*INSA de Lyon*

**2009**

# Introduction aux mathématiques discrètes

**Marc C. Robini**

CREATIS (UMR CNRS 5220, U 630 INSERM) bât. Blaise Pascal

*marc.robini@creatis.insa-lyon.fr*

*Département Biosciences*

**Filière Bioinformatique et Modélisation**

# Table des matières

# Chapitre 1

# Fondations

**Logique** (propositionnelle du premier ordre)

- ♢ Nécessaire à la spécification et à la compréhension des énoncés mathématiques.
- ♢ Constitue la base du raisonnement mathématique et du raisonnement artificiel.

**Techniques de preuve**

- ♢ Comprendre l'articulation des preuves mathématiques et le raisonnement par induction.
- ♢ Notions utiles pour le raisonnement artificiel et dans les preuves de programme.

**Rappels fondamentaux**

- ♢ Calcul ensembliste.
- ♢ Fonctions.

## 1.1 Calcul propositionnel et calcul des prédicats

### 1.1.1 Opérations logiques et formules propositionnelles

**Définition 1.1** *On appelle proposition un énoncé dont on peut dire sans ambiguïté s'il est vrai ou faux. Un symbole représentant une proposition est appelé variable propositionnelle.*

**Exemple 1.1** "$2+3=5$" et "$\pi \in [6,7]$" sont deux propositions (respectivement vraie et fausse) tandis que "votez Bob !" et "la présente affirmation est fausse" n'en sont pas.

**Définition 1.2** *On appelle connecteur une opération permettant de créer de nouvelles propositions à partir de propositions existantes.*

On appelle *négation* le connecteur unaire noté $\neg$ défini par la table de vérité suivante (véracité et fausseté sont respectivement symbolisées par 1 et 0) :

| $p$ | $\neg p$ ("non $p$") |
|---|---|
| 1 | 0 |
| 0 | 1 |

Les connecteurs binaires usuels sont la *conjonction* (ou "et logique") notée $\wedge$, la *disjonction* (ou "ou inclusif") notée $\vee$, l'*implication* notée $\rightarrow$ et l'*équivalence* notée $\leftrightarrow$ :

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ | $p \rightarrow q$ | $p \leftrightarrow q$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 |

Remarques. (i) L'implication $p \rightarrow q$ symbolise les énoncés du type "$p$ entraîne $q$", "si $p$ alors $q$", "$q$ si $p$", "$p$ est une condition suffisante pour $q$" ou encore "$q$ est une condition nécessaire pour $p$".
(ii) L'équivalence traduit les énoncés du type "$p$ si et seulement si $q$" ($p$ ssi $q$) ou "$p$ est une condition nécessaire et suffisante pour $q$".

**Exercice 1.1** Construire la table de vérité des formules propositionnelles suivantes.

1. $(p \to q) \vee (\neg p \to q)$ ;
2. $\neg p \to (q \to r)$.

**Définition 1.3** *Soit $S$ un ensemble de variables propositionnelles et soient $\mathbf{V}$ et $\mathbf{F}$ des symboles représentant respectivement les propositions toujours vraie et toujours fausse. Une formule propositionnelle est une suite de symboles pris dans $S \cup \{\mathbf{V}, \mathbf{F}, \neg, \wedge, \vee, (\ , \ )\}$ satisfaisant les règles de construction suivantes.*

1. *Tout élément de $S \cup \{\mathbf{V}, \mathbf{F}\}$ est une formule.*
2. *Si $\varphi$ est une formule, alors $\neg\varphi$ est une formule.*
3. *Si $\varphi$ et $\psi$ sont deux formules, alors $(\varphi \wedge \psi)$ et $(\varphi \vee \psi)$ sont des formules.*
4. *Toute formule est obtenue par application des règles 1 à 3 ci-dessus un nombre fini de fois.*

Remarques. (i) Une formule propositionnelle n'est qu'une suite de symboles et est donc dénuée de sens. La précision de la signification d'une formule propositionnelle, c'est-à-dire le fait de lui attribuer une valeur "vrai" ou "faux", constitue le rôle de la *sémantique*. Cet aspect est ici dissimulé par souci de clarté.
(ii) La définition 1.3 fait uniquement appel aux connecteurs $\neg$, $\wedge$ et $\vee$. Leur combinaison permet de construire n'importe quel connecteur binaire (il en existe 16 au total) et il est même possible de supprimer $\wedge$ ou $\vee$.
(iii) "$\neg$" est prioritaire sur les connecteurs binaires dans l'interprétation d'une formule et l'usage est de ne pas écrire les deux parenthèses extérieures.

**Exercice 1.2** Écrire la formule propositionnelle traduisant l'affirmation "je lirai ce support de cours si j'ai du temps libre et si je n'ai pas de temps libre alors je perdrai ma dignité à l'examen"

**Définition 1.4** *On appelle tautologie une formule propositionnelle qui demeure vraie quelles que soient les valeurs des variables qui la composent (e.g., $p \vee \neg p$). À l'opposé, une formule propositionnelle qui est toujours fausse (e.g., $p \wedge \neg p$) s'appelle une contradiction.*

**Définition 1.5** *On dit qu'une formule propositionnelle $\varphi$ implique logiquement une formule $\psi$, ce que l'on note $\varphi \Rightarrow \psi$, si $\varphi \to \psi$ est une tautologie (autrement dit, $\varphi \Rightarrow \psi$ si $\psi$ est vraie à chaque fois que $\varphi$ est vraie).*

**Définition 1.6** *Deux formules propositionnelles $\varphi$ et $\psi$ sont dites logiquement équivalentes, ce que l'on note $\varphi \Leftrightarrow \psi$, si $\varphi \leftrightarrow \psi$ est une tautologie (autrement dit, $\varphi \Leftrightarrow \psi$ si $\varphi$ et $\psi$ possèdent la même table de vérité).*

### 1.1.2 Identités logiques

Les équivalences logiques les plus fréquemment utilisées sont appelées *identités logiques*.

| | |
|---|---|
| Identité | $p \wedge \mathbf{V} \Leftrightarrow p, \quad p \vee \mathbf{F} \Leftrightarrow p$ |
| Domination | $p \vee \mathbf{V} \Leftrightarrow \mathbf{V}, \quad p \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$ |
| Idempotence | $p \wedge p \Leftrightarrow p, \quad p \vee p \Leftrightarrow p$ |
| Double négation | $\neg(\neg p) \Leftrightarrow p$ |
| Exclusivité | $p \vee \neg p \Leftrightarrow \mathbf{V}$ |
| Contradiction | $p \wedge \neg p \Leftrightarrow \mathbf{F}$ |
| Commutativité | $p \wedge q \Leftrightarrow q \wedge p, \quad p \vee q \Leftrightarrow q \vee p$ |
| Associativité | $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r, \quad p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$ |
| Distributivité | $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$, |
| | $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ |
| Absorption | $p \wedge (p \vee q) \Leftrightarrow p, \quad p \vee (p \wedge q) \Leftrightarrow p$ |
| Lois de Morgan | $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q, \quad \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ |
| Contre-apposition | $p \to q \Leftrightarrow \neg q \to \neg p$ |
| Implication par disjonction | $p \to q \Leftrightarrow \neg p \vee q$ |
| Équivalence par implications | $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$ |
| Exportation | $p \to (q \to r) \Leftrightarrow (p \wedge q) \to r$ |

**Table 1.1** — Identités logiques.

**Exercice 1.3** En utilisant des identités logiques, démontrer
1. $\big(\neg q \wedge (p \to q)\big) \Rightarrow \neg p$ ;
2. $\neg(p \leftrightarrow q) \Leftrightarrow \neg p \leftrightarrow q$.

### 1.1.3 Prédicats et quantificateurs

Le calcul propositionnel ne permet pas de formuler des énoncés du type "telle propriété est vraie pour tous les éléments de l'ensemble $E$" ou "telle propriété est vraie pour au moins (ou exactement) un élément de $E$". Les notions de prédicat et de quantificateur permettent de lever ces limitations.

**Définition 1.7** *On appelle prédicat une application qui associe une proposition à chaque élément d'un ensemble $E$ appelé univers. Plus généralement, un prédicat sur $E$ est une application $P$ définie sur $E^n$ $(n \geqslant 1)$ à valeurs dans l'ensemble des propositions.*

**Définition 1.8** *Soit $P$ un prédicat défini sur un univers $E$.*

- ♢ *La quantification universelle de $P$ est la proposition notée $(\forall\, x \in E)P(x)$ ou $(\forall\, x)P(x)$ qui est vraie si et seulement si $P(c)$ est vraie pour tout élément $c$ de $E$.*
- ♢ *La quantification existentielle de $P$ est la proposition notée $(\exists\, x \in E)P(x)$ ou $(\exists\, x)P(x)$ qui est vraie si et seulement s'il existe au moins un élément $c$ de $E$ tel que $P(c)$ est vraie.*
- ♢ *La quantification existentielle unique de $P$ est la proposition notée $(\exists\,!\, x \in E)P(x)$ ou $(\exists\,!\, x)P(x)$ qui est vraie si et seulement s'il existe un unique élément $c$ de $E$ tel que $P(c)$ est vraie.*

**Exemple 1.2** Considérons l'énoncé "tout nombre complexe égal à son conjugué est un nombre réel". Ceci revient à dire "pour tout $z \in \mathbb{C}$, si $z = \overline{z}$, alors $z \in \mathbb{R}$," ce qui se formule de la manière suivante : $(\forall\, z \in \mathbb{C})\big[(z = \overline{z}) \to (z \in \mathbb{R})\big]$. L'univers considéré étant $\mathbb{C}$, l'application $P : z \in \mathbb{C} \mapsto ((z = \overline{z}) \to (z \in \mathbb{R}))$ est un prédicat que la quantification universelle $(\forall\, z \in \mathbb{C})P(z)$ transforme en proposition (vraie).

Remarques. (i) La quantification existentielle unique peut s'exprimer à l'aide des quantificateurs universel et existentiel :

$$(\exists\,!\, x)P(x) \Leftrightarrow (\exists\, x)\big[P(x) \wedge (\forall\, y)[(y \neq x) \to \neg P(y)]\big].$$

(ii) Par abus de notation, la véracité d'une proposition quantifiée dont le prédicat est une implication (resp. une équivalence) s'exprime souvent en remplaçant le symbole $\to$ (resp. $\leftrightarrow$) par $\Rightarrow$ (resp. $\Leftrightarrow$). Ainsi, par exemple, $(\forall\, x)\big[P(x) \Rightarrow Q(x)\big]$ signifie "$(\forall\, x)\big[P(x) \to Q(x)\big]$ est vraie".

**Exercice 1.4** Symboliser les énoncés suivants.

1. "Tout entier pair supérieur ou égal à 4 est la somme de deux nombres premiers" ;
2. "Un polynôme de degré $n \geqslant 1$ ne peut s'annuler plus de $n$ fois".

**Univers dépendant d'une variable.** Pour tous les résultats présentés dans le reste de ce paragraphe, on suppose que l'univers de chaque variable ne dépend pas d'une autre variable. Dans le cas contraire, on fera appel aux équivalences qui suivent. Étant donnés deux ensembles $E$ et $F$ tels que $E \subset F$, on a

$$(\forall\, x \in E)P(x) \Leftrightarrow (\forall\, x \in F)\big[(x \in E) \to P(x)\big]\,,$$
$$(\exists\, x \in E)P(x) \Leftrightarrow (\exists\, x \in F)\big[(x \in E) \wedge P(x)\big]\,.$$

En particulier, $(\forall x \in \emptyset)P(x)$ est vraie et $(\exists x \in \emptyset)P(x)$ est fausse.

**Exemple 1.3** Pour $x, y, z \in \mathbb{R}$, la proposition $(\forall\, x \in \mathbb{R})(\exists\, y \in [\mathrm{e}^x, +\infty[\,)(\forall\, z \in [0, y])P(x, y, z)$ est équivalente à $(\forall\, x \in \mathbb{R})(\exists\, y \in \mathbb{R})(\forall\, z \in \mathbb{R})\big[(y \in [\mathrm{e}^x, +\infty[\,) \wedge \big((z \notin [0, y]) \vee P(x, y, z)\big)\big]$.

**Règles d'interversion.** Deux quantificateurs adjacents de même type peuvent être intervertis sans changer la signification d'un énoncé :

$$(\forall\, x)(\forall\, y)P(x, y) \Leftrightarrow (\forall\, y)(\forall x)P(x, y)\,,$$
$$(\exists\, x)(\exists\, y)P(x, y) \Leftrightarrow (\exists\, y)(\exists\, x)P(x, y)$$

(on autorisera de ce fait les notations du type $(\forall\, x, y)P(x, y)$ ou $(\exists\, x, y)P(x, y)$).
En revanche, l'interversion de quantificateurs adjacents de types différents peut changer la signification d'un énoncé :

$$(\exists\, x)(\forall\, y)P(x, y) \Rightarrow (\forall\, y)(\exists\, x)P(x, y)\,,$$
$$\text{MAIS} \quad (\forall\, y)(\exists\, x)P(x, y) \not\Rightarrow (\exists\, x)(\forall\, y)P(x, y)\,.$$

**Exemple 1.4** $(\forall\, y \in \mathbb{C})(\exists\, x \in \mathbb{C})\big[x + y = 0\big]$ est une proposition vraie (tout nombre complexe est symétrisable pour $+$) tandis que $(\exists\, x \in \mathbb{C})(\forall\, y \in \mathbb{C})[x + y = 0]$ est une proposition fausse (il existe un opposé "universel").

**Règles de négation.** On a les équivalences suivantes :

$$\neg(\forall\, x)P(x) \Leftrightarrow (\exists\, x)\neg P(x)\,,$$
$$\neg(\exists\, x)P(x) \Leftrightarrow (\forall\, x)\neg P(x)\,.$$

**Exercice 1.5** Exprimer $\neg(\exists\,!\, x)P(x)$ sans faire appel à la négation.

**Exercice 1.6** Réécrire les propositions qui suivent de façon à ce qu'aucun quantificateur ne soit précédé par un opérateur de négation.

1. $\neg\big((\exists x)(\exists y)\neg P(x,y) \wedge (\forall x)(\forall y)Q(x,y)\big)$ ;
2. $\neg(\forall x)\big[(\exists y)(\forall z)P(x,y,z) \wedge (\exists z)(\forall y)P(x,y,z)\big]$.

**Formes normales.** Une proposition est dite sous forme *normale* si tous ses quantificateurs apparaissent en tête. On a les équivalences suivantes ($A$ représente une proposition) :

$$A \vee (\forall\, x)P(x) \Leftrightarrow (\forall\, x)\big[A \vee P(x)\big]\,,$$
$$A \wedge (\forall\, x)P(x) \Leftrightarrow (\forall\, x)\big[A \wedge P(x)\big]\,,$$
$$(\forall\, x)P(x) \wedge (\forall\, x)Q(x) \Leftrightarrow (\forall\, x)\big[P(x) \wedge Q(x)\big]\,,$$
$$(\forall\, x)P(x) \vee (\forall\, x)Q(x) \Leftrightarrow (\forall\, x)(\forall\, y)\big[P(x) \vee Q(y)\big]\,,$$

$$A \wedge (\exists\, x)P(x) \Leftrightarrow (\exists\, x)\big[A \wedge P(x)\big]\,,$$
$$A \vee (\exists\, x)P(x) \Leftrightarrow (\exists\, x)\big[A \vee P(x)\big]\,,$$
$$(\exists\, x)P(x) \vee (\exists\, x)Q(x) \Leftrightarrow (\exists\, x)\big[P(x) \vee Q(x)\big]\,,$$
$$(\exists\, x)P(x) \wedge (\exists\, x)Q(x) \Leftrightarrow (\exists\, x)(\exists\, y)\big[P(x) \wedge Q(y)\big]\,,$$

$$(\forall\, x)P(x) \wedge (\exists\, x)Q(x) \Leftrightarrow (\forall\, x)(\exists\, y)\big[P(x) \wedge Q(y)\big]\,,$$
$$(\forall\, x)P(x) \vee (\exists\, x)Q(x) \Leftrightarrow (\forall\, x)(\exists\, y)\big[P(x) \vee Q(y)\big]\,.$$

**Exercice 1.7** Mettre les propositions suivantes sous forme normale.

1. $(\forall\, x)P(x) \to (\forall\, x)Q(x)$ ;
2. $(\forall\, x \in \mathbb{R})\neg(\exists\, y \in [x, +\infty[\,)\neg\big[(\forall\, z \in [y, y+x])P(z) \wedge (\forall\, z \in [y, +\infty[\,)Q(z)\big]$.

Remarque. Les équivalences relatives aux formes normales qui font intervenir deux variables distinctes $x$ et $y$ ne s'appliquent que si $x$ et $y$ ont même univers.

## 1.2 Techniques de preuve

### 1.2.1 Définitions préliminaires

**Définition 1.9** *Un théorème est une proposition dont on sait établir la véracité.*

REMARQUE. Les termes *lemme*, *proposition* et *corollaire* sont employés pour certains types de théorèmes : un lemme est une étape intermédiaire intervenant dans la preuve d'un théorème plus important ; une proposition est un théorème "de moindre importance" (et non pas un "théorème qui pourrait ne pas être vrai") ; un corollaire est une conséquence immédiate d'un autre théorème.

**Définition 1.10** *On appelle axiome ou postulat une proposition supposée vraie représentant les hypothèses sous-jacentes aux structures mathématiques étudiées.*

**Définition 1.11** *On appelle règle d'inférence de prémisses $p_1, \ldots, p_n$ et de conclusion $q$ l'implication logique $(p_1 \wedge \cdots \wedge p_n) \Rightarrow q$.*

**Définition 1.12** *Une preuve formelle est une séquence finie de propositions (ou étapes) qui, partant d'un ensemble de prémisses, conduit à la conclusion recherchée en obéissant aux règles suivantes :*

- ♢ *l'ensemble des prémisses d'une preuve peut contenir des axiomes, les hypothèses du théorème à prouver ainsi que d'autres théorèmes dont on a déjà fourni la preuve ;*
- ♢ *chaque étape d'une preuve est soit un prémisse, soit une proposition qui se déduit des étapes précédentes à l'aide d'une règle d'inférence ou d'une équivalence logique.*

REMARQUE. La plupart du temps, on ne fournit pas de preuve formelle. Les preuves sont rédigées de manière concise, mais de façon à ce qu'un lecteur familier avec les techniques de preuve soit capable de "combler les trous".

### 1.2.2 Règles d'inférence

Les règles d'inférence usuelles relatives aux propositions composées sont regroupées dans la table 1.2. Chacune d'elles peut être démontrée à l'aide d'une table de vérité ou d'une succession d'identités logiques.

| Nom | Prémisses | Conclusion |
|---|---|---|
| Addition disjonctive | $p$ | $p \vee q$ |
| Addition conjonctive | $p,\ q$ | $p \wedge q$ |
| Simplification | $p \wedge q$ | $q$ |
| Détachement (modus ponens) | $p \to q,\ p$ | $q$ |
| Réfutation (modus tollens) | $p \to q,\ \neg q$ | $\neg p$ |
| Syllogisme disjonctif | $p \vee q,\ \neg p$ | $q$ |
| Dilemme constructif | $p \vee q,\ p \to r,\ q \to s$ | $r \vee s$ |
| Dilemme | $p \vee q,\ p \to r,\ q \to r$ | $r$ |
| Dilemme destructif | $\neg r \vee \neg s,\ p \to r,\ q \to s$ | $\neg p \vee \neg q$ |
| Syllogisme hypothétique | $p \to q,\ q \to r$ | $p \to r$ |
| Preuve conditionnelle | $p,\ p \wedge q \to r$ | $q \to r$ |
| Contradiction | $\neg p \to \mathbf{F}$ | $p$ |

**Table 1.2** — Règles d'inférence relatives aux propositions composées.

**Exercice 1.8** Démontrer la réfutation de deux manières distinctes.

Concernant les prédicats quantifiés, on dispose des quatre règles d'inférence données dans la table 1.3.

| Nom | Prémisse | Conclusion |
|---|---|---|
| Spécification universelle | $(\forall\, x \in E)P(x)$ | $P(c)$ ($c$ désigne n'importe quel élément de $E$) |
| Généralisation universelle | $P(c)$ avec $c$ élément de $E$ choisi arbitrairement | $(\forall\, x \in E)P(x)$ |
| Spécification existentielle | $(\exists\, x \in E)P(x)$ | $P(c)$ ($c$ désigne un élément de $E$ déterminé) |
| Généralisation existentielle | $P(c)$ pour au moins un élément $c$ de $E$ | $(\exists\, x \in E)P(x)$ |

**Table 1.3** — Règles d'inférence relatives aux prédicats quantifiés.

**Exercice 1.9** Fournir une preuve formelle de l'argument suivant : "Tous les éléphants sont des mammifères. Certains éléphants sont joueurs. Par conséquent, certains mammifères sont joueurs".

### 1.2.3 Types de preuves

**Cas des implications (théorèmes de la forme $p \Rightarrow q$)**

• *Preuve directe* : On suppose que $p$ est vraie et on utilise des axiomes, des règles d'inférence et d'autres théorèmes pour en déduire que $q$ est vraie.

**Exercice 1.10** Donner une preuve directe du théorème suivant : *pour tout $n \in \mathbb{Z}$, si $n$ est impair, alors $n^2$ est impair.*

• *Preuve indirecte* : Puisque $p \to q \Leftrightarrow \neg q \to \neg p$ (contre-apposition), on peut démontrer $p \Rightarrow q$ en prouvant que $\neg q \Rightarrow \neg p$.

**Exercice 1.11** Donner une preuve indirecte du théorème suivant : *pour tout $n \in \mathbb{Z}$, si $n^2$ est pair, alors $n$ est pair.*

• *Preuve par contradiction* ou *raisonnement par l'absurde*. Puisque $\neg p \to \mathbf{F} \Leftrightarrow p \vee \mathbf{F} \Leftrightarrow p$, on peut établir la véracité d'une proposition $p$ en montrant que $\neg p \to \mathbf{F}$ est vraie, c'est-à-dire en supposant $\neg p$ vraie pour aboutir à une contradiction.
On peut donc prouver $p \Rightarrow q$ en démontrant que $\neg(p \to q) \Leftrightarrow \neg(\neg p \vee q) \Leftrightarrow p \wedge \neg q$ implique une contradiction.

**Exercice 1.12** Montrer par l'absurde :
1. $\sqrt{2} \notin \mathbb{Q}$ ;
2. *pour tout $n \in \mathbb{Z}$, si $3n+2$ est impair, alors $n$ est impair.*

• *Preuve par cas* : Si $p$ prends la forme d'une disjonction $p_1 \vee \cdots \vee p_n$, l'équivalence $\big[(p_1 \vee \cdots \vee p_n) \to q\big] \Leftrightarrow \big[(p_1 \to q) \wedge \cdots \wedge (p_n \to q)\big]$ (obtenue via implication par disjonction et loi de Morgan) fait apparaître que l'on peut démontrer $p \Rightarrow q$ en prouvant que $p_i \to q$ est vraie pour chaque $i \in [\![1, n]\!]$.

**Exercice 1.13** Montrer : *pour tout $n \in \mathbb{Z}$, si $n$ est impair, alors $n^2 - 1$ est divisible par 8.*

• *Preuve par disjonction* : Pour démontrer un théorème de la forme $p \Rightarrow (q \vee r)$, il suffit de prouver que $(p \wedge \neg q) \Rightarrow r$ ou $(p \wedge \neg r) \Rightarrow q$.

**Exercice 1.14** Montrer : *pour tout $(a, n) \in \mathbb{Z} \times \mathbb{N}$, si $n$ est premier, alors $n$ divise $a$ ou* $\operatorname{pgcd}(a, n) = 1$.

### Cas des équivalences

Certains théorèmes stipulent que plusieurs propositions $p_1, \ldots, p_n$ sont équivalentes, c'est-à-dire $(\forall\, i)(\forall\, j \neq i)[\, p_i \Leftrightarrow p_j\,]$. Une façon de prouver ce type de théorème consiste à démontrer $p_1 \Rightarrow p_2$ , $p_2 \Rightarrow p_3$ , $\ldots$ , $p_{n-1} \Rightarrow p_n$ et $p_n \Rightarrow p_1$. Il s'agit d'une *preuve par cycle d'implications*.

**Exercice 1.15** Soient $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. On dit que $a$ est *congru à $b$ modulo $m$* et on écrit $a \equiv b \,(\mathrm{mod}\, m)$ si $m$ divise $a - b$. Montrer : *pour tout $n \in \mathbb{Z}$, $n$ n'est pas divisible par 3 si et seulement si* $n^2 \equiv 1 \,(\mathrm{mod}\, 3)$.

### Preuves d'existence

Les *preuves d'existence* concernent les propositions de la forme $(\exists\, x \in E)P(x)$. Elles sont basées sur la règle de généralisation existentielle et se déclinent en deux catégories :

- ♢ les preuves *constructives* qui exhibent un élément $c$ de $E$ tel que $P(c)$ est vraie ;
- ♢ les preuves *non constructives* qui établissent l'existence d'un élément $c$ de $E$ tel que $P(c)$ est vraie sans expliciter $c$ ni même fournir un moyen de le déterminer.

**Exercice 1.16** Montrer :

1. *pour tout $n \in \mathbb{N}^*$, il existe $n$ entiers naturels composites consécutifs* ;
2. *pour tout $n \in \mathbb{N} \setminus \{0, 1\}$, il existe un nombre premier strictement supérieur à $n$.*

Remarques. (i) Les preuves d'existence non constructives sont souvent des preuves par contradiction : on prouve $(\exists\, x)P(x)$ en démontrant que sa négation, $(\forall\, x)\neg P(x)$, implique une contradiction.

(ii) Les preuves établissant l'existence et l'unicité d'un élément particulier sont appelées *preuves d'unicité*. Elles s'articulent en deux parties : la première prouve l'existence de l'élément et la deuxième établit son unicité par contradiction (i.e., on suppose l'existence de deux élément distincts vérifiant la propriété considérée pour aboutir à une contradiction).

### 1.2.4 Induction sur $\mathbb{N}$

NOTATION. Soient $a, b \in \mathbb{N}$. On note $[\![a, b]\!]$ (resp. $[\![a, \infty[\![$ ) l'ensemble des entiers $n$ vérifiant $a \leqslant n \leqslant b$ (resp. $n \geqslant a$).

Le raisonnement par *induction* également appelé raisonnement par *récurrence* est une technique de preuve extrêmement importante pour la démonstration des théorèmes de la forme $(\forall\, n \in [\![n_0, \infty[\![\,)P(n)$, $n_0 \in \mathbb{N}$. On distingue typiquement l'induction faible de l'induction forte, mais ces deux principes sont équivalents.

#### Premier principe d'induction (induction faible)

Le *premier principe d'induction*, ou *principe d'induction faible*, concerne le cas où la véracité de $P(n)$ ne dépend que de $P(n-1)$. Il fait intervenir une étape de *base*, notée (B), et une étape dite *inductive* ou encore de *passage de $n$ à $n+1$* notée (I). Son énoncé est le suivant.

**Théorème 1.1** *Soit $P(n)$ un prédicat dépendant d'un entier $n$ et soit $n_0 \in \mathbb{N}$. Si*

$$\begin{cases} \text{(B)} \;\; P(n_0) \text{ est vraie} \\ \text{(I)} \;\; (\forall\, n \in [\![n_0, \infty[\![\,)\big[P(n) \Rightarrow P(n+1)\big] \end{cases},$$

*alors $(\forall\, n \in [\![n_0, \infty[\![\,)P(n)$.*

**Exercice 1.17** Montrer que les nombres harmoniques $H_k$, $k \in \mathbb{N}^*$, définis par $H_k := \sum_{l=1}^{k} l^{-1}$, vérifient $H_{2^n} \geqslant 1 + n/2$ pour tout $n \in \mathbb{N}$.

### Deuxième principe d'induction (induction forte)

Le deuxième principe d'induction, ou *principe d'induction forte*, permet de traiter des cas pour lesquels $P(n)$ dépend d'un sous-ensemble quelconque de $\{P(n_0), \ldots, P(n-1)\}$ et non plus uniquement de $P(n-1)$. Il s'énonce de la manière suivante.

**Théorème 1.2** *Soit $P(n)$ un prédicat dépendant d'un entier $n$ et soit $(n_0, m) \in \mathbb{N}^2$. Si*

$$\begin{cases} (\mathrm{B}') \quad (\forall\, n \in [\![n_0, n_0+m]\!])P(n) \\ (\mathrm{I}') \quad (\forall\, n \in [\![n_0+m, \infty[\![\,)\big[(\forall\, k \in [\![n_0, n]\!])P(k) \Rightarrow P(n+1)\big] \end{cases},$$

*alors $(\forall\, n \in [\![n_0, \infty[\![\,)P(n)$.*

DÉMONSTRATION. Conséquence immédiate des théorèmes 1.1 et 1.3. □

**Exercice 1.18** Montrer que tout entier strictement supérieur à 1 est premier ou peut s'écrire sous la forme d'un produit de nombres premiers.

