sommet exactement une fois. Si $a_m = a_0$, on parle de *cycle hamiltonien*.

Exemple 4.56. La figure suivante montre des examples de cycles hamiltoniens sur l'icosahèdre et sur le dodécahèdre :



Remarquez que ces cycles hamiltoniens ne sont pas uniques. ◇

On pourrait penser que les cycles hamiltoniens sont similaires aux cycles eulériens : au lieu de traverser chaque arête exactement une fois, on veut traverser chaque sommet exactement une fois. Néanmoins, il s'agit d'objets complètement différents. La théorie de la complexité révèle qu'une caractérisation simple des graphes qui possèdent un cycle hamiltonien est improbable.

De façons intuitive, il est clair que le problème de trouver un cycle hamiltonien devient plus facile si le graphe a beaucoup d'arêtes. Mais combien d'arêtes sont-elles nécessaires ? Le résultat suivant de Dirac donne une borne possible.

Théorème 4.57 (Théorème de Dirac)**.** *Tout graphe sur n sommets dont le degré de chaque sommet est d'au moins $n/2$ posséde un cycle hamiltonien.*

Démonstration. On utilise une récurrence sur le nombre de paires de sommets non adjacents dans le graphe G. Si G n'a pas de sommets qui ne sont pas voisins, alors c'est un graphe complet. Comme on suppose que tout sommet est de degré au moins $n/2$, on en déduit que G est un graphe complet avec au moins 3 arêtes et contient de manière évident un cycle hamiltonien.

Pour l'étape de récurrence, soit x et y deux sommets non adjacents de G. Considerons le graphe G' qui découle de G en ajoutant une arête e entre x et y. Alors G' a moins de sommets qui ne sont pas voisins et admet donc un cycle hamiltonien par hypothèse de récurrence. Si ce cycle n'utilise pas l'arête e, on a fini car il s'agit également d'un cycle hamiltonien dans G. Sinon, il existe un chemin hamiltonien dans G de x à y, disons $x = v_1 - v_2 - \cdots - v_{n-1} - v_n = y$. Comme x et y sont de degré au moins $n/2$, il existe un indice i tel que y est voisin de v_i et x est voisin de v_{i+1}. (Sinon, quand v_i est voisin de y, v_{i+1} n'est pas voisin de x, et comme il existe au moins $n/2$ indices $i > 1$ tel que v_i est voisin de y, il resterait trop peu de voisins pour x). Ainsi

$$x - v_2 - v_3 - \cdots - v_i - y - v_{n-1} - v_{n-2} - \cdots - v_{i+1} - x$$

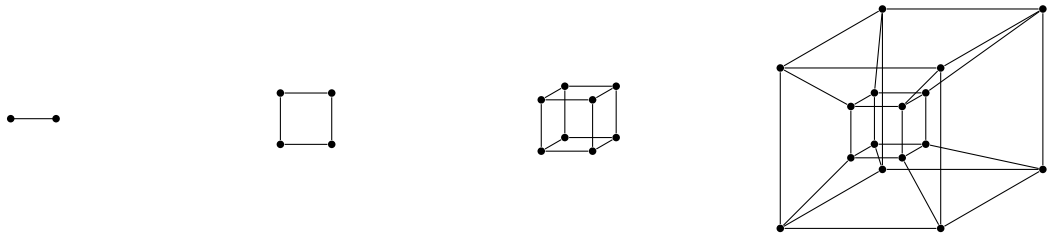
est un cycle hamiltonien de G. □

4.7. Exemple : l'hypercube

Dans cette section on va appliquer certains des concepts que nous avons développés dans ce chapitre sur *l'hypercube*.

Définition 4.58. La *distance de Hamming* $d_H(x, y)$ entre deux vecteurs binaires $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ est le nombre de positions où les deux vecteurs diffèrent : $d_H(x, y) = |\{i \mid x_i \neq y_i\}|$. Le *poids de Hamming* $\mathrm{wgt}_H(x)$ d'un vecteur x est $d_H(x, 0)$, avec 0 le vecteur tout à zéro. C'est-à-dire que le poids de Hamming est le nombre de coordonnées non nulles. Le graphe de l'*hypercube* ou simplement l'*hypercube* $\mathcal{H}_n$ est le graphe $G = (\{0, 1\}^n, E)$ avec $E = \{(x, y) \mid d_H(x, y) = 1\}$.

Exemple 4.59. Voici les hypercubes pour $n = 1, 2, 3, 4$:



$n = 1$ $n = 2$ $n = 3$ $n = 4$

◇

Comme on l'a mentionné dans les dernières sections, il est difficile de déterminer le nombre chromatique ou le nombre d'indépendance de graphes généraux, ou de déterminer si un tel graphe admet un cycle hamiltonien. Mais, pour la famille des hypercubes, ces problèmes se résolvent facilement.

Lemme 4.60. *Soient $x, y \in \{0, 1\}^n$. Alors*

$$\mathrm{wgt}_H(x + y) = \mathrm{wgt}_H(x) + \mathrm{wgt}_H(y) - 2\mathrm{wgt}_H(xy),$$

avec $x + y$ la somme binaire terme à terme de x et y, et xy le produit terme à terme de x et y.

Démonstration. Il suffit de montrer l'affirmation pour $n = 1$, car la fonction poids est additive sur les coordonnées. Une inspection de toutes les valeurs possibles pour x et y nous donne alors le résultat. □

Théorème 4.61. *On a les résultats suivants :*

(1) $\chi(\mathcal{H}_n) = \omega(\mathcal{H}_n) = 2$.

(2) $\alpha(\mathcal{H}_n) = \theta(\mathcal{H}_n) = 2^{n-1}$.

