Mathématiques pour informaticien

MAT-1919

François Laviolette, Josée Desharnais,
Pascal Germain

Automne 2014

(Dernière modification : 2 septembre 2014)

Remerciements

Une partie de la matière de ce cours était autrefois enseignée dans le cadre du cours *Logique et techniques de preuve*. Merci à Jules Desharnais de nous avoir permis d'emprunter certains éléments et exercices des notes de cours qu'il a lui-même rédigées.

Nous remercions également les étudiants des sessions précédentes qui ont signalé des coquilles dans les notes de cours ou suggéré des améliorations à celles-ci, contribuant ainsi à la qualité du document que vous avez sous les yeux : Simon Arsenault, Michael Audet, Abdoul Aziz A. LOM, Vincent Blais, Charles-Alexandre Cantin, Éric Chamberland, Pier-Luc Cormier-Maltais, Sylvain Fillion, Olivier Garant, Jean Bruno Jauvin, Charles Joly Beauparlant, Patrick Landry, Alexandre Laroche, Benjamin Lemelin, Christian Martin, Olivier Petit, Karim Sghari, Sandra Sirois et Joel Trottier-Hébert.

Finalement, les commentaires et corrections des auxiliaires d'enseignement Jean-Francis Roy, Gildas Syla Déogratias Kouko et Catherine Bédard furent aussi d'une aide considérable.

Table des matières

Chapitre 0

Un peu de motivation

> Computer science is no more about computers than astronomy is about telescopes.
>
> Edsger W. Dijkstra (1930 – 2002)

À l'époque où vous entreprenez un programme d'études en informatique, il serait superflu de commencer ce cours en faisant l'éloge de l'utilité de l'informatique, tellement l'usage des ordinateurs est désormais répandu dans toutes les sphères de l'activité humaine. Cependant, il nous parait important d'expliquer que les mathématiques sont d'une utilité cruciale pour quelqu'un qui s'intéresse à l'informatique en tant que science. En effet, il subsiste chez plusieurs étudiants l'impression que l'informatique et les mathématiques sont deux domaines d'études indépendants, et qu'il n'est pas nécessaire de posséder des connaissances mathématiques pour être un bon informaticien [1]. Cela s'explique possiblement par le fait que la plupart des utilisations que nous faisons d'un ordinateur ne requièrent pas, ou peu, de connaissances mathématiques. En effet, tant que nous utilisons des programmes créés par d'autres (que ce soit des outils destinés à tous, tels les traitements de textes, ou des outils plus spécialisés, telles les librairies hauts niveaux de certains langages de programmation), les connaissances mathématiques sont souvent facultatives. Cela dit, quiconque s'intéresse à comprendre le fonctionnement de l'ordinateur, à analyser le comportement des algorithmes ou à concevoir des programmes pour résoudre des nouvelles tâches a besoin d'outils pour guider son raisonnement logique. Les prochains paragraphes ont comme ambition de vous convaincre que, dans chacune de ces circonstances, les mathématiques s'imposent comme la "boîte à outils" de prédilection.

1. Curieusement, il n'existe pas de telles remises en question dans les diverses branches de l'ingénierie.

Les mathématiques et les fondements de l'informatique

Les ordinateurs sont, d'abord et avant tout, des calculatrices très sophistiquées. Les premiers ordinateurs ont d'ailleurs été imaginés par des mathématiciens désireux d'automatiser leurs calculs. De même, le langage binaire à la base des ordinateurs est issu de la logique booléenne, que nous présenterons dès le début du premier chapitre. Le langage mathématique fut donc à la base du développement de l'informatique.

Les mathématiques ne sont donc pas qu'un *outil* en informatique. Bien sûr, les mathématiques se retrouvent dans toutes les branches de la conception d'outils par les humains (toutes les branches du génie, en particulier). Elles fournissent la plupart du temps un langage et des règles de manipulation des données qui sont des *approximations* du langage et des règles de la nature. On étudie le mouvement d'un objet à l'aide d'une fonction mathématique, mais pour cela, on suppose souvent l'absence de friction. Les exemples sont nombreux : en économie, on dessine une courbe d'offre et de la demande en utilisant une fonction continue même si une foule de valeurs n'ont pas de sens dans cette fonction. L'approximation est nécessaire, on ne peut faire mieux sans compliquer trop les choses (ou on ne peut faire mieux, point). Pour l'informatique, c'est différent. L'informatique est née des mathématiques, les programmes sont des langages entièrement créés par l'Homme, ils *sont* mathématiques ! Quand on "utilise" des outils mathématiques pour raisonner sur un programme informatique, on utilise le même langage ! L'informatique est une *application exacte* des mathématiques, et peut-être la seule à être vraiment exacte !

Les mathématiques et l'analyse d'algorithmes

Dans certaines circonstances, peu de connaissances mathématiques sont requises pour concevoir un programme informatique. Par exemple, les actions de trier un tableau de nombres, accéder à une base de données, appliquer un filtre à une image, compresser un vidéo ou crypter un texte font appel à des techniques déjà existantes. Un programmeur peut implémenter ces techniques sans trop se creuser la tête. Parfois, il peut aussi trouver une stratégie pour accomplir la tâche désirée sans nécessairement réfléchir dans un formalisme mathématique.

Cependant, un informaticien sérieux souhaitera analyser le comportement de son nouveau programme, pour répondre à l'une ou l'autre des questions suivantes :

— Est-ce que le temps d'exécution requis par mon programme est raisonnable, même quand le nombre de données à traiter est très grand ?

— Quel est l'espace mémoire requis par mon programme ?

— Puis-je fournir la garantie que mon programme accomplira la tâche demandée dans tous les cas ?
— Est-ce que mon programme comporte des failles de sécurité ?

Dépendamment du contexte, il est très difficile d'obtenir des réponses complètes à ces questions. Plusieurs domaines de recherche en informatique étudient des méthodes pour analyser les algorithmes [2]. On peut présumer que s'il y a, encore de nos jours, autant de failles dans les logiciels, c'est en partie parce que ces méthodes ne sont pas encore assez évoluées pour bénéficier de toute la logique et de la rigueur des mathématiques.

Le deuxième chapitre de ce cours donne un avant-goût de l'analyse d'algorithmes en introduisant les outils de base qui permettront d'évaluer le temps d'exécution d'un algorithme.

Les mathématiques et la conception d'algorithmes

L'informatique étant une science relativement jeune, il existe encore beaucoup de problèmes à résoudre reliés à une grande variété de domaines différents : l'intelligence artificielle, la vision numérique, la création d'horaires, les prévisions économiques, la simulation des systèmes climatiques, l'assemblage de génomes, la compréhension du langage naturel, la vérification automatique de logiciels, etc.

Tous ces problèmes complexes nécessitent d'être formulés rigoureusement avant de pouvoir être résolus à l'aide d'un programme informatique. La plupart du temps, ce sont les mathématiques qui se révèlent le langage approprié pour formuler ces problèmes. Une fois le problème bien formulé, on peut profiter des théories mathématiques déjà existantes pour mieux le comprendre, pour le simplifier ou pour trouver des pistes de solutions possibles [3].

Cette approche est mise en évidence dans le troisième chapitre de ces notes de cours, dédié à la théorie des graphes. En effet, un graphe est une structure mathématique simple qui a été abondamment étudiée. Dans plusieurs cas, il suffit d'exprimer un problème comme un graphe pour avoir accès à plusieurs algorithmes efficaces pour le résoudre.

2. Bien que nous n'irons pas si loin dans le cours, la branche de la recherche nommée la "théorie de la complexité" s'intéresse à des questions encore plus "fondamentales", telles :
– Étant donné un problème, est-ce qu'il existe un algorithme capable de le résoudre en temps raisonnable ?
– Si je trouve un algorithme efficace pour résoudre le problème A, est-ce que ça me permet de résoudre le problème B efficacement ? (Même si les problèmes A et B sont en apparence de natures très différentes.)

3. Ainsi, les équipes de recherche des universités et des compagnies qui travaillent à l'informatique du futur se servent des mathématiques tous les jours. Il suffit de citer l'exemple de compagnies comme *Google* ou *Amazon*, qui bâtissent leur empire grâce à idées novatrices développées notamment à l'aide des outils qu'offrent les mathématiques.

Ce qu'il faut retenir de ce cours

Le cours sera l'occasion d'introduire plusieurs concepts mathématiques et, bien sûr, vous serez évalués sur la maîtrise des différentes notions. Cependant, la compréhension sera toujours privilégiée plutôt que le "par coeur". Comme plusieurs notions abordées ici serviront lors d'autres cours du programme, ces notes de cours pourront aussi servir de référence ultérieure.

Tout le long du cours, nous accorderons une grande importance aux démonstrations mathématiques ; c'est l'un des objectifs du cours. Il s'agit d'un concept qui n'est pas aussi simple qu'on peut le croire au départ. L'écriture d'une démonstration mathématique requiert beaucoup de rigueur, et souvent une certaine créativité. De même, il faut lire et écrire plusieurs démonstrations pour bien en comprendre l'esprit. Les étudiants qui poursuivront leurs études aux cycles supérieurs seront appelés à lire et rédiger des démonstrations lors de leurs travaux de recherche. Cela dit, l'accent mis sur les démonstrations mathématiques ne sera pas seulement utile aux étudiants qui poursuivront une carrière en recherche, mais permettra à tous d'exercer leur raisonnement et leur capacité de déduction face à certains problèmes demandant une dose de réflexion.

Chapitre 1

Théorie des ensembles

C'est à travers la théorie des ensembles que nous introduirons les différentes techniques de démonstration qui devront être maîtrisées dans ce cours. Nous faisons d'une pierre deux coups : pour apprendre comment démontrer, il faut des propositions à démontrer, ce qui est l'occasion d'introduire un sujet, la théorie des ensembles. À la section 1.2, nous introduirons des définitions sur la théorie des ensembles et ensuite des propriétés associées, que nous démontrerons à l'aide de techniques de démonstration. Nous appliquerons ces techniques (et une nouvelle) par la suite dans les chapitres suivants.

C'est Aristote (-384 – -322) qui a développé l'art de la démonstration. Son exemple célèbre est le suivant :

> Tous les hommes sont mortels
> Or Socrate est un homme
> Donc Socrate est mortel

Cette conclusion, appelée syllogisme, nous est naturelle, et toute technique de démonstration s'appuie sur un tel raisonnement naturel. Toutefois, quand de nombreux arguments sont nécessaires pour arriver à une conclusion correcte, il est facile de s'embourber si on n'utilise pas une technique rigoureuse. Le but de ce cours est de vous donner des habitudes et techniques de démonstration qui vous aideront à "garder le fil" !

Voici un autre exemple de syllogisme :

> Quand il pleut sur le campus, Xavier a toujours son parapluie sur lui
> Je constate qu'il pleut sur le campus
> Donc Xavier a son parapluie aujourd'hui.

Par ce raisonnement, on a réussi à *extraire* une information, "Xavier a son parapluie aujourd'hui", à partir de l'affirmation de la première ligne. Par contre, si on rencontre Xavier avec un parapluie à la main, peut-on conclure qu'il pleut ?

1.1 Algèbre booléenne

Pour débuter, nous introduisons un langage qui nous permettra d'écrire de façon concise et sans ambiguïté les définitions et affirmations qui nous intéresseront. Nous introduisons donc les bases de la *logique booléenne*, nommée en l'honneur du mathématicien et philosophe britannique George Boole (1815 – 1864), qui souhaitait développer un formalisme pour traduire des concepts et des pensées en équations. Comme nous le verrons, ce paradigme est très près du langage binaire utilisé en électronique et en informatique.