### Équivalence des deux principes d'induction

**Théorème 1.3** $(\mathrm{B}) \wedge (\mathrm{I}) \;\Leftrightarrow\; (\mathrm{B}') \wedge (\mathrm{I}')$.

DÉMONSTRATION. On a $(\mathrm{B}) \wedge (\mathrm{I}) \Rightarrow (\mathrm{B}') \wedge (\mathrm{I}')$ car $(\mathrm{B}) \wedge (\mathrm{I}) \Rightarrow (\forall\, n \in [\![n_0, \infty[\![\,)P(n) \Rightarrow$ (B') et (I) $\Rightarrow$ $(\forall\, n \in [\![n_0+m, \infty[\![\,)[P(n) \to P(n+1)] \Rightarrow$ (I'). Inversement, si $(\mathrm{B}')$ et $(\mathrm{I}')$ sont vérifiées, (B) est vérifiée et un raisonnement par l'absurde montre que (I) l'est aussi. Supposons en effet que (I) ne soit pas vérifiée, c'est-à-dire que $(\exists\, n \in [\![n_0, \infty[\![\,)\neg\big(P(n) \to P(n+1)\big)$ est vraie, et soit $\tilde{n}$ le plus petit entier $n \in [\![n_0, \infty[\![$ tel que $P(n) \to P(n+1)$ est fausse. Alors $(\forall\, k \in [\![n_0, \tilde{n}]\!])P(k)$ est vraie et $P(\tilde{n}+1)$ est fausse. Il y a contradiction avec $(\mathrm{I}')$ si $\tilde{n} \geqslant n_0 + m$ et contradiction avec $(\mathrm{B}')$ sinon. □

## 1.3 Calcul ensembliste

### 1.3.1 Terminologie

On ne se risque pas à donner une définition des notions premières d'*ensemble* et d'*élément*. On dit qu'un ensemble $E$ est constitué d'éléments et qu'un élément $x$ appartient à $E$ (on écrit : $x \in E$) ou n'appartient pas à $E$ (on écrit : $x \notin E$). L'*ensemble vide*, qui n'a aucun élément, est noté $\emptyset$. Un ensemble ayant un unique élément $x$ est appelé *singleton* et noté $\{x\}$. Un ensemble peut être défini par restriction d'un ensemble plus vaste par le biais d'un prédicat : $\{x \in E \,|\, P(x)\}$ est l'ensemble de tous les éléments d'un univers $E$ vérifiant la propriété $P$, ou *compréhension* de $E$ relativement à $P$. Si $E$ ne peut être précisément défini, on note $\{x \,|\, P(x)\}$ et on parle d'*abstraction*.

Remarque. L'ensemble $\{\emptyset\}$ n'est pas l'ensemble vide. C'est un singleton dont l'élément est l'ensemble vide.

**Définition 1.13** *Deux ensembles $A$ et $B$ sont dits égaux ou identiques s'ils contiennent exactement les mêmes éléments :* $A = B \Leftrightarrow (\forall\, x)\big[(x \in A) \leftrightarrow (x \in B)\big]$.

**Définition 1.14** *On dit que $A$ est un sous-ensemble ou une partie de $B$, et on note $A \subset B$ ou $B \supset A$, si tout élément de $A$ est un élément de $B$ :* $A \subset B \Leftrightarrow (\forall\, x)\big[(x \in A) \rightarrow (x \in B)\big]$. *On dit qu'il s'agit d'un sous-ensemble strict de $B$, ce que l'on note $A \subsetneq B$, si, de plus, $B$ contient au moins un élément n'appartenant pas à $A$ :* $A \subsetneq B \Leftrightarrow (A \subset B) \wedge (\exists\, x)\big[(x \in B) \wedge (x \notin A)\big]$.

Remarques. (i) $\emptyset \subset A$ pour tout ensemble $A$.
(ii) $A = B \Leftrightarrow (A \subset B) \wedge (B \subset A)$.
(iii) $A = \emptyset \Leftrightarrow (\forall\, x)[x \notin A]$.

**Définition 1.15** $\diamondsuit$ *Un ensemble $A$ est dit fini s'il est vide ou s'il peut être mis en bijection avec un sous-ensemble borné de $\mathbb{N}$. Dans ce cas, le nombre d'éléments de $A$ est appelé cardinal de $A$. On le note $|A|$ ou* $\mathrm{Card}(A)$.
$\diamondsuit$ *Un ensemble qui n'est pas fini est dit infini.*
$\diamondsuit$ *Un ensemble est dit dénombrable s'il peut être mis en bijection avec $\mathbb{N}$.*

**Définition 1.16** *On appelle ensemble des parties d'un ensemble $A$ la collection $\mathcal{P}(A)$ de tous ses sous-ensembles : $\mathcal{P}(A) = \{B \,|\, B \subset A\}$.*

**Définition 1.17** *Soient $A$ et $B$ deux ensembles. On appelle produit cartésien de $A$ et $B$ l'ensemble des couples $(x, y)$ tels que $x \in A$ et $y \in B$ : $A \times B = \{(x, y) \,|\, (x \in A) \wedge (y \in B)\}$. Le produit cartésien se généralise à une famille finie d'ensembles : $A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) \,|\, (x_1 \in A_1) \wedge \cdots \wedge (x_n \in A_n)\}$. Si $A_1 = \cdots = A_n = A$ on note en abrégé $A^n$ le produit cartésien $A_1 \times \cdots \times A_n$.*

REMARQUE. $A \times \emptyset = \emptyset \times B = \emptyset \times \emptyset = \emptyset$.

### 1.3.2 Opérations sur les ensembles

**Définition 1.18** *Soient $E$ un ensemble, $A, B \in \mathcal{P}(E)$. On définit*

- ♢ *l'intersection de $A$ et $B$ : $A \cap B = \big\{x \in E \,|\, (x \in A) \wedge (x \in B)\big\}$ ($A$ et $B$ sont dits disjoints si $A \cap B = \emptyset$),*
- ♢ *l'union de $A$ et $B$ : $A \cup B = \big\{x \in E \,|\, (x \in A) \vee (x \in B)\big\}$,*
- ♢ *le complémentaire de $A$ dans $E$ : $\mathsf{C}_E(A) = \{x \in E \,|\, x \notin A\}$, souvent noté $\overline{A}$ s'il n'y a pas ambiguïté.*
- ♢ *la différence de $A$ et $B$ : $A \setminus B = A \cap \mathsf{C}_E(B) = \big\{x \in E \,|\, (x \in A) \wedge (x \notin B)\big\}$,*
- ♢ *la différence symétrique de $A$ et $B$ : $A \triangle B = (A \setminus B) \cup (B \setminus A)$.*

**Exercice 1.19** Montrer :

1. $A \triangle B = (A \cup B) \setminus (A \cap B)$ ;
2. $(A \cap C \neq \emptyset) \vee (B \cap C \neq \emptyset) \Leftrightarrow (A \cup B) \cap C \neq \emptyset$.

REMARQUE. L'intersection et l'union se généralisent à une famille $(A_i)_{i \in I}$ de parties de $E$ (c'est-à-dire une application d'un ensemble $I$ dans $\mathcal{P}(E)$) :

$$\bigcap_{i \in I} A_i \;=\; \big\{x \in E \,|\, (\forall\, i \in I)[x \in A_i]\big\}, \qquad \bigcup_{i \in I} A_i \;=\; \big\{x \in E \,|\, (\exists\, i \in I)[x \in A_i]\big\}.$$

En particulier, $\displaystyle\bigcap_{i \in \emptyset} A_i \;=\; E$ et $\displaystyle\bigcup_{i \in \emptyset} A_i \;=\; \emptyset$.

### Identités sur les ensembles

De nombreuses identités logiques (table 1.1 p. 8) correspondent à des identités sur parties d'un ensemble $E$ si l'on remplace $\wedge$ par $\cap$, $\vee$ par $\cup$, $\neg$ par la complémentation, $\mathbf{V}$ par $E$ et $\mathbf{F}$ par $\emptyset$. Les identités usuelles sur les ensembles sont données dans la table 1.4. De façon générale, une identité sur des ensembles peut être prouvée de trois manières différentes : (i) par *inclusion mutuelle*, c'est-à-dire en démontrant que chacun des membres est un sous-ensemble de l'autre ; (ii) par abstraction et utilisation d'identités logiques ; (iii) à l'aide d'identités usuelles.

| | |
|---|---|
| Identité | $A \cap E = A, \quad A \cup \emptyset = A$ |
| Domination | $A \cup E = E, \quad A \cap \emptyset = \emptyset$ |
| Idempotence | $A \cap A = A, \quad A \cup A = A$ |
| Lois de la complémentation | $\overline{\overline{A}} = A, \quad A \cup \overline{A} = E, \quad A \cap \overline{A} = \emptyset$ |
| Commutativité | $A \cap B = B \cap A, \quad A \cup B = B \cup A$ |
| Associativité | $A \cap (B \cap C) = (A \cap B) \cap C,$ |
| | $A \cup (B \cup C) = (A \cup B) \cup C$ |
| Distributivité | $A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$ |
| | $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ |
| Absorption | $A \cap (A \cup B) = A, \quad A \cup (A \cap B) = A$ |
| Lois de Morgan | $\overline{A \cap B} = \overline{A} \cup \overline{B}, \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$ |

**Table 1.4** — Identités sur les ensembles.

**Exercice 1.20** Montrer : $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$.

**Exercice 1.21** Démontrer par abstraction et identités logiques que, pour toute famille $(A_i)_{i \in I}$ de parties d'un ensemble référentiel $E$,

$$\overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i}.$$

En déduire la généralisation de la deuxième loi de Morgan : $\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}$.

**Exercice 1.22** Soient $A$ une partie d'un ensemble référentiel $E$, $(B_i)_{i \in I}$ une famille de parties de $E$.

1. Montrer : $A \cup \left( \bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} (A \cup B_i)$.
2. En supposant les lois de Morgan généralisées établies (voir exercice 1.21), en déduire

$$A \cap \left( \bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} (A \cap B_i).$$

**Exercice 1.23** Soient $E$ et $F$ deux ensembles. Montrer que, pour toute famille $(A_i)_{i\in I}$ de parties de $E$ et pour toute famille $(B_j)_{j\in J}$ de parties de $F$,

$$\left(\bigcup_{i\in I} A_i\right) \times \left(\bigcup_{j\in J} B_j\right) = \bigcup_{(i,j)\,\in\, I\times J} A_i \times B_j\,.$$

### Notion de partition

**Définition 1.19** *Soient $E$ un ensemble non vide, $\Gamma = (A_i)_{i\in I}$ une famille de parties de $E$. On dit que $\Gamma$ est une partition de $E$ si et seulement si $\Gamma$ est une famille d'ensembles non vides mutuellement disjoints dont l'union est $E$, c'est-à-dire si et seulement si*

1. $(\forall\, i \in I)[\, A_i \neq \emptyset\,]$ ,
2. $(\forall\, i \in I)(\forall\, j \in I)[\, i \neq j \;\Rightarrow\; A_i \cap A_j = \emptyset\,]$,
3. $E = \bigcup_{i\in I} A_i$ .

### Propriétés des cardinaux

**Proposition 1.1** *Soient $A$ et $B$ deux ensembles finis.*

1. *Si $A$ et $B$ sont disjoints, alors $|A \cup B| = |A| + |B|$ .*
2. *Si $A \subset B$ et $|A| = |B|$, alors $A = B$.*
3. *Si $(C_i)_{i\in I}$ est une partition de $A$, alors $|A| = \sum_{i\in I} |C_i|$ .*
4. $|A \setminus B| = |A| - |A \cap B|$ .
5. $|A \cup B| = |A| + |B| - |A \cap B|$ .
6. $|A \times B| = |A| \cdot |B|$ .
7. $|\mathcal{P}(A)| = 2^{|A|}$.

## 1.4 Fonctions : le minimum vital

### 1.4.1 Définitions et premières propriétés

**Définition 1.20** *Soient $E$, $F$ deux ensembles.*

- ♢ *On appelle correspondance de $E$ vers $F$ tout triplet $f = (E, F, \mathcal{R})$, $\mathcal{R} \in \mathcal{P}(E \times F)$.*
- ♢ *Soit $x \in E$. On appelle image de $x$ par $f$ tout élément $y \in F$ tel que $(x, y) \in \mathcal{R}$. Inversement, tout élément $x \in E$ tel que $(x, y) \in \mathcal{R}$ pour un $y \in F$ donné est appelé antécédent de $y$ par $f$.*
- ♢ *On appelle respectivement domaine et image de $f$ les ensembles*

$$\mathrm{Dom}(f) = \big\{x \in E \,|\, (\exists\, y \in F)\big[(x, y) \in \mathcal{R}\big]\big\}$$
$$\text{et} \quad \mathrm{Im}(f) = \big\{y \in F \,|\, (\exists\, x \in E)\big[(x, y) \in \mathcal{R}\big]\big\}.$$

NOTATION. Soient $A \in \mathcal{P}(E)$, $B \in \mathcal{P}(F)$.

- ♢ On note $f(A)$ l'ensemble des images des éléments de $A$ par $f$ :

$$f(A) = \big\{y \in F \,|\, (\exists\, x \in A)\big[(x, y) \in \mathcal{R}\big]\big\}.$$

- ♢ On note $f^{-1}(B)$ l'ensemble des antécédents des éléments de $B$ par $f$ :

$$f^{-1}(B) = \big\{x \in E \,|\, (\exists\, y \in B)\big[(x, y) \in \mathcal{R}\big]\big\}.$$

En particulier, $\mathrm{Dom}(f) = f^{-1}(F)$ et $\mathrm{Im}(f) = f(E)$.

**Définition 1.21**

- ♢ *On dit qu'une correspondance $f = (E, F, \mathcal{R})$ est une fonction si tout élément $x \in E$ a au plus une image par $f$ que l'on note $f(x)$. Dans ce cas, la fonction $f$ est notée $f : E \to F$.*
- ♢ *On dit qu'une fonction $f : E \to F$ est une application si $\mathrm{Dom}(f) = E$.*
- ♢ *L'ensemble des applications de $E$ dans $F$ est noté $F^E$.*

**Définition 1.22** *L'application $\mathrm{Id}_E : E \to E$ définie par $(\forall x \in E)[\mathrm{Id}_E(x) = x]$ est appelée application identique de $E$ dans $E$ ou plus simplement identité de $E$.*

**Définition 1.23** *Soient $f : E \to F$ une application.*

- ♢ *Soit $A \in \mathcal{P}(E)$. On appelle restriction de $f$ à $A$ l'application $f|_A : A \to F$ définie par $(\forall x \in A)[f|_A(x) = f(x)]$.*
- ♢ *Soit $B \in \mathcal{P}(F)$. Si $f(E) \subset B$, on appelle corestriction de $f$ à $B$ l'application $f|^B : E \to B$ définie par $(\forall x \in E)[f|^B(x) = f(x)]$.*

**Définition 1.24** *Soit $f$ une application de $E^n$ dans $E$, $n \in \mathbb{N}^*$. On dit qu'une partie $A$ de $E$ est stable pour $f$ si et seulement si $f(x_1, \ldots, x_n) \in A$ pour tout $(x_1, \ldots, x_n) \in A^n$.*

**Exemple 1.5** (i) $\mathbb{Z}$ et $\mathbb{Q}$ sont stables pour l'addition et la multiplication dans $\mathbb{R}$.
(ii) L'ensemble des entiers naturels composites est stable pour la multiplication dans $\mathbb{N}$.
(iii) L'ensemble des nombres premiers n'est pas stable pour la multiplication dans $\mathbb{N}$.

**Définition 1.25** *Soient $f : E \to F$, $g : F \to G$ deux applications. On appelle composition de $f$ et $g$ l'application $g \circ f : E \to G$ définie par $(\forall x \in E)\big[g \circ f(x) = g\big(f(x)\big)\big]$.*

**Proposition 1.2** *Soient $f : E \to F$ une application, $A$ et $B$ des parties de $E$.*

1. $f(A \cup B) = f(A) \cup f(B)$ ;
2. $f(A \cap B) \subset f(A) \cap f(B)$ *(l'inclusion est stricte en général, mais $f(A \cap B) = f(A) \cap f(B)$ si $f$ est injective)* ;
3. $A \subset f^{-1} \circ f(A)$ .

**Proposition 1.3** *Soient $f : E \to F$ une application, $A'$ et $B'$ des parties de $F$.*

1. $f^{-1}(A' \cap B') = f^{-1}(A') \cap f^{-1}(B')$ ;
2. $f^{-1}(A' \cup B') = f^{-1}(A') \cup f^{-1}(B')$ ;
3. $f \circ f^{-1}(A') \subset A'$ *(l'inclusion est stricte en général, mais $f \circ f^{-1}(A') = A'$ si $f$ est surjective)* ;
4. $f^{-1}\big(\mathsf{C}_F(A')\big) = \mathsf{C}_E\big(f^{-1}(A')\big)$ .

### 1.4.2 Injection, surjection, bijection

**Définition 1.26** *Une application $f : E \to F$ est dite injective (resp. surjective, bijective) si tout élément de $F$ a au plus (resp. au moins, exactement) un antécédent par $f$. En d'autres termes,*

- ♢ *$f$ est injective ssi $(\forall\, x, y \in E)[\, f(x) = f(y) \implies x = y\,]$ ou, de manière équivalente, ssi $(\forall\, x, y \in E)[\, x \neq y \implies f(x) \neq f(y)\,]$ ;*
- ♢ *$f$ est surjective ssi $(\forall\, y \in F)(\exists\, x \in E)\big[f(x) = y\big]$, c'est-à-dire ssi $f(E) = F$ ;*
- ♢ *$f$ est bijective ssi $(\forall\, y \in F)(\exists\,!\, x \in E)\big[f(x) = y\big]$, c'est-à-dire ssi $f$ est à la fois injective et surjective.*

Remarque. En termes de cardinaux :

- ♢ $f$ injective $\iff (\forall\, y \in F)\big[\big|\, f^{-1}(\{y\})\big| \leqslant 1\big]$ ;
- ♢ $f$ surjective $\iff (\forall\, y \in F)\big[\big|\, f^{-1}(\{y\})\big| \geqslant 1\big]$ ;
- ♢ $f$ bijective $\iff (\forall\, y \in F)\big[\big|\, f^{-1}(\{y\})\big| = 1\big]$.

**Définition 1.27** *Soit $f : E \to F$ une application bijective. L'application $f^{-1} : F \to E$ qui à $y \in F$ associe l'unique élément $x \in E$ tel que $y = f(x)$ est appelée bijection réciproque de $f$.*

Remarque. Ne pas confondre la bijection réciproque (définie ssi $f$ est bijective) et l'application $f^{-1} : \mathcal{P}(F) \to E$ qui à une partie $B$ de $F$ associe l'ensemble $f^{-1}(B)$ des antécédents des éléments de $B$ par $f$ (définie pour toute application $f : E \to F$).

**Proposition 1.4** *Soit $f : E \to F$ une application avec $E$ et $F$ non vides.*
*$f$ est injective (resp. surjective) ssi il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ (resp. $f \circ g = \mathrm{Id}_F$)*

**Proposition 1.5** *Soit $f : E \to F$ une application.*
*$f$ est bijective ssi il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$. S'il en est ainsi, alors $g$ est unique et $g = f^{-1}$.*

**Proposition 1.6** *Soient $f : E \to F$, $g : F \to G$ deux applications. On a*

1. *$f$ et $g$ injectives $\implies$ $g \circ f$ injective ;*
2. *$f$ et $g$ surjectives $\implies$ $g \circ f$ surjective ;*
3. *$f$ et $g$ bijectives $\implies$ $g \circ f$ bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

### 1.4.3 Comportements asymptotiques

Les définitions qui suivent portent sur deux fonctions $f$ et $g$ de $\mathbb{D}$ dans $\mathbb{R}$, où $\mathbb{D}$ désigne $\mathbb{Z}$ ou $\mathbb{R}$.

**Définition 1.28** *On dit que $g$ <u>domine</u> $f$ et on note $f = O(g)$ (on dit parfois que $f$ est "grand o" de $g$) si*

$$(\exists\, C \in \mathbb{R}_+^*)(\exists\, x_0 \in \mathbb{D})(\forall\, x \in \mathbb{D})\big[\, x \geqslant x_0 \implies |f(x)| \leqslant C|g(x)|\,\big]$$

*On dit que $f$ et $g$ sont du <u>même ordre</u> et on note $f = \Theta(g)$ (on dit parfois que $f$ est "theta" de $g$) si $f = O(g)$ et $g = O(f)$.*

**Exemple 1.6** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ est $O(x^m)$ pour tout $m \geqslant n$ et $\Theta(x^n)$ si $a_n \neq 0$.

Remarques. (i) $O(\,\cdot\,)$ désigne une classe de fonctions. Écrire $f = O(g)$ est un abus de notation car il y a appartenance et non égalité.
(ii) Les classes les plus couramment utilisées sont $O(1) \subset O(\ln x) \subset O(x) \subset O(x \ln x) \subset O(x^n)$ $(n \in \mathbb{N} \setminus \{0,1\}) \subset O(2^x) \subset O(x!) \subset O(x^x)$.

**Propriétés 1.1** $\diamondsuit$ Si $f_1 = O(g)$ et $f_2 = O(g)$, alors $(\forall\, \alpha, \beta \in \mathbb{R})\big[\alpha f_1 + \beta f_2 = O(g)\big]$.
$\diamondsuit$ Si $f_1 = O(g_1)$ et $f_2 = O(g_2)$, alors $f_1 + f_2 = O\big(\max(|g_1|, |g_2|)\big)$ et $f_1 f_2 = O(g_1 g_2)$.
$\diamondsuit$ Si $f = O(g)$ et $h = O(f)$, alors $h = O(g)$.

**Définition 1.29** *On dit que $f$ est <u>négligeable</u> devant $g$ et on note $f = o(g)$ (on dit parfois que $f$ est "petit o" de $g$) si*

$$(\forall\, \varepsilon \in \mathbb{R}_+^*)(\exists\, x_0 \in \mathbb{D})(\forall\, x \in \mathbb{D})\big[\, x \geqslant x_0 \implies |f(x)| \leqslant \varepsilon|g(x)|\,\big]\,.$$

**Exemple 1.7** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ est $o(x^m)$ pour tout $m > n$.

Remarque. Si $g$ est à valeurs dans $\mathbb{R}_+^*$ ou dans $\mathbb{R}_-^*$, alors

$$f = o(g) \iff \lim_{x\to+\infty} f(x)/g(x) = 0.$$

**Propriétés 1.2** ♢ Si $f_1 = o(g)$ et $f_2 = o(g)$, alors $(\forall\, \alpha, \beta \in \mathbb{R})\big[\alpha f_1 + \beta f_2 = o(g)\big]$.
♢ Si $f_1 = o(g_1)$ et $f_2 = o(g_2)$, alors $f_1 + f_2 = o\big(\max(|g_1|, |g_2|)\big)$ et $f_1 f_2 = o(g_1 g_2)$.
♢ Si $f = o(g)$, alors $f = O(g)$ (mais pas l'inverse).
♢ Si $f = O(g)$ et $h = o(f)$, alors $h = o(g)$.
♢ Si $f = o(g)$ et $h = O(f)$, alors $h = o(g)$.
♢ Si $f_1 = o(g_1)$ et $f_2 = O(g_2)$, alors $f_1 f_2 = o(g_1 g_2)$.

**Définition 1.30** *On dit que $f$ et $g$ sont asymptotiquement équivalentes et on note $f \sim g$ si $f - g = o(g)$.*

Remarques. (i) $f \sim g$ n'implique pas $\lim_{x\to+\infty}(f-g)(x) = 0$.
(ii) Si $f_1$ et $f_2$ sont de même signe pour $x$ suffisamment grand, alors $f_1 \sim g_1$ et $f_2 \sim g_2$ implique $f_1 + f_2 \sim g_1 + g_2$.
(iii) Si $g$ est à valeurs dans $\mathbb{R}_+^*$ ou dans $\mathbb{R}_-^*$, alors $f \sim g \iff \lim_{x\to+\infty} f(x)/g(x) = 1$.

**Exemple 1.8** (i) $\ln x \sim \ln 2x$ mais $\ln x - \ln 2x = -\ln 2$.
(ii) $x + x^{-2} \sim x$ et $-x + x^{-3} \sim -x$ mais $(x + x^{-2}) + (-x + x^{-3}) = x^{-2} + x^{-3} \sim x^{-2} \not\sim x + (-x) = 0$.

**Propriétés 1.3** ♢ Si $f_1 \sim g_1$ et $f_2 \sim g_2$, alors $f_1 f_2 \sim g_1 g_2$ .
♢ $(\forall\, n \in \mathbb{N}^*)[(f \sim g) \Rightarrow (f^n \sim g^n)]$.
♢ Si $f \sim g$ avec $f$ et $g$ à valeurs dans $\mathbb{R}_+^*$ ou dans $\mathbb{R}_-^*$, alors $1/f \sim 1/g$.
♢ Si $f \sim g$ avec $g$ à valeurs dans $\mathbb{R}_+^*$, alors $(\forall\, \alpha \in \mathbb{R})[f^\alpha \sim g^\alpha]$.

# Chapitre 2

# Dénombrement

**Analyse combinatoire**

♢ Arrangements et combinaisons.

♢ Coefficients binomiaux : propriétés élémentaires et formule du binôme.

**Principe d'exclusion-inclusion**

▷ Exprimer le cardinal d'une union finie d'ensembles finis en fonction des cardinaux de leurs intersections.

**Récurrences linéaires à coefficients constants**

▷ Résolution de relations du type

$$u_n = a_1 u_{n-1} + \cdots + a_k u_{n-k} + f(n)\,, \quad (a_1, \ldots, a_k) \in \mathbb{C}^k\,,$$

pour certaines applications $f : \mathbb{N} \to \mathbb{C}$.

## 2.1 Rappels d'analyse combinatoire

### 2.1.1 Arrangements et combinaisons

Nous rappelons ici les outils de base permettant de compter les arrangements ordonnés et les sélections non ordonnées d'objets distincts d'un ensemble fini. Soit donc $E$ un ensemble fini et posons $n = |E|$.

**Définition 2.1** *Soit $k \in [\![1, n]\!]$. On appelle arrangement d'ordre $k$ de $E$, ou $k$-arrangement de $E$, toute disposition ordonnée de $k$ éléments distincts de $E$, c'est-à-dire toute injection de $[\![1, k]\!]$ dans $E$.*

**Exemple 2.1** Soit $E = \{a, b, c\}$. Les arrangements d'ordre 2 de $E$ sont les couples $(a, b)$, $(b, a)$, $(a, c)$, $(c, a)$, $(b, c)$ et $(c, b)$. Noter que $(a, b, b)$ n'est pas un arrangement.

**Proposition 2.1** *Le nombre $A_n^k$ d'arrangements d'ordre $k$ de $E$ est égal à* $\dfrac{n!}{(n-k)!}$.

Remarque. Une *permutation* de $E$ est un arrangement d'ordre $n$ de $E$, c'est-à-dire une bijection de $[\![1, n]\!]$ dans $E$. Le nombre de permutations d'un ensemble de cardinal $n$ est égal à $n!$.

**Définition 2.2** *Soit $k \in [\![1, n]\!]$. On appelle combinaison d'ordre $k$ de $E$, ou $k$-combinaison de $E$, toute partie de $E$ de cardinal $k$. Une combinaison d'ordre $k$ de $E$ peut donc être caractérisée par l'image d'une injection de $[\![1, k]\!]$ dans $E$.*

**Exemple 2.2** Soit $E = \{a, b, c\}$. Alors, $\{a, b\}$, $\{a, c\}$ et $\{b, c\}$ sont les combinaisons d'ordre 2 de $E$. Noter que $\{b, a\}$ désigne la même combinaison que $\{a, b\}$ et que $\{a, a\} = \{a\}$ n'est pas une 2-combinaison de $E$.

**Proposition 2.2** *Le nombre $C_n^k$ de combinaisons d'ordre $k$ de $E$ est égal à* $\dfrac{n!}{k!\,(n-k)!}$.

Remarques. (i) Par définition, $(\forall\, k \in [\![0, n]\!])\big[\, C_n^k \in \mathbb{N}^* \big]$ et donc $k!$ divise $A_n^k$.
(ii) $(\forall\, n \in \mathbb{N})\big[\, C_n^0 = C_n^n = 1 \,\big]$.