(3) $\mathcal{H}_n$ *admet un cycle hamiltonien.*

Démonstration. (1) Soit f l'application de $\{0,1\}^n \to \{0,1\}$ qui associe 0 à tous les x de poids pair, et 1 à tous les x de poids impair. Pour montrer qu'il s'agit d'un coloriage valide de l'hypercube, il suffit de montrer que tous les vecteurs de poids pair (impair) ne sont pas connectés les uns aux autres dans $\mathcal{H}_n$. Les voisins de $x \in \{0,1\}^n$ sont les vecteurs $x + e_i$, $i = 1, \ldots, n$, avec e_i égal à un en une seule coordonné i. Ainsi, par le lemme 4.60, $\mathrm{wgt}_H(x+e_i) \equiv \mathrm{wgt}_H(x)+1 \bmod 2$, ce qui montre que la parité du poids de x est différente de celles de tous ses voisins. Cela montre que $\chi(\mathcal{H}_n) = 2$. Comme $\mathcal{H}_n$ a des cliques de taille 2 (chaque arête), on a aussi $\omega(\mathcal{H}_n) \geq 2$, de telle manière que dans le théorème 4.54 (1) on ait égalité dans tous les cas.

(2) D'après la discussion ci-dessus, on sait que les vecteurs de poids pair ne sont pas connectés ensemble, ils forment donc un ensemble indépendant. Leur nombre est $\sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{i} = 2^{n-1}$. Si S est un ensemble indépendant, soit S_0 l'intersection de S avec l'ensemble des mots de poids pair et S_1 son intersection avec les mots de poids impair. On a $|S_0| + |S_1| = |S|$. Comme S est indépendant, $S_0 + e_1$ est d'intersection vide avec S_1, où $S_0 + e_1 = \{x + e_1 \mid x \in S_0\}$.

Ainsi, $|S_1| \leq 2^{n-1} - |S_0 + e_1| = 2^{n-1} - |S_0|$, et donc $|S| \leq 2^{n-1}$. Cela montre que $\alpha(\mathcal{H}_n) = 2^{n-1}$. D'un autre côté, $\theta(\mathcal{H}_n) \leq 2^{n-1}$, car on peut partitionner $\mathcal{H}_n$ en 2^{n-1} 2-cliques de la forme $\{x, x+e_1\}$ où x décrit tous les vecteurs de poids pair. En appliquant le théorème 4.54 (2) on voit qu'on a des égalités de partout.

(3) On fait une récurrence sur n. Si $n = 1$, alors il existe bien un cycle hamiltonien. Supposons que $n > 1$. Alors $\mathcal{H}_{n-1}$ a un cycle hamiltonien, disons

$$v_1 - v_2 - \cdots - v_{2^{n-1}} - v_1,$$

avec $\{v_1, \ldots, v_{2^{n-1}}\} = \{0,1\}^{n-1}$. De là, on construit un cycle hamiltonien pour $\mathcal{H}_n$ de la façon suivante. Pour $v \in \{0,1\}^{n-1}$ on note $(1 \mid v)$ le vecteur qui a pour première coordonnée 1 et pour les restantes les mêmes que v. De manière similaire, on définit $(0 \mid v)$. Alors, le cycle suivant est un cycle hamiltonien de $\mathcal{H}_n$:

$$(0 \mid v_1) - (0 \mid v_2) - \cdots - (0 \mid v_{2^{n-1}}) - (1 \mid v_{2^{n-1}}) - (1 \mid v_{2^{n-1}-1}) - \cdots - (1 \mid v_2) - (1 \mid v_1) - (0 \mid v_1).$$

Ce qui termine la preuve. □

Exemple 4.62. Un cycle hamiltonien de $\mathcal{H}_n$ est appelé un *code de Gray* de longueur n. En suivant la méthode de la preuve précédente, on peut obtenir de manière récursive des codes de Gray pour divers n :
Pour $n = 1$ on a

$$0, 1\ .$$

Pour $n = 2$ on a

$$(00), (01), (11), (10)\ .$$

Pour $n = 3$ on a

$$(000), (001), (011), (010), (110), (111), (101), (100)\ .$$

Pour $n = 4$ on a

(0000), (0001), (0011), (0010), (0110), (0111), (0101), (0100),
(1100), (1101), (1111), (1110), (1010), (1011), (1001), (1000) .

◇

Chapitre 5
Dénombrement

5.1. Fonctions génératrices

5.1.1. Séries formelles

Supposons qu'on ait un problème dont la solution soit une suite de nombres $a_0, a_1, \ldots$. On aimerait « savoir » de quelle suite il s'agit. Que veut-on dire par là ? Une réponse possible est d'obtenir une formule close pour les a_n. Par exemple, si on trouve que $a_n = 3n + 1$, on serait satisfait de la réponse. Néanmoins, il n'est pas toujours possible de trouver une forme close. Par exemple pour la suite $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ où a_n est le $n^{\text{ème}}$ nombre premier, il ne serait pas raisonnable d'espérer une expression close. Ainsi, même si une formule simple pour les a_n n'existe pas toujours, il peut être possible de donner une formule pour la somme formelle : $\sum_{n\geq 1} a_n x^n$. Une telle expression est une *série formelle*.

Définition 5.1. Une *série formelle* P est une application f de $\mathbb{N}$ dans $\mathbb{R}$. On représente une série formelle par l'expression $P = \sum_{n\geq 0} f(n)x^n$. Les séries formelles peuvent être additionnées et multipliées à l'aide des règles suivantes :

$$\begin{aligned} \sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n &:= \sum_{n\geq 0} (a_n + b_n) x^n \\ \left(\sum_{n\geq 0} a_n x^n\right) \cdot \left(\sum_{n\geq 0} b_n x^n\right) &:= \sum_{n\geq 0} \left(\sum_{i+j=n} a_i b_j\right) x^n. \end{aligned}$$

L'ensemble des séries formelles est noté $\mathbb{R}[[x]]$.