1.1.1 Expressions booléennes

Une **expression booléenne** correspond à un regroupement d'affirmations. On désigne par le terme **expression booléenne atomique** une expression booléenne contenant une seule affirmation. Une affirmation est une phrase, généralement de la forme "sujet-verbe-complément", à laquelle il est possible d'attribuer une **valeur de vérité**. Autrement dit, il est possible de déterminer si l'affirmation est vraie ou fausse. Par exemple, les quatre affirmations suivantes peuvent être considérées comme des expressions booléennes atomiques :

— *Manille est la capitale des Philippines.*
— *Cinq est un nombre impair.*
— *La distance entre la terre et la lune est inférieure à trois kilomètres.*
— *Dix est plus petit que sept.*

Les deux premières affirmations sont vraies tandis que les deux dernières sont fausses.

On peut aussi exprimer des expressions booléennes par des formules mathématiques. Par exemple :

— $5 + 5 + 5 = 3 \cdot 5$.
— $10 < 7$.

Dans ce dernier exemple, la première expression est toujours vraie et la deuxième est toujours fausse. Remarquons que ces deux expressions mathématiques correspondent aussi à des phrases de la forme "sujet-verbe-complément". Pour la première expression, le membre de gauche fait office de sujet, "=" est le verbe et le membre de droite est le complément. Similairement, pour la deuxième expression, on a que "10" est le sujet de la phrase, "est plus petit que" représente le groupe verbe et "7" le complément". Notez également qu'on peut réécrire ces expressions sous forme d'un texte français : "*Cinq plus cinq plus cinq égale trois fois cinq.*" et "*Dix est plus petit que sept.*".

Certaines expressions booléennes changent de valeur de vérité dépendamment du contexte dans lequel elles sont évaluées. Par exemple :

— *La capitale de ma province est la ville de Québec.*
— $x < 7$.

La valeur de la première expression dépend de la province identifiée par les termes "ma province". De même, la deuxième expression dépend de la valeur de la variable x. Si aucune valeur n'est attribuée à la variable x, on dit qu'il s'agit d'une **variable libre**, auquel cas il est impossible d'assigner une valeur de vérité à l'expression "$x < 7$". Cependant, pour chaque valeur de x possible, on peut assigner une valeur de vérité à l'expression. Ainsi, l'expression est fausse si $x \geq 7$, sinon elle est vraie.

Nous nous intéressons maintenant à la combinaison d'expressions booléennes atomiques en expressions booléennes plus complexes. Nous effectuons de telles combinaisons dans nos conversations de tous les jours, notamment à l'aide des mots "et", "ou" et "si-alors". Par exemple :

— *J'habite à Chicoutimi* et *la capitale de ma province est la ville de Québec.*
— Si *j'habite à Chicoutimi,* alors *la capitale de ma province est la ville de Québec.*
— *Mon prénom contient la lettre P* ou *mon prénom contient la lettre S.*

Pour vérifier la véracité de ces expressions booléennes, il suffit d'évaluer séparément la véracité de chacune des expressions booléennes atomiques les constituant. Ainsi, dans le cas du premier exemple, nous évaluons d'abord la véracité de l'expression "*J'habite à Chicoutimi.*", puis nous évaluons ensuite la véracité de l'expression "*La capitale de ma province est la ville de Québec.*". Nous pouvons enfin juger de la véracité de l'expression booléenne dans son entier en combinant les valeurs des deux expressions atomiques. Nous procéderons de façon similaire pour évaluer la valeur de toute expression booléenne. Cette méthodologie permet de mécaniser l'évaluation d'expressions booléennes complexes.

1.1.2 Opérateurs booléens et tables de vérité

L'**algèbre booléenne** est le domaine qui permet de combiner plusieurs expressions booléennes atomiques pour former des expressions booléennes plus complexes. Cela est possible grâce aux **opérateurs booléens**. Les pages qui suivent présentent les cinq opérateurs booléens qui sont utilisés dans ce cours, c'est-à-dire la négation "$\neg$", la conjonction "$\wedge$", la disjonction "$\vee$", l'implication "$\Rightarrow$" et le si et seulement si "$\Leftrightarrow$". Ces opérateurs sont définis en représentant les expressions booléennes par des **variables booléennes** qui prennent la

valeur `vrai` ou `faux`. De manière équivalente, on choisit parfois de représenter la valeur `vrai` par la lettre `v` ou le chiffre 1, ainsi que la valeur `faux` par la lettre `f` ou le chiffre 0.

Les trois opérateurs booléens de base

Afin de définir les trois premiers opérateurs booléens, nous avons recours à des **tables de vérité**, qui associent à chaque combinaison de valeurs booléennes le résultat de l'évaluation de l'expression formée par l'opérateur. La définition 1.1.1 présente les opérateurs suivants :

— L'opérateur de **négation** "¬", correspondant au "non" du français ;
— L'opérateur de **conjonction** "∧", correspondant au "et" du français ;
— L'opérateur de **disjonction** "∨", correspondant au "ou" du français.

Définition 1.1.1. *Définitions des trois opérateurs booléens de base.*
Soit p et q des expressions booléennes. Pour chaque combinaison de valeurs de vérité possibles, les tables de vérité ci-dessous indiquent le résultat de l'évaluation de la négation, de la conjonction et de la disjonction.

Négation :

p	$\neg p$
v	f
f	v

Conjonction :

p	q	$p \wedge q$
v	v	v
v	f	f
f	v	f
f	f	f

Disjonction :

p	q	$p \vee q$
v	v	v
v	f	v
f	v	v
f	f	f

Une table de vérité se lit une ligne à la fois ; la première ligne nomme les variables et l'expression (ou les expressions) à évaluer et les autres lignes énumèrent les différents cas. Par exemple, pour la conjonction, la ligne en rouge signifie : si p est vrai et q est faux, alors l'expression que l'on note $p \wedge q$ est fausse.

L'opérateur d'implication

Nous avons défini les trois premiers opérateurs booléens (la négation "¬", la conjonction "∧" et la disjonction "∨") en présentant leur table de vérité. La logique booléenne repose entièrement sur ces trois premiers opérateurs, puisqu'ils permettent de définir les deux derniers opérateurs booléens que nous utiliserons [1]. Bien entendu, il est possible de déduire

1. En fait, grâce à la loi de De Morgan (Proposition 1.1.4), on n'aurait qu'à définir la conjonction "∧" et la négation "¬", car la disjonction "∨" peut être définie comme "$p \vee q \Leftrightarrow \neg(\neg p \wedge \neg q)$".

les tables de vérité de ces deux derniers opérateurs à partir de leur définition.

Introduisons d'abord les opérateurs d'**implication** "$\Rightarrow$" (le plus utilisé) et d'**implication inverse** "$\Leftarrow$". Dans ce document, nous utilisons le symbole de **définition** "$\stackrel{\text{def}}{=}$" pour spécifier qu'une expression mathématique est définie grâce à une autre expression.

Définition 1.1.2. *Définition de l'opérateur d'implication*
Soit p et q des expressions booléennes, alors :

$$p \Rightarrow q \stackrel{\text{def}}{=} \neg p \vee q\,.$$

Spécifions que l'expression "$p \Rightarrow q$" se traduit en français par "p implique q" ou "si p alors q". Parfois, nous utilisons le symbole "$\Leftarrow$" pour désigner l'implication inverse :

$$p \Leftarrow q \stackrel{\text{def}}{=} q \Rightarrow p\,.$$

Les tables de vérité suivantes sont obtenues par l'application directe de la définition 1.1.2.

Implication :

p	q	$p \Rightarrow q$
v	v	v
v	f	f
f	v	v
f	f	v

Implication inverse :

p	q	$p \Leftarrow q$
v	v	v
v	f	v
f	v	f
f	f	v

PENSEZ-Y!

L'expression "$p \Rightarrow q$" est évaluée à `faux` seulement lorsque $p =$ `vrai` et $q =$ `faux`. Ce fait peut être difficile à accepter au premier abord, mais il est important de bien le comprendre.

Pour illustrer ce fait, considérez l'expression suivante :

— *"Si le Père Noël existe, alors je recevrai un Nintendo en cadeau."*

On peut réécrire cette expression à l'aide de l'opérateur d'implication :

— *"Le Père Noël existe."* $\Rightarrow$ *"Je recevrai un Nintendo en cadeau."*

Par la définition 1.1.2, ceci est équivalent à l'expression suivante :

— $\neg$(*"Le Père Noël existe."*) $\vee$ *"Je recevrai un Nintendo en cadeau."*

On constate que cette expression est fausse si et seulement si le Père Noël existe et que je ne reçois pas de Nintendo en cadeau. Aussi, le fait que le Père Noël n'existe pas n'exclut pas la possibilité que je reçoive un Nintendo en cadeau !

Les enfants comprennent bien ce raisonnement logique lorsqu'ils remettent en question la parole d'un compère en prononçant une expression telle que :

— *"Si tu es capable de traverser le fleuve à la nage, alors moi je suis le Pape !"*

Ici, il est clair que, puisque "je" n'est pas le Pape, la seule manière que l'affirmation soit vraie est que "tu" ne soit pas capable de traverser le fleuve à la nage.

L'opérateur "si et seulement si"

Nous présentons finalement l'opérateur **si et seulement si** "$\Leftrightarrow$", qui est défini par la conjonction de deux implications.

Définition 1.1.3. *Définition de l'opérateur si et seulement si.*
Soit p et q des expressions booléennes, alors :

$$p \Leftrightarrow q \stackrel{\text{def}}{=} (p \Rightarrow q) \wedge (q \Rightarrow p) \qquad \textit{(Définition du si et seulement si)}$$

Notez que l'expression "$(p \Rightarrow q) \wedge (p \Leftarrow q)$" serait une définition équivalente du si et seulement si. L'expression "$p \Leftrightarrow q$" se dit "p si et seulement si q" et s'écrit de manière abrégée "p ssi q".

La table de vérité suivante est obtenue par l'application directe de la définition 1.1.3.

Si et seulement si :

p	q	$p \Leftrightarrow q$
v	v	v
v	f	f
f	v	f
f	f	v

On constate que l'expression "$p \Leftrightarrow q$" est vraie lorsque les variables p et q sont égales (c'est-à-dire qu'elles possèdent la même valeur de vérité). De même, l'expression "$p \Leftrightarrow q$" est fausse lorsque les variables p et q sont différentes. L'opérateur si et seulement si "$\Leftrightarrow$" permet

donc d'exprimer la notion d'équivalence entre deux expressions booléennes. C'est pourquoi cet opérateur apparaît fréquemment dans les propriétés présentées à la section 1.1.3.

Évaluation d'une expression booléenne

On évalue une expression booléenne de manière similaire à la plupart des expressions arithmétiques communes. Ainsi, il faut d'abord donner priorité aux expressions entre parenthèses. Ensuite, on évalue l'expression selon l'ordre de priorité des opérateurs.

La table 1.1 présente la **priorité des opérateurs booléens** lors de l'évaluation d'une expression booléenne. On évalue les opérateurs dans l'ordre décroissant de leur priorité.

TABLE 1.1 – Priorité des opérateurs booléens.