**Exercice 2.1** Soit $n \in \mathbb{N}^*$. Déterminer le cardinal de l'ensemble $\Omega_n^k$ des $k$-arrangements $(i_1, \ldots, i_k)$ de $[\![1, n]\!]$ tels que $1 \leqslant i_1 < \cdots < i_k \leqslant n$.

| $n$ | $k=0$ | $k=1$ | $k=2$ | $k=3$ | $k=4$ | $k=5$ | $k=6$ | $\cdots$ | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | | | | | | | | | |
| 1 | 1 | 1 | | | | | | | | |
| 2 | 1 | 2 | 1 | | | | | | | |
| 3 | 1 | 3 | 3 | 1 | | | | | | |
| 4 | 1 | 4 | 6 | 4 | 1 | | | | | |
| 5 | 1 | 5 | 10 | 10 | 5 | 1 | | | | |
| 6 | 1 | 6 | 15 | 20 | 15 | 6 | 1 | | | |
| $\vdots$ | $\vdots$ | | | | | | | | | |
| $m-1$ | 1 | $m-1$ | $\cdots$ | $C_{m-1}^{k-1}$ | $C_{m-1}^{k}$ | $\cdots$ | $\cdots$ | $m-1$ | 1 | |
| $m$ | 1 | $m$ | $\cdots$ | $\cdots$ | $C_{m}^{k}$ | $\cdots$ | $\cdots$ | $\cdots$ | $m$ | 1 |

**Table 2.1** — Triangle de Pascal.

### 2.1.2 Coefficients binomiaux

Les coefficients $C_n^k$ introduits dans la proposition 2.2 sont également notés $\binom{n}{k}$ et appelés *coefficients binomiaux*.

**Proposition 2.3** *Soit $n \in \mathbb{N}$. On a*

1. $\big(\forall\, k \in [\![0,n]\!]\big)\big[\, C_n^k = C_n^{n-k} \,\big]$ ;
2. $\big(\forall\, k \in [\![0,n-1]\!]\big)\Big[\, C_n^{k+1} = \frac{n-k}{k+1}\, C_n^k \,\Big]$ ;
3. $\big(\forall\, k \in [\![1,n]\!]\big)\big[\, C_n^k = C_{n-1}^k + C_{n-1}^{k-1} \,\big]$ *(identités de Pascal, fondamental !).*

Remarques. (i) Le deuxième groupe d'identités montre que, pour $n \in \mathbb{N}^*$, la suite $(C_n^k)_{k\in[\![0,n]\!]}$ est croissante sur $[\![0, \lfloor (n+1)/2 \rfloor]\!]$ et décroissante sur $[\![\lceil (n-1)/2 \rceil, n]\!]$. Le maximum est atteint en $n/2$ si $n$ est pair et en $(n \pm 1)/2$ si $n$ est impair.
(ii) Les identités de Pascal permettent de retrouver les $C_n^k$ à l'aide du *triangle de Pascal* dont la construction est schématisée par le tableau 2.1.

**Exercice 2.2** Soit $n \in \mathbb{N} \setminus \{0,1\}$ et soit $k \in [\![2,n]\!]$. On pose

$$\begin{aligned}\Omega_n^k &= \left\{(i_1,\dots,i_k) \in [\![1,n]\!]^k \;\middle|\; 1 \leqslant i_1 < \cdots < i_k \leqslant n\right\},\\ \Upsilon_{n+1}^k &= \left\{(i_1,\dots,i_{k-1},n+1) \in [\![1,n+1]\!]^k \;\middle|\; 1 \leqslant i_1 < \cdots < i_{k-1} \leqslant n\right\}.\end{aligned}$$

Montrer que $\Omega_n^k \cup \Upsilon_{n+1}^k = \Omega_{n+1}^k$.

**Exercice 2.3** Démontrer par induction :

1. pour tout $(n,r) \in \mathbb{N}^2$, $\displaystyle\sum_{k=0}^{r} C_{n+k}^k = C_{n+r+1}^r$ ;
2. pour tout $(n,r) \in \mathbb{N}^2$ tel que $n \geqslant r \geqslant 0$, $\displaystyle\sum_{k=r}^{n} C_k^r = C_{n+1}^{r+1}$.

**Proposition 2.4 (convolution de Vandermonde)**
*Soient $(m,n) \in \mathbb{N}^2$, $r \in [\![0, \min(m,n)]\!]$. On a :*

$$C_{m+n}^r = \sum_{k=0}^{r} C_m^k C_n^{r-k}.$$

**Théorème 2.1 (formule du binôme de Newton)** *Soient $(A,+,\cdot\,)$ un anneau, $a,b$ deux éléments permutables de $A$ (i.e., tels que $a \cdot b = b \cdot a$), $n \in \mathbb{N}$. Alors,*

$$(a+b)^n \;=\; \sum_{k=0}^{n} C_n^k (a^k \cdot b^{n-k})$$

*(où, par convention, $a^0 = b^0 = 1_A$).*

**Corollaire 2.1**

1. $(\forall n \in \mathbb{N})\left[\sum_{k=0}^{n} C_n^k = 2^n\right]$,
2. $(\forall n \in \mathbb{N}^*)\left[\sum_{k=0}^{n} (-1)^k C_n^k = 0\right]$.

Démonstration. Formule du binôme dans $(\mathbb{R},+,\times)$ avec $a=b=1$ puis $a=-1$ et $b=1$. □

Remarque. Le premier groupe d'identités prouve la dernière égalité de la proposition 1.1 (p. 22).

**Exercice 2.4** Démontrer l'identité de Vandermonde en déterminant le coefficient de $a^r b^{m+n-r}$ dans $(a+b)^{m+n}$ puis dans $(a+b)^m (a+b)^n$.

## 2.2 Principe d'exclusion-inclusion

**Théorème 2.2 (formule de Sylvester)** *Soit $(A_i)_{i\in[\![1,n]\!]}$, $n \geqslant 2$, une famille finie d'ensembles finis. On a*

$$\begin{aligned}\left|\bigcup_{i=1}^n A_i\right| &= |A_1| + \cdots + |A_n| - \sum_{1\leqslant i_1<i_2\leqslant n} |A_{i_1}\cap A_{i_2}| + \sum_{1\leqslant i_1<i_2<i_3\leqslant n} |A_{i_1}\cap A_{i_2}\cap A_{i_3}| \\ &\quad + \cdots + (-1)^{k-1} \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} |A_{i_1}\cap\cdots\cap A_{i_k}| + \cdots + (-1)^{n-1}|A_1\cap\cdots\cap A_n| \\ &= \sum_{k=1}^n (-1)^{k-1} \sum_{(i_1,\ldots,i_k)\in\,\Omega_n^k} |A_{i_1}\cap\cdots\cap A_{i_k}|\,,\end{aligned}$$

*où* $\Omega_n^k = \big\{(i_1,\ldots,i_k)\in[\![1,n]\!]^k \;\big|\; 1\leqslant i_1<\cdots<i_k\leqslant n\big\}$.

**Exercice 2.5** Sur un total de 2092 étudiants suivant au moins un cours parmi les options anglais (A), espagnol (E) et russe (R), 1232 suivent A, 879 suivent E, 114 suivent R, 103 suivent A et E, 23 suivent A et R, et 14 suivent E et R. Combien d'étudiants suivent les 3 options ?

**Exercice 2.6** Une permutation d'une disposition ordonnée d'objets qui ne laisse aucun objet à sa position originale est appelée un dérangement. Par exemple, $(2,1,4,5,3)$ est un dérangement de $(1,2,3,4,5)$, mais $(2,1,5,4,3)$ n'en est pas un. On se propose de déterminer le nombre $D_n$ de dérangements de $n$ objets.
On dira qu'une permutation vérifie la propriété $P_i$ si elle laisse le $i$-ème élément dans sa position originale et on notera $\mathcal{N}\big(P_{i_1},\ldots,P_{i_k}\big)$, $k\in[\![1,n]\!]$, le nombre de permutations vérifiant $P_{i_1},\ldots,P_{i_k}$.

1. Donner l'expression de $D_n$ en fonction du nombre total $N$ de permutations de $n$ objets et des $\mathcal{N}\big(P_{i_1},\ldots,P_{i_k}\big)$.
2. Donner les expressions de $N$ et des $\mathcal{N}\big(P_{i_1},\ldots,P_{i_k}\big)$ en fonction de $n$ et $k$.
3. En déduire : $D_n \underset{n\infty}{\sim} n!/\mathrm{e}$.

**Proposition 2.5** *Soient $A$ et $B$ deux ensembles non vides et posons $m = |A|$ et $n = |B|$.*

1. *Le nombre d'applications de $A$ dans $B$ est égal à $n^m$.*
2. *Le nombre d'injections de $A$ dans $B$ est égal à $A_n^m$ si $m \leqslant n$, 0 sinon.*
3. *Le nombre de surjections de $A$ dans $B$ est égal à 0 si $m < n$, $n!$ si $m = n$ et $\sum_{k=0}^{n}(-1)^k C_n^k (n-k)^m$ si $m > n$.*

DÉMONSTRATION. **1.** Il y a $n$ choix possibles pour l'image de chacun des $m$ éléments de $A$, soit un total de $n^m$ possibilités.
**2.** Voir définition 2.1 et proposition 2.1.
**3.** Seul le cas $m > n$ nécessite une preuve (les cas $m < n$ et $m = n$ sont triviaux). Soit $E$ l'ensemble des applications de $A$ dans $B$. Le nombre de surjections de $A$ dans $B$ est

$$\begin{aligned} N &= |E| - \left|\left\{f \in E \mid f \text{ non surjective}\right\}\right| \\ &= n^m - \left|\left\{f \in E \mid (\exists\, y \in B)[y \notin f(A)]\ \right\}\right|. \end{aligned}$$

En notant $y_1, \ldots, y_n$ les éléments de $B$ et en posant $E_i = \left\{f \in E \mid y_i \notin f(A)\right\}$, nous obtenons $N = n^m - \left|\bigcup_{i=1}^{n} E_i\right|$, soit encore, d'après la formule de Sylvester,

$$N = n^m - \sum_{k=1}^{n} (-1)^{k-1} \sum_{(i_1,\ldots,i_k)\in\,\Omega_n^k} |E_{i_1} \cap \cdots \cap E_{i_k}|.$$

Or $|E_{i_1} \cap \cdots \cap E_{i_k}| = \left|\left\{f \in E \mid (y_{i_1} \notin f(A)) \wedge \cdots \wedge (y_{i_k} \notin f(A))\right\}\right|$ est égal au nombre d'applications de $A$ dans $B \setminus \{y_{i_1}, \ldots, y_{i_k}\}$, c'est à dire $(n-k)^m$. Ainsi,

$$N = n^m - \sum_{k=1}^{n} (-1)^{k-1} \sum_{(i_1,\ldots,i_k)\in\,\Omega_n^k} (n-k)^m.$$

Puisque $\left\{\{i_1, \ldots, i_k\} \mid 1 \leqslant i_1 < \cdots < i_k \leqslant n\right\}$ est l'ensemble des parties de $[\![1, n]\!]$ de cardinal $k$, nous avons donc

$$N = n^m - \sum_{k=1}^{n} (-1)^{k-1} C_n^k (n-k)^m$$

et le résultat final s'obtient en remarquant que $n^m = C_n^0 (n-0)^m$. □

## 2.3 Relations de récurrence linéaires à coefficients constants

**Définition 2.3** *Soient $E$ un $\mathbb{K}$-espace vectoriel, $(a_1, \ldots, a_k) \in \mathbb{K}^k$ avec $a_k \neq 0_{\mathbb{K}}$, $f$ une application de $\mathbb{N}$ dans $E$. On définit une relation de récurrence sur $E$, linéaire, d'ordre $k$, à coefficients constants, par une équation de la forme*

$$u_n \;=\; \sum_{i=1}^{k} a_i u_{n-i} \;+\; f(n)\,, \quad n \in [\![k, \infty[\![. \tag{2.1}$$

♢ *La relation est dite homogène si $f = 0_{E^{\mathbb{N}}}$ et non homogène dans le cas contraire.*
♢ *On dit qu'une suite $(u_n)_{n\in\mathbb{N}}$ dans $\mathbb{K}$ est solution de la récurrence (2.1) si elle vérifie cette relation pour tout $n \in [\![k, \infty[\![$.*
♢ *On appelle conditions initiales les valeurs affectées à $u_0, \ldots, u_{k-1}$ pour démarrer la récurrence.*

**Proposition 2.6** *Les conditions initiales étant fixées, la récurrence (2.1) admet une solution unique.*

Démonstration. L'existence est immédiate. L'unicité s'établit en vérifiant $(\forall n \in \mathbb{N})[u_n = u'_n]$ par induction pour $(u_n)_{n\in\mathbb{N}}$ et $(u'_n)_{n\in\mathbb{N}}$ solutions de (2.1) telles que $(\forall m \in [\![0, k-1]\!])[u_m = u'_m]$. □

### 2.3.1 Récurrences homogènes

Nous considérons ici les relations de récurrence linéaires homogénes d'ordre $k$ à coefficients constants de la forme

$$u_n \;=\; \sum_{i=1}^{k} a_i u_{n-i}\,, \quad n \in [\![k, \infty[\![. \tag{2.2}$$

où les $a_i$ sont des complexes et où les solutions sont à rechercher parmi les suites dans $\mathbb{C}$.

**Proposition 2.7** *L'ensemble $\mathcal{S}^0$ des solutions de (2.2) est un sous-espace vectoriel de dimension $k$ du $\mathbb{C}$-espace vectoriel des suites complexes.*

**Définition 2.4** *Le polynôme caractéristique de la récurrence (2.2) est l'élément $P$ de $\mathbb{C}[X]$ défini par*

$$P \;=\; X^k \;-\sum_{i=1}^{k} a_i X^{k-i}.$$

**Théorème 2.3** *Si $P$ possède $k$ racines deux à deux distinctes $r_1, \ldots, r_k$, alors les solutions de (2.2) sont de la forme*

$$u_n \;=\; \sum_{j=1}^{k} \alpha_j \, r_j^n \,,$$

*où les $\alpha_j$ sont des constantes complexes fixées par les conditions initiales.*

**Exercice 2.7** Suite de Fibonacci. Trouver la solution de la relation de récurrence $u_n = u_{n-1} + u_{n-2}$ avec les conditions initiales $(u_0, u_1) = (0, 1)$.

**Théorème 2.4** *(généralisation du théorème 2.3) Si $P$ admet $p$ racines deux à deux distinctes $r_1, \ldots, r_p$, alors les solutions de (2.2) sont de la forme*

$$u_n \;=\; \sum_{j=1}^{p} \Bigg( \sum_{l=0}^{m_j-1} \alpha_{\,j,l} \; n^l \Bigg) r_j^n \,,$$

*où $m_j$ désigne l'ordre de multiplicité de $r_j$ et où les $\alpha_{\,j,l}$ sont des constantes complexes fixées par les conditions initiales.*

**Exercice 2.8** Trouver la solution de chacune des relations de récurrence suivantes.

1. $u_n = -3u_{n-1} - 3u_{n-2} - u_{n-3}, \quad (u_0, u_1, u_2) = (1, -2, -1)$ ;
2. $u_n = 7u_{n-2} + 6u_{n-3}, \quad (u_0, u_1, u_2) = (9, 10, 32)$ ;
3. $u_n = -3u_{n-1} + 4u_{n-3}, \quad (u_0, u_1, u_2) = (3, -9, 33)$.

### 2.3.2 Récurrences non homogènes

On s'intéresse ici aux relations de récurrence linéaires non homogènes à coefficients constants de la forme (2.1) où les $a_i$ sont des complexes et dont les solutions sont à rechercher parmi les suites dans $\mathbb{C}$.

**Proposition 2.8** *Notons $\mathcal{S}$ l'ensemble des solutions de (2.1) et soit $\mathcal{S}^0$ l'ensemble des solutions de la récurrence homogène (2.2) associée. On a, pour toute suite $(u_n)_{n\in\mathbb{N}} \in \mathcal{S}$,*

$$\mathcal{S} \;=\; \left\{ \left(u_n + u_n^0\right)_{n\in\mathbb{N}} \,\middle|\, \left(u_n^0\right)_{n\in\mathbb{N}} \in \mathcal{S}^0 \right\}.$$

Autrement dit, la *solution générale* de (2.1) est la somme d'une *solution particulière* de (2.1) et de la solution générale de la récurrence homogène (2.2) associée. Il n'existe cependant pas de méthode universelle pour la recherche d'une solution particulière, excepté pour certaines classes de fonctions $f$.

**Théorème 2.5** *Soit $s \in \mathbb{C}^*$ et soit $Q$ un polynôme non nul de $\mathbb{C}[X]$. On considère la relation de récurrence*

$$u_n \;=\; \sum_{i=1}^{k} a_i u_{n-i} \;+\; s^n Q(n) \tag{2.3}$$

*et on note $P$ le polynôme caractéristique de la relation homogène qui lui est associée. Toute solution de (2.3) est solution de la relation de récurrence homogène d'ordre $k+\deg(Q)+1$ de polynôme caractéristique*

$$(X-s)^{\deg(Q)+1} P.$$

Remarque. Si le "second membre" $f$ est de la forme $\sum_{j=1}^{l} f_j$, la somme des solutions particulières des $l$ relations

$$u_n^{(j)} \;=\; \sum_{i=1}^{k} a_i u_{n-i}^{(j)} \;+\; f_j(n)\,, \qquad j = 1, \ldots, l\,,$$

est une solution particulière de (2.1).

**Corollaire 2.2** *Soit $P$ le polynôme caractéristique de la relation homogène associée à (2.3). Une solution particulière de (2.3) est de la forme*

$$\begin{cases} s^n R(n) & \text{si } s \text{ n'est pas une racine de } P \\ s^n n^m R(n) & \text{si } s \text{ est une racine d'ordre de multiplicité } m \text{ de } P, \end{cases}$$

*où $R$ est un polynôme de $\mathbb{C}[X]$ de même degré que $Q$.*

**Exercice 2.9** Donner la forme d'une solution particulière de la récurrence $u_n = 6u_{n-1} - 9u_{n-2} + f(n)$ pour (i) $f(n) = 3^n$, (ii) $f(n) = n \cdot 3^n$, (iii) $f(n) = n^2 \cdot 2^n$ et (iv) $f(n) = (n^2 + 1)3^n$.

**Exercice 2.10** Donner l'ensemble des solutions des relations de récurrence suivantes.

1. $u_n = 4u_{n-1} - 4u_{n-2} + (n+1)2^n$ ;
2. $u_n = 5u_{n-1} - 6u_{n-2} + 2^n + 3n$ .

**Exercice 2.11** Soit $u_n = \sum_{k=1}^{n} k(k+1)/2$ la somme des $n$ premiers nombres triangulaires. Vérifier que la suite $(u_n)_{n\in\mathbb{N}^*}$ est solution d'une relation de récurrence linéaire d'ordre 1 que l'on résoudra.

# Chapitre 3

# Relations et ensembles ordonnés

**Relations**

♢ Relations : représentation des liaisons entre les éléments d'un ensemble et les éléments d'un autre ensemble, ou entre les éléments d'un même ensemble (relation interne).

♢ Relations d'équivalence : relations internes réflexives, symétriques et transitives (exemple trivial : égalité sur $\mathbb{R}$).

**Ensembles ordonnés**

♢ Formalise la comparaison des éléments d'un même ensemble.

♢ Exemples : $(\mathbb{N}, \leqslant)$, $(\mathcal{P}(E), \subset)$.

# 3.1 Relations

## 3.1.1 Définitions et propriétés

**Définition 3.1** *Une relation (binaire) d'un ensemble $A$ vers un ensemble $B$ est une partie $\mathcal{R}$ de $A \times B$. Lorsque $A = B$, on parle de relation (binaire interne) sur $A$. On note $a\mathcal{R}b$ pour indiquer que $(a, b) \in \mathcal{R}$.*

Remarques. (i) $(A, B, \mathcal{R})$ est une correspondance de $A$ vers $B$ (définition 1.20).
$\mathcal{R}$ représente donc une application si et seulement si $(\forall a \in A)(\exists! b \in B)[\, a\mathcal{R}b\,]$.
(ii) Une relation portant sur une collection d'ensembles $\{A_1, \ldots, A_n\}$, $n \geqslant 2$, est dite *$n$-aire*. Il s'agit d'une partie de $A_1 \times \cdots \times A_n$.

**Exemple 3.1** (i) "est valeur propre de" de $\mathbb{C}$ vers $\mathrm{M}_n(\mathbb{C})$ :
$\big\{(\lambda, A) \in \mathbb{C} \times \mathrm{M}_n(\mathbb{C}) \,\big|\, (\exists X \in \mathrm{M}_{n,1}(\mathbb{C}))\big[(X \neq 0_{\mathrm{M}_{n,1}(\mathbb{C})}) \wedge (AX = \lambda X)\big]\big\}$ ;
(ii) $\underset{\infty}{\sim}$ sur le $\mathbb{C}$-espace vectoriel $\mathcal{S}$ des suites à valeurs complexes : $\big\{\big((u_n)_n, (v_n)_n\big) \in \mathcal{S}^2 \big| u_n - v_n = \mathcal{O}_\infty(v_n)\big\}$.

### Opérations sur les relations

Une relation étant un ensemble, on a $\mathcal{R}_1 \subset \mathcal{R}_2 \;\Leftrightarrow\; \big(\forall\,(a, b) \in A \times B\big)\big[\, a\mathcal{R}_1 b \;\to\; a\mathcal{R}_2 b\,\big]$.
On définit également
$\diamondsuit$ l'*intersection* de $\mathcal{R}_1$ et $\mathcal{R}_2$ : $\mathcal{R}_1 \cap \mathcal{R}_2 = \big\{(a, b) \in A \times B \;\big|\; (a\mathcal{R}_1 b) \wedge (a\mathcal{R}_2 b)\big\}$ ;
$\diamondsuit$ la *réunion* de $\mathcal{R}_1$ et $\mathcal{R}_2$ : $\mathcal{R}_1 \cup \mathcal{R}_2 = \big\{(a, b) \in A \times B \;\big|\; (a\mathcal{R}_1 b) \vee (a\mathcal{R}_2 b)\big\}$ ;
$\diamondsuit$ le *complémentaire* de $\mathcal{R}$ : $\overline{\mathcal{R}} = \big\{(a, b) \in A \times B \;\big|\; \neg(a\mathcal{R}b)\big\}$.

**Définition 3.2** *Soit $\mathcal{R}$ une relation de $A$ vers $B$. On définit la relation réciproque de $\mathcal{R}$, notée $\mathcal{R}^{-1}$, de $B$ vers $A$, par*

$$\big(\forall\,(b, a) \in B \times A\big)\big[\, b\mathcal{R}^{-1}a \;\Leftrightarrow\; a\mathcal{R}b\,\big].$$

**Exercice 3.1** Soient $\mathcal{R}$, $\mathcal{R}_1$ et $\mathcal{R}_2$ des relations binaires sur un ensemble $A$. Montrer :

1. $\big(\mathcal{R}^{-1}\big)^{-1} = \mathcal{R}$ ;
2. $\big(\overline{\mathcal{R}}\big)^{-1} = \overline{\mathcal{R}^{-1}}$ ;
3. $\big(\mathcal{R}_1 \cup \mathcal{R}_2\big)^{-1} = \mathcal{R}_1^{-1} \cup \mathcal{R}_2^{-1}$ ;
4. $\big(\mathcal{R}_1 \cap \mathcal{R}_2\big)^{-1} = \mathcal{R}_1^{-1} \cap \mathcal{R}_2^{-1}$ ;
5. $\mathcal{R}_1 \subset \mathcal{R}_2 \;\Leftrightarrow\; \mathcal{R}_1^{-1} \subset \mathcal{R}_2^{-1}$.

**Définition 3.3** *Étant données une relation $\mathcal{R}_1$ de $A$ vers $B$ et une relation $\mathcal{R}_2$ de $B$ vers $C$, on définit le produit (ou la relation composée) de $\mathcal{R}_1$ et $\mathcal{R}_2$, noté $\mathcal{R}_1 \cdot \mathcal{R}_2$, par*

$$(\forall\,(a,c) \in A \times C)\big[\, a(\mathcal{R}_1 \cdot \mathcal{R}_2)c \;\Leftrightarrow\; (\exists\, b \in B)[(a\mathcal{R}_1 b) \wedge (b\mathcal{R}_2 c)]\,\big].$$

**Proposition 3.1** *Le produit de relations est associatif.*

REMARQUE. Le produit de relations binaires sur un ensemble $A$ admet pour élément neutre la *relation identité* sur $A$, notée $\mathrm{Id}_A$, définie par $\mathrm{Id}_A = \big\{(a,b) \in A^2 \,|\, a = b\big\}$.

**Exercice 3.2** Soient $\mathcal{R}$, $\mathcal{R}_1$ et $\mathcal{R}_2$ des relations binaires sur un ensemble $A$. Montrer :

1. $\big(\mathcal{R}_1 \cdot \mathcal{R}_2\big)^{-1} = \mathcal{R}_2^{-1} \cdot \mathcal{R}_1^{-1}$ ;
2. $\big(\mathcal{R}_1 \cup \mathcal{R}_2\big) \cdot \mathcal{R} = \big(\mathcal{R}_1 \cdot \mathcal{R}\big) \cup \big(\mathcal{R}_2 \cdot \mathcal{R}\big)$ et $\mathcal{R} \cdot \big(\mathcal{R}_1 \cup \mathcal{R}_2\big) = \big(\mathcal{R} \cdot \mathcal{R}_1\big) \cup \big(\mathcal{R} \cdot \mathcal{R}_2\big)$ (i.e., le produit est distributif par rapport à l'union).

**Définition 3.4** *Soit $\mathcal{R}$ une relation binaire sur un ensemble $A$. On appelle itéré de $\mathcal{R}$ et on note $\mathcal{R}^*$ la relation $\bigcup_{n\in\mathbb{N}} \mathcal{R}^n$ sur $A$ définie par $\mathcal{R}^0 = \mathrm{Id}_A$ et $(\forall\, n \in \mathbb{N})[\mathcal{R}^{n+1} = \mathcal{R}\cdot\mathcal{R}^n]$. On appelle itéré strict de $\mathcal{R}$ et on note $\mathcal{R}^+$ la relation $\bigcup_{n\in\mathbb{N}^*} \mathcal{R}^n$ sur $A$.*

**Exemple 3.2** Pour $\mathcal{R} = \big\{(k,l) \,|\, k+1 = l\big\}$ sur $\mathbb{N}$, on a $\mathcal{R}^+ = <$ et $\mathcal{R}^* = \leqslant$.

**Exercice 3.3** Soient $\mathcal{R}_1$ et $\mathcal{R}_2$ deux relations binaires sur un ensemble $A$. Montrer :
$\mathcal{R}_1 \subset \mathcal{R}_2 \;\Rightarrow\; \mathcal{R}_1^+ \subset \mathcal{R}_2^+$.

**Exercice 3.4** Soit $\mathcal{R}$ une relation binaire sur un ensemble $A$.

1. Montrer : $(\forall\, n \in \mathbb{N}^*)\big[(\mathrm{Id}_A \cup \mathcal{R})^n = \bigcup_{i=0}^{n} \mathcal{R}^i\big]$.
2. En déduire : $(\mathrm{Id}_A \cup \mathcal{R})^+ = \mathcal{R}^*$.

### Quelques propriétés des relations binaires internes

Une relation binaire $\mathcal{R}$ sur un ensemble $A$ est dite

$\diamondsuit$ *totale à gauche* si $(\forall\, a \in A)(\exists\, b \in A)[\, a\mathcal{R}b\,]$ ;

$\diamondsuit$ *totale à droite* si $(\forall\, b \in A)(\exists\, a \in A)[\, a\mathcal{R}b\,]$ ;

$\diamondsuit$ *réflexive* si $(\forall\, a \in A)[\, a\mathcal{R}a\,]$ ;

$\diamondsuit$ *irréflexive* si $(\forall\, a \in A)\big[\neg(a\mathcal{R}a)\big]$ ;

$\diamondsuit$ *symétrique* si $(\forall\, a, b \in A)[\, a\mathcal{R}b \;\Rightarrow\; b\mathcal{R}a\,]$ ;

$\diamondsuit$ *antisymétrique* si $(\forall\, a, b \in A)\big[\,(a\mathcal{R}b) \wedge (b\mathcal{R}a) \;\Rightarrow\; a = b\,\big]$ ;

$\diamondsuit$ *transitive* si $(\forall\, a, b, c \in A)\big[\,(a\mathcal{R}b) \wedge (b\mathcal{R}c) \;\Rightarrow\; a\mathcal{R}c\,\big]$ .