L'adjectif « formel » veut dire qu'on ne s'intéresse pas à la convergence d'une telle série. On s'intéresse uniquement aux propriétés combinatoires des coefficients d'une telle série.

Théorème 5.2. *L'ensemble $\mathbb{R}[[x]]$ muni des opérations d'addition et de multiplication est un anneau. Les séries formelles $0 = \sum_{n\geq 0} 0x^n$ et $1 = 1 + \sum_{n\geq 1} 0x^n$ sont respectivement les éléments neutres de l'addition et de la multiplication. Un élément $\sum_{n\geq 0} a_n x^n$ est inversible dans cet anneau si et seulement si $a_0 \neq 0$.*

Démonstration. La seule assertion difficile est l'inversibilité. Supposons que $P = \sum_{n\geq 0} a_n x^n$. Soit $Q = \sum_{n\geq 0} b_n x^n$. Si $a_0 = 0$, alors le coefficient x^0 de PQ est 0, ainsi on voit que ce produit ne peut jamais valoir 1 et que donc P n'a pas d'inverse pour la multiplication. Inversement, supposons $a_0 \neq 0$. On veut calculer par récurrence les coefficients b_n de Q de telle manière que $PQ = 1$. Le coefficient de x^0 dans PQ est $a_0 b_0$, donc on doit avoir $b_0 = 1/a_0$. Supposons maintenant qu'on ait déjà calculé pour $n \geq 1$ les coefficients $b_0, b_1, \ldots, b_{n-1}$ de telle manière que les coefficients de $x^1, \ldots, x^{n-1}$ dans PQ soient nuls et que le coefficient de x^0 dans ce produit soit 1. Le coefficient de x^n dans ce produit est $a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0$. Pour qu'il soit nul, on doit poser $b_n = -(a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0)/a_0$, ce que l'on peut faire car $a_0 \neq 0$ par hypothèse. Cette construction termine la preuve. □

Définition 5.3. Si P est une série formelle et Q est son inverse, alors on écrit $Q = 1/P$. Plus généralement, $Q = T/P$ pour des séries formelles Q, T, P veut dire que $PQ = T$.

Proposition 5.4. *On a les identités suivantes dans* $\mathbb{R}[[x]]$ *:*

(1) $1/(1-x) = \sum_{n\geq 0} x^n$.

(2) *Si* a, b, c, d *sont des nombres réels avec* $a \neq b$*, alors on a*

$$\frac{c+dx}{(1-ax)(1-bx)} = \sum_{n\geq 0} (Aa^n + Bb^n)\, x^n,$$

avec $A = (d+ac)/(a-b)$ *et* $B = c - A$*.*

Démonstration. (1) On a $(1-x)\sum_{n\geq 0} x^n = \sum_{n\geq 0} x^n - \sum_{n\geq 1} x^n = 1$.

(2) Un simple calcul nous montre que

$$\frac{c+dx}{(1-ax)(1-bx)} = \frac{A}{1-ax} + \frac{B}{1-bx}.$$

En appliquant le résultat précédent avec ax et bx à la place de x, on obtient l'affirmation. □

Définition 5.5. Soit $a_0, a_1, a_2, \ldots$ une suite de nombre réels. Alors la série formelle $A := \sum_{n\geq 0} a_n x^n$ est appelée la *fonction génératrice* de cette suite.

On est maintenant en mesure de donner un premier exemple de l'utilisation des séries génératrices en obtenant une formule close pour la suite des nombres de Fibonacci.

Théorème 5.6. *Pour* $n \geq 0$*, définissons la suite* F_n *par* $F_0 := 0$*,* $F_1 := 1$*,* $F_n = F_{n-1} + F_{n-2}$ *pour* $n \geq 2$*. alors on a pour tout* n

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Démonstration. Soit $F := \sum_{n\geq 0} F_n x^n$. Comme $F_n - F_{n-1} - F_{n-2} = 0$ pour tout $n \geq 2$, on a

$$F - \sum_{n\geq 1} F_{n-1}x^n - \sum_{n\geq 2} F_{n-2}x^n = F_0 + F_1 x = x.$$

On peut maintenant remarquer que $\sum_{n\geq 1} F_{n-1}x^n = \sum_{n\geq 0} F_n x^{n+1} = xF$. De manière similaire, $\sum_{n\geq 2} F_{n-2}x^n = x^2F$. Ainsi, on a $F(1-x-x^2) = x$, ce qui nous donne

$$F = \frac{x}{1-x-x^2}$$

dans $\mathbb{R}[[x]]$. En utilisant la formule de la proposition 5.4 (2), on obtient le résultat. □

Voici un autre exemple.

Exemple 5.7. Supposons que $a_0, a_1, \ldots$ soit une suite d'entiers avec $a_0 = 0$, et $a_n = 2a_{n-1} + 1$ pour $n \geq 1$. On aimerait trouver une formule close pour a_n. Soit $f := \sum_{n\geq 0} a_n x^n$ la fonction génératrice de cette suite. Alors $f = \sum_{n\geq 1}(2a_{n-1}+1)x^n$. Remarquez que $\sum_{n\geq 1} a_{n-1}x^n = xf$, et que $\sum_{n\geq 1} x^n = 1/(1-x) - 1 = x/(1-x)$, de telle sorte que $f = 2xf + x/(1-x)$. Ou encore $f = x/(1-x)(1-2x)$. En appliquant la proposition 5.4 (b) on en déduit que

$$f = \sum_{n\geq 0}(2^n - 1)x^n,$$

et donc que $a_n = 2^n - 1$ pour $n \geq 0$. ◇

5.1.2. L'opérateur de dérivation

Définition 5.8. L'*opérateur de dérivation* $\partial\colon \mathbb{R}[[x]] \to \mathbb{R}[[x]]$ est définit par $\partial(\sum_{n\geq 0} a_n x^n) := \sum_{n\geq 1} n a_n x^{n-1}$.