Symbole(s)	Nom(s)	
$\neg$	Négation	*(priorité élevée)*
$\wedge$ $\vee$	Conjonction, Disjonction	
$\Rightarrow$	Implication	
$\Leftrightarrow$	Si et seulement si	*(priorité faible)*

Grâce à cette convention, l'expression "$p \wedge \neg q \Leftrightarrow r$" équivaut à l'expression "$(p \wedge (\neg q)) \Leftrightarrow r$". Si on pose les valeurs $p :=$ `vrai` et $q := r :=$ `faux`, on évalue l'expression selon la séquence suivante :

1. $p \wedge \neg q \Leftrightarrow r$;
2. `vrai` $\wedge \neg$`faux` $\Leftrightarrow$ `faux` ;
3. `vrai` $\wedge$ `vrai` $\Leftrightarrow$ `faux` ;
4. `vrai` $\Leftrightarrow$ `faux` ;
5. `faux` .

Nous avons utilisé la notation := pour attribuer des valeurs à p, q, et r. C'est une notation fréquente dans les langages de programmation, elle signifie que l'on attribue une certaine valeur à une variable. On réserve la plupart du temps (mais pas toujours) le symbole "=" pour faire une affirmation (comme $x + x = 2x$) qui peut être vraie ou fausse [2].

En guise de récapitulation, la table de vérité 1.2 présente la synthèse des six opérateurs booléens que nous utiliserons dans le cours.

Vous devez apprendre ces tables par coeur. En fait, il faut surtout mémoriser la signification des symboles $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$ le plus vite possible et les tables se déduiront facilement,

2. Notons que c'est la principale différence entre le raisonnement mathématique classique et le raisonnement mathématique nécessaire à l'informatique ! Dans les problèmes habituels de mathématique classique, plutôt que faire *évoluer* les variables au cours d'un raisonnement, on choisit une *nouvelle* variable...

TABLE 1.2 – Table de vérité présentant une synthèse des opérateurs booléens utiles dans ce cours.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftarrow q$	$p \Leftrightarrow q$
v	v	f	v	v	v	v	v
v	f		f	v	f	v	f
f	v	v	f	v	v	f	f
f	f		f	f	v	v	v

car tout ça est très *logique*. Seul l'opérateur $\Rightarrow$ demande un peu plus de réflexion.

De la logique booléenne à l'informatique

La logique booléenne présentée dans cette première section sera un outil essentiel tout au long du cours, particulièrement lors des démonstrations mathématiques. Bien que cette forme de logique peut paraître simpliste à première vue, étant donné qu'une expression booléenne peut prendre seulement deux valeurs de vérité (`vrai` ou `faux`), elle est à la base de l'informatique telle que nous la connaissons. En effet, les circuits électroniques de nos ordinateurs sont des agencements savants de "portes logiques" qui sont la matérialisation de nos trois opérateurs booléens de base, c'est-à-dire la conjonction "$\wedge$", la disjonction "$\vee$" et la négation "$\neg$". De même, le langage binaire utilisé par un ordinateur n'est qu'une succession de 0 et de 1, c'est-à-dire de valeurs booléennes !

1.1.3 Propriétés des opérateurs et démonstrations par cas

Maintenant que nous avons défini les six opérateurs booléens, nous allons énoncer quelques-unes de leurs propriétés de base. À l'aide de ces propriétés, il sera possible de transformer des expressions booléennes complexes en des expressions équivalentes. Ce sera des outils essentiels pour effectuer plusieurs démonstrations mathématiques.

En plus de présenter certaines propriétés des opérateurs booléens, cette section introduit une première technique de démonstration, qui consiste à vérifier qu'une expression booléenne est vraie dans tous les cas possibles.

Lois de De Morgan

Les premières propriétés que nous présentons permettent de transformer une conjonction d'expressions booléennes en disjonction d'expressions booléennes (et vice-versa). Il s'agit des

lois de De Morgan, nommées en l'honneur du mathématicien britannique Auguste De Morgan (1806 – 1871).

Dans l'énoncé des propositions, nous utilisons fréquemment l'opérateur **si et seulement si** "⇔" pour signifier que deux expressions sont équivalentes. Notez que, même s'il s'agit du même opérateur booléen présenté par la définition 1.1.3 (page 10), nous lui attribuons ici une signification particulière, puisqu'il sert à exprimer que deux expressions ont *toujours* la même valeur de vérité.

Proposition 1.1.4. *Lois de De Morgan.*
Soit p et q des expressions booléennes, alors les expressions suivantes sont vraies :

a :	$\neg(p \wedge q)$	$\Leftrightarrow$	$\neg p \vee \neg q$	*(Première loi de De Morgan)*
b :	$\neg(p \vee q)$	$\Leftrightarrow$	$\neg p \wedge \neg q$	*(Deuxième loi de De Morgan)*

En mathématiques (comme dans la vie !), une bonne pratique est de confronter chaque nouvel énoncé à son propre sens de la logique. Cela permet de mieux comprendre la signification de cet énoncé et de juger s'il est plausible[3]. Dans le cas qui nous intéresse, les lois de De Morgan sont habituellement bien comprises intuitivement. Par exemple, nous pouvons appliquer ces lois à des expressions formulées sous forme de phrases :

— Exemple illustrant la proposition 1.1.4-a (Première loi de De Morgan).
Les deux expressions suivantes sont équivalentes :
  ◦ *"Il n'est pas vrai que Paul a payé son loyer et son compte d'électricité."*
  ◦ *"Paul n'a pas payé son loyer ou il n'a pas payé son compte d'électricité."*

— Exemple illustrant la proposition 1.1.4-b (Deuxième loi de De Morgan).
Les deux expressions suivantes sont équivalentes :
  ◦ *"Il n'est pas vrai que Paul a voyagé en Italie ou en Suisse."*
  ◦ *"Paul n'a pas voyagé en Italie et Paul n'a pas voyagé en Suisse."*

Même si ces exemples d'énoncés semblent suggérer que les lois de De Morgan sont cohérentes, ils ne nous assurent pas qu'elles sont valides dans *tous* les cas. Afin de se convaincre de la véracité d'un énoncé mathématique, il faut en faire la démonstration. Ainsi, nous allons démontrer la première loi de De Morgan en utilisant le seul outil présentement à notre disposition, c'est-à-dire la table de vérité.

Une **démonstration par table de vérité** est une façon structurée de faire une **démonstration par cas**[4]. Nous évaluons donc la proposition 1.1.4-a pour toutes les combinaisons

3. Mais attention, car certaines vérités sont contre-intuitives, et ce n'est pas parce qu'un énoncé semble invraisemblable qu'il est nécessairement faux (dans les mathématiques comme dans la vie !).
4. Nous reviendrons sur le principe général d'une démonstration par cas à la section 1.3.7.

de valeurs de vérité possibles que peuvent prendre les expressions booléennes p et q. Il y a quatre possibilités, c'est-à-dire : $p = \texttt{v}$ et $q = \texttt{v}$, $p = \texttt{v}$ et $q = \texttt{f}$, $p = \texttt{f}$ et $q = \texttt{v}$, $p = \texttt{f}$ et $q = \texttt{f}$ (notez que ces 4 cas sont énumérés dans les deux premières colonnes de la table présentée dans la démonstration de la proposition 1.1.4-a ci-bas).

À la fin de la démonstration, l'acronyme "**C.Q.F.D.**" signifie "Ce qu'il fallait démontrer", et indique au lecteur que nous avons complété la démonstration avec succès.

Démonstration de la première loi de De Morgan. (Proposition 1.1.4-a)
Soit p et q deux expressions booléennes. Démontrons "$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$" à l'aide d'une table de vérité :

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$(\neg p \vee \neg q)$	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$
v	v	v	f	f	f	f	v
v	f	f	v	f	v	v	v
f	v	f	v	v	f	v	v
f	f	f	v	v	v	v	v

Les colonnes 3 à 7 sont des calculs intermédiaires qui nous permettent de conclure à la 8e colonne. Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$" est toujours vraie.

C.Q.F.D.

Notez que nous avons vraiment fait **C**e **Q**u'il **F**allait faire pour **D**émontrer la véracité de l'énoncé, car nous avons démontré que la première loi de De Morgan est vraie dans tous les cas. Le lecteur est invité à démontrer la deuxième loi de De Morgan par la même technique.

Propriétés de la négation, de la conjonction et de la disjonction

Les propositions 1.1.5, 1.1.6 et 1.1.7 introduisent quelques équivalences constituées de négations, de conjonctions et de disjonction. Ces propriétés se révéleront utiles lors de plusieurs démonstrations.

Proposition 1.1.5. *Propriétés de la négation.*
Soit p une expression booléenne, alors :

a :	$\neg(\neg p)$	$\Leftrightarrow p$	*(Double négation)*
b :	$p \vee \neg p$	$\Leftrightarrow$ vrai	*(Tiers exclu)*
c :	$p \wedge \neg p$	$\Leftrightarrow$ faux	*(Contradiction)*

Proposition 1.1.6. *Propriétés de la conjonction.*
Soit p, q et r des expressions booléennes, alors :

`a :`	$p \wedge$ `vrai`	$\Leftrightarrow$	p	*(Élément neutre)*
`b :`	$p \wedge$ `faux`	$\Leftrightarrow$	`faux`	*(Élément absorbant)*
`c :`	$p \wedge p$	$\Leftrightarrow$	p	*(Idempotence)*
`d :`	$p \wedge q$	$\Leftrightarrow$	$q \wedge p$	*(Commutativité)*
`e :`	$(p \wedge q) \wedge r$	$\Leftrightarrow$	$p \wedge (q \wedge r)$	*(Associativité)*
`f :`	$(p \vee q) \wedge r$	$\Leftrightarrow$	$(p \wedge r) \vee (q \wedge r)$	*(Distributivité)*

Proposition 1.1.7. *Propriétés de la disjonction.*
Soit p, q et r des expressions booléennes, alors :

`a :`	$p \vee$ `faux`	$\Leftrightarrow$	p	*(Élément neutre)*
`b :`	$p \vee$ `vrai`	$\Leftrightarrow$	`vrai`	*(Élément absorbant)*
`c :`	$p \vee p$	$\Leftrightarrow$	p	*(Idempotence)*
`d :`	$p \vee q$	$\Leftrightarrow$	$q \vee p$	*(Commutativité)*
`e :`	$(p \vee q) \vee r$	$\Leftrightarrow$	$p \vee (q \vee r)$	*(Associativité)*
`f :`	$(p \wedge q) \vee r$	$\Leftrightarrow$	$(p \vee r) \wedge (q \vee r)$	*(Distributivité)*

L'énoncé `b :` contient une redondance. Il aurait pu se lire $p \vee$ `vrai` tout simplement. Comme la Proposition 1.1.7 peut être démontrée comme vraie, il est toujours vrai.

Essayons de confronter notre propre sens logique aux énoncés de quelques une de ces propriétés. Par exemple :

— Exemple illustrant la proposition 1.1.5-b (Tiers exclu).
L'expression suivante est toujours vraie[5] :
  ◦ *"La porte est ouverte ou fermée."*

— Exemple illustrant la proposition 1.1.6-d (Commutativité de la conjonction).
Les deux expressions suivantes sont équivalentes :
  ◦ *"J'habite à Chicoutimi et la capitale de ma province est la ville de Québec."*
  ◦ *"La capitale de ma province est la ville de Québec et j'habite à Chicoutimi."*

5. Le lecteur peut objecter qu'une porte peut être entrouverte (ou presque fermée). Ce scénario est difficile à modéliser en logique booléenne, parce que cette dernière ne considère que deux valeurs de vérité, soit le vrai et le faux. Toutefois, il existe d'autres paradigmes en mathématiques qui permettent d'exprimer davantage. C'est le cas de la "logique floue" ou de la logique modale, par exemple. La logique modale est particulièrement intéressante en informatique (en fait, plus particulièrement en sécurité et en analyse de programmes), car elle permet de modéliser des concepts comme "dans le futur" ou "il est possible que", etc. Mais ceci est une autre histoire que vous aurez l'occasion de voir durant vos études d'informatique.