**Exemple 3.3** (i) $\mathcal{R} = \big\{(a,b) \,|\, \|\, a - b \,\|_2 = 1\big\}$ sur $\mathbb{R}^n$ est irréflexive et symétrique ;
(ii) $\mathcal{R} = \big\{(a,b) \,|\, a \subset b\big\}$ sur $\mathcal{P}(\mathbb{N})$ est réflexive, antisymétrique et transitive ;
(iii) $\mathcal{R} = \big\{(a,b) \,|\, |a \cap b| < +\infty\big\}$ sur $\mathcal{P}(\mathbb{N})$ est seulement symétrique.

**Exercice 3.5** Soient $\mathcal{R}$, $\mathcal{R}_1$ et $\mathcal{R}_2$ des relations binaires sur un ensemble $A$. Montrer que :

1. $\mathcal{R} \cap \mathcal{R}^{-1}$ et $\mathcal{R} \cup \mathcal{R}^{-1}$ sont symétriques ;
2. si $\mathcal{R}_1$ et $\mathcal{R}_2$ sont transitives, alors $\mathcal{R}_1 \cap \mathcal{R}_2$ est transitive.

**Proposition 3.2** *Une relation binaire interne $\mathcal{R}$ est transitive si et seulement si $\mathcal{R} = \mathcal{R}^+$.*

**Exercice 3.6** Soit $\mathcal{R}$ une relation binaire sur un ensemble $A$. Montrer :

1. $(\forall\, i, j \in \mathbb{N})\big[\mathcal{R}^{i+j} = \mathcal{R}^i \cdot \mathcal{R}^j\big]$ ;
2. $\mathcal{R}$ symétrique $\Rightarrow$ $\mathcal{R}^+$ symétrique.

### 3.1.2 Représentation matricielle

Une relation $\mathcal{R}$ d'un ensemble $A = \{a_1, \ldots, a_m\}$ vers un ensemble $B = \{b_1, \ldots, b_n\}$ peut être représentée par la matrice booléenne $M_{\mathcal{R}} = [\theta_{ij}] \in \mathbf{M}_{m,n}(\{0,1\})$ définie par

$$\theta_{ij} = \begin{cases} 1 & \text{si } a_i \mathcal{R} b_j\,, \\ 0 & \text{sinon}\,. \end{cases}$$

**Exemple 3.4** Représentation de la relation $\mathcal{R} = \big\{(a,b)\,|\,a<b\big\}$ de $A=\{1,2\}$ vers $B=\{1,2,3\}$ :

$$M_{\mathcal{R}} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

**Définition 3.5** *Soient $U=[u_{ij}]$ et $V=[v_{ij}]$ deux matrices de $\mathbf{M}_{m,n}(\{0,1\})$. On appelle disjonction de $U$ et $V$, et on note $U \vee V$ la matrice $[u_{ij} \vee v_{ij}]$ de $\mathbf{M}_{m,n}(\{0,1\})$. De même, $U \wedge V = [u_{ij} \wedge v_{ij}] \in \mathbf{M}_{m,n}(\{0,1\})$ désigne la conjonction de $U$ et $V$.*

**Définition 3.6** *Soient $U=[u_{il}] \in \mathbf{M}_{m,k}(\{0,1\})$ et $V=[v_{lj}] \in \mathbf{M}_{k,n}(\{0,1\})$. On appelle produit booléen de $U$ par $V$, et on note $U \odot V$ la matrice $[\theta_{ij}] \in \mathbf{M}_{m,n}(\{0,1\})$ définie par*

$$\big(\forall (i,j) \in [\![1,m]\!] \times [\![1,n]\!]\big)\Big[\,\theta_{ij} = \textstyle\bigvee_{l=1}^{k}(u_{il} \wedge v_{lj})\,\Big].$$

Soient $A$, $B$ deux ensembles finis et soient $\mathcal{R}_1$, $\mathcal{R}_2$ et $\mathcal{R}$ trois relations de $A$ vers $B$. On a

$$M_{\mathcal{R}_1 \cup \mathcal{R}_2} \;=\; M_{\mathcal{R}_1} \vee M_{\mathcal{R}_2}\,, \qquad M_{\mathcal{R}_1 \cap \mathcal{R}_2} \;=\; M_{\mathcal{R}_1} \wedge M_{\mathcal{R}_2} \quad \text{et} \quad M_{\mathcal{R}^{-1}} \;=\; {}^{t}M_{\mathcal{R}}\,.$$

Si $\mathcal{R}_2$ est une relation de $B$ vers un autre ensemble fini $C$, alors

$$M_{\mathcal{R}_1 \cdot \mathcal{R}_2} \;=\; M_{\mathcal{R}_1} \odot M_{\mathcal{R}_2}\,.$$

Enfin, dans le cas d'une une relation binaire $\mathcal{R}$ sur un ensemble fini $A$ on a

$$\begin{aligned}
&\diamondsuit\ \mathcal{R} \text{ réflexive} && \Leftrightarrow && \mathrm{Tr}(M_{\mathcal{R}}) = |A|\,; \\
&\diamondsuit\ \mathcal{R} \text{ irréflexive} && \Leftrightarrow && \mathrm{Tr}(M_{\mathcal{R}}) = 0\,; \\
&\diamondsuit\ \mathcal{R} \text{ symétrique} && \Leftrightarrow && M_{\mathcal{R}} \text{ symétrique}\,; \\
&\diamondsuit\ \mathcal{R} \text{ antisymétrique} && \Leftrightarrow && M_{\mathcal{R}} \wedge {}^{t}M_{\mathcal{R}} \text{ diagonale}\,.
\end{aligned}$$

### 3.1.3 Clôture de relations

**Définition 3.7** *Soit $\mathcal{R}$ une relation sur un ensemble $A$. La clôture de $\mathcal{R}$ relativement à une propriété $P$ donnée est une relation $\mathcal{R}'$ sur $A$ telle que*

1. $\mathcal{R}' \supset \mathcal{R}$ ,
2. $\mathcal{R}'$ *possède la propriété* $P$,
3. $\mathcal{R}' \subset \rho$ *pour toute relation* $\rho$ *sur* $A$ *satisfaisant les deux points qui précèdent.*

**Proposition 3.3** *Pour toute relation $\mathcal{R}$ sur un ensemble $A$ donné,*

1. *la clôture réflexive de* $\mathcal{R}$ *est* $\mathcal{R} \cup \mathrm{Id}_A$ ,
2. *la clôture symétrique de* $\mathcal{R}$ *est* $\mathcal{R} \cup \mathcal{R}^{-1}$,
3. *la clôture transitive de* $\mathcal{R}$ *est* $\mathcal{R}^+$.

### 3.1.4 Relations d'équivalence

**Définition 3.8** *Soit $\mathcal{R}$ une relation binaire sur un ensemble $A$. On dit que $\mathcal{R}$ est une relation d'équivalence si et seulement si elle est réflexive, symétrique et transitive.*

**Définition 3.9** *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble $A$.*

- ♢ *Pour tout $a \in A$, on appelle classe d'équivalence de $a$, et on note $\mathcal{R}[a]$ l'ensemble $\{b \in A \,|\, a\mathcal{R}b\}$.*
- ♢ *On appelle ensemble quotient de $A$ par $\mathcal{R}$, et on note $A/\mathcal{R}$ l'ensemble des classes d'équivalence $\{\,\mathcal{R}[a]\,;\, a \in A\}$.*

**Exemple 3.5** Pour tout $m \in \mathbb{N}^*$, la relation $\mathcal{R} = \big\{(a,b) \in \mathbb{Z}^2 \,|\, a \equiv b \,(\mathrm{mod}\, m)\big\}$ est une relation d'équivalence et $(\forall\, a \in \mathbb{Z})\big[\,\mathcal{R}[a] = \{a + km\,;\, k \in \mathbb{Z}\}\big]$.

**Exercice 3.7** Soit $\mathcal{R}$ une relation binaire interne. Montrer que la clôture transitive de la clôture symétrique de la clôture réflexive de $\mathcal{R}$ est une relation d'équivalence.

**Proposition 3.4** *Soit $\mathcal{R}$ est une relation binaire interne. La plus petite relation d'équivalence contenant $\mathcal{R}$ est $\big(\mathcal{R} \cup \mathcal{R}^{-1}\big)^*$.*

**Proposition 3.5** *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble $A$ et soient $a, b$ deux éléments de $A$. On a $a\mathcal{R}b \Leftrightarrow \mathcal{R}[a] \cap \mathcal{R}[b] \neq \emptyset \Leftrightarrow \mathcal{R}[a] = \mathcal{R}[b]$.*

**Proposition 3.6** *Soit $A$ un ensemble.*

1. *Pour toute relation d'équivalence $\mathcal{R}$ sur $A$, $A/\mathcal{R}$ est une partition de $A$.*
2. *Réciproquement, pour toute partition $\Gamma = (A_i)_{i \in I}$ de $A$, il existe une relation d'équivalence $\mathcal{R}$ sur $A$ telle que $\Gamma = A/\mathcal{R}$.*

## 3.2 Ensembles ordonnés

### 3.2.1 Définitions

**Définition 3.10** *Soit $\mathcal{R}$ une relation binaire sur un ensemble $A$.*

- ♢ *On dit que $\mathcal{R}$ est une relation d'ordre large si et seulement si elle est réflexive, antisymétrique et transitive.*
- ♢ *Si $\mathcal{R}$ est irréflexive et transitive, on dit que $\mathcal{R}$ est une relation d'ordre strict.*

**Définition 3.11** *Soit $\mathcal{R}$ une relation d'ordre sur un ensemble $A$. On dit que $\mathcal{R}$ est un ordre total si et seulement si $(\forall\, a, b \in A)\big[\, a \neq b \;\Rightarrow\; (a\mathcal{R}b) \vee (b\mathcal{R}a)\,\big]$. Dans le cas contraire, on dit qu'il s'agit d'un ordre partiel.*

**Exemple 3.6** (i) $\leqslant$ et $<$ usuels sur $\mathbb{R}$ sont des ordres totaux.
(ii) La relation de divisibilité (notée $|$) sur $\mathbb{N}$ est un ordre partiel.
(iii) $\subset$ sur $\mathcal{P}(E)$ est un ordre partiel.

NOTATION. Une relation d'ordre large (resp. strict) quelconque est notée $\preccurlyeq$ (resp. $\prec$).

**Définition 3.12** *Un ordre large $\preccurlyeq$ et un ordre strict $\prec$ sur un même ensemble $A$ sont dits associés si et seulement si $\preccurlyeq = \prec \cup \mathrm{Id}_A$ ($\Leftrightarrow \prec = \preccurlyeq \setminus \mathrm{Id}_A$). Autrement dit, pour tout $(a, b) \in A^2$, $a \preccurlyeq b \;\Leftrightarrow\; (a \prec b) \vee (a = b)$ et $a \prec b \;\Leftrightarrow\; (a \preccurlyeq b) \wedge (a \neq b)$.*

**Proposition 3.7** *Soient $\preccurlyeq$ et $\prec$ un ordre large et un ordre strict associés.*

1. *$b \prec a \Leftrightarrow \neg(a \preccurlyeq b)$ si $\preccurlyeq$ est total.*
2. *$b \prec a \Rightarrow \neg(a \preccurlyeq b)$ si $\preccurlyeq$ est partiel.*

**Définition 3.13** *On appelle ensemble ordonné tout couple $(A, \preccurlyeq)$ où $A$ est un ensemble et $\preccurlyeq$ une relation d'ordre large sur $A$.*

**Définition 3.14** *Soit $(A, \preccurlyeq)$ un ensemble ordonné.*

- ♢ *Deux éléments $a$ et $b$ de $A$ sont dits comparables si et seulement si $a \preccurlyeq b$ ou $b \preccurlyeq a$.*
- ♢ *$(A, \preccurlyeq)$ est dit totalement ordonné si et seulement si tous les éléments de $A$ sont deux à deux comparables, c'est-à-dire si et seulement si $\preccurlyeq$ est ordre total. Dans le cas contraire, $(A, \preccurlyeq)$ est dit partiellement ordonné.*

### 3.2.2 Représentation schématique

On représente un ensemble ordonné fini $(A, \preccurlyeq)$ de la façon suivante.

- ♢ À chaque élément de $A$ on associe un point du plan.
- ♢ Le fait que $a \preccurlyeq b$ est représenté par un segment (ou un arc) d'extrémités $a$ et $b$ n'intersectant aucun autre point et orienté par une flèche de $a$ vers $b$.
- ♢ Pour alléger le schéma, on ne considère pas toute la relation d'ordre :
  - ▷ on ne trace pas les boucles d'un élément vers lui-même (réduction réflexive) ;
  - ▷ si $a \preccurlyeq c$ mais $(\exists b \in A \setminus \{a, c\})[(a \preccurlyeq b) \wedge (b \preccurlyeq c)]$, alors on ne trace pas le segment (ou l'arc) d'extrémités $a$ et $c$ (réduction transitive).

Remarque. Si, de plus, pour chaque couple $(a, b) \in A^2$ tel que $a \preccurlyeq b$, on s'arrange pour que l'ordonnée du point associé à $a$ soit inférieure à l'ordonnée du point associé à $b$, alors il n'est pas nécessaire d'orienter les arcs et on obtient une représentation de $(A, \preccurlyeq)$ appelée *diagramme de Hasse*.

**Exemple 3.7** La représentation de la relation de divisibilité sur $[\![1, 6]\!]$ est donnée figure 3.1 et le diagramme de Hasse correspondant apparaît figure 3.2.

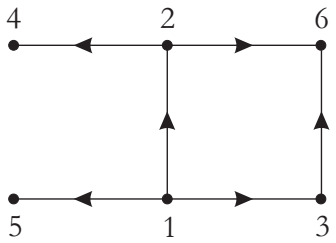


**Figure 3.1** — Représentation de $\big([\![1, 6]\!], |\big)$.

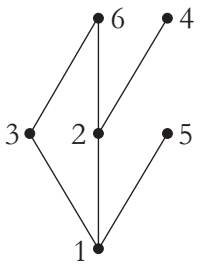


**Figure 3.2** — Diagramme de Hasse associé à $\big([\![1, 6]\!], |\big)$.

### 3.2.3 Produits d'ensembles ordonnés

**Définition 3.15** *Soient* $(A_1, \preccurlyeq_1)$ *et* $(A_2, \preccurlyeq_2)$ *deux ensembles ordonnés. On appelle produit direct de* $(A_1, \preccurlyeq_1)$ *et* $(A_2, \preccurlyeq_2)$ *l'ensemble ordonné* $(A_1 \times A_2, \preccurlyeq_{\mathrm{P}})$ *dont l'ordre* $\preccurlyeq_{\mathrm{P}}$*, appelé ordre produit, est défini par*

$$\big(\forall\,(a_1,a_2),\,(b_1,b_2) \in A_1 \times A_2\big)\big[\,(a_1,a_2) \preccurlyeq_{\mathrm{P}} (b_1,b_2) \;\Leftrightarrow\; (a_1 \preccurlyeq_1 b_1) \wedge (a_2 \preccurlyeq_2 b_2)\,\big].$$

**Exercice 3.8** Soient $(A_1, \preccurlyeq_1)$ et $(A_2, \preccurlyeq_2)$ deux ensembles ordonnés.

1. Montrer que $(A_1 \times A_2, \preccurlyeq_{\mathrm{P}})$ est un ensemble ordonné.
2. On suppose $|A_1| \geqslant 2$ et $|A_2| \geqslant 2$. Montrer que $(A_1 \times A_2, \preccurlyeq_{\mathrm{P}})$ n'est pas totalement ordonné même si $(A_1, \preccurlyeq_1)$ et $(A_2, \preccurlyeq_2)$ le sont.

**Définition 3.16** *Soient* $(A_1, \preccurlyeq_1)$ *et* $(A_2, \preccurlyeq_2)$ *deux ensembles ordonnés. On appelle produit lexicographique de* $(A_1, \preccurlyeq_1)$ *et* $(A_2, \preccurlyeq_2)$ *l'ensemble ordonné* $(A_1 \times A_2, \preccurlyeq_{\mathrm{L}})$ *dont l'ordre* $\preccurlyeq_{\mathrm{L}}$ *est défini par*

$$\big(\forall\,(a_1,a_2),\,(b_1,b_2) \in A_1 \times A_2\big)$$
$$\big[\,(a_1,a_2) \preccurlyeq_{\mathrm{L}} (b_1,b_2) \;\Leftrightarrow\; (a_1 \prec_1 b_1) \vee \big((a_1 = b_1) \wedge (a_2 \preccurlyeq_2 b_2)\big)\,\big].$$

**Exercice 3.9** Soient $(A_1, \preccurlyeq_1)$ et $(A_2, \preccurlyeq_2)$ deux ensembles ordonnés. Montrer que

1. $(A_1 \times A_2, \preccurlyeq_{\mathrm{L}})$ est un ensemble ordonné ;
2. $(A_1 \times A_2, \preccurlyeq_{\mathrm{L}})$ est totalement ordonné si $(A_1, \preccurlyeq_1)$ et $(A_2, \preccurlyeq_2)$ le sont.

Remarque. Le produit lexicographique peut être étendu au produit cartésien de $n$ ensembles $A_1, \ldots, A_n$ respectivement ordonnés par $\preccurlyeq_1, \ldots, \preccurlyeq_n$. Il s'agit de $(A_1 \times \cdots \times A_n, \preccurlyeq_{\mathrm{L}})$ où l'ordre strict $\prec_{\mathrm{L}}$ associé à $\preccurlyeq_{\mathrm{L}}$ est défini par

$$(a_1, \ldots, a_n) \prec_{\mathrm{L}} (b_1, \ldots, b_n) \;\Leftrightarrow$$
$$(a_1 \prec_1 b_1) \vee \big(\exists\, i \in [\![1, n-1]\!]\big)\big[(a_1 = b_1) \wedge \cdots \wedge (a_i = b_i) \wedge (a_{i+1} \prec_{i+1} b_{i+1})\big].$$

### 3.2.4 Éléments remarquables

**Définition 3.17** *Soient $(A, \preccurlyeq)$ un ensemble ordonné, $A' \in \mathcal{P}(A)$, $x \in A$.*

- ♢ *On dit que $x$ est un majorant (resp. minorant) de $A'$ dans $A$ si et seulement si $(\forall\, a \in A')[a \preccurlyeq x]$ (resp. $(\forall\, a \in A')[x \preccurlyeq a]$). On note $\mathrm{maj}_A(A')$ (resp. $\min_A(A')$) l'ensembles des majorants (resp. minorants) de $A'$ dans $A$.*
- ♢ *On dit que $x$ est un plus grand (resp. petit) élément de $A'$ si et seulement si $x \in A' \cap \mathrm{maj}_A(A')$ (resp. $x \in A' \cap \min_A(A')$).*
- ♢ *On dit que $x$ est un élément maximal (resp. minimal) de $A'$ si et seulement si $(x \in A') \wedge (\forall\, a \in A')[\neg(x \prec a)]$ (resp. $(x \in A') \wedge (\forall\, a \in A')[\neg(a \prec x)]$).*

**Exemple 3.8** (i) Soient $A = [\![1, 6]\!]$ et $A' = [\![3, 6]\!]$. On considère l'ensemble ordonné $(A, \preccurlyeq)$ représenté figure 3.3. Dans $(A, \preccurlyeq)$, $A'$ admet deux minorants (1 et 2), deux éléments minimaux (3 et 4), et deux

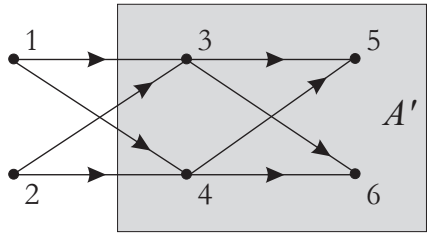


**Figure 3.3** — Représentation schématique d'un ensemble ordonné.

éléments maximaux (5 et 6). Il n'admet ni plus grand élément, ni plus petit élément.
Dans $\big(A, \preccurlyeq \cup \{(3, 4)\}\big)$, $A'$ admet trois minorants (1, 2 et 3) et un plus petit élément, 3.

(ii) Dans $([\![2, +\infty[\![\,, \mid)$, $[\![2, +\infty[\![$ n'admet ni majorant, ni minorant, et donc ni plus grand élément, ni plus petit élément. Il admet en revanche une infinité d'éléments minimaux, qui sont les nombres premiers.

**Proposition 3.8** *Soit $(A, \preccurlyeq)$ un ensemble ordonné. Une partie $A'$ de $A$ admet au plus un plus grand élément et au plus un plus petit élément. Autrement dit, $|A' \cap \mathrm{maj}_A(A')| \leqslant 1$ et $|A' \cap \min_A(A')| \leqslant 1$ .*

Notation. Si $A'$ admet un plus grand (resp. petit) élément, celui-ci est noté $\mathrm{pge}_A(A')$ (resp. $\mathrm{ppe}_A(A')$).

Remarque. Si une partie $A'$ de $A$ admet un unique élément maximal, cet élément n'est pas nécessairement le plus grand élément de $A'$.

**Exemple 3.9** Soit $\mathbb{N} \cup \{\omega\}$ l'ensemble obtenu en ajoutant un élément $\omega \notin \mathbb{N}$ à l'ensemble des entiers naturels et soit $\preccurlyeq$ une relation d'ordre sur $\mathbb{N} \cup \{\omega\}$ vérifiant

$$\begin{cases} (\forall\, n, m \in \mathbb{N})[\, n \preccurlyeq m \Leftrightarrow n \leqslant m\,] \\ \big|\{n \in \mathbb{N} \mid n \prec \omega\}\big| < +\infty \\ \{n \in \mathbb{N} \mid \omega \prec n\} = \emptyset \end{cases} .$$

Dans $(\mathbb{N} \cup \{\omega\}, \preccurlyeq)$, toute partie $\Omega$ de $\mathbb{N} \cup \{\omega\}$ telle que $\omega \in \Omega$ et $|\Omega| = +\infty$ a un unique élément maximal, qui est $\omega$, mais n'admet pas de plus grand élément.

**Proposition 3.9** *Dans un ensemble totalement ordonné $(A, \preccurlyeq)$, toute partie $A'$ de $A$ admet au plus un élément maximal (resp. minimal) qui est alors aussi le plus grand (resp. petit) élément de $A'$.*

**Définition 3.18** *Soient $(A, \preccurlyeq)$ un ensemble ordonné, $A' \in \mathcal{P}(A)$.*

- ♢ *Si $\mathrm{maj}_A(A')$ admet un plus petit élément $x$, $x$ est appelé la borne supérieure de $A'$ dans $A$, notée $\sup_A(A')$.*
- ♢ *Si $\min_A(A')$ admet un plus grand élément $x$, $x$ est appelé la borne inférieure de $A'$ dans $A$, notée $\inf_A(A')$.*

*Autrement dit,* $$\begin{cases} x = \sup_A(A') \;\Leftrightarrow\; x \in \mathrm{maj}_A(A') \cap \min_A\big(\mathrm{maj}_A(A')\big) \\ x = \inf_A(A') \;\Leftrightarrow\; x \in \min_A(A') \cap \mathrm{maj}_A\big(\min_A(A')\big)\,. \end{cases}$$

Remarques. (i) On parle de "la" borne supérieure ou inférieure car il y en a au plus une d'après la proposition 3.8.
(ii) Lorsque $A'$ est l'image d'un ensemble $X$ par une fonction $f$ à valeurs dans $A$, on note généralement $\sup_{x \in X}\, f(x)$ (resp. $\inf_{x \in X}\, f(x)$ ) au lieu de $\sup_A(f(X))$ (resp. $\inf_A(f(X))$ ).

**Proposition 3.10** *Soient $(A, \preccurlyeq)$ un ensemble ordonné, $A' \in \mathcal{P}(A)$, $x \in A'$. L'élément $x$ est le plus grand (resp. petit) élément de $A'$ si et seulement si $x \in A'$ et $x = \sup_A(A')$ (resp. $x \in A'$ et $x = \inf_A(A')$).*

**Exemple 3.10** (i) Soient $A = [\![0, 8]\!]$ et $A' = [\![3, 6]\!]$. On considère l'ensemble ordonné $(A, \preccurlyeq)$ représenté figure 3.4. $\mathrm{maj}_A(A') = \{7, 8\}$ admet un plus petit élément, qui est 7 ; donc $\sup_A(A') = 7$. En revanche,

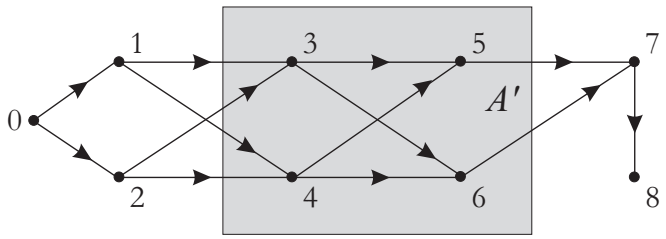


**Figure 3.4** — Représentation schématique d'un ensemble ordonné.

$A'$ n'admet pas de borne inférieure car $\min_A(A') = \{0, 1, 2\}$ n'admet pas de plus grand élément (1 et 2 ne sont pas comparables).

(ii) Dans $(\mathbb{Q}, \leqslant)$, $[0, \sqrt{2}\,[ \cap \mathbb{Q}$ n'admet pas de borne supérieure.

(iii) Dans $(\mathbb{N}^*, |\,)$, on a, pour tous $a, b \in \mathbb{N}^*$, $\sup_{\mathbb{N}^*}(\{a, b\}) = \mathrm{ppcm}(a, b)$ et $\inf_{\mathbb{N}^*}(\{a, b\}) = \mathrm{pgcd}(a, b)$.

**Exercice 3.10** Soit $(\mathcal{P}(E), \subset)$, où $E$ est un ensemble, et soit $(A_i)_{i\in I}$ une famille de parties de $E$. Montrer que $\sup_{\mathcal{P}(E)}\big((A_i)_{i\in I}\big) = \bigcup_{i\in I} A_i$ et $\inf_{\mathcal{P}(E)}\big((A_i)_{i\in I}\big) = \bigcap_{i\in I} A_i$.

**Proposition 3.11** *Soient $X$ et $Y$ deux ensembles, $(A, \preccurlyeq)$ un ensemble ordonné, $f : X \times Y \to A$ une application. Sous réserve d'existence,*

$$\sup_{x\in X}\Big(\sup_{y\in Y} f(x, y)\Big) = \sup_{(x,y)\in X\times Y} f(x, y),$$

$$\inf_{x\in X}\Big(\inf_{y\in Y} f(x, y)\Big) = \inf_{(x,y)\in X\times Y} f(x, y),$$

$$\textit{et} \qquad \sup_{x\in X}\Big(\inf_{y\in Y} f(x, y)\Big) \preccurlyeq \inf_{y\in Y}\Big(\sup_{x\in X} f(x, y)\Big).$$

### 3.2.5 Treillis

**Définition 3.19** *Un ensemble ordonné $(A, \preccurlyeq)$ dont chacune des paires d'éléments admet une borne inférieure et une borne supérieure est appelé un treillis. Pour tout $(a, b) \in A^2$, on note $a \sqcup b := \sup_A(\{a, b\})$ et $a \sqcap b := \inf_A(\{a, b\})$.*

REMARQUES. (i) Pour tout $(a, b) \in A^2$, on a $a \sqcup b = b \Leftrightarrow a \preccurlyeq b \Leftrightarrow a \sqcap b = a$.
(ii) $(A, \preccurlyeq)$ est un treillis si et seulement si toute partie finie non vide de $A$ admet une borne inférieure et une borne supérieure.

**Exemple 3.11** (i) Tout ensemble totalement ordonné est un treillis.
(ii) $(\mathbb{N}^*, |)$ est un treillis, les opérations binaires $\sqcup$ et $\sqcap$ étant respectivement le ppcm et le pgcd.
(iii) Pour tout ensemble $E$ non vide, $(\mathcal{P}(E), \subset)$ est un treillis : les opération binaires $\sqcup$ et $\sqcap$ sont respectivement $\cup$ et $\cap$.

**Exercice 3.11** Montrer que les deux lois de composition internes $\sqcap$ et $\sqcup$ associées à un treillis sont monotones, i.e., si $a \preccurlyeq a'$ et $b \preccurlyeq b'$ alors $a \sqcap b \preccurlyeq a' \sqcap b'$ et $a \sqcup b \preccurlyeq a' \sqcup b'$.