L'opérateur de dérivation est similaire à la notion usuelle de « dérivée » que vous avez apprise en analyse, excepté qu'il est juste défini de manière formelle.

Proposition 5.9. *Soient $f, g \in \mathbb{R}[[x]]$. Alors $\partial(f+g) = \partial(f) + \partial(g)$ et $\partial(fg) = \partial(f)g + f\partial(g)$.*

Démonstration. L'affirmation sur la linéarité est triviale. On montre la formule pour le produit en regardant les termes de la « base » des séries formelles x^n : $\partial(x^n \cdot x^m) = \partial(x^{n+m}) = (n+m)x^{n+m-1}$. D'un autre côté, $\partial(x^n)x^m + \partial(x^m)x^n = (n+m)x^{n+m-1}$. □

Corollaire 5.10. *Soient $f, g, h \in \mathbb{R}[[x]]$ et supposons que $f = g/h$. Alors*

$$\partial(f) = \frac{h\partial(g) - g\partial(h)}{h^2}.$$

Démonstration. On sait que $fh = g$ et par la proposition 5.9 on a $h\partial(f) + f\partial(h) = \partial(g)$, c'est-à-dire $h\partial(f) = \partial(g) - f\partial(h)$. En multipliant les deux côtés par h et en remarquant que $fh = g$, on obtient $h^2\partial(f) = h\partial(g) - g\partial(h)$, ce que l'on voulait montrer. □

Une application immédiate de l'opérateur de dérivation est la suivante.

Proposition 5.11. *On a $\sum_{n\geq 0} nx^n = x/(1-x)^2$.*

Démonstration. On a $\sum_{n\geq 0} nx^n = x\sum_{n\geq 0} nx^{n-1} = x\partial(\sum_{n\geq 0} x^n) = x\partial(1/(1-x))$. D'après la proposition précédente $\partial(1/(1-x)) = 1/(1-x)^2$ et on obtient donc l'affirmation. □

Exemple 5.12. Pour $n \geq 0$ soit la suite a_n donnée par $a_0 = 0$ et $a_n = 2a_{n-1} + n$ pour $n \geq 1$. On aimerait trouver une formule close pour a_n. Encore une fois, on construit la série génératrice. Soit $f := \sum_{n\geq 0} a_n x^n = \sum_{n\geq 1} a_n x^n$. Alors $f = 2\sum_{n\geq 1} a_{n-1}x^n + \sum_{n\geq 1} nx^n = 2xf + \sum_{n\geq 0} nx^n$. Ainsi, en utilisant la proposition précédente, on trouve que

$$f = \frac{x}{(1-x)^2(1-2x)}.$$

L'astuce est de trouver les valeurs A, B, C qui vérifient $f = A/(1-x)^2 + B/(1-x) + C/(1-2x)$ (il s'agit de la décomposition en éléments simples de f que vous avez peut être déjà vue en analyse pour intégrer un quotient de polynômes). On a

$$\begin{aligned}\frac{A}{(1-x)^2} + \frac{B}{1-x} + \frac{C}{1-2x} &= \frac{A(1-2x) + B(1-x)(1-2x) + C(1-x)^2}{(1-x)^2(1-2x)} \\ &= \frac{(A+B+C) + (-2A-3B-2C)x + (2B+C)x^2}{(1-x)^2(1-2x)}.\end{aligned}$$

On doit donc avoir

$$\begin{aligned} A + B + C &= 0 \\ -2A - 3B - 2C &= 1 \\ 2B + C &= 0 \end{aligned}$$

L'unique solution de ce système d'équations est $A = B = -1, C = 2$. Ainsi,

$$f = -\frac{1}{(1-x)^2} - \frac{1}{1-x} + \frac{2}{1-2x}.$$

Remarquez que $1/(1-x)^2 = \partial(1/(1-x)) = \sum_{n\geq 0} nx^{n-1} = \sum_{n\geq 0}(n+1)x^n$, que $1/(1-x) = \sum_{n\geq 0} x^n$, et que $2/(1-2x) = \sum_{n\geq 0} 2^{n+1}x^n$. On en déduit

$$f = \sum_{n\geq 0} \left(-n - 2 + 2^{n+1}\right) x^n.$$

Et donc que $a_n = 2^{n+1} - n - 2$ pour tout $n \geq 0$. ◇

5.1.3. Nombre de partitions d'un ensemble à n éléments

Quel est le nombre de partitions en k parties de $\underline{n}$? En d'autres termes, quel est le nombre de relations d'équivalence que l'on peut définir sur $\underline{n}$ et qui ont exactement k classes d'équivalences ? Ce nombre est noté $\left\{ {n \atop k} \right\}$ et est appelé un *nombre de Stirling de seconde espèce*. On va trouver une formule close pour ces nombres à l'aide des fonctions génératrices.

Commençons par traiter les cas particuliers. Si $k > n$, alors de manière évidente $\left\{ {n \atop k} \right\} = 0$. Si $k = 0$ et $n \neq 0$, alors $\left\{ {n \atop k} \right\} = 0$. On définit $\left\{ {0 \atop 0} \right\} = 1$.