— Exemple illustrant la proposition 1.1.7-f (Distributivité de la disjonction).
On peut écrire les conditions d'admissibilité à un programme d'études des deux manières équivalentes suivantes :
  - *"Pour être admis, l'étudiant doit satisfaire l'un ou l'autre des deux critères ci-bas :*
    i. *Détenir un DEC et réussir un examen de français ;*
    ii. *Être âgé de plus de 21 ans."*
  - *"Pour être admis, l'étudiant doit satisfaire à la fois les deux critères ci-bas :*
    i. *Détenir un DEC ou être âgé de plus de 21 ans ;*
    ii. *Réussir un examen de français ou être âgé de plus de 21 ans."*

Le lecteur suspicieux est encouragé à démontrer les autres énoncés des propositions 1.1.5, 1.1.6 et 1.1.7 par la méthode de démonstration par table de vérité.

En guise d'exemple, démontrons la distributivité de la conjonction à l'aide de cette méthode. Il s'agit de vérifier que les valeurs de vérité des expressions "$(p \vee q) \wedge r$" et "$(p \wedge r) \vee (q \wedge r)$" sont égales pour chaque combinaison possible de valeurs pour les variables p, q et r. Il y a $2^3 = 8$ combinaisons possibles, car il y a 2 valeurs possibles pour chacune des 3 variables.

Démonstration de la distributivité de la conjonction. (Proposition 1.1.6-f)
Soit p, q et r trois expressions booléennes. Démontrons "$(p \vee q) \wedge r \;\Leftrightarrow\; (p \wedge r) \vee (q \wedge r)$" à l'aide d'une table de vérité :

p	q	r	$p \vee q$	$(p \vee q) \wedge r$	$p \wedge r$	$q \wedge r$	$(p \wedge r) \vee (q \wedge r)$	Prop. 1.1.6-f
v	v	v	v	v	v	v	v	v
v	v	f	v	f	f	f	f	v
v	f	v	v	v	v	f	v	v
v	f	f	v	f	f	f	f	v
f	v	v	v	v	f	v	v	v
f	v	f	v	f	f	f	f	v
f	f	v	f	f	f	f	f	v
f	f	f	f	f	f	f	f	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p, q et r, la proposition est vraie.

C.Q.F.D.

Transitivité du "si et seulement si"

La proposition 1.1.8 ci-dessous jouera un rôle fondamental dans la technique de démonstration par successions d'équivalences présentée à la section 1.1.4 (page 19). Il est intéressant de remarquer la similitude entre la transitivité de l'opérateur booléen si et seulement si "$\Leftrightarrow$" et la transitivité de l'opérateur arithmétique d'égalité "$=$". En effet, si x, y et z sont des nombres, $x = y$ et $y = z$ implique $x = z$.

Proposition 1.1.8. *Transitivité de l'opérateur "si et seulement si".*
Soit p, q et r des expressions booléennes, alors :

$$(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \quad \Rightarrow \quad (p \Leftrightarrow r)$$

Démontrons maintenant la proposition par une table de vérité. Contrairement aux démonstrations précédentes, nous devons démontrer une proposition de la forme "$a \Rightarrow b$" plutôt qu'une proposition de la forme "$a \Leftrightarrow b$". Rappelons qu'une expression de la forme "$a \Rightarrow b$" est vraie ssi l'expression b est vraie lorsque l'expression a est vraie (il n'est pas nécessaire que b soit vraie si a est faux).

Démonstration de la transitivité du "si et seulement si". (Proposition 1.1.8)
Soit p, q et r des expressions booléennes. Pour démontrer "$(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \ \Rightarrow \ (p \Leftrightarrow r)$", nous vérifions à l'aide d'une table de vérité qu'elle est vraie pour toutes les valeurs de vérité de p et q.

p	q	r	$p \Leftrightarrow q$	$q \Leftrightarrow r$	$(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)$	$p \Leftrightarrow r$	Prop. 1.1.8
v	v	v	v	v	v	v	v
v	v	f	v	f	f	f	v
v	f	v	f	f	f	v	v
v	f	f	f	v	f	f	v
f	v	v	f	v	f	f	v
f	v	f	f	f	f	v	v
f	f	v	v	f	f	f	v
f	f	f	v	v	v	v	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p, q et r, l'expression "$(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \Rightarrow (p \Leftrightarrow r)$" est toujours vraie.

C.Q.F.D.

Contraposition

La proposition 1.1.9 présente la propriété de **contraposition**, sur laquelle repose la technique de démonstration par contraposition. Nous y reviendrons dans la section 1.3.9.

Nous présentons ici une démonstration par table de vérité de la propriété de contraposition. À la prochaine section, nous allons présenter une autre démonstration possible de la même propriété, qui repose sur une nouvelle technique de démonstration que nous appellerons "démonstration par succession d'équivalences".

Proposition 1.1.9. *Contraposition.*
Soit p et q des expressions booléennes, alors :

$$p \Rightarrow q \quad \Leftrightarrow \quad \neg q \Rightarrow \neg p$$

Démonstration de la contraposition. (Proposition 1.1.9)
Soit p et q deux expressions booléennes.

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$	Prop. 1.1.9
v	v	v	f	f	v	v
v	f	f	v	f	f	v
f	v	v	f	v	v	v
f	f	v	v	v	v	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$p \Rightarrow q \Leftrightarrow (\neg q \Rightarrow \neg p)$" est toujours vraie. **C.Q.F.D.**

PENSEZ-Y!

L'étude de la propriété de contraposition permet de mieux comprendre l'opérateur d'implication.

En posant $p :=$ *"Le Père Noël existe."* et $q :=$ *"Je recevrai un Nintendo en cadeau."*, la propriété de contraposition nous permet d'écrire :

"Si le Père Noël existe, alors je recevrai un Nintendo en cadeau."
$\Leftrightarrow$ *"Si je ne reçois pas de Nintendo en cadeau, alors le Père Noël n'existe pas".*

De la même manière, on obtient :

"Si tu es capable de traverser le fleuve à la nage, alors je suis le Pape."
$\Leftrightarrow$ *"Si je ne suis pas le Pape, alors tu n'es pas capable de traverser le fleuve à la nage."*

Affaiblissement de la conjonction et renforcement de la disjonction

Les deux prochaines propriétés sont aussi des outils très utiles pour effectuer certaines démonstrations.

Proposition 1.1.10. *Affaiblissement et renforcement.*
Soit p et q des expressions booléennes, alors :

a :	$p \wedge q$	$\Rightarrow$	p	*(Affaiblissement de la conjonction)*
b :	p	$\Rightarrow$	$p \vee q$	*(Renfoncement de la disjonction)*

Démonstration de l'affaiblissement de la conjonction. (Propriété 1.1.10-a)
Soit p et q deux expressions booléennes.

p	q	$p \wedge q$	$p \wedge q \Rightarrow p$
v	v	v	v
v	f	f	v
f	v	f	v
f	f	f	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$p \wedge q \Rightarrow p$" est toujours vraie. **C.Q.F.D.**

L'**affaiblissement de la conjonction** affirme que si l'expression "$p \wedge q$" est vraie, alors l'expression "p" est aussi vraie. Nous reviendrons sur cette propriété à la section 1.3.9. Nous laissons la démonstration du **renfoncement de la disjonction** en exercice.

1.1.4 Démonstrations par succession d'équivalences

Les démonstrations par tables de vérité présentées jusqu'à maintenant consistent à valider la véracité d'une expression booléenne en vérifiant tous les cas possibles. Cette technique peut

être très longue lorsque l'expression booléenne contient plusieurs variables[6]. Dans ce cas, il peut être préférable de démontrer l'expression booléenne en se basant sur les propriétés que nous avons déjà vérifiées. Comme les mathématiciens disent souvent, il s'agit ici d'être *intelligemment* paresseux.

Dans le cadre de ce cours, nous désignons par le terme **démonstration par succession d'équivalences** une démonstration structurée où chaque ligne est une manière équivalente d'exprimer le contenu de la ligne qui la précède[7]. Chaque passage d'une ligne à une autre sera justifié par l'application d'une définition ou d'une propriété déjà démontrée.

Ainsi, chaque nouvelle proposition peut être utilisée dans les démonstrations d'autres propositions. La démonstration d'une propriété mathématique est comparable à l'ajout d'une "brique" au "château des mathématiques". De ce point de vue métaphorique, les mathématiciens de l'Antiquité ont construit les fondations de ce château, et chaque génération de mathématiciens contribue à sa construction en posant sa brique sur celles de ses prédécesseurs...

Contraposition

Nous présentons ci-dessous une démonstration par succession d'équivalences de la propriété de contraposition (Proposition 1.1.9, page 18). Chaque passage d'une expression à l'expression suivante y correspond à l'application d'une propriété. Comme chaque propriété utilisée est démontrable par une table de vérité, la véracité de chaque étape de la démonstration est indéniable.

Démonstration de la contraposition. (Proposition 1.1.9)
Soit p et q deux expressions booléennes. Démontrons "$p \Rightarrow q \;\Leftrightarrow\; \neg q \Rightarrow \neg p$" :

$$
\begin{array}{ll}
 & p \Rightarrow q \\
\Leftrightarrow & \quad \langle \textit{ Déf 1.1.2 – Définition de l'implication } \rangle \\
 & \neg p \vee q \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.5-a – Double négation, avec } [p := q] \rangle \\
 & \neg p \vee \neg(\neg q) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.7-d – Commutativité de la disjonction, avec } [p := \neg p] \textit{ et } [q := \neg(\neg q)] \rangle \\
 & \neg(\neg q) \vee \neg p \\
\Leftrightarrow & \quad \langle \textit{ Déf 1.1.2 – Définition de l'implication, avec } [p := \neg q] \textit{ et } [q := \neg p] \rangle \\
 & \neg q \Rightarrow \neg p
\end{array}
$$

C.Q.F.D.

6. En effet, pour une expression booléenne à n variables, la table de vérité nécessite 2^n lignes !
7. Le cours *Logique et techniques de preuve* se spécialise dans ce type de démonstrations.

Dans la démonstration ci-dessus, nous avons identifié, dans un commentaire, la propriété permettant de transformer chaque expression en une expression équivalente. Nous l'avons fait de façon détaillée : lorsque les variables utilisées ne sont pas les mêmes dans la démonstration et l'énoncé d'une propriété, nous l'avons précisé à l'aide du symbole de **substitution de variable** " := ". Par exemple, le passage de l'expression "$\neg p \vee \neg(\neg q)$" à l'expression "$\neg(\neg q) \vee \neg p$" est justifié par le commentaire *"Prop 1.1.7-d – Commutativité de la disjonction, avec* $[p := \neg p]$ *et* $[q := \neg(\neg q)]$*"*, ce qui signifie que les variables p et q sont respectivement remplacées par les expressions "$\neg p$" et "$\neg(\neg q)$" dans l'énoncé de la proposition 1.1.7-d.