**Proposition 3.12** *Soit $(A, \preccurlyeq)$ un treillis et soient $a$, $b$ et $c$ trois éléments de $A$. Les opérations binaires $\sqcup$ et $\sqcap$ associées à $(A, \preccurlyeq)$ possèdent les propriétés suivantes.*

1. *Idempotence : $a \sqcup a = a$, $a \sqcap a = a$.*
2. *Commutativité : $a \sqcup b = b \sqcup a$, $a \sqcap b = b \sqcap a$.*
3. *Associativité : $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$, $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$.*
4. *Absorption : $a \sqcap (a \sqcup b) = a \sqcup (a \sqcap b) = a$.*

**Proposition 3.13** *Soit $A$ un ensemble muni de deux lois de compositions internes, $\perp$ et $\top$, idempotentes, commutatives et associatives, vérifiant les propriétés d'absorption, i.e.,*

$$(\forall\, a, b \in A)\big[\, a \top (a \perp b) = a \perp (a \top b) = a \,\big].$$

*La relation $\preccurlyeq$ sur $A$ définie par $(\forall\, a, b \in A)[\, a \preccurlyeq b \Leftrightarrow a \perp b = b\,]$ est un ordre et $(A, \preccurlyeq)$ est un treillis tel que, pour tout $(a, b) \in A^2$, $\sup_A(\{a, b\}) = a \perp b$ et $\inf_A(\{a, b\}) = a \top b$.*

REMARQUE. Sous les hypothèses de la proposition 3.13, on a, pour tout $(a, b) \in A^2$, $a \perp b = b \Leftrightarrow a \top b = a$. L'ordre $\preccurlyeq$ peut donc également être défini par $a \preccurlyeq b \Leftrightarrow a \top b = a$.

**Définition 3.20** *Un treillis $(A, \preccurlyeq)$ est dit distributif si et seulement si l'une des lois $\sqcup$ ou $\sqcap$ est distributive par rapport à l'autre, c'est-à-dire si et seulement si* $(\forall\, a,b,c \in A)\big[\, a\sqcup(b\sqcap c) = (a\sqcup b)\sqcap(a\sqcup c)\,\big]$ *ou* $(\forall\, a,b,c \in A)\big[\, a\sqcap(b\sqcup c) = (a\sqcap b)\sqcup(a\sqcap c)\,\big]$ *(ces deux propriétés sont équivalentes).*

**Exemple 3.12** (i) Tout ensemble totalement ordonné est un treillis distributif.
(ii) $(\mathbb{N}^*, |\,)$ est un treillis distributif.
(iii) Pour tout ensemble $E$ non vide, $(\mathcal{P}(E), \subset)$ est un treillis distributif.

**Exercice 3.12** Montrer que la distributivité de $\sqcap$ par rapport à $\sqcup$ et la distributivité de $\sqcup$ par rapport à $\sqcap$ sont des propriétés équivalentes.

**Définition 3.21** *Un treillis $(A, \preccurlyeq)$ est dit borné si et seulement si $A$ admet un plus grand élément, noté $1$, et un plus petit élément, noté $0$.*

Remarque. Pour tout $a \in A$, on a $a \sqcup 0 = a,\ a \sqcap 0 = 0,\ a \sqcap 1 = a$ et $a \sqcup 1 = 1$.

**Définition 3.22** *Un treillis $(A, \preccurlyeq)$ est dit complémenté si et seulement s'il est borné et s'il existe une application $\gamma : A \to A$ telle que* $(\forall\, a \in A)\big[\,(a \sqcup \gamma(a) = 1) \wedge (a \sqcap \gamma(a) = 0)\,\big]$ *($\gamma(a)$ est appelé complément de $a$).*

**Exemple 3.13** (i) Pour tout ensemble $E$ non vide, $(\mathcal{P}(E), \subset)$ est un treillis (distributif) complémenté : son plus petit élément est $\emptyset$, son plus grand élément est $E$, et, pour tout $a \in \mathcal{P}(E)$, $\gamma(a) = \mathsf{C}_E(a)$.
(ii) Tout ensemble totalement ordonné à deux éléments, c'est-à-dire de la forme $\big(\{0,1\}, \{(0,0),(0,1),(1,1)\}\big)$ est un treillis distributif complémenté : les lois $\sqcup$ et $\sqcap$ sont définies de la même façon que les connecteurs logiques $\vee$ et $\wedge$, et l'application $\gamma$ s'identifie alors à la négation.

Remarques. (i) $(\forall\, a \in A)\big[a \neq \gamma(a)\big]$.
(ii) $\gamma(0) = 1$ et $\gamma(1) = 0$.

**Proposition 3.14** *Un treillis $(A, \preccurlyeq)$ distributif et complémenté admet une unique opération de complémentation $\gamma$. De plus, cette opération vérifie*

1. $\gamma \circ \gamma = \mathrm{Id}_A$ *($\gamma$ est une involution) ;*
2. $(\forall\, a,b \in A)[\gamma(a \sqcup b) = \gamma(a) \sqcap \gamma(b)\big]$ *et* $(\forall\, a,b \in A)[\gamma(a \sqcap b) = \gamma(a) \sqcup \gamma(b)\big]$ *(lois de Morgan) ;*
3. $(\forall\, a,b \in A)\big[a \preccurlyeq b \Leftrightarrow \gamma(b) \preccurlyeq \gamma(a)\big]$.

# Chapitre 4

# Graphes

**Graphes**

♢ Introduits au XVIII-ème siècle par Leonhard Euler (mathématicien suisse, 1707-1783).

♢ Applications : gestion de réseaux, problèmes de routage, recherche d'un plus court chemin, ordonnancement, etc.

**Arbres**

♢ Graphes particuliers introduits en 1857 par Arthur Cayley (mathématicien anglais, 1821-1895).

♢ Applications : recherche dans une liste, tri, codage, décision, etc.

# 4.1 Introduction et terminologie

## 4.1.1 Premières définitions

**Définition 4.1** *Un graphe non orienté est un triplet $G = (S, A, \delta)$ où $S$ et $A$ sont deux ensembles disjoints et $\delta$ est une application de $A$ dans $\big\{\mathsf{c} \subset S \,\big|\, |\mathsf{c}| \in \{1, 2\}\big\}$. Les éléments de $S$ et de $A$ sont appelés respectivement les sommets et les arêtes de $G$.*

**Exemple 4.1** La figure 4.1 représente un graphe non orienté à trois sommets ($s$, $t$ et $u$) et six arêtes $a_i$, $i \in [\![1, 6]\!]$, avec $\delta(a_1) = \delta(a_2) = \{s, t\}$, $\delta(a_3) = \delta(a_4) = \{s\}$, $\delta(a_5) = \{t, u\}$ et $\delta(a_6) = \{s, u\}$.

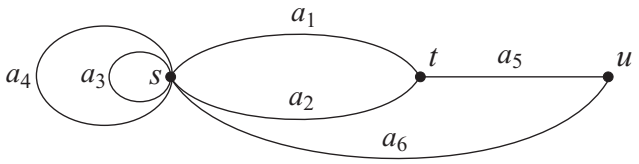


**Figure 4.1** — Exemple de graphe non orienté.

**Définition 4.2** *Dans un graphe non orienté, deux sommets $s$ et $t$ distincts sont dits adjacents si et seulement s'ils sont reliés par une même arête, c'est-à-dire si et seulement si $(\exists\, a \in A)\big[\delta(a) = \{s, t\}\big]$.*

**Définition 4.3** *Un graphe orienté est un quadruplet $(S, A, \alpha, \beta)$ où $S$ est un ensemble de sommets, $A$ est un ensemble d'arêtes disjoint de $S$, et $\alpha$, $\beta$ sont deux application de $A$ dans $S$ associant respectivement à chaque arête un sommet d'origine et un sommet but.*

**Exemple 4.2** La figure 4.2 représente un graphe orienté à trois sommets ($s$, $t$ et $u$) et six arêtes $a_i$, $i \in [\![1, 6]\!]$, avec $\alpha(a_1) = \alpha(a_3) = \alpha(a_4) = \alpha(a_6) = s$, $\alpha(a_2) = t$, $\alpha(a_5) = u$, $\beta(a_1) = \beta(a_5) = t$, $\beta(a_2) = \beta(a_3) = \beta(a_4) = s$ et $\beta(a_6) = u$.

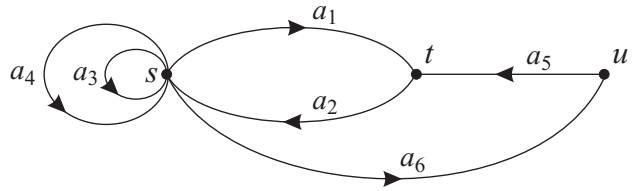


**Figure 4.2** — Exemple de graphe orienté.

On peut toujours passer d'un graphe orienté à un graphe non orienté en "oubliant" le sens des arêtes. Réciproquement, on peut construire un graphe orienté à partir d'un graphe non orienté en donnant un sens arbitraire à chacune des arêtes. Ces transformations sont précisées dans la définition qui suit.

**Définition 4.4** *Soient $G = (S, A, \delta)$ et $H = (S, A, \alpha, \beta)$ un graphe non orienté et un graphe orienté ayant le même ensemble de sommets $S$ et le même ensemble d'arêtes $A$. On dit que $G$ est associé à $H$, ou que $H$ est une orientation de $G$, si et seulement si $(\forall\, a \in A)\big[\, \delta(a) = \{\alpha(a), \beta(a)\}\big]$.*

**Définition 4.5** *Un graphe est dit fini si et seulement si $|S| < \infty$ et $|A| < \infty$.*

**Définition 4.6** *Une arête dont les extrémités reposent sur un même sommet est appelée une boucle. En d'autres termes, $a \in A$ est une boucle si et seulement si $|\delta(a)| = 1$ dans le cas d'un graphe non orienté ou $\alpha(a) = \beta(a)$ dans le cas d'un graphe orienté.*

**Définition 4.7** *On dit qu'un graphe comporte des arêtes multiples s'il possède des arêtes distinctes ayant les mêmes extrémités, c'est-à-dire s'il existe $a, b \in A$ avec $a \neq b$ tels que $\delta(a) = \delta(b)$ dans le cas d'un graphe non orienté et $\big(\alpha(a), \beta(a)\big) = \big(\alpha(b), \beta(b)\big)$ pour un graphe orienté.*

**Définition 4.8** *Un graphe est dit simple si et seulement s'il ne contient ni boucle ni arête multiple.*

### 4.1.2 Représentation matricielle

• Un graphe non orienté fini $G = (S, A, \delta)$ sans arête multiple peut être représenté par une matrice booléenne $M_G = [\theta_{ij}] \in \mathbf{M}_{|S|}(\{0,1\})$, appelée *matrice d'adjacence*, définie en fonction d'un arrangement $(s_1, \ldots, s_{|S|})$ des sommets par

$$\theta_{ij} = \begin{cases} 1 & \text{si } (\exists a \in A)[\delta(a) = \{s_i, s_j\}] \\ 0 & \text{sinon} \end{cases} .$$

• Dans le cas d'un graphe orienté $G = (S, A, \alpha, \beta)$ sans arête multiple, le triplet $(A, \alpha, \beta)$ peut être représenté par la relation binaire interne

$$\mathcal{R}_G = \big\{(s,t) \in S^2 \mid (\exists\, a \in A)\big[\big(\alpha(a), \beta(a)\big) = (s,t)\big]\big\}.$$

Si, de plus, $G$ est fini, on peut le représenter par la matrice de la relation $\mathcal{R}_G$ (voir §3.1.2) relativement à un arrangement des sommets donné.

**Exemple 4.3** Représentation matricielle des graphes $G$ et $H$ représentés figure 4.3 :

$$M_G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \qquad M_H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

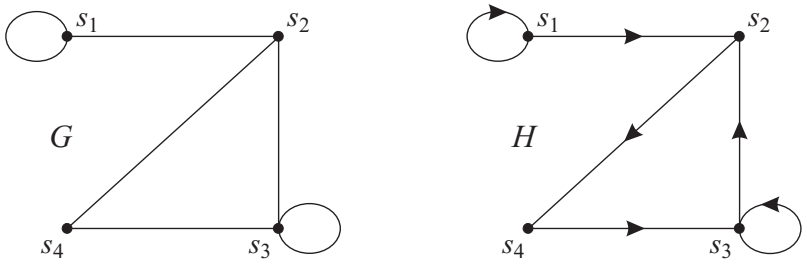


**Figure 4.3** — Graphe non orienté $G$ et graphe orienté $H$.

### 4.1.3 Graphes partiels et sous-graphes

Étant donné un graphe $G$, orienté ou non, on obtient un *graphe partiel* de $G$ en lui retirant certaines de ses arêtes, et on obtient un *sous-graphe* de $G$ en lui retirant certains de ses sommets ainsi que les arêtes qui s'appuient sur ces derniers. Ces notions sont illustrées figure 4.4 et formalisées dans les définitions qui suivent.

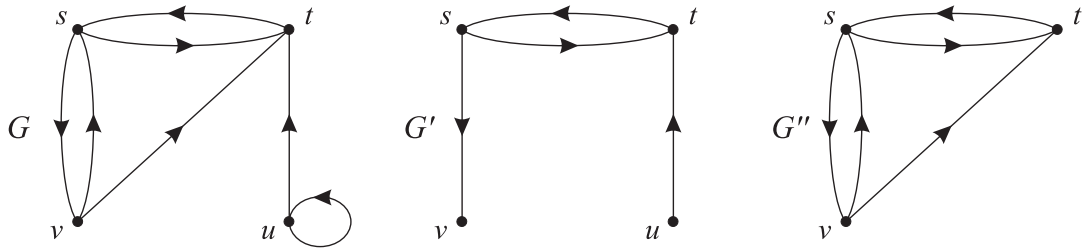


**Figure 4.4** — $G'$ est un graphe partiel de $G$ et $G''$ est un sous-graphe de $G$

**Définition 4.9** *Soit $G = (S, A, \delta)$ un graphe non orienté.*

♢ *On dit que $G' = (S', A', \delta')$ est un graphe partiel de $G$ si et seulement si $S' = S,\ A' \subset A$ et $\delta' = \delta|_{A'}$.*

♢ *On dit que $G' = (S', A', \delta')$ est un sous-graphe de $G$ si et seulement si $S' \subset S,\ A' = \{a \in A \mid \delta(a) \subset S'\}$ et $\delta' = \delta|_{A'}$.*

**Définition 4.10** *Soit $G = (S, A, \alpha, \beta)$ un graphe orienté.*

♢ *On dit que $G' = (S', A', \alpha', \beta')$ est un graphe partiel de $G$ si et seulement si $S' = S,\ A' \subset A,\ \alpha' = \alpha|_{A'}$ et $\beta' = \beta|_{A'}$.*

♢ *On dit que $G' = (S', A', \alpha', \beta')$ est un sous-graphe de $G$ si et seulement si $S' \subset S,\ A' = \{a \in A \mid \{\alpha(a), \beta(a)\} \subset S'\},\ \alpha' = \alpha|_{A'}$ et $\beta' = \beta|_{A'}$.*

Remarque. Un sous-graphe d'un graphe partiel est appelé *sous-graphe partiel*.

### 4.1.4 Graphes isomorphes

On dit de deux graphes qu'ils sont *isomorphes* s'ils ne diffèrent que par l'étiquetage de leurs sommets et de leurs arêtes (ils peuvent alors être considérés comme identiques).

**Définition 4.11** *Deux graphes non orientés $G = (S, A, \delta)$ et $G' = (S', A', \delta')$ sont dits isomorphes si et seulement s'il existe deux bijection $f_S : S \to S'$ et $f_A : A \to A'$ telles que $(\forall\, a \in A)\big[\delta' \circ f_A(a) = f_S(\delta(a))\big]$.*

**Exemple 4.4** Les graphes représentés figure 4.5 sont isomorphes. Les images de $s$, $t$, $u$, $v$ et $w$ par $f_S$ sont respectivement $t'$, $v'$, $s'$, $u'$ et $w'$. Les images de $a_1$, $a_2$, $a_3$, $a_4$ et $a_5$ par $f_A$ sont respectivement $a'_4$, $a'_1$, $a'_2$, $a'_5$ et $a'_3$.

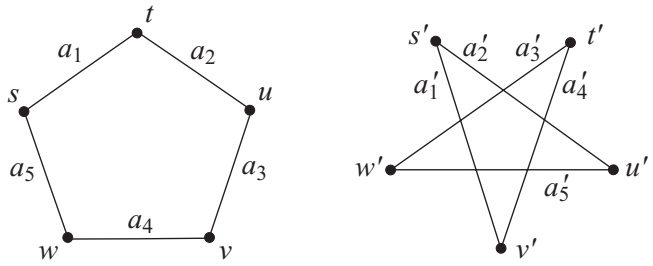


**Figure 4.5** — Graphes non orientés isomorphes.

**Définition 4.12** *Deux graphes orientés $G = (S, A, \alpha, \beta)$ et $G' = (S', A', \alpha', \beta')$ sont dits isomorphes si et seulement s'il existe deux bijection $f_S : S \to S'$ et $f_A : A \to A'$ telles que $\alpha' \circ f_A = f_S \circ \alpha$ et $\beta' \circ f_A = f_S \circ \beta$.*

**Exemple 4.5** Les graphes représentés figure 4.6 sont isomorphes. Les images de $s$, $t$, $u$ et $v$ par $f_S$ sont respectivement $s'$, $u'$, $t'$ et $v'$. Les images de $a_1$, $a_2$, $a_3$, $a_4$ et $a_5$ par $f_A$ sont respectivement $a'_1$, $a'_2$, $a'_4$, $a'_3$ et $a'_5$.

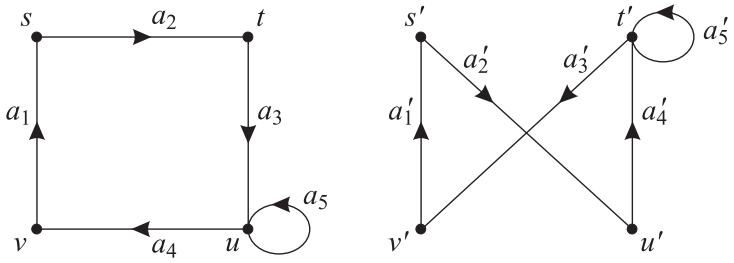


**Figure 4.6** — Graphes orientés isomorphes.

Remarque. La relation "est isomorphe à" est une relation d'équivalence.

**Définition 4.13** *On appelle matrice de permutation toute matrice du type*

$$\left[\delta_{\sigma^{-1}(i),j}\right]_{(i,j)\in[\![1,n]\!]^2} \overset{\text{not.}}{=} P_\sigma$$

*où $\sigma$ est une permutation de $[\![1,n]\!]$ et $\delta_{ij}$ désigne le symbole de Kronecker.*

**Proposition 4.1** *Soient $G$ et $G'$ deux graphes finis (orientés ou non) ayant le même nombre de sommets, sans arête multiple, respectivement représentés par les matrices $M_G$ et $M_{G'}$. Alors $G$ et $G'$ sont isomorphes si et seulement s'il existe une matrice de permutation $P_\sigma$ telle que $M_{G'} = P_\sigma M_G P_{\sigma^{-1}}$.*

**Exercice 4.1** Soient $G$ et $G'$ comme dans les hypothèses de la proposition 4.1.

1. Donner une condition nécessaire simple pour que $G$ et $G'$ soient isomorphes.
2. Les graphes associés aux couples de matrices suivants sont-ils isomorphes ?

(a) $M_G = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$, $M_{G'} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ ;

(b) $M_G = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, $M_{G'} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ ;

(c) $M_G = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$, $M_{G'} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$.

### 4.1.5 Degré d'un sommet

Nous nous intéressons ici aux graphes dont chacun des sommets supporte un nombre fini d'arêtes. De tels graphes peuvent être fini ou infini.

**Définition 4.14** *Le degré $d(s)$ d'un sommet $s$ d'un graphe non orienté $G = (S, A, \delta)$ est égal au nombre d'arêtes reposant sur $s$, étant entendu que chaque boucle s'appuyant sur $s$ est comptée deux fois :*

$$d(s) \;=\; \big|\big\{a \in A \,|\, s \in \delta(a)\big\}\big| + \big|\delta^{-1}(\{s\})\big| \,.$$

**Exercice 4.2** Soit $G = (S, A, \delta)$ un graphe non orienté, simple, fini, tel que $|S| > 1$.

1. Montrer : $(\forall s \in S)[d(s) < |S|]$.
2. Est-il possible d'avoir simultanément un sommet de degré nul et un sommet de degré $|S| - 1$ ?
3. En déduire $(\exists (s,t) \in S^2)\big[(s \neq t) \wedge (d(s) = d(t))\big]$.

**Proposition 4.2** *Soit $G = (S, A, \delta)$ un graphe non orienté fini. On a*

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

Démonstration. Informellement : chaque arête compte pour deux dans la somme des degrés. Rigoureusement : par induction sur le nombre d'arêtes. □

**Proposition 4.3** *Tout graphe non orienté fini possède un nombre pair de sommets de degré impair.*

**Définition 4.15** *Dans un graphe orienté $G = (S, A, \alpha, \beta)$, on appelle degré entrant d'un sommet $s$, et on note $d^-(s)$, le nombre d'arêtes dont le but est $s$. Le degré sortant de $s$, noté $d^+(s)$, est égal au nombre d'arêtes ayant $s$ pour origine. Autrement dit,*

$$d^-(s) \;=\; \big|\beta^{-1}(\{s\})\big| \quad \textit{et} \quad d^+(s) \;=\; \big|\alpha^{-1}(\{s\})\big| \,.$$

**Proposition 4.4** *Soit $G = (S, A, \alpha, \beta)$ un graphe orienté fini. On a*

$$\sum_{s \in S} d^-(s) \;=\; \sum_{s \in S} d^+(s) \;=\; |A| \,.$$

Démonstration. Informellement : chaque arête compte pour un dans la somme des degrés entrants et dans la somme des degrés sortants. Rigoureusement : par induction sur le nombre d'arêtes. □

## 4.2 Chaînes et chemins

**Définition 4.16** *Dans un graphe non orienté $G = (S, A, \delta)$, une chaîne est une succession $s_0, a_1, s_1, a_2, \ldots, s_{k-1}, a_k, s_k$ de sommets et d'arêtes telle que $(\forall\, i \in [\![1, k]\!])\big[\delta(a_i) = \{s_{i-1}, s_i\}\big]$. Un cycle est une chaîne telle que $s_0 = s_k$.*

**Définition 4.17** *Dans un graphe orienté $G = (S, A, \alpha, \beta)$, un chemin est une succession $a_1, a_2, \ldots, a_k$ d'arêtes telle que $(\forall\, i \in [\![1, k-1]\!])\big[\beta(a_i) = \alpha(a_{i+1})\big]$. Les sommets $\alpha(a_1)$ et $\beta(a_k)$ sont appelés respectivement l'origine et le but du chemin. Un circuit est un chemin tel que $\alpha(a_1) = \beta(a_k)$.*

**Définition 4.18** *On appelle longueur d'une chaîne $c = s_0, a_1, s_1, a_2, \ldots, s_{k-1}, a_k, s_k$ ou d'un chemin $c = a_1, a_2, \ldots, a_k$ le nombre $k$ d'arêtes contenues dans $c$.*

**Exercice 4.3** Soient $G$ un graphe orienté fini sans arête multiple, $M_G$ la matrice représentant $G$ relativement à un arrangement $(s_1, s_2, \ldots, s_n)$ des sommets de $G$. Montrer par induction que le nombre de chemins distincts de longueur $k \in \mathbb{N}^*$ reliant deux sommets $s_i$ et $s_j$ est égal au coefficient $(i, j)$ de $(M_G)^k$.

**Définition 4.19** *Une chaîne ou un chemin est dit simple si et seulement s'il ne contient pas deux fois la même arête.*

**Définition 4.20** *On dit qu'une chaîne est élémentaire si et seulement si elle ne contient pas deux fois le même sommet, à l'exception du sommet situé à ses extrémités s'il s'agit d'un cycle. Un chemin est dit élémentaire si et seulement s'il ne contient pas deux arêtes de même origine ou de même but.*

**Exemple 4.6** (i) Dans le graphe non orienté $G$ de la figure 4.7 :
- $s, a_1, t, a_2, t, a_3, u, a_4, v, a_5, s, a_6, v$ est une chaîne simple,
- $s, a_1, t, a_3, u, a_4, v$ est une chaîne élémentaire.

(ii) Dans le graphe orienté $H$ de la figure 4.7 :
- $a_1, a_2, a_3, a_4, a_7, a_5$ est un chemin simple,
- $a_1, a_2, a_3$ est un chemin élémentaire.

Remarques. (i) "élémentaire" $\Rightarrow$ "simple" excepté pour les cycles du type $s, a, t, a, s$.
(ii) Dans un graphe non orienté, s'il existe une chaîne joignant deux sommets $s$ et $t$ distincts, alors il existe une chaîne élémentaire reliant $s$ et $t$. De même, dans un graphe orienté, l'existence d'un chemin d'origine $s$ et de but $t$ implique l'existence d'un chemin élémentaire conduisant de $s$ à $t$.

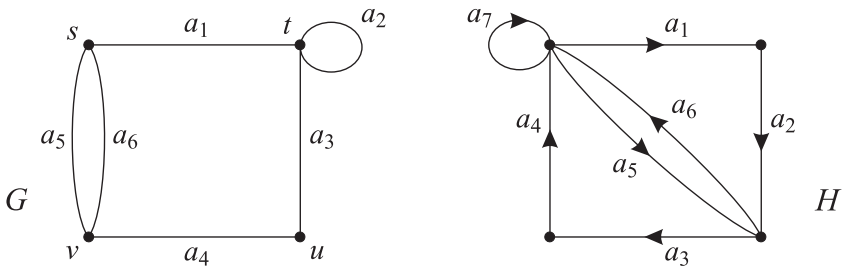


**Figure 4.7** — Graphe non orienté $G$ et graphe orienté $H$.

**Définition 4.21** *Dans un graphe non orienté, on appelle distance entre deux sommets $s$ et $t$ et on note $d(s,t)$ la longueur de la plus courte chaîne reliant $s$ et $t$, si elle existe. On pose $d(s,t) = 0$ si $s = t$ et $d(s,t) = +\infty$ s'il n'existe pas de chaîne reliant $s$ et $t$.*

**Définition 4.22** *Dans un graphe orienté, on appelle distance entre deux sommets $s$ et $t$ et on note également $d(s,t)$ la longueur du plus court chemin d'origine $s$ et de but $t$, s'il existe. On pose $d(s,t) = 0$ si $s = t$ et $d(s,t) = +\infty$ s'il n'existe pas de chemin conduisant de $s$ à $t$.*

Remarques. (i) Dans le cas d'un graphe non orienté, le couple $(S, d)$ formé par l'ensemble $S$ des sommets du graphe et l'application $d : (s,t) \in S^2 \mapsto d(s,t)$ est un espace métrique. En effet, $d$ vérifie :

- $(\forall\, s,t \in S)\big[\, d(s,t) = d(t,s)\,\big]$ (symétrie) ;
- $(\forall\, s,t \in S)\big[\, d(s,t) = 0 \;\Leftrightarrow\; s = t\,\big]$ (séparation) ;
- $(\forall\, s,t,u \in S)\big[\, d(s,u) \leqslant d(s,t) + d(t,u)\,\big]$ (inégalité triangulaire).

(ii) La distance entre deux sommets d'un graphe orienté n'est pas symétrique dans le cas général.

**Définition 4.23** *Soient $G$ un graphe (orienté ou non), $S$ l'ensemble des sommets de $G$. On appelle respectivement diamètre et rayon de $G$ les quantités*

$$D(G) \;=\; \sup_{(s,t)\in S^2} d(s,t) \qquad \text{et} \qquad R(G) \;=\; \inf_{s\in S} \sup_{t\in S} d(s,t)\,,$$

*où le* sup *et l'*inf *sont dans $\mathbb{N} \cup \{+\infty\}$.*

**Proposition 4.5** *$R(G) \leqslant D(G) \leqslant 2R(G)$ pour tout graphe $G$ (orienté ou non).*

## 4.3 Connexité

Étant donné un graphe $G$ (orienté ou non), on définit la relation binaire interne $\mathcal{C}_G$ sur l'ensemble $S$ des sommets de $G$ par

$$\mathcal{C}_G = \left\{(s,t) \in S^2 \;\middle|\; d(s,t) \neq +\infty\right\}.$$

Si $G$ est non orienté, $\mathcal{C}_G$ est une relation d'équivalence sur $S$.
Si $G$ est orienté, $\mathcal{C}_G$ est reflexive et transitive, mais pas symétrique dans le cas général.