Lemme 5.13. *On a pour tout* $(n, k) \neq (0, 0)$ *et* $0 \leq k \leq n$ *:*

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}.$$

Démonstration. Une partition de $\underline{n}$ en k parties peut avoir l'une des deux formes suivantes : soit la partie qui contient l'élément $n-1$ est formée d'un seul élément, soit elle en a plusieurs. Dans le premier cas, on sépare l'élément $n-1$ des autres et on obtient une partition de $\underline{n-1}$ en $k-1$ parties. Dans le second cas, on obtient une partition de $\underline{n-1}$ en k parties. Réciproquement, si on a une partition de $\underline{n-1}$ en $k-1$ on peut créer de façon unique une partition de $\underline{n}$ en k parties en prenant pour la $k^{\text{ème}}$ partie l'élément $n-1$ tout seul. Et si on a une partition de $\underline{n-1}$ en k parties, on peut placer l'élément $n-1$ dans n'importe laquelle de ces parties pour obtenir une partition de $\underline{n}$ en k parties. Pour ce dernier cas il y a donc k possibilités, d'où le résultat. □

Maintenant, pour $k \geq 0$, définissons

$$P_k := \sum_{n \geq 0} \left\{ {n \atop k} \right\} x^n.$$

Remarquez que $P_0 = 1$ avec cette notation. Ainsi, le lemme précédent nous montre que

$$\begin{aligned}
P_k &= \sum_{n \geq 0} \left\{ {n \atop k} \right\} x^n \\
&= \sum_{n \geq k} \left\{ {n \atop k} \right\} x^n \\
&= \sum_{n \geq k} \left\{ {n-1 \atop k-1} \right\} x^n + k \sum_{n \geq k} \left\{ {n-1 \atop k} \right\} x^n \\
&= x \sum_{n \geq k} \left\{ {n-1 \atop k-1} \right\} x^{n-1} + xk \sum_{n \geq k} \left\{ {n-1 \atop k} \right\} x^{n-1} \\
&= xP_{k-1} + kxP_k.
\end{aligned}$$

De là, on obtient

$$P_k = \frac{x}{1-kx} P_{k-1}, \quad P_0 = 1.$$

Ce qui nous montre (par récurrence) que

$$P_k = \frac{x^k}{(1-x)(1-2x)(1-3x)\cdots(1-kx)}.$$

Le but est maintenant de trouver une décomposition en éléments simples de la fonction de droite. Pour cela, il suffit de trouver $a_1, \ldots, a_k$ tels que

$$\frac{1}{(1-x)(1-2x)(1-3x)\cdots(1-kx)} = \sum_{j=1}^{k} \frac{a_j}{1-jx}.$$

Pour cela, pour tout $r = 1, 2, \ldots, k$, on multiplie les deux côtés par $1 - rx$ et on évalue les deux expressions en $x = 1/r$. Ensuite, le terme de droite vaut a_r, alors que le terme de gauche vaut

$$\frac{1}{(1-1/r)(1-2/r)\cdots(1-(r-1)/r)(1-(r+1)/r)\cdots(1-k/r)} = (-1)^{k-r} \frac{r^{k-1}}{(r-1)!(k-r)!}.$$

On voit donc que

$$\begin{aligned} P_k &= \sum_{r=1}^{k}(-1)^{k-r}\frac{r^{k-1}}{(r-1)!(k-r)!}\sum_{n\geq 0} r^n x^{n+k} \\ &= \sum_{n\geq k}\left(\sum_{r=1}^{k}(-1)^{k-r}\frac{r^{k-1}}{(r-1)!(k-r)!}r^{n-k}\right)x^n \\ &= \sum_{n\geq k}\left(\sum_{r=1}^{k}(-1)^{k-r}\frac{r^{n}}{r!(k-r)!}\right)x^n \end{aligned}$$

et donc que

$$\left\{ {n \atop k} \right\} = \sum_{r=1}^{k}(-1)^{k-r}\frac{r^n}{r!(k-r)!}$$

pour $n, k \geq 0$.

5.1.4. Fonctions génératrices caractéristiques

Considérons le problème suivant : étant donné un entier $n \in \mathbb{N}$, trouver le nombre A_n de quadruplets $(a, b, c, d) \in \mathbb{N}^4$ de somme n tels que

- a est divisible par 3,
- b est inférieur à 6,
- c est divisible par 7,
- d est inférieur à 2.

Comme on peut s'en douter, ce problème n'est pas simple. Par exemple, pour $n = 8$, les possibilités sont les suivantes :

a	6	6	6	3	3	3	0	0	0
b	2	1	0	5	4	3	6	1	0
c	0	0	0	0	0	0	0	7	7
d	0	1	2	0	1	2	2	0	1

si bien que $A_8 = 9$. Afin d'étudier de tels problèmes, on introduit la notation suivante :

Définition 5.14. Soit $S \subseteq \mathbb{N}$. On appelle *fonction génératrice caractéristique de* S, et on note C_S, la fonction

$$C_S := \sum_{n\geq 0}\chi_S(n)x^n,$$

où $\chi_S(n) = 1$ si $n \in S$ et $\chi_S(n) = 0$ sinon.

Exemple 5.15. Supposons que S soit l'ensemble des entiers divisibles par un entier non-nul d. Alors $C_S = \sum_{n\geq 0} x^{dn} = 1/(1-x^d)$.