La première ligne de la démonstration ci-dessus ("$p \Rightarrow q$") correspond au terme de gauche de la propriété de contraposition et la dernière ligne ("$\neg q \Rightarrow \neg p$") correspond au terme de droite. En vertu de la transitivité de l'opérateur "si et seulement si" (voir la proposition 1.1.8, page 17), la série d'équivalences "$\Leftrightarrow$" à chaque ligne permet d'affirmer que le premier et le dernier terme sont équivalents (en se permettant l'abus de notation expliqué au paragraphe suivant). Comme dans les démonstrations précédentes, l'acronyme "**C.Q.F.D.**" à la fin de la démonstration indique que la démonstration est terminée.

Soulignons ici qu'on se permet un abus de notation [8] dans le formalisme utilisé lors des démonstrations par succession d'équivalences. Par exemple, une succession de trois équivalences de la forme "$A \Leftrightarrow B \Leftrightarrow C$" devrait plutôt s'écrire en isolant chaque transformation d'une expression équivalente à l'autre "$(A \Leftrightarrow B) \wedge (B \Leftrightarrow C)$", ce qui permettrait de conclure "$A \Leftrightarrow C$" (en appliquant la transitivité du "si et seulement si"). Comme cela alourdirait les démonstrations, on juge qu'il est suffisant, dans ce contexte précis, de disposer en retrait les symboles "$\Leftrightarrow$" entre les lignes équivalentes :

$$\begin{array}{rl} & A \\ \Leftrightarrow & B \\ \Leftrightarrow & C \end{array}$$

Notez qu'on fait le même type d'abus de notation lorsque, dans un calcul, on liste ligne après ligne une série d'égalités comme dans l'exemple suivant :

$$\begin{array}{rcl} (1+4)*3+7 & = & 5*3+7 \\ & = & 15+7 \\ & = & 22\,. \end{array}$$

8. En mathématiques, on *fait un abus de notation* lorsqu'on enfreint les règles que l'on s'est donné pour l'écriture des expressions. Ce faisant, on s'accorde certaines libertés pour alléger la lecture du texte. Il est important de s'assurer, lorsqu'on fait des abus de notation, que la signification des expressions demeure claire.

Réécriture de l'opérateur "si et seulement si"

Afin de présenter un autre exemple de démonstration par succession d'équivalences, nous allons démontrer l'énoncé suivant :

Proposition 1.1.11. *Réécriture de l'opérateur "si et seulement si".*
Soit p et q des expressions booléennes, alors :

$$(p \Leftrightarrow q) \quad \Leftrightarrow \quad (p \wedge q) \vee (\neg p \wedge \neg q)\,.$$

Dans la démonstration qui suit, contrairement à la démonstration de la proposition 1.1.9, nous omettons volontairement de spécifier les changements de variables dans les commentaires lorsque ceux-ci sont évidents. De même, nous regroupons quelques fois deux opérations en une seule étape. Une fois qu'on se "permet" de ne pas donner tous les détails, il n'y a pas de règles qui dictent la "bonne" manière de présenter une démonstration et le niveau de détails requis[9]. Il est important cependant que la démarche demeure très claire pour le lecteur qui doit comprendre la démonstration.

Démonstration de la réécriture du "si et seulement si". (Proposition 1.1.11)
Soit p et q deux expressions booléennes. Démontrons "$p \Leftrightarrow q \;\Leftrightarrow\; (p \wedge q) \vee (\neg p \wedge \neg q)$" :

$$
\begin{array}{ll}
 & p \Leftrightarrow q \\
\Leftrightarrow & \quad \langle\ \textit{Déf 1.1.3 – Définition du "si et seulement si"}\ \rangle \\
 & (p \Rightarrow q) \wedge (q \Rightarrow p) \\
\Leftrightarrow & \quad \langle\ \textit{Déf 1.1.2 – Définition de l'implication, 2 fois}\ \rangle \\
 & (\neg p \vee q) \wedge (\neg q \vee p) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.6-f – Distributivité de la conjonction, avec } [p := \neg p] \textit{ et } [r := (\neg q \vee p)]\ \rangle \\
 & (\neg p \wedge (\neg q \vee p)) \vee (q \wedge (\neg q \vee p)) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.6-d – Commutativité de la conjonction, 2 fois}\ \rangle \\
 & ((\neg q \vee p) \wedge \neg p) \vee ((\neg q \vee p) \wedge q) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.6-f – Distributivité de la conjonction, 2 fois}\ \rangle \\
 & ((\neg q \wedge \neg p) \vee (p \wedge \neg p)) \vee ((\neg q \wedge q) \vee (p \wedge q)) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.5-c – Contradiction, 2 fois}\ \rangle \\
 & ((\neg q \wedge \neg p) \vee \texttt{faux}) \vee (\texttt{faux} \vee (p \wedge q))
\end{array}
$$

9. Dans le cours *Logique et techniques de preuves*, tous les détails doivent être donnés et les démonstrations doivent être présentées exactement sous la forme présentée ici (incluant la position des éléments sur la page).

$\Leftrightarrow$ ⟨ *Prop 1.1.7-d – Commutativité de la disjonction, 2 fois* ⟩

$((p \wedge q) \vee \texttt{faux}) \vee ((\neg q \wedge \neg p) \vee \texttt{faux})$

$\Leftrightarrow$ ⟨ *Prop 1.1.7-a – Elément neutre, 2 fois* ⟩

$(p \wedge q) \vee (\neg p \wedge \neg q)$ **C.Q.F.D.**

Message important !

Les deux types de démonstrations présentées jusqu'à maintenant sont également valides. En effet, pour démontrer l'équivalence entre deux expressions booléennes, il est aussi valide d'effectuer une démonstration par table de vérité que par succession d'équivalences.

Et pourquoi conclut-on que la 1ère ligne est équivalente à la dernière ?

Comme mentionné au début de ce chapitre, les démonstrations mathématiques sont basées sur les travaux d'Aristote. Rappelons les deux exemples déjà présentés :

Tous les hommes sont mortels
Or Socrate est un homme
Donc Socrate est mortel

Cette conclusion nous est naturelle, et nous voulons insister ici sur le fait qu'elle est basée sur les lois de la logique que nous avons vues jusqu'ici. Un tel raisonnement est une forme de syllogisme ; il est appelé le *modus ponens*[10].

L'exemple suivant est aussi un syllogisme :

Quand il pleut sur le campus, Xavier a toujours son parapluie sur lui.
Je constate qu'il pleut sur le campus.
Donc Xavier a son parapluie aujourd'hui.

Par ce raisonnement, on a réussi à *extraire* une information, "Xavier a son parapluie aujourd'hui", à partir de l'affirmation de la première ligne. Le canevas général de cet exemple est le suivant

Si $P \Rightarrow Q$ est un théorème (*c'est-à-dire qu'il est démontré/accepté comme vrai*)
et P est vrai
alors Q est aussi vrai

Cette conclusion est basée sur les lois de la logique que nous avons vues puisque si P est vrai, la seule façon que $P \Rightarrow Q$ soit vrai est que (selon la table de vérité de l'implication) Q soit aussi vrai. L'exemple de Socrate est sensiblement le même :

10. L'autre forme de syllogisme est le *modus tollens* : c'est le modus ponens combiné à la contraposition.

Si $P(x) \Rightarrow Q(x)$ est vrai pour tout x possible,
et si $P(Socrate)$ est vrai,
alors $Q(Socrate)$ est vrai.

En fait, les démonstrations par succession d'équivalence utilisent ce raisonnement. Ces démonstrations (lorsqu'elles ont 2 équivalences) sont correctes grâce à la démonstration suivante (pour toutes expressions booléennes A, B et C) :

Si "$(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \ \Rightarrow \ (A \Leftrightarrow C)$" est vrai pour tout A, B et C, (1)
et si "$(A \Leftrightarrow B) \wedge (B \Leftrightarrow C)$" est vrai, (2)
alors "$A \Leftrightarrow C$" aussi vrai. (3)

Lorsqu'on fait une démonstration par succession d'équivalences, on considère que la ligne (1) ci-dessus est démontrée (c'est la transitivité du "si et seulement si", c'est-à-dire la proposition 1.1.8 de la page 17). On montre ensuite que la ligne (2) est vraie (c'est la succession d'équivalences à proprement dit), ce qui nous permet finalement de conclure à la ligne (3). Bien sûr, cette démarche est implicite dans la vaste majorité des démonstrations mathématiques.

Notons que l'on peut facilement étendre le raisonnement présenté ici, qui s'applique à une succession d'équivalences de seulement trois lignes (A, B et C), pour justifier les démonstrations par succession d'équivalences qui ont plusieurs lignes...

1.1.5 Le problème de satisfiabilité d'une équation booléenne

Le **problème de satisfiabilité** d'une équation booléenne, communément appelé le problème **SAT**, est fondamental en informatique théorique. Bien que très simple dans sa formulation, le problème SAT suscite beaucoup d'intérêt en informatique, tant du point de vue pratique que théorique. Une raison à cet intérêt est qu'il est possible de traduire plusieurs autres problèmes, de natures très variées, en un problème SAT.

Satisfiabilité

Une **instance du problème SAT** consiste en une équation booléenne contenant des variables libres. Une telle instance est dite **satisfiable** lorsqu'il existe une assignation de variables telle que l'équation est évaluée à `vrai`. L'instance ϕ_a ci-dessous est satisfiable puisque

si $x_1 := \texttt{vrai}$, $x_2 := \texttt{vrai}$ et $x_3 := \texttt{faux}$, l'expression est évaluée à `vrai`.

$$\phi_a : \quad \neg[\,(x_1 \vee x_2 \vee x_3) \;\Rightarrow\; (x_1 \wedge x_3) \vee (x_2 \wedge x_3)\,]\,.$$

Une instance est **insatisfiable** lorsqu'aucune assignation de variables ne permet à son expression booléenne d'être vraie. Par exemple, l'instance ϕ_b suivante est insatisfiable :

$$\phi_b : \quad \neg x_1 \wedge (x_2 \vee x_3) \wedge (x_2 \vee \neg x_3) \wedge (x_1 \vee \neg x_2)\,.$$

Pour montrer qu'une instance du problème SAT est satisfiable, il suffit de trouver *une* assignation de variables pour laquelle l'expression est vraie (comme nous l'avons fait pour l'instance ϕ_a). Par contre, pour montrer qu'une instance est insatisfiable, il faut montrer que pour *toutes* les assignations de variables possibles, l'expression est fausse. Une méthode simple d'accomplir cette tâche est de vérifier tous les cas à l'aide d'une table de vérité. À titre d'exemple, la table de vérité suivante montre que l'instance ϕ_b est insatisfiable :

x_1	x_2	x_3	c_1 $\neg x_1$	c_2 $x_2 \vee x_3$	c_3 $x_2 \vee \neg x_3$	c_4 $x_1 \vee \neg x_2$	ϕ_b $c_1 \wedge c_2 \wedge c_3 \wedge c_4$
v	v	v	f	v	v	v	f
v	v	f	f	v	v	v	f
v	f	v	f	v	f	v	f
v	f	f	f	f	v	v	f
f	v	v	v	v	v	f	f
f	v	f	v	v	v	f	f
f	f	v	v	v	f	v	f
f	f	f	v	f	v	v	f

Forme normale conjonctive

L'équation définissant une instance du problème SAT est généralement exprimée sous une forme standard que l'on désigne par **forme normale conjonctive**. On parle alors d'un problème **SAT-CNF** (l'abréviation CNF vient de l'anglais "conjunctive normal form"). L'instance ϕ_b du problème SAT présentée plus haut est sous la forme CNF, tandis que l'instance ϕ_a ne l'est pas. Voici un autre exemple d'instance du problème SAT-CNF :

$$\phi_c : \quad (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3) \wedge (\neg x_2 \vee \neg x_3) \wedge (x_1 \vee x_2 \vee x_3)\,.$$

En logique mathématique, le terme **littéral** désigne une variable booléenne ou la négation d'une variable booléenne (dans l'expression ϕ_c, "x_1" et "$\neg x_1$" sont des littéraux) et le terme **clause** désigne une disjonction de littéraux (l'expression ϕ_c comporte quatre clauses, dont la première est "$x_1 \vee x_2$"). Considérant ces définitions, une forme normale conjonctive est une conjonction de clauses. À moins de spécifications contraires, une clause peut contenir un nombre quelconque de littéraux.