**Définition 4.24** *Un graphe non orienté (resp. orienté) $G$ est dit connexe (resp. fortement connexe) si et seulement si $\mathcal{C}_G = S^2$.*

**Définition 4.25** *Soit $G$ un graphe non orienté (resp. orienté) connexe (resp. fortement connexe). On dit qu'un sommet de $G$ est un point d'articulation si sa suppression conduit à un sous-graphe de $G$ qui n'est pas connexe (resp. fortement connexe). De même, on dit qu'une arête de $G$ est un isthme si sa suppression conduit à un graphe partiel de $G$ qui n'est pas connexe (resp. fortement connexe).*

**Définition 4.26** *Dans un graphe non orienté $G$, la classe d'équivalence $\mathcal{C}_G[s]$ d'un sommet $s$ est appelée composante connexe de $s$.*

**Exercice 4.4**

1. Quel est le nombre maximum d'arêtes d'un graphe simple non orienté ?
2. Montrer qu'un graphe simple non orienté à $n$ sommets ($n \geqslant 2$) est connexe si le nombre de ses arêtes est strictement supérieur à $(n-1)(n-2)/2$.

**Exercice 4.5** Soient $G = (S, A, \delta)$ un graphe non orienté connexe, $a \in A$ une arête d'extrémités $s$ et $t$ distinctes, $G'$ le graphe partiel de $G$ obtenu en supprimant $a$. Montrer : $S = \mathcal{C}_{G'}[s] \cup \mathcal{C}_{G'}[t]$.

**Proposition 4.6** *Soit $G$ un graphe non orienté possédant $k$ composantes connexes. Tout graphe partiel de $G$ obtenu en lui retirant une arête possède $k$ ou $k+1$ composantes connexes.*

**Proposition 4.7** *Soit $G = (S, A, \delta)$ un graphe non orienté fini possédant $k$ composantes connexes. Alors, $|A| \geqslant |S| - k$.*

## 4.4 Chaînes eulériennes et hamiltoniennes

**Définition 4.27** *Dans un graphe non orienté (resp. orienté) fini $G$, une chaîne ou un cycle (resp. un chemin ou un circuit) est dit eulérien s'il est simple et s'il contient toutes les arêtes de $G$.*

**Exemple 4.7** Au XVIII-ème siècle, la ville de Königsberg (aujourd'hui Kaliningrad, en Russie) possédait sept ponts répartis comme illustré figure 4.8. À l'époque, le mathématicien suisse Leonhard Euler (1707-1783) se pencha sur la question de savoir s'il était possible de visiter la ville en traversant chaque pont une fois et une seule. Le problème consiste à déterminer si le graphe non orienté représenté sur la droite de la figure 4.8 possède une chaîne eulérienne. La réponse, qui s'avère être négative, s'obtient à l'aide du théorème 4.1.

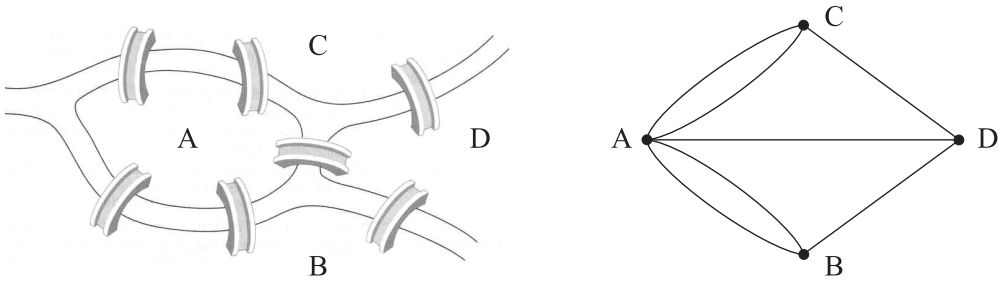


**Figure 4.8** — Ponts de la ville de Königsberg et représentation par graphe associée.

**Théorème 4.1 (Euler, 1736)** *Un graphe non orienté, fini et connexe possède une chaîne eulérienne (resp. un cycle eulérien) si et seulement si seuls deux de ses sommets sont de degré impair (resp. tous ses sommets sont de degré pair). Dans le cas d'une chaîne eulérienne, les deux sommets de degré impair sont les extrémités de la chaîne.*

**Définition 4.28** *Dans un graphe non orienté (resp. orienté) fini $G$, une chaîne ou un cycle (resp. un chemin ou un circuit) est dit hamiltonien s'il est élémentaire et s'il passe par tous les sommets de $G$.*

Contrairement aux chaînes eulériennes, il n'existe vraisemblablement pas de condition nécessaire et suffisante simple pour l'existence d'une chaîne hamiltonienne. On dispose toutefois d'assez nombreux résultats permettant de gérer des situations particulières ; la proposition 4.8 et le théorème 4.2 en sont deux exemples.

**Proposition 4.8** *Soit $G$ un graphe non orienté comportant au moins trois sommets. Si $G$ possède un cycle hamiltonien, alors $G$ ne possède ni point d'articulation ni isthme.*

Démonstration informelle. Soient $G$ un graphe non orienté comportant au moins trois sommets, $c$ un cycle de $G$ contenant l'ensemble des sommets de $G$ ($G$ est donc connexe).

- Si $G$ possède un point d'articulation $\mathfrak{s}$, la suppression de $\mathfrak{s}$ conduit à $k$ ($\geqslant 2$) sous-graphes de $G$ connexes et $c$ passe donc nécessairement au moins $k$ fois par $\mathfrak{s}$.
- Si $G$ comporte un isthme $\mathfrak{a}$, alors $c$ emprunte au moins deux fois $\mathfrak{a}$ pour passer de l'une à l'autre des deux composantes connexes du graphe partiel obtenu en supprimant $\mathfrak{a}$ de $G$. Les deux sommets extrémités de $\mathfrak{a}$ apparaissent donc chacun au moins deux fois dans $c$. □

**Théorème 4.2 (Dirac, 1952)** *Soit $G = (S, A, \delta)$ un graphe non orienté, simple et fini. Si $|S| \geqslant 3$ et $(\forall\, s \in S)\big[d(s) \geqslant |S|/2\big]$, alors $G$ possède un cycle hamiltonien.*

## 4.5 Graphes planaires

Informellement, un *graphe planaire* est un graphe que l'on peut dessiner dans un plan sans que ses arêtes ne se croisent. En voici une définition plus précise.

**Définition 4.29** *Un graphe non orienté $G = (S, A, \delta)$ est dit planaire s'il est fini et s'il peut être représenté dans un plan affine $\mathcal{E}$ en respectant les règles qui suivent.*

1. *À chaque sommet $s \in S$ on associe un point de $\mathcal{E}$ via une injection $\mathsf{p} : S \to \mathcal{E}$.*
2. *Chaque arête $a \in A$ est représentée par la trajectoire $\mathcal{T}_a$ d'une courbe dont les extrémités sont les points associés aux éléments de $\delta(a)$.*
3. $(\forall (s, a) \in S \times A)[\, \mathsf{p}(s) \in \mathcal{T}_a \Leftrightarrow s \in \delta(a)\,]$.
4. $(\forall\, a, b \in A)\big[\, a \neq b \Rightarrow \mathcal{T}_a \cap \mathcal{T}_b = \mathsf{p}\big(\delta(a) \cap \delta(b)\big)\big]$.

**Exemple 4.8** La figure 4.9 représente deux exemples de graphes planaires $G$ et $H$.

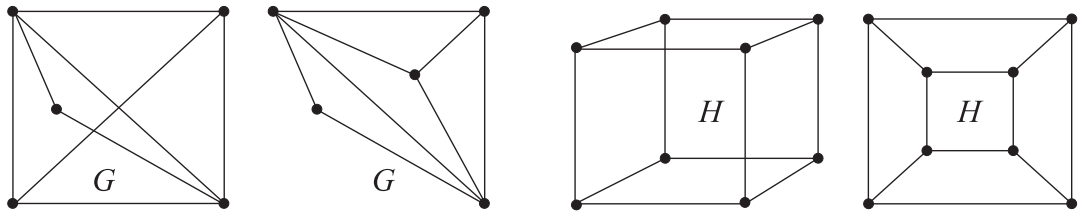


**Figure 4.9** — Graphes planaires $G$ et $H$.

### 4.5.1 Formule d'Euler

La représentation, selon les règles de la définition 4.29, d'un graphe planaire $G$ dans un plan affine $\mathcal{E}$ divise l'espace directeur de $\mathcal{E}$ en parties connexes par arcs appelées *faces*. Si $G$ est simple, le nombre de faces est directement relié au nombre de sommets et au nombre d'arêtes, comme le précise le théorème suivant.

**Théorème 4.3 (Euler, 1752)** *Soit $G = (S, A, \delta)$ un graphe simple, fini, connexe et planaire comportant $\ell$ faces. Alors $|S| - |A| + \ell = 2$.*

**Corollaire 4.1** *Soit $G = (S, A, \delta)$ un graphe simple, fini, connexe et planaire comportant au moins trois sommets. Alors $|A| \leqslant 3|S| - 6$.*

**Corollaire 4.2** *Soit $G = (S, A, \delta)$ un graphe simple, fini, connexe et planaire comportant au moins trois sommets. Si $G$ ne possède pas de cycle de longueur 3, alors $|A| \leqslant 2|S| - 4$.*

### 4.5.2 Condition nécessaire et suffisante de planarité

**Définition 4.30** *On appelle graphe complet à $n$ sommets et on note $K_n$ le graphe non orienté simple dont chacun des sommets est adjacent à tous les autres sommets.*

**Définition 4.31** *On appelle graphe biparti complet à $m + n$ sommets et on note $K_{m,n}$ le graphe non orienté simple dont l'ensemble des sommets est partitionné en deux sous-ensembles, $S_1$ et $S_2$, tels que $|S_1| = m$, $|S_2| = n$ et*

- *chaque sommet de $S_1$ est adjacent à tous les sommets de $S_2$,*
- *chaque sommet de $S_1$ (resp. $S_2$) n'est adjacent à aucun autre sommet de $S_1$ (resp. $S_2$).*

**Exemple 4.9** La figure 4.10 offre une représentation des graphes $K_5$ et $K_{3,3}$, tous deux non-planaires.

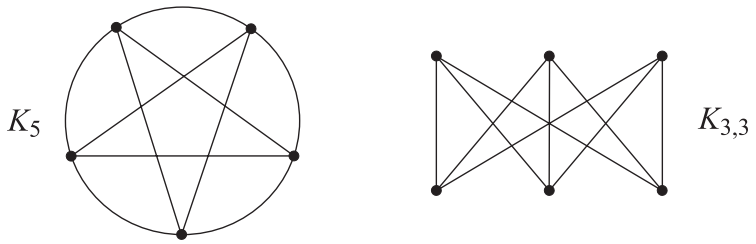


**Figure 4.10** — Graphe complet à 5 sommets et graphe biparti complet à 3+3 sommets.

**Exercice 4.6** Montrer que les graphes $K_5$ et $K_{3,3}$ sont non-planaires.

**Définition 4.32** *Dans un graphe non orienté, on appelle division élémentaire l'opération qui consiste à remplacer une arête d'extrémités $\{s,t\}$ par un nouveau sommet $u$ et deux nouvelles arêtes d'extrémités $\{s,u\}$ et $\{t,u\}$.*

**Définition 4.33** *Soit $G$ un graphe non orienté. On dit qu'un graphe $G'$ est une subdivision de $G$ si et seulement s'il s'obtient à partir de $G$ via une séquence de divisions élémentaires.*

**Exemple 4.10** Dans la figure 4.11, seul le graphe $G'$ est une subdivision de $K_5$. En effet, dans $G''$, le nouveau sommet $u$ est de degré 4 alors qu'une séquence de divisions élémentaires n'introduit que des sommets de degré 2.

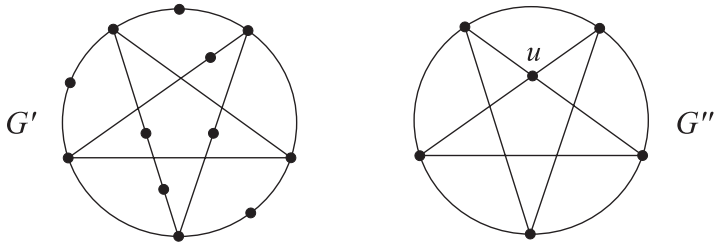


**Figure 4.11** — $G'$ est une subdivision de $K_5$, mais $G''$ n'en est pas une.

**Théorème 4.4 (Kuratowsky, 1930)** *Un graphe est non planaire si et seulement si l'un de ses sous-graphes est une subdivision de $K_5$ ou de $K_{3,3}$.*

**Exemple 4.11** Le graphe $G$ de la figure 4.12 est non planaire : en supprimant le sommet $s_3$ et les arêtes dont $s_3$ est l'une des extrémités, on obtient le sous-graphe $G'$ qui est une subdivision de $K_{3,3}$.

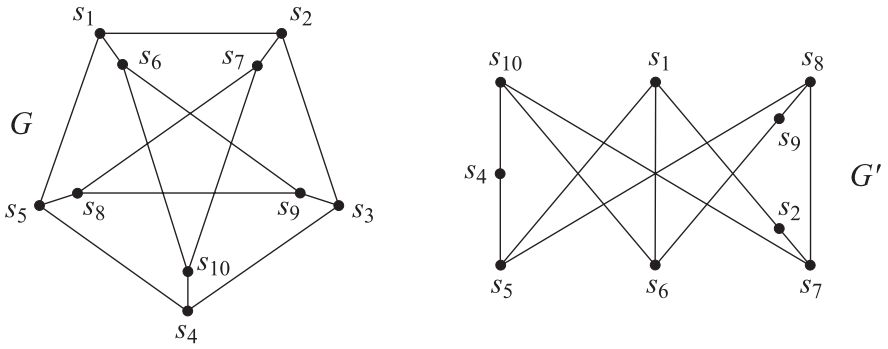


**Figure 4.12** — Graphe de Petersen $G$ et sous-graphe $G'$ de $G$.

### 4.5.3 Coloration d'un graphe planaire

**Définition 4.34** *Soient $G = (S, A, \delta)$ un graphe simple non orienté, $k \in \mathbb{N}^*$, $C$ un ensemble comportant $k$ éléments. Une k-coloration des sommets de $G$ est une application $\gamma : S \to C$ telle que $\gamma(s) \neq \gamma(t)$ pour toute paire $\{s, t\}$ de sommets adjacents. Les éléments de $C$ sont appelés des couleurs.*

**Définition 4.35** *Soit $G = (S, A, \delta)$ un graphe simple non orienté. Le plus petit entier $k \in \mathbb{N}^*$ tel que $G$ admette une $k$-coloration de ses sommets est appelé le nombre chromatique de $G$ et noté $\chi(G)$.*

**Théorème 4.5 (Appel et Haken, 1977)** *Tout graphe simple et planaire $G$ admet une 4-coloration de ses sommets (i.e., $\chi(G) \leqslant 4$).*

**Théorème 4.6 (Grötzsch, 1959)** *Soit $G$ un graphe simple et planaire. Si $G$ ne possède pas de cycle de longueur 3, alors $\chi(G) \leqslant 3$.*

## 4.6 Arbres et arborescences

### 4.6.1 Arbres

**Définition 4.36** *Un graphe simple, non orienté et sans cycle élémentaire de longueur* $\geqslant 3$ *est appelé une forêt. Une forêt connexe est appelée un arbre.*

**Exemple 4.12** Parmi les graphes représentés figure 4.13, $G_1$ n'est ni une forêt ni un arbre (il possède un cycle élémentaire passant par $s_1$, $s_2$, $s_5$ et $s_4$), $G_2$ est une forêt et $G_3$ et $G_4$ sont des arbres.

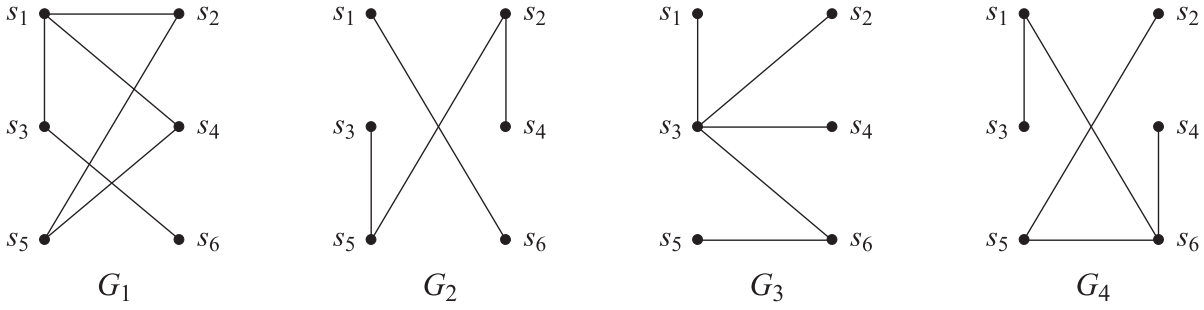


**Figure 4.13** — Exemples de graphes. Seuls $G_3$ et $G_4$ sont des arbres.

**Théorème 4.7** *Soit $G$ un graphe simple non orienté comportant au moins trois sommets. Les propriétés suivantes sont équivalentes.*

1. *$G$ est connexe et ne possède pas de cycle élémentaire de longueur $\geqslant 3$ (i.e., $G$ est un arbre).*
2. *$G$ ne possède pas de cycle élémentaire de longueur $\geqslant 3$, mais l'ajout d'une seule arête entre deux sommets distincts non adjacents de $G$ introduit un cycle élémentaire de longueur $\geqslant 3$.*
3. *$G$ est connexe et toute arête de $G$ est un isthme.*
4. *Toute paire de sommets distincts de $G$ est reliée par une unique chaîne élémentaire.*

[ **Indications.** **2** $\Rightarrow$ **3** est de la forme $p_1 \wedge p_2 \Rightarrow q_1 \wedge q_2$ avec $p_1 =$ "$G$ ne possède pas de cycle élémentaire de longueur $\geqslant 3$," $p_2 =$ "l'ajout d'une arête entre deux sommets non adjacents de $G$ introduit un cycle élémentaire de longueur $\geqslant 3$," $q_1 =$ "$G$ est connexe" et $q_2 =$ "toute arête de $G$ est un isthme." Il suffit de montrer : (i) $\neg q_1 \Rightarrow \neg p_2$ et (ii) $q_1 \wedge \neg q_2 \Rightarrow \neg p_1$. En effet, on a alors $\neg q_1 \vee (q_1 \wedge \neg q_2) \Rightarrow \neg p_2 \vee \neg p_1$ par dilemme constructif, ce qui établit la contre-apposée de $p_1 \wedge p_2 \Rightarrow q_1 \wedge q_2$ (car $\neg q_1 \vee (q_1 \wedge \neg q_2) \Leftrightarrow \neg q_1 \vee \neg q_2$).

**3** $\Rightarrow$ **4** est de la forme $p_1 \wedge p_2 \Rightarrow \neg(q_1 \vee q_2)$, avec $p_1 =$ "$G$ est connexe," $p_2 =$ "toute arête de $G$ est un isthme," $q_1 = (\exists (s,t) \in S^2)[(s \neq t) \wedge$ "il n'existe pas de chaîne élémentaire reliant $s$ et $t$"], et $q_2 = (\exists (s,t) \in S^2)[(s \neq t) \wedge$ "il existe deux chaînes élémentaires distinctes reliant $s$ et $t$"]. Il suffit de montrer : (i) $q_1 \Rightarrow \neg p_1$ et (ii) $\neg q_1 \wedge q_2 \Rightarrow \neg p_2$. En effet, on a alors $q_1 \vee (\neg q_1 \wedge q_2) \Rightarrow \neg p_1 \vee \neg p_2$ par dilemme constructif, ce qui établit la contre-apposée de $p_1 \wedge p_2 \Rightarrow \neg(q_1 \vee q_2)$ (car $q_1 \vee (\neg q_1 \wedge q_2) \Leftrightarrow q_1 \vee q_2$). ]

**Proposition 4.9** *Soit $G = (S, A, \delta)$ un graphe simple, non orienté, fini et connexe. Alors, $G$ est un arbre si et seulement si $|A| = |S| - 1$.*

**Exercice 4.7** Montrer qu'une forêt est un graphe planaire. Quel est le nombre de faces d'un arbre ?

### 4.6.2 Arborescences

**Définition 4.37** *Une arborescence est un graphe orienté $G$ tel que :*

1. *le graphe non orienté associé à $G$ (voir définition 4.4) est un arbre ;*
2. *le degré entrant de chaque sommet de $G$ est égal à 1, à l'exception d'un unique sommet, appelé la racine, dont le degré entrant est nul.*

**Définition 4.38** *Soient $G = (S, A, \alpha, \beta)$ une arborescence, $(s,t) \in S^2$. On dit que $t$ est le fils de $s$ et que $s$ est le père de $t$ si et seulement si $(\exists\, a \in A)\big[\big(\alpha(a), \beta(a)\big) = (s,t)\big]$. Tout sommet possédant au moins un fils est dit interne et tout sommet sans fils est appelé une feuille.*

**Proposition 4.10** *Soit $G$ un arbre fini. Pour tout sommet $s$ de $G$, il existe une unique orientation de $G$ (voir définition 4.4) qui en fait une arborescence de racine $s$.*

**Exemple 4.13** La figure 4.14 représente les deux arborescences, $G_1$ et $G_2$, obtenues par orientation de l'arbre $G$ en choisissant respectivement $s_2$ et $s_3$ pour racine.

Remarque. Une arborescence $G$ impose un ordre partiel $\preccurlyeq_G$ sur l'ensemble $S$ de ses sommets : $s \preccurlyeq_G t \Leftrightarrow (s = t) \vee (s$ appartient à l'unique chemin reliant la racine à $t) \Leftrightarrow s\, \mathcal{C}_G\, t$. Dans l'ensemble ordonné $(S, \preccurlyeq_G)$, la racine est le plus petit élément de $S$ et les éléments maximaux de $S$ sont les feuilles.

**Proposition 4.11** *Soient $G$ une arborescence, $S$ l'ensemble des sommets de $G$. Pour tout $s \in S$, le sous-graphe de $G$ dont l'ensemble des sommets est $\{t \in S \mid s\, \mathcal{C}_G\, t\}$ est une arborescence de racine $s$.*

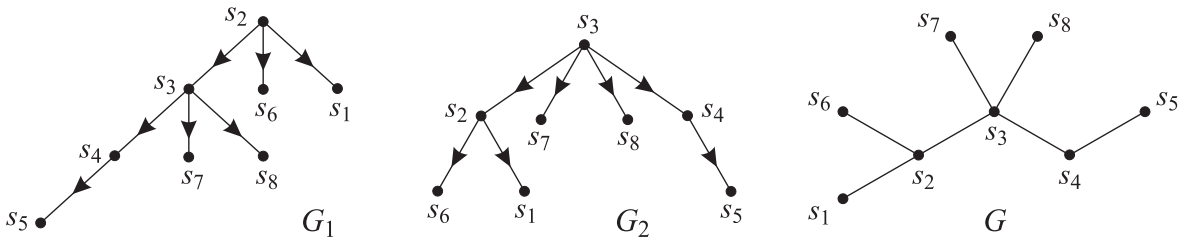


**Figure 4.14** — Exemples d'arborescences, $G_1$ et $G_2$, construites à partir d'un même arbre $G$.

**Définition 4.39** *Soit $m \in \mathbb{N} \setminus \{0, 1\}$. Une arborescence est dite m-aire (resp. m-aire complète) si et seulement si chacun de ses sommets internes possède au plus (resp. exactement) $m$ fils.*

**Exercice 4.8** Montrer qu'une arborescence binaire complète finie possède un nombre impair de sommets.

**Proposition 4.12** *Soit $G$ une arborescence $m$-aire complète à $n$ sommets possédant $p$ sommets internes. Alors, $n = mp + 1$ et le nombre de feuilles de $G$ est égal à $\big(n(m-1)+1\big)/m$.*

**Définition 4.40** *Soient $G$ une arborescence, $S$ l'ensemble des sommets de $G$, $r$ la racine de $G$, $s \in S \setminus \{r\}$. On appelle niveau de $s$ et on note $\nu(s)$ la longueur de l'unique chemin qui relie $s$ à $r$. Par convention, $\nu(r) = 0$. On appelle hauteur de $G$ la quantité*

$$h(G) = \sup_{s \in S} \nu(s)\,.$$

**Proposition 4.13** *Une arborescence $m$-aire de hauteur $h$ possède au plus $m^h$ feuilles.*

# Chapitre 5

# Langages rationnels et automates finis

**Langages**

♢ Les langages sont ici abordés en tant qu'ensembles de suites finies d'éléments d'un alphabet.

♢ Nous nous intéressons plus particulièrement aux langages dits "rationnels" dont la description s'effectue à l'aide de motifs, appelés expressions régulières, définis de façon récursive.

**Automates**

♢ Un automate peut être assimilé à un système réagissant à des stimuli. Selon le stimulus appliqué, il peut se bloquer, changer d'état, ou conserver son état courant. La notion de "reconnaissance" de séquences de stimuli par un automate correspond au fait de parvenir dans un certain sous-ensemble d'états à partir d'un état initial donné.

♢ Les automates considérés ici réagissent aux éléments d'un alphabet dans le but de reconnaître des langages. Nous fournissons notamment une preuve du théorème de Kleene, qui stipule que les notions de langage rationnel et de langage reconnaissable par automate fini se confondent.

## 5.1 Langages rationnels et expressions régulières

### Définition d'un langage

**Définition 5.1** *On appelle alphabet un ensemble fini non vide de symboles appelés lettres. Un mot sur un alphabet $A$ est une suite finie, éventuellement vide, d'éléments de $A$.*

NOTATION. Le mot vide est représenté par le symbole $\lambda$ et un mot $(a_1, a_2, \ldots, a_n)$ est simplement noté $a_1a_2\cdots a_n$. Si $a_1 = \cdots = a_n = a$, on note en abrégé $a^n$ le mot $a_1a_2\cdots a_n$ avec la convention $a^0 = \lambda$.

**Définition - Notation 5.2** *Soit $A$ un alphabet. On note $A^*$ l'ensemble des mots sur $A$. Cette ensemble est muni d'une loi de composition interne $\dagger$ appelée concaténation : $a_1a_2\cdots a_n \dagger b_1b_2\cdots b_m = a_1a_2\cdots a_nb_1b_2\cdots b_m$ ($\dagger$ est associative et admet le mot vide $\lambda$ pour élément neutre). On appelle langage sur $A$ toute partie de $A^*$.*

REMARQUE. $\emptyset$ est un langage sur tout alphabet $A$ que l'on appelle *langage vide*.

### Opérations sur les langages

**Définition 5.3** *Soit $A$ un alphabet. On définit les trois opérations fondamentales suivantes sur $\mathcal{P}(A^*)$.*

- ♢ *La réunion $L_1 + L_2$ de deux langages $L_1, L_2 \in \mathcal{P}(A^*)$ est l'ensemble des mots qui appartiennent à $L_1$ ou à $L_2$ :*
$$L_1 + L_2 = \big\{u \in A^* \,|\, (u \in L_1) \vee (u \in L_2)\big\} = L_1 \cup L_2.$$
- ♢ *Le produit $L_1 \cdot L_2$ de deux langages $L_1, L_2 \in \mathcal{P}(A^*)$ est l'ensemble des mots obtenus par concaténation d'un mot de $L_1$ et d'un mot de $L_2$ :*
$$L_1 \cdot L_2 = \big\{uv \in A^* \,|\, (u \in L_1) \wedge (v \in L_2)\big\}.$$
- ♢ *L'itéré $L^*$ d'un langage $L \in \mathcal{P}(A^*)$ est l'ensemble des mots obtenus par concaténation d'un nombre fini (éventuellement nul) de mots de $L$ :*
$$L^* = \textstyle\bigcup_{n\in\mathbb{N}} L^n \;\; \text{avec} \;\; L^0 = \{\lambda\} \;\; \text{et} \;\; (\forall\, n \in \mathbb{N})[\, L^{n+1} = L \cdot L^n\,].$$
*On appelle itéré strict de $L$ et on note $L^+$ le langage $\bigcup_{n\in\mathbb{N}^*} L^n$.*

REMARQUES. (i) On veillera à ne pas confondre le produit de deux langages $L_1$ et $L_2$ avec leur produit cartésien $L_1 \times L_2$.
(ii) La réunion et le produit de langages sont des opérations associatives et le produit est distributif par rapport à la réunion.
(iii) Puisque $\emptyset \cdot \{\lambda\} = \emptyset$, on a $\emptyset^* = \{\lambda\}$.
(iv) $(\forall\, i, j \in \mathbb{N})\big[L^{i+j} = L^i \cdot L^j\big]$ (procéder comme dans l'exercice 3.6).
(v) $L^* = \{\lambda\} + L^+$.
(vi) $L^+ = L \cdot L^* = L^* \cdot L$ (voir exercice 5.2).