On dispose du résultat suivant :

Théorème 5.16. *Soient $S, T \subseteq \mathbb{N}$ et soit $A_n := |\{(a, b) \in S \times T \mid a + b = n\}|$. Alors*

$$\sum_{n\geq 0} A_n x^n = C_S \cdot C_T.$$

Démonstration. On a

$$C_S C_T = \sum_{n\geq 0}\left(\sum_{k=0}^{n}\chi_S(k)\chi_T(n-k)\right)x^n.$$

Notons que $\chi_S(k)\chi_T(n-k) = 1$ ssi $k \in S, n-k \in T$ et $\chi_S(k)\chi_T(n-k) = 0$ sinon. Il s'ensuit que

$$\sum_{k=0}^{n}\chi_S(k)\chi_T(n-k) = |\{(m, n-m) \mid m \in S, n-m \in T\}| = |\{(a, b) \in S \times T \mid a + b = n\}| = A_n,$$

ce qui prouve le théorème. □

En raisonnant par récurrence, le résultat précédent s'étend comme suit :

Théorème 5.17. *Soient $S_1, S_2, \ldots, S_t \subseteq \mathbb{N}$, et pour $n \in \mathbb{N}$ posons*

$$A_n := \{(a_1, \ldots, a_t) \in S_1 \times \cdots \times S_t \mid a_1 + \cdots + a_t = n\}.$$

Alors on a

$$\sum_{n\geq 0} A_n x^n = C_{S_1} \cdot C_{S_2} \cdots C_{S_t}.$$

Armé de ce résultat, nous pouvons désormais résoudre le problème de dénombrement du début du paragraphe. À cette fin, soient S_1 l'ensemble des entiers divisibles par 3, S_2 l'ensemble des entiers inférieurs à 6, S_3 l'ensemble des entiers inférieurs à 7 et S_4 l'ensemble des entiers inférieurs à 2. On a alors

$$\begin{aligned} C_{S_1} &= \sum_{n\geq 0} x^{3n} = \frac{1}{1-x^3} \\ C_{S_2} &= 1 + x + \cdots + x^6 = \frac{1-x^7}{1-x} \\ C_{S_3} &= \sum_{n\geq 0} x^{7n} = \frac{1}{1-x^7} \\ C_{S_4} &= 1 + x + x^2 = \frac{1-x^3}{1-x}. \end{aligned}$$

Ainsi, grâce au théorème 5.17, si $A_n = |\{(a,b,c,d) \in S_1 \times \cdots \times S_4 \mid a+b+c+d = n\}|$, alors

$$\sum_{n\geq 0} A_n x^n = \prod_{i=1}^{4} C_{S_i} = \frac{1}{1-x^3}\frac{1-x^7}{1-x}\frac{1}{1-x^7}\frac{1-x^3}{1-x} = \frac{1}{(1-x)^2}.$$

Comme $1/(1-x)^2 = \partial(1/(1-x)) = \sum_{n\geq 0}(n+1)x^n$, on en déduit que $A_n = n+1$.

Comme autre exemple, calculons pour tout $n \in \mathbb{N}$ le nombre B_n de triplets $(a,b,c) \in \mathbb{N}^3$ tels que $a+b+c = n$. Dans ce cas, $S_1 = S_2 = S_3 = \mathbb{N}$ et on a

$$\sum_{n\geq 0} B_n x^n = \left(\frac{1}{1-x}\right)^3.$$

Mais $\frac{1}{(1-x)^3} = \partial(1/(1-x)^2)/2$, si bien que

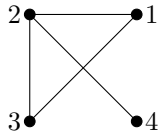
$$\begin{aligned} \sum_{n\geq 0} B_n x^n &= \frac{1}{(1-x)^3} \\ &= \frac{1}{2}\partial\left(\frac{1}{(1-x)^2}\right) \\ &= \frac{1}{2}\sum_{n\geq 0} n(n+1)x^{n-1} \\ &= \frac{1}{2}\sum_{n\geq 0}(n+1)(n+2)x^n \\ &= \sum_{n\geq 0}\binom{n+2}{2}x^n, \end{aligned}$$

et finalement $B_n = \binom{n+2}{2}$.

5.2. Double comptage

Théorème 5.18. *Soit G un graphe avec n sommets qui ne contient pas $K_{2,2}$ comme sous-graphe. Alors G a au plus $(n^{3/2}+n)/2$ arêtes.*

Démonstration. Notons V l'ensemble des sommets de G et E l'ensemble de ses arêtes. Considérons alors la matrice M avec $\binom{n}{2}$ lignes et n colonnes : les lignes de cette matrice sont indexées par les ensembles $\{v, v'\}$ avec $v, v' \in V$; les colonnes sont indexées par les éléments de V. Il y a un 1 à l'intersection d'une ligne $\{v, v'\}$ et d'une colonne u ssi v et v' sont tous deux voisins de u. Voici un exemple de la matrice M pour le graphe ci-dessous :



	1	2	3	4
{1,2}	0	0	1	0
{1,3}	0	1	0	0
{1,4}	0	1	0	0
{2,3}	1	0	0	0
{2,4}	0	0	0	0
{3,4}	0	1	0	0

On va compter le nombre N de 1 dans cette matrice de deux façons différentes : colonne par colonne et ligne par ligne. Dans chaque ligne, on a au plus un 1, sinon il existe deux sommets $v, v' \in V$ et deux sommets $u, u' \in V$ tels que v et v' sont tous deux voisins de u et de u'. C'est une contradiction car le graphe ne contient pas de sous-graphe isomorphe à $K_{2,2}$ par hypothèse. Ainsi, N est majoré par le nombre de lignes de M, c'est-à-dire $N \leq \binom{n}{2}$. Regardons maintenant le nombre de 1 dans une colonne correspondant à $u \in V$. Si u est de degré d, alors cette colonne a $\binom{d}{2}$ 1, un pour chaque paire de sommets auxquels u est relié. Si $d_1, \ldots, d_n$ est la suite des degrés de G, on a donc

$$N = \sum_{i=1}^{n} \binom{d_i}{2} \leq \binom{n}{2},$$

ce qui nous donne

$$\sum_{i=1}^{n} (d_i - 1)^2 < 2 \sum_{i=1}^{n} \binom{d_i}{2} \leq 2\binom{n}{2} < n^2.$$