Une instance d'un problème SAT-CNF comprend exclusivement les opérateurs de base présentés par la définition 1.1.1 (page 8) : la disjonction "$\vee$", la conjonction "$\wedge$" et la négation "$\neg$". Rappelons que les deux autres opérateurs booléens présentés par les définitions 1.1.2 (page 9) et 1.1.3 (page 10), peuvent être réécrits en utilisant seulement les trois opérateurs de base. Cependant, il est souvent insuffisant de la réécrire à l'aide des trois opérateurs de base pour transformer une expression booléenne sous forme normale conjonctive (c'est-à-dire une conjonction de clauses). Pour ce faire, on peut transformer l'expression en appliquant les lois de De Morgan (proposition 1.1.4) et les propriétés des opérateurs (propositions 1.1.6, 1.1.7 et 1.1.5). À titre d'exemple, transformons l'instance SAT ϕ_a en instance SAT-CNF :

$$
\begin{aligned}
& \neg[\,(x_1 \vee x_2 \vee x_3) \;\Rightarrow\; (x_1 \wedge x_3) \vee (x_2 \wedge x_3)\,] \\
\Leftrightarrow \quad & \langle\ \textit{Déf 1.1.2 – Implication, avec } [p := (x_1 \vee x_2 \vee x_3)] \textit{ et } [q := (x_1 \wedge x_3) \vee (x_2 \wedge x_3)]\ \rangle \\
& \neg[\,\neg(x_1 \vee x_2 \vee x_3) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)\,] \\
\Leftrightarrow \quad & \langle\ \textit{Prop 1.1.4-b – De Morgan, avec } [p := \neg(x_1 \vee x_2 \vee x_3)] \textit{ et } [q := (x_1 \wedge x_3) \vee (x_2 \wedge x_3)]\ \rangle \\
& \neg\neg(x_1 \vee x_2 \vee x_3) \wedge \neg(\,(x_1 \wedge x_3) \vee (x_2 \wedge x_3)\,) \\
\Leftrightarrow \quad & \langle\ \textit{Prop 1.1.5-a – Double négation}\ \rangle \\
& (x_1 \vee x_2 \vee x_3) \wedge \neg(\,(x_1 \wedge x_3) \vee (x_2 \wedge x_3)\,) \\
\Leftrightarrow \quad & \langle\ \textit{Prop 1.1.4-a – De Morgan, avec } [p := (x_1 \wedge x_3)] \textit{ et } [q := (x_2 \wedge x_3)]\ \rangle \\
& (x_1 \vee x_2 \vee x_3) \wedge \neg(x_1 \wedge x_3) \wedge \neg(x_2 \wedge x_3) \\
\Leftrightarrow \quad & \langle\ \textit{Prop 1.1.4-b – De Morgan, 2 fois}\ \rangle \\
& (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_3) \wedge (\neg x_2 \vee \neg x_3)
\end{aligned}
$$

La complexité du problème SAT

Lorsqu'une instance du problème SAT comprend peu de variables, un programme informatique peut très rapidement déterminer si cette instance est satisfiable ou non à l'aide d'une

table de vérité. Cependant, le nombre de lignes requis par la table de vérité augmente exponentiellement en fonction du nombre de variables de l'instance (une instance de n variables nécessite 2^n lignes). Ainsi, une instance comportant plusieurs centaines de variables peut être très longue à résoudre par cette méthode, même sur un ordinateur très rapide.

Chaque année, de nouveaux programmes informatiques s'affrontent lors d'une compétition internationale dont le but est de résoudre de grandes instances du problème SAT le plus rapidement possible[11]. Bien que ces programmes emploient des stratégies astucieuses pour réduire le temps de calcul nécessaire à l'obtention d'une solution, personne n'a découvert, à ce jour, une méthode "efficace" pour résoudre le problème SAT. Le temps de calcul "en pire cas" nécessaire à ces programmes SAT croît toujours exponentiellement en fonction du nombre de variables de l'instance du problème SAT à résoudre. En fait, la découverte d'un algorithme pour résoudre le problème SAT dont le temps d'exécution serait polynomial en fonction du nombre de variables d'instance aurait un impact majeur sur l'informatique, comme nous l'apprennent les recherches en théorie de la complexité.

En informatique théorique, la **théorie de la complexité** divise les problèmes en familles de problèmes de complexité similaires. La famille des problèmes "NP-complets" regroupe plusieurs problèmes dignes d'intérêt dont le temps d'exécution du meilleur algorithme connu pour les résoudre est exponentiel, même si une fois la solution trouvée, il est facile de vérifier qu'elle est bonne. Le problème SAT appartient à cette famille[12], comme l'a montré en 1971 le mathématicien et informaticien Stephen Cook. Il s'agit d'un résultat important dans l'histoire de l'informatique théorique, car ce fut le premier problème "NP-complet" identifié. Depuis, plusieurs autres problèmes se sont joints à la famille des problèmes "NP-complets". La découverte d'un algorithme "efficace" pour résoudre un seul de ces problèmes permettrait de résoudre tous les autres efficacement. Nous arrêtons ici notre court survol de la théorie de la complexité. Ce passionnant sujet est abordé dans le cadre du cours "Conception et analyse d'algorithmes".

11. Voir http://www.satcompetition.org/

12. En effet, pour trouver la solution d'un problème SAT à n variables, on peut être obligé de considérer les 2^n affectations de variables possibles (car si on est malchanceux, ce sera la dernière qui sera la bonne). Cependant, une fois la solution trouvée, on peut rapidement vérifier qu'elle est bonne en ne considérant que cette affectation.

1.1.6 Exercices sur l'algèbre booléenne

Exercice 1

Donnez des valeurs de vérité à p et q telles que

1. $p \vee q$ est vrai et $p \wedge q$ est faux
2. $p \vee q$ est vrai et $p \Rightarrow q$ est faux
3. $p \Rightarrow q$ et $q \Rightarrow p$ sont vrais

Exercice 2

Existe-t-il des valeurs de vérité pour p et q telles que (justifiez)

1. $p \wedge q$ est vrai et $p \vee q$ est faux
2. $p \Rightarrow q$ est vrai et $p \vee q$ est faux
3. $p \Rightarrow q$ est vrai et $q \Rightarrow p$ est faux
4. $q \Rightarrow (p \vee \neg p)$ est vrai
5. $(p \vee \neg p) \Rightarrow (q \wedge \neg q)$ est vrai

Exercice 3

Démontrez les propriétés suivantes à l'aide d'une table de vérité :

a) Deuxième loi de De Morgan (Proposition 1.1.4-b) : $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$.

b) Distributivité de la disjonction (Proposition 1.1.7-f) : $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$.

Exercice 4

Quand on veut démontrer des énoncés complexes, il est essentiel de savoir, en quelque sorte, éliminer les signes de négation qui sont dans le chemin. Faites-le pour les expressions suivantes (c'est une démonstration par succession d'équivalence, mais on ne sait pas à quoi on va arriver) : une négation ne doit se retrouver que devant une variable simple et non devant une parenthèse. Il suffit d'utiliser les règles de De Morgan, la double négation et la définition de l'implication (voilà pourquoi il faut savoir ces règles par coeur !!!) On ne demande pas d'autre transformation ici.

1. $\neg(p \vee \neg q)$
2. $\neg(\neg(p \wedge q))$
3. $\neg(p \Rightarrow q)$
4. $\neg(\neg p \wedge (q \vee \neg p))$
5. $\neg(\neg p \Rightarrow (q \vee \neg p))$

Exercice 5

Démontrez les propriétés suivantes à l'aide de la technique de démonstration par succession d'équivalences :

a) Deuxième loi de De Morgan (Proposition 1.1.4-b) : $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$.
NB : Vous pouvez utiliser la Première loi de De Morgan (Proposition 1.1.4-a) et la propriété de la double négation (Proposition 1.1.5-a).

b) Distributivité de la disjonction (Proposition 1.1.7-f) : $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$.
NB : Vous pouvez utiliser les lois de De Morgan (Proposition 1.1.4), la distributivité de la conjonction (Proposition 1.1.6-f) et la propriété de la double négation (Proposition 1.1.5-a).

c) Contradiction (Proposition 1.1.5-c) : $p \wedge \neg p \Leftrightarrow$ `faux`. Vous pouvez utiliser les propositions qui viennent avant... ! et c'est plus facile de commencer par l'expression de droite.

Exercice 6

Considérez l'opérateur **ou exclusif** "$\underline{\vee}$" possédant la table de vérité suivante :

p	q	$p \mathbin{\underline{\vee}} q$
v	v	f
v	f	v
f	v	v
f	f	f

Écrivez une définition possible de l'opérateur "$\underline{\vee}$" en utilisant seulement (justifiez brièvement vos réponses) :

a) L'opérateur de négation "$\neg$", de disjonction "$\vee$" et de conjonction "$\wedge$" ;

b) L'opérateur de négation "$\neg$" et de disjonction "$\vee$" ;

c) L'opérateur de négation "$\neg$" et le si et seulement si "$\Leftrightarrow$" .

Exercice 7

Démontrez chacune des propriétés suivantes à l'aide des deux techniques de démonstration vues jusqu'à maintenant : (*i*) par une table de vérité et (*ii*) par une succession d'équivalences :

a) $(\neg p \Leftrightarrow \neg q) \Leftrightarrow (p \Leftrightarrow q)$

b) $(\neg p \Leftrightarrow q) \Leftrightarrow (p \Leftrightarrow \neg q)$

c) $(\neg p \Leftrightarrow q) \Leftrightarrow \neg(p \Leftrightarrow q)$

d) $(\neg p \Rightarrow (p \Rightarrow q))$

e) $(p \Rightarrow (\neg p \Rightarrow q))$

f) $(p \Rightarrow$ `faux`$) \Leftrightarrow \neg p$

Exercice 8

Déterminez si les instances suivantes du problème SAT sont satisfiables. Pour les instances satisfiables, fournissez une assignation de variables telle que l'expression booléenne est vraie. Pour les instances insatisfiables, démontrez votre résultat à l'aide d'une table de vérité.

a) $\psi_a = (x_1 \vee x_2) \wedge x_3 \wedge (\neg x_1 \vee \neg x_3) \wedge (\neg x_2 \vee \neg x_3)$.

b) $\psi_b = (x_1 \vee x_2) \wedge x_3 \wedge (x_1 \vee \neg x_3) \wedge (\neg x_2 \vee \neg x_3)$.

c) $\psi_c = (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_3)$.

d) $\psi_d = (\neg x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_2 \vee x_3 \vee \neg x_4)$.