**Exercice 5.1** Soit $L$ un langage sur un alphabet $A$. Montrer que $L^{**} = L^* \cdot L^* = L^*$.

**Exercice 5.2** Soient $A$ un alphabet, $L$ un langage sur $A$, $(L_i)_{i\in I}$ une famille de langages sur $A$. Montrer :

1. $L \cdot \Big(\bigcup_{i\in I} L_i\Big) = \bigcup_{i\in I}(L \cdot L_i)$ ;
2. $\Big(\bigcup_{i\in I} L_i\Big) \cdot L = \bigcup_{i\in I}(L_i \cdot L)$.

### Langages rationnels

**Définition 5.4** *Un langage sur un alphabet $A$ est dit rationnel s'il peut être construit à partir de langages finis sur $A$ en utilisant uniquement la réunion, le produit et l'itéré un nombre fini de fois.*

**Proposition 5.1** *L'ensemble des langages rationnels sur un alphabet $A$, noté $R(A)$, est la plus petite partie de $\mathcal{P}(A^*)$ qui contienne le langage vide et les singletons $\{a\}$, $a \in A$, et qui soit stable pour la réunion, le produit et l'itéré.*

### Expressions régulières

On décrit le plus souvent un langage rationnel par une formule appelée *expression régulière*.

**Définition 5.5** *Une expression régulière sur un alphabet $A$ est une suite de symboles pris dans $A \cup \{\emptyset, \lambda, +, \cdot, *, (, )\}$ satisfaisant les règles de construction suivantes :*

1. *$\emptyset$ est une expression régulière ;*
2. *$\lambda$ et toute lettre de $A$ est une expression régulière ;*
3. *si $\boldsymbol{e}$ est une expression régulière, alors $\boldsymbol{e}^*$ est une expression régulière ;*
4. *si $\boldsymbol{e}_1$ et $\boldsymbol{e}_2$ sont des expressions régulières, alors $(\boldsymbol{e}_1 + \boldsymbol{e}_2)$ et $(\boldsymbol{e}_1 \cdot \boldsymbol{e}_2)$ sont des expressions régulières ;*
5. *toute expression régulière est obtenue par application des règles 1 à 4 ci-dessus un nombre fini de fois.*

Remarques. (i) "$*$" est prioritaire sur "$+$" et sur "$\cdot$" dans l'interprétation d'une expression régulière.
(ii) L'usage est de considérer "$\cdot$" prioritaire sur "$+$" et de ne pas écrire les parenthèses rendues de ce fait inutiles. De plus, on convient généralement de supprimer le symbole "$\cdot$" et les deux parenthèses extérieures. Ainsi, par exemple, $ab^* + (a+b)^*b$ correspond à l'expression $\big((a \cdot b^*) + ((a+b)^* \cdot b)\big)$.
(iii) Pour éviter de trop longues expressions, on pourra bien sûr ajouter aux lettres de l'alphabet d'autres symboles représentant des sous-expressions.

Strictement parlant, les expression régulières sont des suites de symboles. Elles sont donc dénuées de sens ; d'où la nécessité d'une sémantique.

**Définition 5.6** *Soit $A$ un alphabet. On note $\mathcal{E}(A)$ l'ensemble des expressions régulières sur $A$. La sémantique des expressions régulières est définie par une application $\mathcal{L} : \mathcal{E}(A) \to R(A)$ construite d'après les règles suivantes :*

1. *$\mathcal{L}(\emptyset)$ est le langage vide ;*
2. *$\mathcal{L}(\lambda) = \{\lambda\}$ et, pour toute lettre $a$ de $A$, $\mathcal{L}(a) = \{a\}$ ;*
3. *Pour tout $\boldsymbol{e} \in \mathcal{E}(A)$, $\mathcal{L}(\boldsymbol{e}^*) = \mathcal{L}(\boldsymbol{e})^*$ ;*
4. *Pour tous $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathcal{E}(A)$, $\mathcal{L}((\boldsymbol{e}_1 + \boldsymbol{e}_2)) = \mathcal{L}(\boldsymbol{e}_1) + \mathcal{L}(\boldsymbol{e}_2)$ et $\mathcal{L}((\boldsymbol{e}_1 \cdot \boldsymbol{e}_2)) = \mathcal{L}(\boldsymbol{e}_1) \cdot \mathcal{L}(\boldsymbol{e}_2)$.*

**Exemple 5.1** (i) Sur l'alphabet $\{a, b\}$, $\mathcal{L}\big((a + \lambda)b^*\big) = \{ab^n \,;\, n \in \mathbb{N}\} \cup \{b^n \,;\, n \in \mathbb{N}\}$.
(ii) Sur $\{a, b\}$, $\mathcal{L}\big((a + b)^*b + \lambda\big)$ est l'ensemble des mots qui ne se terminent pas par $a$ (le mot vide en fait partie).
(iii) Sur $\{a, b, c\}$, $\mathcal{L}\big((a + b)(a + b + c)^*cb\big)$ est l'ensemble des mots qui commencent par $a$ ou par $b$ et qui finissent par $cb$.
(iv) Sur l'ensemble des caractères alphanumériques, $\mathbf{A}(\mathbf{A}+\mathbf{B})^*$ avec $\mathbf{A} = (a+b+\cdots+z+A+B+\cdots+Z)$ et $\mathbf{B} = (0 + 1 + \cdots + 9)$ décrit l'ensemble des mots commençant par une lettre.

**Exercice 5.3** Écrire des expressions régulières décrivant les langages suivants sur l'alphabet $\{a, b\}$ :

1. l'ensemble des mots contenant exactement un $a$ ;
2. l'ensemble des mots contenant au plus un $a$ ;
3. l'ensemble des mots contenant au moins un $a$ ;
4. l'ensemble des mots tels que deux lettres consécutives soient toujours distinctes.

**Exercice 5.4** Soit $A$ alphabet. On dit de deux expressions régulières $\boldsymbol{e}_1$ et $\boldsymbol{e}_2$ sur $A$ qu'elles sont équivalentes, ce que l'on note $\boldsymbol{e}_1 \equiv \boldsymbol{e}_2$, si elles décrivent le même langage. Montrer que, pour tous $\boldsymbol{e}_1,\ \boldsymbol{e}_2 \in \mathcal{E}(A)$,

1. $(\boldsymbol{e}_1\boldsymbol{e}_2)^* \equiv \lambda + \boldsymbol{e}_1(\boldsymbol{e}_2\boldsymbol{e}_1)^*\boldsymbol{e}_2$ ;
2. $(\boldsymbol{e}_1 + \boldsymbol{e}_2)^* \equiv \boldsymbol{e}_1^*(\boldsymbol{e}_2\boldsymbol{e}_1^*)^*$.

## 5.2 Automates finis

### 5.2.1 Automates finis déterministes

#### Description

**Définition 5.7** *Un automate fini déterministe (AFD) est un quintuplet $(S, A, \tau, \sigma, F)$ où $S$ est un ensemble fini non vide d'éléments appelés états, $A$ est un alphabet, $\tau$ est une fonction de $S \times A$ dans $S$, $\sigma$ est un élément de $S$ appelé état initial, et $F$ est une partie non vide de $S$ dont les éléments sont appelés états terminaux.*

Noter que $\tau$ est une fonction, et non une application (on n'a pas nécessairement $\mathrm{Dom}(\tau) = S \times A$). On appelle *transition* tout élément $(s, a, t)$ de $S \times A \times S$ tel que $\tau(s, a) = t$.

Un état non terminal qu'aucune transition ne permet de quitter est dit *bloquant*. Autrement dit, $s \in S$ est bloquant si et seulement si

$$(s \notin F) \wedge (\forall\, a \in A)\big[\big((s, a) \in \mathrm{Dom}(\tau)\big) \to \big(\tau(s, a) = s\big)\big].$$

À tout AFD $\mathcal{A} = (S, A, \tau, \sigma, F)$ on peut associer un graphe orienté $(S, \mathcal{T}, \alpha, \beta)$ dont les arêtes sont étiquetées par les lettres de $A$ :

- l'ensemble des arêtes du graphe est l'ensemble $\mathcal{T}$ des transitions de $\mathcal{A}$ ;
- les applications $\alpha$, $\beta : \mathcal{T} \to S$ sont définies par $\alpha\big((s, a, t)\big) = s$ et $\beta\big((s, a, t)\big) = t$ ;
- l'étiquetage est l'application de $\mathcal{T}$ dans $A$ qui à $(s, a, t)$ fait correspondre $a$.

**Exemple 5.2** La figure 5.1 représente l'AFD défini par $S = \{s_0, s_1, s_2, s_3, s_4, s_5\}$, $A = \{a, b\}$, $\sigma = s_0$, $F = \{s_0, s_3, s_4\}$, et par les transitions précisées dans la table 5.1. L'état initial est désigné par la flèche en dents de scie et les états terminaux sont entourés de deux cercles. L'état $s_2$ est bloquant.

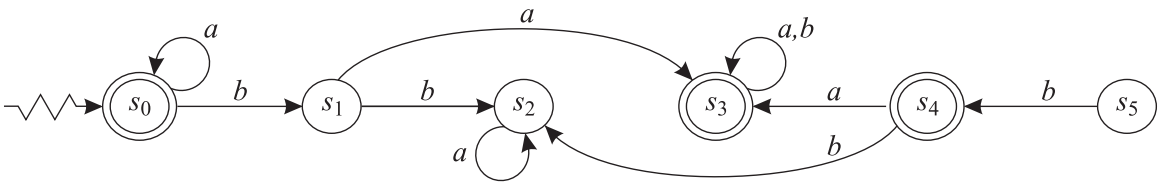


**Figure 5.1** — Exemple d'automate fini déterministe.

| | $a$ | $b$ |
|---|---|---|
| $s_0$ | $s_0$ | $s_1$ |
| $s_1$ | $s_3$ | $s_2$ |
| $s_2$ | $s_2$ | $\diamond$ |
| $s_3$ | $s_3$ | $s_3$ |
| $s_4$ | $s_3$ | $s_2$ |
| $s_5$ | $\diamond$ | $s_4$ |

**Table 5.1** — Table des transitions de l'AFD représenté figure 5.1. Pour $(s, c) \in \mathrm{Dom}(\tau)$, l'état figurant à la ligne $s$ et à la colonne $c$ est $\tau(s, c)$ ; le symbole $\diamond$ indique que $(s, c) \notin \mathrm{Dom}(\tau)$.

### Calculs d'un automate fini déterministe

**Définition 5.8** *Soit $\mathcal{A} = (S, A, \tau, \sigma, F)$ un AFD et introduisons un nouvel état $\omega \notin S$, appelé état puits.*

- ♢ *On formalise l'extension de $\tau$ à $A^*$ (c'est-à-dire l'extension de $\tau$ aux mots sur $A$) par l'application $\gamma : S \times A^* \to S \cup \{\omega\}$ définie par $(\forall\, s \in S)\big[\gamma(s, \lambda) = s\big]$ et $\forall\, s \in S$, $\forall\, a \in A$, $\forall\, u \in A^*$,*

$$\gamma(s, ua) = \begin{cases} \tau\big(\gamma(s, u), a\big) & \text{si } \big(\gamma(s, u), a\big) \in \mathrm{Dom}(\tau)\,, \\ \omega & \text{si } \big(\gamma(s, u), a\big) \notin \mathrm{Dom}(\tau)\,. \end{cases}$$

- ♢ *On appelle calcul de $\mathcal{A}$ pour le mot $u$ la séquence des étapes nécessaires à l'évaluation de $\gamma(\sigma, u)$.*
- ♢ *Un état $s \in S$ est dit inaccessible si et seulement si*

$$(s \neq \sigma) \wedge (\forall\, u \in A^*)[\gamma(\sigma, u) \neq s].$$

Le calcul d'un AFD $\mathcal{A}$ pour un mot $u$ non vide peut être caractérisé par le chemin suivi dans le graphe orienté associé à $\mathcal{A}$ en partant du sommet correspondant à l'état initial $\sigma$ et en suivant successivement les arêtes étiquetées par les lettres de $u$. Le cas $\gamma(\sigma, u) = \omega$ indique la fin prématurée du parcours provoquée par l'absence de la lettre courante parmi les étiquettes des arêtes alors utilisables.

**Exemple 5.3** Dans le cas de l'AFD représenté figure 5.1, le calcul pour le mot *abab* fait successivement intervenir les transitions $(s_0, a, s_0)$, $(s_0, b, s_1)$, $(s_1, a, s_3)$ et $(s_3, b, s_3)$ tandis que le calcul pour n'importe quel mot de $a^*bba^*b(a+b)^*$ bloque l'automate dans l'état $s_2$ à l'arrivée du troisième $b$. Les états $s_4$ et $s_5$ sont inaccessibles.

### Langage reconnu par un automate fini déterministe

**Définition 5.9** *Soient $\mathcal{A} = (S, A, \tau, \sigma, F)$ un AFD, $\gamma$ l'extension de $\tau$ à $A^*$.*

- ♢ *On dit qu'un mot $u$ sur $A$ est reconnu par $\mathcal{A}$ si et seulement si $\gamma(\sigma, u) \in F$.*
- ♢ *Le langage reconnu par $\mathcal{A}$, noté $L(\mathcal{A})$, est l'ensemble des mots reconnus par $\mathcal{A}$.*

**Exemple 5.4** L'automate de la figure 5.1 reconnaît le langage $\mathcal{L}\big(a^* + a^*ba(a+b)^*\big)$, tout comme les deux automates de la figure 5.2 (celui de gauche résulte de la suppression de l'état bloquant et des états inaccessibles).

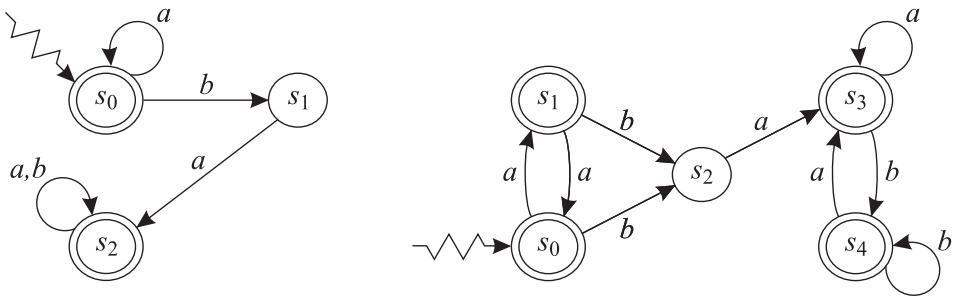


**Figure 5.2** — Exemples d'automates reconnaissant le même langage que l'automate de la figure 5.1.

Remarque. L'exemple 5.4 montre que deux AFD distincts peuvent définir le même langage, ce qui nous amène à la définition suivante : un AFD $\mathcal{A}$ est dit *minimal* si tout AFD reconnaissant $L(\mathcal{A})$ possède au moins autant d'états que $\mathcal{A}$. Il existe des algorithmes permettant de construire des AFD minimaux, ou encore de transformer un AFD en AFD minimal. Nous n'aborderons toutefois pas ce sujet.

**Exercice 5.5** Concevoir des AFD reconnaissant les langages considérés dans l'exercice 5.3.

### 5.2.2 Automates finis non déterministes

#### Description

**Définition 5.10** *Un automate fini non déterministe (AFND) est un quintuplet* $(S, A, \phi, \Sigma, F)$ *où* $S$ *est un ensemble fini non vide d'éléments appelés états,* $A$ *est un alphabet,* $\phi$ *est une application de* $S \times A$ *dans* $\mathcal{P}(S)$*,* $\Sigma$ *est une partie non vide de* $S$ *dont les éléments sont appelés états initiaux, et* $F$ *est une partie non vide de* $S$ *dont les éléments sont appelés états terminaux.*

Deux points essentiels diffèrent de la description d'un AFD (définition 5.7) et expliquent pourquoi l'on parle de non-déterminisme : (i) une application $\phi$ à valeurs dans $\mathcal{P}(S)$ remplace la fonction $\tau$ à valeurs dans $S$ ; (ii) on ne se limite plus à un unique état initial.

Les transitions d'un AFND sont les éléments $(s, a, t)$ de $S \times A \times S$ tels que $t \in \phi(s, a)$ et le graphe orienté associé à un AFND se construit de la même façon que pour un AFD. Le cas $\phi(s, a) = \emptyset$ indique que la lettre $a$ ne permet pas de quitter l'état $s$ et les états bloquants sont les états $s \in S \setminus F$ tels que $(\forall\, a \in A)\big[\phi(s, a) \subset \{s\}\big]$.

**Exemple 5.5** La figure 5.3 représente l'AFND défini par $S = \{s_0, s_1, s_2, s_3, s_4\}$, $A = \{a, b\}$, $\Sigma = \{s_0, s_4\}$, $F = \{s_3\}$, et par les transitions précisées dans la table 5.2.

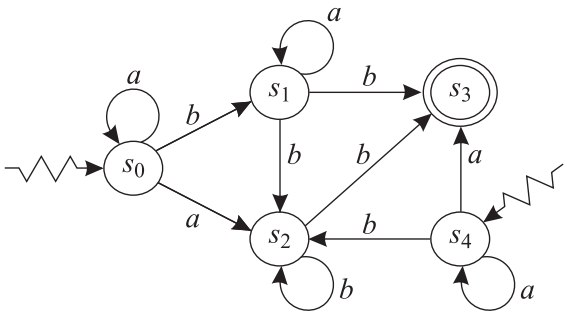


**Figure 5.3** — Exemple d'automate fini non déterministe.

| | $a$ | $b$ |
|---|---|---|
| $s_0$ | $\{s_0, s_2\}$ | $\{s_1\}$ |
| $s_1$ | $\{s_1\}$ | $\{s_2, s_3\}$ |
| $s_2$ | $\emptyset$ | $\{s_2, s_3\}$ |
| $s_3$ | $\emptyset$ | $\emptyset$ |
| $s_4$ | $\{s_3, s_4\}$ | $\{s_2\}$ |

**Table 5.2** — Table des transitions de l'AFND de la figure 5.3. L'ensemble figurant à la ligne $s$ et à la colonne $c$ est $\phi(s, c)$

### Calculs d'un automate fini non déterministe

**Définition 5.11** *Soit $\mathcal{A} = (S, A, \phi, \Sigma, F)$ un AFND.*

♢ *On formalise l'extension de $\phi$ à $A^*$ (c'est-à-dire l'extension de $\phi$ aux mots sur $A$) par l'application $\zeta : S \times A^* \to \mathcal{P}(S)$ définie par $(\forall\, s \in S)\big[\zeta(s, \lambda) = \{s\}\big]$ et $\forall\, s \in S$, $\forall\, a \in A$, $\forall\, u \in A^*$,*

$$\zeta(s, ua) \;=\; \bigcup_{t \in \zeta(s,u)} \phi(t, a)\,. \tag{5.1}$$

♢ *Étant donné $\sigma \in \Sigma$, on appelle calcul de $\mathcal{A}$ pour l'initialisation $\sigma$ et le mot $u$ la séquence des étapes nécessaires à l'évaluation de $\zeta(\sigma, u)$.*

♢ *Un état $s \in S$ est dit inaccessible si et seulement si*

$$(s \notin \Sigma) \wedge (\forall\, \sigma \in \Sigma)(\forall\, u \in A^*)[s \notin \zeta(\sigma, u)].$$

Le calcul d'un AFND $\mathcal{A}$ pour une initialisation $\sigma$ et un mot $u$ peut être représenté par une arborescence dont les chemins menant de la racine aux feuilles correspondent aux chemins que le mot $u$ permet d'emprunter dans le graphe associé à $\mathcal{A}$ en partant de $\sigma$. Notons $n$ le nombre de lettre de $u$. Si $u$ n'est pas le mot vide, les sommets de même niveau $k$, $k \in [\![1, n]\!]$, forment le résultat de la $k$-ème itération sur la formule (5.1) dans l'évaluation de $\zeta(\sigma, u)$. En particulier, $\zeta(\sigma, u)$ est défini par les feuilles de niveau $n$.

**Exemple 5.6** Le calcul de l'AFND de la figure 5.3 pour l'initialisation $s_0$ et le mot $abb$ est schématisé par l'arborescence de la figure 5.4. Partant de $\zeta(s_0, \lambda) = \{s_0\}$, la formule (5.1) est itérée 3 fois : $\zeta(s_0, a) = \{s_0, s_2\},\ \zeta(s_0, ab) = \{s_1, s_2, s_3\},\ \zeta(s_0, abb) = \{s_2, s_3\}$.

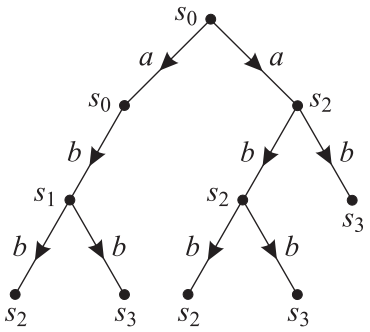


**Figure 5.4** — Calcul de l'AFND de la figure 5.3 pour l'initialisation $s_0$ et le mot $abb$.

## Langage reconnu par un automate fini non déterministe

**Définition 5.12** *Soient $\mathcal{A} = (S, A, \phi, \Sigma, F)$ un AFND, $\zeta$ l'extension de $\phi$ à $A^*$.*

♢ *On dit qu'un mot $u$ sur $A$ est reconnu par $\mathcal{A}$ si et seulement si*

$$(\exists\, \sigma \in \Sigma)\big[\zeta(\sigma, u) \cap F \neq \emptyset\big].$$

♢ *Le langage reconnu par $\mathcal{A}$, noté $L(\mathcal{A})$, est l'ensemble des mots reconnus par $\mathcal{A}$.*

**Exemple 5.7** L'AFND $\mathcal{A}$ de la figure 5.3 reconnaît les mots de chacun des langages suivants :
- $L_1 = \mathcal{L}(a^*ba^*b)$ (initialisation $s_0$, passage par $s_1$),
- $L_2 = \mathcal{L}(a^*ba^*bb^*b)$ (initialisation $s_0$, passage par $s_1$ puis $s_2$),
- $L_3 = \mathcal{L}(a^*ab^*b)$ (initialisation $s_0$, passage par $s_2$),
- $L_4 = \mathcal{L}(a^*a)$ (initialisation $s_4$, arrivée en $s_3$).
- $L_5 = \mathcal{L}(a^*bb^*b)$ (initialisation $s_4$, passage par $s_2$),

On a donc

$$\begin{aligned} L(\mathcal{A}) \;=\; \textstyle\bigcup_{i=1}^{5} L_i \;&=\; \mathcal{L}\big(\, a^*ba^*b + a^*ba^*bb^*b + a^*ab^*b + a^*a + a^*bb^*b \,\big) \\ &=\; \mathcal{L}\big(\, a^*\big(ba^*b(\lambda + b^*b) + a(b^*b + \lambda) + bb^*b\big)\,\big) \\ &=\; \mathcal{L}\big(\, a^*\big(ba^*bb^* + ab^* + bb^*b\big)\,\big) \quad (\text{car } b^*b \equiv b^+ \text{ et } \lambda + b^+ \equiv b^*) \\ &=\; \mathcal{L}\big(\, a^*\big(ba^*bb^* + ab^*\big)\,\big) \quad (\text{car } \mathcal{L}(bb^*b) = \mathcal{L}(bbb^*) \subset \mathcal{L}(ba^*bb^*)) \\ &=\; \mathcal{L}\big(\, a^*\big(ba^*b + a\big)b^*\,\big). \end{aligned}$$

**Exercice 5.6** Concevoir un AFND sur l'alphabet $A = \{a, b, c, \ldots, z, 0, 1, \ldots, 9\}$ reconnaissant l'ensemble des mots contenant la chaîne "3bim".

### Comparaison avec les automates finis déterministes

Il est beaucoup plus facile de savoir si un mot donné appartient au langage reconnu par un automate lorsque ce dernier est déterministe ; alors pourquoi introduire des automates non déterministes ? L'intérêt des AFND est qu'il est généralement bien plus simple de concevoir un AFND plutôt qu'un AFD pour un langage donné. L'exemple du langage $\mathcal{L}\big((a+b)^*ab\big)$ sur $\{a,b\}$ est assez éloquent. S'il est clair que l'AFND de la figure 5.5 reconnaît ce langage, il est plus difficile de se convaincre que l'AFD de la figure 5.6 convient également. Ceci soulève le problème de la construction d'un AFD reconnaissant le même langage qu'un AFND donné ; problème que nous traitons dans la section suivante.

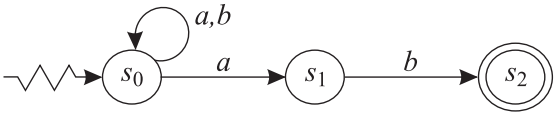


**Figure 5.5** — AFND reconnaissant le langage $\mathcal{L}\big((a+b)^*ab\big)$ sur $\{a,b\}$.

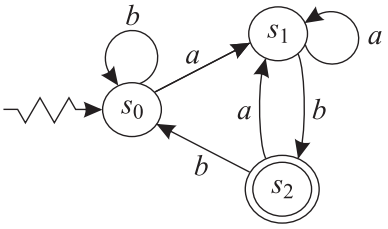


**Figure 5.6** — AFD reconnaissant le même langage que l'AFND représenté figure 5.5.

### 5.2.3 "Déterminisation" d'un automate

Le problème de la "déterminisation" d'un AFND $\mathcal{A} = (S, A, \phi, \Sigma, F)$ consiste à trouver un AFD $\mathcal{A}_{\rm d} = \big(\widetilde{S}, A, \tau, \sigma, \widetilde{F}\big)$ reconnaissant le même langage que $\mathcal{A}$, c'est-à-dire tel que $L(\mathcal{A}) = L(\mathcal{A}_{\rm d})$. Un tel automate peut être défini par

$$\begin{aligned}
\widetilde{S} &= \mathcal{P}(S) \setminus \{\emptyset\}\,, \\
\sigma &= \Sigma\,, \\
\widetilde{F} &= \big\{ X \in \widetilde{S} \,\big|\, X \cap F \neq \emptyset \big\}\,, \\
\tau(X,a) &= \textstyle\bigcup_{s\in X} \phi(s,a) \quad \text{sur} \quad \mathrm{Dom}(\tau) = \big\{ (X,a) \in \widetilde{S} \times A \,\big|\, \textstyle\bigcup_{s\in X} \phi(s,a) \neq \emptyset \big\}\,.
\end{aligned}$$

**Proposition 5.2** *Soient $\gamma$ et $\zeta$ les extensions de $\tau$ et $\phi$ à $A^*$ pour les automates $\mathcal{A}$ et $\mathcal{A}_{\rm d}$ considérés ci-dessus. Pour tout $X \in \widetilde{S}$ et pour tout $u \in A^*$ tels que $\gamma(X,u) \neq \omega$, on a*

$$\gamma(X,u) = \bigcup_{s\in X} \zeta(s,u)\,.$$

**Corollaire 5.1** $L(\mathcal{A}) = L(\mathcal{A}_{\rm d})\,.$

**Exemple 5.8** Considérons l'AFND $\mathcal{A}$ de la figure 5.5. Il lui correspond l'AFD $\mathcal{A}_{\rm d}$ représenté figure 5.7 dont les transitions sont données par la table 5.3. Comme dans la plupart des cas, l'AFD obtenu possède de nombreux états inaccessibles ($\{s_1\}$, $\{s_2\}$, $\{s_1, s_2\}$ et $\{s_0, s_1, s_2\}$) qu'il est possible de supprimer. En pratique, pour éviter d'avoir à considérer ces états inutiles, on constitue la table des transitions en partant de $\Sigma$ et en écrivant les lignes nécessaires au fur et à mesure des besoins (c'est-à-dire au fur et à mesure de leur apparition dans les colonnes). Dans le cadre de notre exemple, nous obtenons ainsi la table 5.4 définissant l'AFD représenté figure 5.8.