En appliquant maintenant l'inégalité de Cauchy-Schwarz aux vecteurs $x = (d_1 - 1, \ldots, d_n - 1)$ et $y = (1, 1, \ldots, 1)$ de $\mathbb{R}^n$ on obtient

$$||y \cdot x||^2 = \left(\sum_{i=1}^{n} (d_i - 1) \right)^2 \leq ||y||^2 ||x||^2 = n \sum_{i=1}^{n} (d_i - 1)^2 \leq n^3,$$

c'est-à-dire $\sum_{i=1}^{n} (d_i - 1) \leq n^{3/2}$ et

$$|E| = \frac{1}{2} \sum_{i=1}^{n} d_i \leq \frac{1}{2}(n^{3/2} + n).$$

Cela termine la preuve. □

Théorème 5.19 (Plotkin)**.** *Supposons que l'on ait N vecteurs binaires de dimension n tels que la distance de Hamming entre n'importe quelle paire de vecteurs soit au moins d. Alors, si $d > n/2$, on a $N \leq 2d/(2d - n)$.*

Démonstration. On écrit les N vecteurs dans une matrice A de taille $N \times n$ pour laquelle chaque ligne correspond à l'un de ces vecteurs. Notons S l'ensemble de ces vecteurs. On aimerait calculer le nombre $M := \sum_{x,y \in S, x \neq y} d_H(x, y)$ de deux façons différentes, où $d_H(x, y)$ est la distance de Hamming entre x et y.

Premièrement, comme on sait que $d_H(x, y) \geq d$, on obtient

$$M \geq dN(N - 1),$$

car il y a $N(N-1)$ paires ordonnées d'éléments de S. Ensuite, on regarde les colonnes de la matrice A. Supposons que l'on ait m_i 1 dans la $i^{\text{ème}}$ colonne. Alors la contribution de cette colonne à M est $2m_i(N - m_i)$: c'est le nombre de paires de vecteurs qui diffèrent sur la position i. Ainsi

$$dN(N-1) \leq M = \sum_{i=1}^{n} 2m_i(N - m_i) = \sum_{i=1}^{n} (N^2 - (m_i^2 + (N - m_i)^2)) \leq nN^2 - \frac{1}{2} \sum_{i=1}^{n} (m_i + N - m_i)^2 = \frac{nN^2}{2}.$$

Finalement, $d(N - 1) \leq nN/2$, i.e., $N(2d - n) \leq 2d$, ce qui implique notre affirmation. □

5.3. La méthode probabiliste

Dans cette section, nous nous intéressons à démontrer l'existence de certaines structures combinatoires. Pour cela, la méthode probabiliste consiste à définir une variable aléatoire dont l'espérance correspond au nombre moyen de telles structures. En montrant que cette espérance est positive, on peut ainsi montrer l'existence de telles structures. On va montrer quelques exemples de cette méthode.

5.3.1. 2-Coloriage d'ensemble

Définition 5.20. Soient X un ensemble fini et $\mathcal{M} \subseteq P(X)$. $\mathcal{M}$ est dit 2-*coloriable* s'il existe une fonction $f\colon X \to \{0,1\}$ telle que pour tout $S \in \mathcal{M}$ il existe $x, y \in S$ tels que $f(x) \neq f(y)$, c'est à dire que tous les éléments de $\mathcal{M}$ contiennent les deux couleurs.

Supposons que chaque ensemble dans $\mathcal{M}$ a exactement k éléments. Quel est la plus petite taille $m(k)$ de $\mathcal{M}$ pour laquelle $\mathcal{M}$ n'est pas 2-coloriable ? Pour s'échauffer, voici un résultat.

Proposition 5.21. *On a* $m(2) = 3$.

Démonstration. Dans ce cas, les sous-ensembles dans $\mathcal{M}$ peuvent être vus comme des arêtes d'un graphe avec comme sommets X et on veut savoir quand le graphe est biparti. S'il n'est pas biparti, il a au moins 3 arêtes et donc $m(2) \geq 3$. D'un autre côté, si $|X| = 3$ et $\mathcal{M}$ est l'ensemble de tous les sous-ensembles à 2 éléments de X, alors $\mathcal{M}$ n'est pas 2-coloriable. On a donc $m(2) \leq 3$ et donc $m(2) = 3$. □

Trouver $m(3)$ est déjà plus difficile comme on le verra en exercice. Avec la méthode probabiliste, on va montrer le théorème suivant :

Théorème 5.22. *On a* $m(k) \geq 2^{k-1}$*, c'est-à-dire, si* $\mathcal{M}$ *contient moins de* 2^{k-1} *éléments, alors il est* 2*-coloriable.*

Démonstration. La stratégie de la preuve est la suivante : on va colorier les éléments de X aléatoirement. On assigne ainsi à chaque élément de manière aléatoire et indépendante une valeur 0 ou 1, chacune avec probabilité $1/2$. Ensuite, on va calculer une borne supérieure sur la probabilité qu'un ensemble de $\mathcal{M}$ soit monochromatique. Si cette probabilité est plus petite que 1, alors on aura montré que la probabilité qu'aucun des éléments de $\mathcal{M}$ soit monochromatique est positive, c'est-à-dire qu'il existe un 2-coloriage de $\mathcal{M}$.