Exercice 9

En utilisant les propriétés que nous avons vues dans cette section, réécrivez les expressions suivantes sous forme normale conjonctive :

a) $x_1 \Leftrightarrow x_2$

b) $(x_1 \vee x_2) \wedge (x_3 \vee x_4)$

c) $(x_1 \wedge x_2) \vee (x_3 \wedge x_4)$

d) $(x_1 \Rightarrow x_2) \Rightarrow ((x_3 \Rightarrow x_4) \Rightarrow x_5)$

Exercice 10

Imaginons qu'on vous demande d'écrire un "solveur SAT", c'est-à-dire un programme informatique qui reçoit en entrée une instance du problème SAT-CNF (soit une expression booléenne sous forme normale conjonctive) et détermine si cette instance est satisfiable.

a) Votre programme reçoit en entrée une instance du problème SAT-CNF décrite ainsi :
   — Un nombre n indiquant le nombre de variables du problème. On représente ces variables par $x_1, x_2, \ldots, x_n$;
   — Une collection de m clauses que l'on représente par $C_1, C_2, \ldots, C_m$.

   On vous fournit une fonction déjà programmée "`évaluerClause`$(C_j, a_1, a_2, \ldots, a_n)$" qui retourne le résultat de l'évaluation de la clause C_j (c'est-à-dire `vrai` ou `faux`) avec l'assignation de valeurs $x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$.

   Expliquez, en vos mots ou à l'aide d'un pseudo-code, la procédure que doit employer votre programme pour vérifier si une instance est satisfiable ou insatisfiable. Inspirez-vous de la méthode que vous utilisez pour bâtir une table de vérité.

b) Serait-il possible d'utiliser votre programme pour vérifier si une expression booléenne est toujours vraie ? Si oui, expliquez comment. Sinon, expliquez pourquoi.

Exercice 11

À la page 55 du présent document, la section 1.3 débute par une citation d'Eugène Ionesco, digne représentant du théâtre de l'absurde. Dans cette citation, un prétendu logicien affirme : "Tous les chats sont mortels. Socrate est mortel. Donc Socrate est un chat."

a) Expliquez dans vos propres mots pourquoi ce raisonnement est erroné ;

b) Réécrivez l'affirmation de l'aspirant logicien en utilisant les opérateurs booléens. Pour simplifier la tâche, considérez l'affirmation sous la forme : "Si Socrate est un chat, alors il est mortel. Socrate est mortel. Donc Socrate est un chat.". De même, utilisez les variables c et m pour représenter les expressions suivantes :

$$\begin{aligned} c &= \textit{Socrate est un chat}, \\ m &= \textit{Socrate est mortel}. \end{aligned}$$

c) À partir de l'expression booléenne trouvée en (b), démontrez à l'aide d'une table de vérité que l'affirmation du pauvre logicien est fausse ;

d) Suggérez une modification à l'affirmation du logicien afin qu'elle soit toujours vraie.

1.2 Ensembles

> Maintenant que nous sommes ensemble,
> ça va mieux.
>
> Wajdi Mouawad, *Incendies* (2003)

La théorie des ensembles fut introduite par le mathématicien allemand Georg Cantor (1845 – 1918). Un ensemble est une structure mathématique très simple qui permet de regrouper plusieurs éléments. Au même titre que nous avons défini des opérateurs booléens et des expressions booléennes à la section précédente, nous allons maintenant définir des opérateurs ensemblistes et des expressions ensemblistes. Ces notions permettent de manipuler des ensembles pour en créer de nouveaux et de démontrer certaines de leurs propriétés. Les propriétés ensemblistes sont très similaires aux propriétés de l'algèbre de Boole que nous avons vues à la section précédente. En fait ces deux domaines sont intimement liés.

1.2.1 Égalité entre deux ensembles (Axiome d'extensionnalité)

Un **ensemble** est une collection d'éléments non ordonnée et sans répétitions. Les variables représentant des ensembles sont habituellement des lettres majuscules et les éléments d'un ensemble sont indiqués entre accolades. Dans l'exemple qui suit, l'ensemble A contient les nombres entiers compris entre 1 et 5 inclusivement :

$$A \;:=\; \{1, 2, 3, 4, 5\}\,.$$

L'ordre des éléments dans la présentation de l'ensemble n'a pas d'importance, de même que la présence de répétitions. L'ensemble A peut donc s'écrire de plusieurs manières équivalentes :

$$A \;=\; \{5, 1, 3, 2, 4\} \;=\; \{1, 2, 2, 3, 3, 3, 4, 4, 5\} \;=\; \{2, 1, 3, 2, 4, 3, 5\}\,.$$

Ainsi, un ensemble est défini uniquement par la nature de ses éléments. Il s'agit d'un choix fait lors de la définition de cette structure mathématique [13]. Ce choix est énoncé par l'**axiome d'extensionnalité**, qui définit rigoureusement l'opérateur d'**égalité** entre ensembles "=".

La définition 1.2.1 présente deux manières équivalentes d'exprimer l'axiome d'extensionnalité. Le deuxième énoncé fait appel au quantificateur universel "∀" que nous présenterons ultérieurement à la section 1.2.4.

13. Lorsqu'on souhaite considérer l'ordre des éléments ou leur multiplicité, on doit se donner des axiomes supplémentaires (en mathématiques, un **axiome** est une convention sur laquelle repose une théorie). C'est ce qu'on fera à la section 1.4 sur la théorie des relations, en définissant notamment la notion d'ordre partiel.

Définition 1.2.1. *Axiome d'extensionnalité*
Soit S et T deux ensembles, alors :

$$S = T \stackrel{\text{def}}{=} \begin{cases} \text{Pour tout élément } e, e \text{ appartient à l'ensemble } S \text{ si et seulement si} \\ e \text{ appartient à l'ensemble } T. \end{cases}$$

De manière équivalente, on écrit :

$$S = T \stackrel{\text{def}}{=} (\forall e \mid e \in S \Leftrightarrow e \in T) \ .$$

On utilise aussi parfois l'opérateur d'**inégalité entre deux ensembles** "$\neq$", qui est défini par l'équivalence suivante :

$$S \neq T \stackrel{\text{def}}{=} \neg(S = T) \, .$$

1.2.2 Définition d'un ensemble et opérateur d'appartenance

Bien que nous travaillerons fréquemment avec des ensembles de nombres, les **éléments** d'un ensemble peuvent être de type quelconque. On peut définir des ensembles de mots français, des ensembles de phrases, des ensembles programmes informatiques, des ensembles d'expressions booléennes, des ensembles d'ensembles, etc. Voici quelques exemples d'ensembles :

- $B := \{\texttt{a}, \texttt{e}, \texttt{i}, \texttt{o}, \texttt{u}, \texttt{y}\}$, l'ensemble des voyelles de l'alphabet ;
- $C := \{\texttt{Laviolette}, \texttt{Desharnais}, \texttt{Germain}\}$, l'ensemble des auteurs de ce document ;
- $D := \{2, 4, 6, 8, \ldots\}$, l'ensemble des nombres pairs positifs ;
- $\mathbb{B} := \{\texttt{faux}, \texttt{vrai}\}$, l'ensemble des **booléens** ;
- $\mathbb{N} := \{0, 1, 2, 3, \ldots\}$, l'ensemble des **nombres naturels** ;
- $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, l'ensemble des **nombres relatifs** ;
- $E := \{B, C, D, \mathbb{B}, \mathbb{N}, \mathbb{Z}\}$, l'ensemble des ensembles énumérés dans la présente liste.

L'opérateur d'**appartenance** "$\in$" exprime si un élément appartient à un ensemble. L'expression "$e \in S$" se dit "l'élément e appartient à l'ensemble S". Il s'agit d'une expression booléenne. Elle est donc évaluée à `vrai` ou `faux`. En utilisant les exemples énumérés plus haut, on a :

$$\begin{array}{lll} \texttt{w} \in B \text{ est faux}, & 42 \in D \text{ est vrai}, & \texttt{faux} \in \mathbb{B} \text{ est vrai}, \\ -5 \in \mathbb{N} \text{ est faux}, & -5 \in \mathbb{Z} \text{ est vrai}, & \mathbb{N} \in E \text{ est vrai} \, . \end{array}$$

Nous écrivons aussi l'expression "l'élément e n'appartient pas à l'ensemble S" avec la notation "$e \notin S$". L'opérateur "$\notin$" est donc défini par l'équivalence suivante :

$$e \notin S \stackrel{\text{def}}{=} \neg(e \in S)\,.$$

Ainsi, toutes les expressions suivantes sont vraies ($\mathbb{R}$ désigne l'ensemble des **nombres réels**) :

$$\texttt{w} \notin B, \quad 42 \in D, \quad \texttt{faux} \in \mathbb{B}, \quad -5 \notin \mathbb{N}, \quad -5 \in \mathbb{R}, \quad \mathbb{N} \in E\,.$$

Définition par extension versus définition par compréhension

Jusqu'à maintenant, nous avons présenté les ensembles par leur **définition par extension**, c'est-à-dire en énumérant les éléments de l'ensemble (par exemple, "$A := \{1, 2, 3, 4, 5\}$"). Nous introduisons maintenant la **définition par compréhension** qui consiste plutôt à présenter les propriétés que respectent les éléments d'un ensemble.

Pour définir un ensemble par compréhension, nous utilisons la notation "$S := \{\ f(x) \mid R(x)\ \}$", qu'on lit "$S$ est l'ensemble des $f(x)$ tels que $R(x)$", où :

— $f(x)$ est une fonction qui décrit les éléments de l'ensemble ;

— $R(x)$ est une expression booléenne qui permet de restreindre le contenu de l'ensemble.

Autrement dit, on a $f(x) \in S$ si et seulement si $R(x)$ est `vrai`.

Voici quelques exemples d'ensembles définis par compréhension :

— $A := \{x \mid x \in \mathbb{N} \wedge 1 \leq x \leq 5\}$, l'ensemble des nombres entiers entre 1 et 5 inclusivement ;

— $B := \{x \mid x \text{ est une voyelle }\}$, l'ensemble des voyelles de l'alphabet ;

— $\mathbb{N}^* := \{x \mid x \in \mathbb{N} \wedge x \neq 0\}$, l'ensemble des **nombres naturels excluant le zéro** ;

— $F := \{2x \mid x \in \mathbb{N}^*\}$, l'ensemble des nombres pairs positifs ;

— $G := \{2^x \mid x \in \mathbb{N} \wedge x \leq 8\}$, l'ensemble des puissances de 2 de 1 à 256 ;

— $\mathbb{Z} := \{x \mid x \in \mathbb{N} \vee -x \in \mathbb{N}\}$, l'ensemble des nombres relatifs ;

— $\mathbb{Q} := \left\{\dfrac{x}{y} \mid x \in \mathbb{Z} \wedge y \in \mathbb{N}^*\right\}$, l'ensemble des **nombres rationnels**.

PENSEZ-Y!

La manière dont est défini un ensemble (par extension ou par compréhension) n'a aucune influence sur sa composition. Par exemple, on peut imaginer une multitude de manières de définir l'ensemble des nombres pairs positifs :

$$\{2, 4, 6, 8, \ldots\} \;=\; \{2x \mid x \in \mathbb{N}^*\} \;=\; \{x \mid x \in \mathbb{N}^* \wedge x \bmod 2 = 0\} \;=\; \{x \mid x \textit{ est pair}\} \;=\; \ldots$$

Similairement, plusieurs langages de programmation informatiques implémentent un type de donnée correspondant à un ensemble, habituellement désigné par le mot-clé anglais "set". C'est entre autres le cas du *C++*, du *Python* et du *Java*. L'utilisateur du type de donnée "set" effectue des opérations d'ajout et de retrait d'éléments sans se soucier de l'ordre dans lequel les données sont emmagasinées dans la mémoire de l'ordinateur.