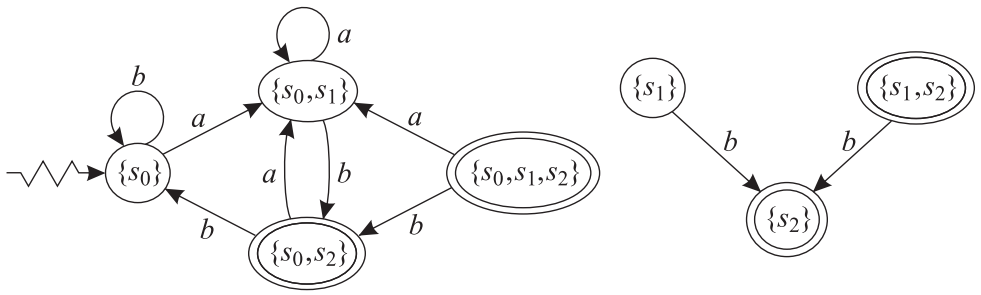


**Figure 5.7** — Résultat de la déterminisation de l'AFND représenté figure 5.5.

| | $a$ | $b$ |
|---|---|---|
| $\{s_0\}$ | $\{s_0, s_1\}$ | $\{s_0\}$ |
| $\{s_1\}$ | $\diamond$ | $\{s_2\}$ |
| $\{s_2\}$ | $\diamond$ | $\diamond$ |
| $\{s_0, s_1\}$ | $\{s_0, s_1\}$ | $\{s_0, s_2\}$ |
| $\{s_0, s_2\}$ | $\{s_0, s_1\}$ | $\{s_0\}$ |
| $\{s_1, s_2\}$ | $\diamond$ | $\{s_2\}$ |
| $\{s_0, s_1, s_2\}$ | $\{s_0, s_1\}$ | $\{s_0, s_2\}$ |

**Table 5.3** — Table des transitions de l'AFD de la figure 5.7

| | $a$ | $b$ |
|---|---|---|
| $\{s_0\}$ | $\{s_0, s_1\}$ | $\{s_0\}$ |
| $\{s_0, s_1\}$ | $\{s_0, s_1\}$ | $\{s_0, s_2\}$ |
| $\{s_0, s_2\}$ | $\{s_0, s_1\}$ | $\{s_0\}$ |

**Table 5.4** — Table de transitions correspondant à la déterminisation de l'AFND de la figure 5.5

Remarque. Le comportement d'un AFD $(S, A, \tau, \sigma, F)$ peut être reproduit de façon exacte par l'AFND $(S, A, \phi, \{\sigma\}, F)$ défini par

$$\phi : S \times A \to \mathcal{P}(S), \quad (s, a) \mapsto \begin{cases} \{\tau(s, a)\} & \text{si } (s, a) \in \mathrm{Dom}(\tau), \\ \emptyset & \text{sinon.} \end{cases}$$

Par conséquent, compte tenu du corollaire 5.1, il n'est pas nécessaire de faire la distinction entre AFD et AFND du point de vue de la reconnaissance de langages. Dans ce contexte, on pourra donc parler d'*automates finis* sans préciser s'ils sont déterministes ou non.

**Exercice 5.7** Déterminiser l'automate de l'exercice 5.6.

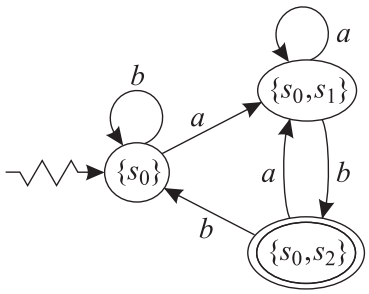


**Figure 5.8** — AFD associé à la table de transitions 5.4.

## 5.3 Théorème de Kleene

Nous démontrons ici le théorème fondamental suivant.

**Théorème 5.1 (Kleene)** *Un langage est rationnel si et seulement s'il est reconnu par un automate fini.*

Après quelques notions préliminaires exposées dans la section 5.3.1, nous fournissons une preuve constructive établissant que tout langage rationnel est reconnu par un AFND (section 5.3.2), puis nous montrons par induction que tout langage reconnu par un AFND est rationnel (section 5.3.3).

### 5.3.1 Notions préliminaires

**Définition 5.13** *Dans un AFND $\mathcal{A} = (S, A, \phi, \Sigma, F)$, on appelle chemin de trace $u$, $u = a_1 \cdots a_n \in A^* \setminus \{\lambda\}$, toute succession $s_0, a_1, s_1, a_2, \ldots, s_{n-1}, a_n, s_n$ d'états et de lettres telle que $(\forall\, i \in [\![1, n]\!])\big[s_i \in \phi(s_{i-1}, a_i)\big]$. Les états $s_0$ et $s_n$ sont respectivement appelés l'origine et le but du chemin ; tout autre état est dit interne. On autorise de plus l'existence de chemins vides, c'est-à-dire de chemins de trace $\lambda$, dont l'origine et le but se confondent.*

Notations. Soit $\mathcal{A} = (S, A, \phi, \Sigma, F)$ un AFND.

- ♢ On note $\mathcal{C}_\mathcal{A}$ l'ensemble des chemins de $\mathcal{A}$.
- ♢ Soit $c \in \mathcal{C}_\mathcal{A}$. On note respectivement $\alpha_\mathcal{A}(c)$, $\beta_\mathcal{A}(c)$ et $\mathrm{tr}_\mathcal{A}(c)$ l'origine, le but et la trace de $c$.
- ♢ On note $\xrightarrow{u}_\mathcal{A}$ la relation
$$\big\{(s,t) \in S^2 \;\big|\; (\exists\, c \in \mathcal{C}_\mathcal{A})\big[\big(\alpha_\mathcal{A}(c) = s\big) \wedge \big(\beta_\mathcal{A}(c) = t\big) \wedge \big(\mathrm{tr}_\mathcal{A}(c) = u\big)\big]\big\}.$$

♢ On désigne par $\varepsilon_{\mathcal{A}}(s)$ le chemin vide de $\mathcal{A}$ reposant sur l'état $s$.

REMARQUES. (i) Pour tout $(s,t) \in S^2$, $s = t \iff s \xrightarrow{\lambda}_{\mathcal{A}} t$.
(ii) Pour tout $(s,t) \in S^2$ et pour tous $u, v \in A^*$,

$$s \xrightarrow{uv}_{\mathcal{A}} t \iff (\exists\, s' \in S)\big[(s \xrightarrow{u}_{\mathcal{A}} s') \wedge (s' \xrightarrow{v}_{\mathcal{A}} t)\big].$$

**Proposition 5.3** *Soient $\mathcal{A} = (S, A, \phi, \Sigma, F)$ un AFND, $\zeta$ l'extension de $\phi$ à $A^*$. Pour tout $(s,t) \in S^2$ et pour tout $u \in A^*$, on a*

$$t \in \zeta(s,u) \iff s \xrightarrow{u}_{\mathcal{A}} t$$

*et il s'en suit :* $u \in L(\mathcal{A}) \iff (\exists\, \sigma \in \Sigma)(\exists\, t \in F)[\,\sigma \xrightarrow{u}_{\mathcal{A}} t\,]$.

**Définition 5.14** *Soit $\mathcal{A}$ un AFND et soient $c = s_0, a_1, \ldots, s_n$ et $c' = s'_0, a'_1, \ldots, s'_m$ deux chemins non vides de $\mathcal{A}$ tels que $s_n = s'_0$, c'est-à-dire tels que $\beta_{\mathcal{A}}(c) = \alpha_{\mathcal{A}}(c')$. On appelle concaténation de $c$ et $c'$ et on note $cc'$ le chemin $s_0, a_1, \ldots, s_n, a'_1, \ldots, s'_m$. Par convention, $c\,\varepsilon_{\mathcal{A}}(s_n) = c$, $\varepsilon_{\mathcal{A}}(s'_0)\,c' = c'$ et $(\forall s \in S)\big[\varepsilon_{\mathcal{A}}(s)\,\varepsilon_{\mathcal{A}}(s) = \varepsilon_{\mathcal{A}}(s)\big]$.*

**Définition 5.15** *Soient $\mathcal{A}$ un AFND, $C, C' \in \mathcal{P}(\mathcal{C}_{\mathcal{A}})$. On appelle produit de $C$ et $C'$ et on note $C \cdot C'$ l'ensemble des chemins s'obtenant par concaténation d'un chemin de $C$ et d'un chemin de $C'$ :* $C \cdot C' = \big\{\, cc' \;\big|\; (c \in C) \wedge (c' \in C') \wedge \big(\beta_{\mathcal{A}}(c) = \alpha_{\mathcal{A}}(c')\big)\big\}$.

**Définition 5.16** *Soient $\mathcal{A}$ un AFND, $C \in \mathcal{P}(\mathcal{C}_{\mathcal{A}})$. On appelle itéré de $C$ et on note $C^*$ l'ensemble des chemins s'obtenant par concaténation d'un nombre fini (éventuellement nul) de chemins de $C$ :*

$$C^* = \bigcup_{n\in\mathbb{N}} C^n \;\text{ avec }\; C^0 = \bigcup_{c\in C} \big\{\varepsilon_{\mathcal{A}}\big(\beta_{\mathcal{A}}(c)\big)\big\} \;\text{ et }\; (\forall\, n \in \mathbb{N})[\,C^{n+1} = C \cdot C^n\,].$$

**Exercice 5.8** Soit $\mathcal{A}$ un AFND. Pour toute partie $C$ de $\mathcal{C}_{\mathcal{A}}$, on note $L(C)$ l'ensemble $\{\mathrm{tr}_{\mathcal{A}}(c) \,|\, c \in C\}$. Soient $C, C' \in \mathcal{P}(\mathcal{C}_{\mathcal{A}})$. Montrer :

1. $L(C \cup C') = L(C) + L(C')$ ;
2. $L(C \cdot C') \subset L(C) \cdot L(C')$ ;
3. $L(C \cdot C') = L(C) \cdot L(C')$ si $(\forall c \in C)(\forall c' \in C')[\beta_{\mathcal{A}}(c) = \alpha_{\mathcal{A}}(c')]$ ;
4. $L(C^*) \subset (L(C))^*$ $\big($établir $L(C^*) = \bigcup_{n\in\mathbb{N}} L(C^n)$ puis $(\forall n \in \mathbb{N})[L(C^n) \subset (L(C))^n]\big)$ ;
5. $L(C^*) = (L(C))^*$ si $(\forall c \in C)[\beta_{\mathcal{A}}(c) = \alpha_{\mathcal{A}}(c)]$.

### 5.3.2 Des langages rationnels aux automates finis

Nous prouvons ici la première implication du théorème de Kleene, à savoir que tout langage rationnel est reconnu par un automate fini (AF). Compte tenu de la description des langages rationnels fournie par les expressions régulières (voir définitions 5.5 et 5.6), il suffit de démontrer les quatre points suivants.

1. Il existe un AF "reconnaissant" le langage vide.
2. Il existe un AF reconnaissant $\{\lambda\}$ et, pour toute lettre $a$ de l'alphabet considéré, il existe un AF reconnaissant $\{a\}$.
3. Pour tout AF $\mathcal{A}_1$ et pour tout AF $\mathcal{A}_2$, il existe un AF reconnaissant $L(\mathcal{A}_1)+L(\mathcal{A}_2)$ et un AF reconnaissant $L(\mathcal{A}_1)\cdot L(\mathcal{A}_2)$.
4. Pour tout AF $\mathcal{A}$, il existe un AF reconnaissant $L(\mathcal{A})^*$.

Les deux premiers points sont triviaux (considérer par exemple les automates representés figures 5.9(a), (b) et (c)). Les propositions 5.4 et 5.5 qui suivent établissent la véracité du troisième point. La proposition 5.6 prouve le quatrième point car $L(\mathcal{A})^* = \{\lambda\} + L(\mathcal{A})^+$.

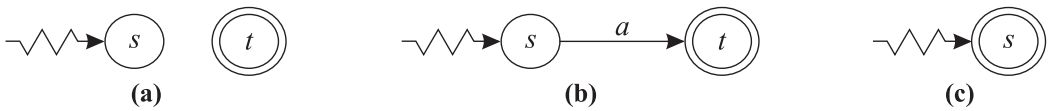


**Figure 5.9** — Automates finis reconnaissant (a) $\emptyset$, (b) $\{a\}$ et (c) $\{\lambda\}$.

**Proposition 5.4 (Union)** *Soient* $\mathcal{A}_1 = (S_1, A, \phi_1, \Sigma_1, F_1)$ *et* $\mathcal{A}_2 = (S_2, A, \phi_2, \Sigma_2, F_2)$ *deux AFND définis sur un même alphabet* $A$ *et dont les ensembles d'états* $S_1$ *et* $S_2$ *sont disjoints. Alors,* $L(\mathcal{A}) = L(\mathcal{A}_1) + L(\mathcal{A}_2)$ *pour l'AFND* $\mathcal{A} = (S, A, \phi, \Sigma, F)$ *défini par*

$$S = S_1 \cup S_2\,, \qquad \Sigma = \Sigma_1 \cup \Sigma_2\,, \qquad F = F_1 \cup F_2$$

$$et \quad \phi(s,a) = \begin{cases} \phi_1(s,a) & si\ s \in S_1\,, \\ \phi_2(s,a) & si\ s \in S_2\,. \end{cases}$$

**Proposition 5.5 (Produit)** *Soient* $\mathcal{A}_1 = (S_1, A, \phi_1, \Sigma_1, F_1)$ *et* $\mathcal{A}_2 = (S_2, A, \phi_2, \Sigma_2, F_2)$ *deux AFND définis sur un même alphabet* $A$ *et dont les ensembles d'états* $S_1$ *et* $S_2$ *sont disjoints. Alors,* $L(\mathcal{A}) = L(\mathcal{A}_1) \cdot L(\mathcal{A}_2)$ *pour l'AFND* $\mathcal{A} = (S, A, \phi, \Sigma, F)$ *défini par*

$$S = S_1 \cup S_2\,, \qquad F = F_2\,, \qquad \Sigma = \begin{cases} \Sigma_1 & si\ \ \Sigma_1 \cap F_1 = \emptyset\,, \\ \Sigma_1 \cup \Sigma_2 & sinon\,, \end{cases}$$

$$et \quad \phi(s,a) = \begin{cases} \phi_1(s,a) & si\ \ s \in S_1\ \ et\ \ \phi_1(s,a) \cap F_1 = \emptyset\,, \\ \phi_1(s,a) \cup \Sigma_2 & si\ \ s \in S_1\ \ et\ \ \phi_1(s,a) \cap F_1 \neq \emptyset\,, \\ \phi_2(s,a) & si\ \ s \in S_2\,. \end{cases}$$

**Proposition 5.6 (Itéré)** *Soit* $\mathcal{A} = (S, A, \phi, \Sigma, F)$ *un AFND. Alors,* $L(\mathcal{A}') = L(\mathcal{A})^+$ *pour l'AFND* $\mathcal{A}' = (S, A, \phi', \Sigma, F)$ *défini par*

$$\phi'(s,a) = \begin{cases} \phi(s,a) & si\ \ \phi(s,a) \cap F = \emptyset\,, \\ \phi(s,a) \cup \Sigma & si\ \ \phi(s,a) \cap F \neq \emptyset\,. \end{cases}$$

**Exemple 5.9** La figure 5.10 illustre la construction d'un AF reconnaissant le langage $\mathcal{L}\big((ab)^*b\big)$ à l'aide des résultats qui précèdent.

- On commence par construire un automate reconnaissant $\{l\}$ pour chaque lettre $l$ apparaissant dans l'expression $\boldsymbol{e}$ qui définit le langage (figures 5.10(a) et (b)).
- Si $\boldsymbol{e}$ contient le symbole "$\lambda$" ou le symbole "$*$", on construit également un automate reconnaissant $\{\lambda\}$ (figure 5.10(c)).
- On fait ensuite appel aux propositions 5.4, 5.5 et 5.6 en respectant les priorités, ce qui nous amène à construire successivement les automates reconnaissant $\mathcal{L}(ab)$, $\mathcal{L}\big((ab)^*\big) = \{\lambda\} + \mathcal{L}\big((ab)^+\big)$ et $\mathcal{L}\big((ab)^*b\big)$ (figures 5.10(d), (e) et (f), respectivement).
- Enfin, on supprime les éventuels états bloquants ou inaccessibles (figure 5.10(g)).

La déterminisation de l'AFND obtenu conduit à l'AFD représenté figure 5.11.

**Exercice 5.9** Construire un AFND sur l'alphabet $\{a, b\}$ reconnaissant le langage $\mathcal{L}((a + ba^*)^+)$ puis déterminiser cet automate.

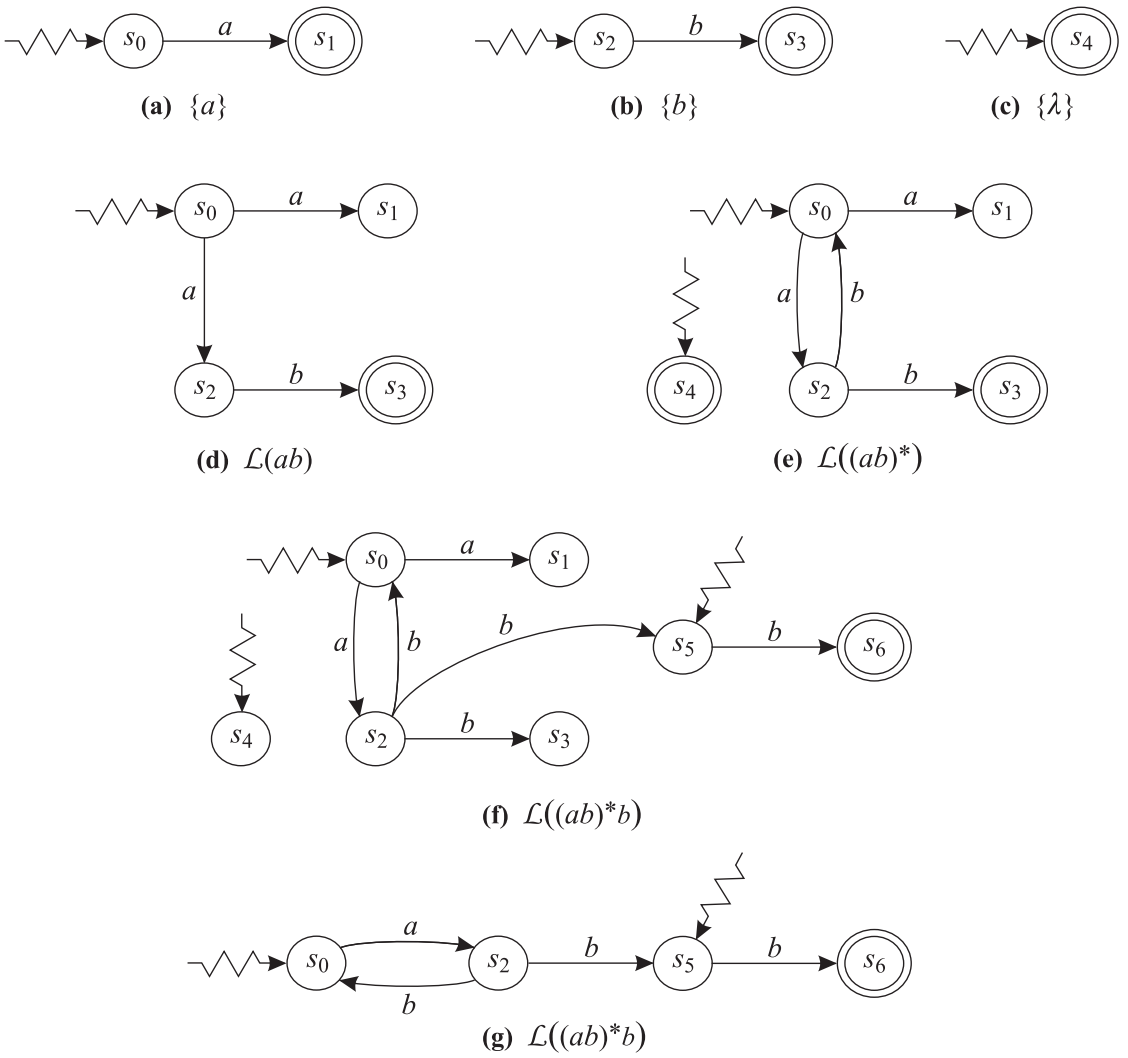


**Figure 5.10** — Construction d'un AFND reconnaissant $\mathcal{L}\big((ab)^*b\big)$.

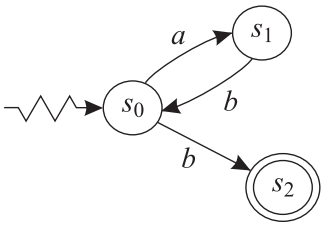


**Figure 5.11** — AFD reconnaissant $\mathcal{L}\big((ab)^*b\big)$.

### 5.3.3 Des automates finis aux langages rationnels

Nous démontrons ici la deuxième implication du théorème de Kleene : "tout langage reconnu par un AF est rationnel".

Soit $\mathcal{A} = (S, A, \phi, \Sigma, F)$ un AFND. On considère un arrangement $(s_1, \ldots, s_{|S|})$ des états de $\mathcal{A}$. Pour tous $i, j, k \in [\![1, |S|]\!]$, on note :

- ♢ $C_{ij}^k$ l'ensemble des chemins de $\mathcal{A}$ d'origine $s_i$ et de but $s_j$ dont les états internes sont des éléments de $\{s_1, \ldots, s_k\}$.
- ♢ $L_{ij}^k$ l'ensemble des traces des chemins de $C_{ij}^k$.

Avec ces notations,

$$L(\mathcal{A}) = \sum_{(s,t)\in \Sigma\times F} L^{|S|}_{\nu(s)\nu(t)} = \sum_{(i,j)\in \nu(\Sigma)\times\nu(F)} L_{ij}^{|S|},$$

où $\nu : S \to [\![1, |S|]\!]$ est la bijection qui à chaque état $s$ fait correspondre l'entier $i$ pour lequel $s_i = s$. Par conséquent, puisque toute réunion finie de langages rationnels est un langage rationnel, la proposition suivante permet de conclure que $L(\mathcal{A}) \in R(A)$.

**Proposition 5.7** *Pour tous* $i, j, k \in [\![1, |S|]\!]$, $L_{ij}^k \in R(A)$.

## 5.4 Langages non rationnels

Nous montrons ici qu'il existe des langages non rationnels. Nous commençons par fournir un exemple que nous traitons de façon spécifique, puis nous démontrons un résultat général permettant d'isoler certaines classes de langages non rationnels.

### 5.4.1 Un exemple de Langage non rationnel

**Proposition 5.8** *Le langage* $L = \{a^n b^n\,;\, n \in \mathbb{N}\}$ *sur l'alphabet* $A = \{a, b\}$ *n'est pas rationnel.*

DÉMONSTRATION. Supposons $L \in R(A)$. Compte tenu du Théorème 5.1, il existe un AFD $\mathcal{A} = (S, A, \tau, s_0, F)$ tel que $L(\mathcal{A}) = L$. Pour toute paire $(s,t) \in S^2$ et pour tout mot $u \in A^*$, on note $s \xrightarrow{u} t$ pour indiquer que $\gamma(s,u) = t$, où $\gamma$ désigne l'extension de $\tau$ à $A^*$ (voir définition 5.8).
Étant donné $n \in \mathbb{N}^*$, on définit l'état $s_n$ par $s_0 \xrightarrow{a^n} s_n$ (définition justifiée par le fait que le calcul de $a^n$ ne bloque pas $\mathcal{A}$ puisque celui-ci reconnaît $a^n b^n$). L'automate $\mathcal{A}$ étant fini, il existe nécessairement deux entiers $i$ et $j$ tels que $0 \leqslant i < j \leqslant |S|$ et $s_i = s_j$. Comme $s_i \xrightarrow{a^{j-i}} s_j$, on a $s_i \xrightarrow{a^{j-i}} s_i$ et il s'en suit que

$$(\forall k \in \mathbb{N})\big[\, s_0 \xrightarrow{a^{i+k(j-i)}} s_i \,\big].$$

Parallèlement, puisque $a^i b^i$ est reconnu par $\mathcal{A}$, on a $s_i \xrightarrow{b^i} s_{\mathrm{f}}$ avec $s_{\mathrm{f}} \in F$. Ainsi a t-on

$$(\forall k \in \mathbb{N})\big[\, s_0 \xrightarrow{a^{i+k(j-i)}b^i} s_{\mathrm{f}} \,\big],$$

ce qui établit que $\mathcal{A}$ reconnaît des mots qui ne sont pas dans $L$ : contradiction. □

### 5.4.2 Le lemme de l'étoile

**Lemme 5.1 (lemme de l'étoile)** *Soit $L$ un langage rationnel sur un alphabet $A$.*
*Il existe un entier $m$ tel que, pour tout mot $u \in L$ de longueur supérieure ou égale à $m$, il existe $x, y \in A^*$ et $v \in A^* \setminus \{\lambda\}$ tels que*

$$\begin{cases} u = xvy \\ v \text{ est de longueur inférieure où égale à } m \\ (\forall n \in \mathbb{N})[\, xv^n y \in L \,] \end{cases}$$

*($v^n$ étant défini par $v^0 = \lambda$ et $(\forall n \in \mathbb{N})[v^{n+1} = vv^n]$).*

DÉMONSTRATION. Soit $\mathcal{A} = (S, A, \tau, s_0, F)$ un AFD tel que $L(\mathcal{A}) = L$. Pour toute paire $(s,t) \in S^2$ et pour tout mot $u \in A^*$, on note $s \xrightarrow{u} t$ pour indiquer que $\gamma(s,u) = t$, où $\gamma$ désigne l'extension de $\tau$ à $A^*$ (voir définition 5.8).
Soit $u = a_1 \cdots a_n$ un mot de $L$ de longueur $n \geqslant |S|$. Pour tout $l \in [\![1, n]\!]$, on définit l'état $s_l$ par $s_0 \xrightarrow{a_1 \cdots a_l} s_l$ (ce qui a bien du sens puisque $\mathcal{A}$ reconnaît $a_1 \cdots a_n$ et ne peut donc être bloqué par le calcul de $a_1 \cdots a_l$).
L'automate $\mathcal{A}$ étant fini, il existe nécessairement deux entiers $i$ et $j$ tels que $0 \leqslant i < j \leqslant |S|$ et $s_i = s_j$.
On pose :

$$x = \begin{cases} a_1 \cdots a_i & \text{si } i \geqslant 1 \\ \lambda & \text{sinon} \end{cases}, \qquad v = a_{i+1} \cdots a_j \quad \text{et} \quad y = \begin{cases} a_{j+1} \cdots a_n & \text{si } j \leqslant n \\ \lambda & \text{sinon} \end{cases}.$$

On a bien $u = xvy$. En outre,

$$s_0 \xrightarrow{x} s_i \xrightarrow{v} s_j = s_i \xrightarrow{y} s_{\mathrm{f}}$$

avec $s_{\mathrm{f}} \in F$. Puisque $(\forall n \in \mathbb{N})\big[\, s_i \xrightarrow{v^n} s_i \,\big]$, on a donc également $(\forall n \in \mathbb{N})\big[\, s_0 \xrightarrow{xv^n y} s_{\mathrm{f}} \,\big]$, ce qui achève la démonstration (choisir $m = |S|$). □

**Exemple 5.10** Montrons que le langage $L = \{a^n b^n \,;\, n \in \mathbb{N}\}$ sur $A = \{a, b\}$ n'est pas rationnel en utilisant le lemme de l'étoile.
Supposons $L \in R(A)$ et soit $m \in \mathbb{N}$ tel que les propriétés du lemme 5.1 soient satisfaites. Étant donné $n \in \mathbb{N}^*$ tel que $2n \geqslant m$, il existe donc $x, y \in A^*$ et $v \in A^* \setminus \{\lambda\}$ tels que $a^n b^n = xvy$ et $(\forall p \in \mathbb{N})[\, xv^p y \in L\,]$. Le mot $v$ est nécessairement de la forme $a^k b^l$ avec $k, l \in [\![0, n]\!]$ et $(k,l) \neq (0,0)$, mais on vérifie alors que $xv^2y \notin L$ (contradiction). En effet :

- si $k \neq 0$ et $l \neq 0$, alors $xv^2y = xa^k b^l a^k b^l y \notin L$ ;
- si $k \neq 0$ et $l = 0$, alors $x = a^{n-k}$ et $y = b^n$ et donc $xv^2y = a^{n+k}b^n \notin L$ ;
- si $k = 0$ et $l \neq 0$, alors $x = a^n$ et $y = b^{n-l}$ et donc $xv^2y = a^n b^{n+l} \notin L$.

**Exercice 5.10** Montrer que les langages $L_1$ et $L_2$ suivants sur $A = \{a, b\}$ ne sont pas rationnels :

- $L_1 = \{a^n b^p \,;\, p \in \mathbb{N},\, n \in [\![p, \infty[\![\}$ ;
- $L_2 = \{a^n b a^n \,;\, n \in \mathbb{N}\}$.