Soit $m = |\mathcal{M}|$ et pour $i = 1, \ldots, m$ soit A_i l'événement « l'ensemble numéro i est monochromatique ». Alors $\Pr[A_i] = 2 \cdot 2^{-k}$: la probabilité que tous les éléments du $i^{\text{ème}}$ ensemble aient la valeur 0 est 2^{-k}, de même pour la valeur 1. La probabilité qu'il y ait un ensemble de $\mathcal{M}$ monochromatique est donc

$$\Pr[A_1 \cup A_2 \cup \cdots \cup A_m] \leq \sum_{i=1}^{m} \Pr[A_i] = m2^{1-k}.$$

Ainsi, si $m < 2^{k-1}$, cette probabilité est plus petite que 1 et la probabilité de l'événement contraire est strictement positive. On vient de montrer que $\mathcal{M}$ est 2-coloriable. □

5.3.2. Le nombre d'indépendance

Théorème 5.23. *Soit* $G = (V, E)$ *un graphe. Alors*

$$\alpha(G) \geq \sum_{v \in V} \frac{1}{\deg(v) + 1}.$$

Démonstration. Sans perte de généralité on peut supposer que $V = \underline{n}$. Soit π une variable aléatoire sur l'ensemble des permutations de V, avec $\Pr[\pi] = 1/n!$. Soit $M(\pi)$ l'ensemble de tous les sommets $v \in V$ tels que pour tous les voisins w de v on ait $\pi(w) > \pi(v)$. Alors, $M(\pi)$ est un ensemble indépendant : sinon, si $v, w \in M(\pi)$ et $(v, w) \in E$, alors $\pi(v) > \pi(w)$ et $\pi(w) > \pi(v)$, ce qui n'est pas possible. On en déduit pour tout π :

$$\alpha(G) \geq |M(\pi)|.$$

Notez que $M(\pi)$ est une variable aléatoire sur $P(V)$, l'ensemble des parties de V. Pour montrer l'affirmation, il suffit de montrer que $\mathrm{E}[|M(\pi)|]$ est plus grande que la partie droite dans la formule du théorème, avec $\mathrm{E}[|M(\pi)|]$

l'espérance de $M(\pi)$. Cela provient du fait que $\mathrm{E}[|M(\pi)|]$ est la taille moyenne de $M(\pi)$ et que si cette taille moyenne est d'au moins q, alors il existe certains π pour lesquels $M(\pi)$ a au moins q éléments. On a

$$\mathrm{E}[|M(\pi)|] = \sum_{v \in V} \Pr[v \in M(\pi)].$$

Si π est une permutation choisie aléatoirement et uniformément parmi l'ensemble de toutes les permutations de V, alors tous les ordres possibles de l'ensemble $N_v \cup \{v\}$ sont équiprobables, avec N_v l'ensemble des voisins de v. Il s'ensuit que la probabilité que $\pi(v)$ est plus petite que $\pi(w)$ pour tout $w \in N_v$ est $1/(\deg(v)+1)$, donc

$$\mathrm{E}[|M(\pi)|] = \sum_{v \in V} \frac{1}{\deg(v)+1},$$

ce qui prouve le théorème. □

5.3.3. Grand sous-graphe biparti

Théorème 5.24. *Soit $G = (V, E)$ un graphe avec $2n$ sommets et $m > 0$ arêtes. Alors il existe une partition de V en sous-ensembles A et B, chacun de taille n, tel qu'il y a au moins $m/2$ arêtes entre A et B, c'est-à-dire, $|\{(x, y) \in E \mid x \in A \wedge y \in B\}| \geq m/2$.*

Démonstration. On choisit un sous-ensemble A de taille n de V de manière uniforme et aléatoire parmi tous les $\binom{2n}{n}$ choix possibles et l'on pose $B := V - A$. Ainsi, A est une variable aléatoire. Soit N le nombre d'arêtes entre A et B. N est également une variable aléatoire. On va montrer que $\mathrm{E}[N] \geq m/2$, ce qui montre qu'il existe un ensemble A tel que le nombre d'arêtes entre A et B est d'au moins $m/2$.

Pour calculer $\mathrm{E}[N]$, on va, pour toute arête du graphe, calculer la probabilité que cette arête relie un sommet de A à un sommet de B. Plus précisément, pour toute arête e on définit la variable aléatoire X_e sur $\{0, 1\}$ dont la valeur est zéro ssi les deux sommets de e appartiennent tous les deux à A ou à B. Alors $N = \sum_{e \in E} X_e$ et par linéarité de l'espérance, $\mathrm{E}[N] = \sum_{e \in E} E[X_e]$. Remarquez que $\mathrm{E}[X_e] = 1 \Pr[X_e = 1] + 0 \Pr[X_e = 0] = \Pr[X_e = 1]$, donc

$$\mathrm{E}[N] = \sum_{e \in E} \Pr[X_e = 1].$$

On va montrer que $\Pr[X_e = 1] > 1/2$. Pour cela, soient u et v les deux sommets de l'arête e. Si on impose que $u \in A$, mais que $v \notin A$, alors on peut choisir les $n-1$ éléments restants de A de $\binom{2n-2}{n-1}$ façons. On obtient le même nombre de choix pour A si on impose que $u \notin A$ et $v \in A$. Ainsi,

$$\Pr[X_e = 1] = 2\frac{\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1} > \frac{1}{2}.$$

On en déduit que $\mathrm{E}[N] = \sum_{e \in E} \frac{n}{2n-1} > \sum_{e \in E} 1/2 = m/2$, ce qui prouve le théorème. □