Notation abrégée

Remarquons que les ensembles définis par compréhension prennent souvent la forme "$\{x \mid x \in T \wedge \ldots\}$", où on peut interpréter l'ensemble T comme le type de la variable x, et où $f(x) = x$. En mathématiques, il est fréquent d'utiliser la notation abrégée "$\{x \in T \mid \ldots\}$" pour faciliter l'écriture des ensembles. Par exemple, nous pourrions écrire l'ensemble des nombres entiers entre 1 et 5 de la manière suivante :

$$A := \{x \in \mathbb{N} \mid 1 \leq x \leq 5\}\,.$$

Ensemble vide

On utilise le symbole "$\emptyset$" pour désigner l'**ensemble vide**, c'est-à-dire l'ensemble qui ne contient aucun élément. Par exemple, l'ensemble des nombres plus petits que 1 et plus grand que 5 est vide : $\{x \mid x < 1 \wedge x > 5\} = \emptyset$.

PENSEZ-Y!

Notons que l'ensemble $\{\emptyset\}$ ne correspond pas à l'ensemble vide. En effet, l'ensemble $\{\emptyset\}$ contient 1 élément, cet élément étant l'ensemble vide. On a donc :

$$\emptyset \neq \{\emptyset\} \quad \text{et} \quad \emptyset \in \{\emptyset\}\,.$$

Cardinalité d'un ensemble

La **cardinalité d'un ensemble** correspond au nombre d'éléments qu'il contient. On note $|S|$ la cardinalité de l'ensemble S. En considérant les définitions d'ensembles données en

exemple dans les pages précédentes, on a $|A| = 5$, $|B| = |E| = 6$, $|G| = 9$ et $|\mathbb{B}| = 2$. Comme l'ensemble vide ne contient aucun élément, on a $|\emptyset| = 0$. Par contre, $|\{\emptyset\}| = 1$.

Notons que les ensembles suivants contiennent un nombre infini d'éléments : F, $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. Nous reviendrons de la notion de cardinalité d'un ensemble infini à la section 1.5.

1.2.3 Diagramme de Venn et ensemble universel

Bien qu'il ne fut pas le premier à représenter les ensembles par un schéma, on doit au mathématicien anglais John Venn (1834 – 1923) les **diagrammes de Venn** utilisés communément aujourd'hui. Un tel diagramme permet d'illustrer les relations entre les ensembles que l'on étudie.

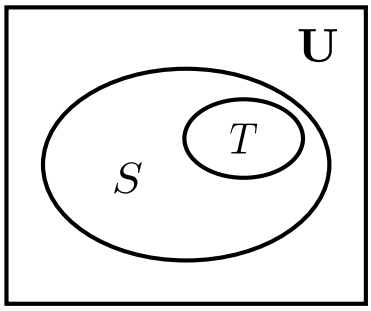
Tout diagramme de Venn est délimité par un rectangle représentant l'ensemble universel. L'**ensemble universel**, désigné par le symbole **U**, contient tous les éléments possibles du problème étudié. Par exemple, si on s'intéresse à un problème ne concernant que les nombres naturels, on détermine que $\mathbf{U} := \mathbb{N}$. Par contre, si on s'intéresse aux noms des auteurs possibles d'un document alors l'ensemble **U** pourrait représenter tous les noms de famille possibles.

À l'intérieur du diagramme de Venn, chaque ensemble est représenté par une ellipse. La figure 1.1 présente trois exemples de diagrammes de Venn.

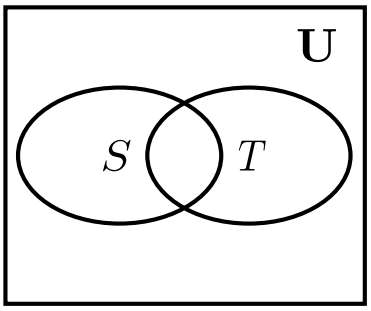
— Figure 1.1a : L'ensemble T est un sous-ensemble de l'ensemble S, c'est-à-dire que S contient tous les éléments de T.
— Figure 1.1b : L'ensemble S et l'ensemble T peuvent posséder certains éléments en commun.
— Figure 1.1c : L'ensemble S et l'ensemble T n'ont aucun élément en commun.

La présence d'un élément dans un ensemble est représentée par un point. Au besoin, on peut attribuer une étiquette à cet élément. La figure 1.2 présente quelques exemples de tels diagrammes de Venn :

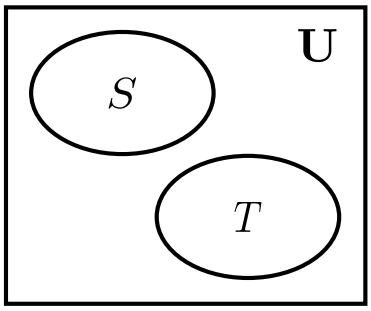
— Figure 1.2a : L'ensemble T est un sous-ensemble strict de l'ensemble S, c'est-à-dire que S contient tous les éléments de T et au moins un élément appartient à S sans appartenir à T.
— Figure 1.2b : L'ensemble S et l'ensemble T possèdent au moins un élément en commun. Cet élément est désigné par e.
— Figure 1.2c : L'ensemble S et l'ensemble T n'ont aucun élément en commun et l'ensemble S contient au moins trois éléments, désignés par les chiffres 1, 2 et 3.



(a) T est inclus dans S.

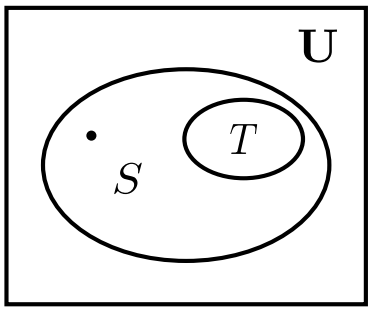


(b) S et T peuvent partager certains éléments.

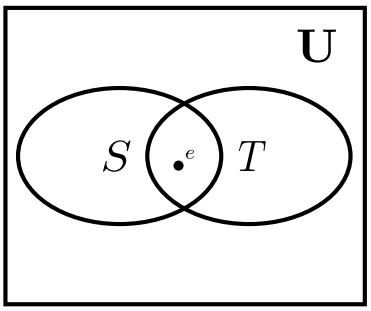


(c) S et T sont disjoints.

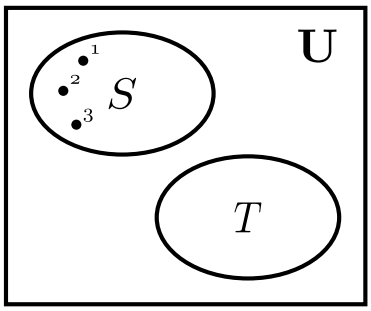
FIGURE 1.1 – Diagrammes de Venn illustrant trois relations possibles entre deux ensembles.



(a) T est strictement inclus dans S.



(b) S et T partagent au moins l'élément e.



(c) S et T sont disjoints et S possède au moins 3 éléments (désignés par 1, 2 et 3).

FIGURE 1.2 – Trois autres exemples de diagrammes de Venn.

Remarquons que les diagrammes de Venn représentés par les figures 1.1b et 1.2b sont semblables. La distinction entre ces deux diagrammes est que, dans la figure 1.1b, il est possible que les ensembles S et T ne possèdent aucun élément en commun. Cependant, la figure 1.2b précise que les deux ensembles partagent *au moins* un élément.

1.2.4 Quantificateur universel et quantificateur existentiel

La logique booléenne, introduite à la section 1.1 n'est pas assez *expressive* pour exprimer toutes les propositions qui nous intéressent en théorie des ensembles. Nous devons "monter d'un niveau", vers ce qui s'appelle la **logique du premier ordre**. Celle-ci inclut les quantificateurs **universel** et **existentiel** et des prédicats impliquant des variables, comme "$P(x)$",

qui pourrait signifier x est pair, ou x est le gène de la bosse des maths, etc.

Considérons l'ensemble A des nombres entiers compris entre 1 et 5 inclusivement. Cette section introduit donc la notation qui permet de formuler des expressions telles que :

— *Tous les éléments de A sont inférieurs à la valeur* 10.
— *Il existe un élément de A qui soit inférieur à la valeur* 10.
— *Tous les éléments de A sont pairs.*
— *Il existe un nombre pair parmi les éléments de l'ensemble A.*

Remarquons que ces quatre phrases sont des expressions booléennes. Elles possèdent donc une valeur de vérité (`vrai` ou `faux`). On remarque aussi qu'elles n'impliquent que deux prédicats : "$x < 10$" et "x est pair" ; on ne veut pas traiter ces quatre phrases comme quatre expressions atomiques, mais bien utiliser le fait qu'elles sont construites à partir des prédicats mentionnés.

Quantificateur universel

Le **quantificateur universel** "$\forall$" permet d'exprimer si tous les éléments d'un ensemble possèdent une certaine propriété (exprimée sous forme d'expression booléenne). La notation du quantificateur universel est la suivante :

$$(\forall x \mid P(x)\,)\,.$$

Cette expression est évaluée à `vrai` si l'expression $P(x)$ est vraie pour toutes les valeurs x. On la traduit habituellement en français par la phrase "pour tout x, x satisfait $P(x)$", ou "pour tout x, $P(x)$ est vrai".

Considérons l'ensemble $A := \{1, 2, 3, 4, 5\}$. L'expression "*Tous les éléments de A sont inférieurs à la valeur* 10" s'écrit ainsi à l'aide du quantificateur universel :

$$(\forall x \mid x \in A \Rightarrow x < 10)\,.$$

Pour évaluer l'expression, il suffit de vérifier si chaque élément de l'ensemble A est inférieur à la valeur 10, ce qui est équivalent à évaluer l'expression booléenne suivante :

$$(1 < 10) \ \wedge \ (2 < 10) \ \wedge \ (3 < 10) \ \wedge \ (4 < 10) \ \wedge \ (5 < 10)\,.$$

Il y a donc un fort lien entre le quantificateur universel "$\forall$" et l'opérateur de conjonction "$\wedge$" introduit à la section 1.1.2.

Quantificateur existentiel

Le **quantificateur existentiel** "$\exists$" permet quant à lui d'exprimer si au moins un des éléments d'un ensemble possède une certaine propriété. La notation du quantificateur existentiel est la suivante :

$$(\exists x \mid P(x)\,).$$

Cette expression est évaluée à `vrai` si l'expression $P(x)$ est vraie pour au moins une valeur de x. On la traduit en français par la phrase "il existe un x tel que x satisfait $P(x)$", ou "il existe x tel que $P(x)$ est vrai".

L'expression "*Il existe un nombre pair parmi les éléments de l'ensemble A*" se traduit ainsi à l'aide du quantificateur existentiel [14] :

$$(\exists x \mid x \in A \wedge x \bmod 2 = 0)\,.$$

Pour évaluer l'expression, il suffit de vérifier si l'un ou l'autre des éléments de l'ensemble A est pair, ce qui est équivalent à évaluer l'expression booléenne suivante :

$$(1 \bmod 2 = 0) \ \vee \ (2 \bmod 2 = 0) \ \vee \ (3 \bmod 2 = 0) \ \vee \ (4 \bmod 2 = 0) \ \vee \ (5 \bmod 2 = 0)\,.$$

Il y a donc un fort lien entre le quantificateur existentiel "$\exists$" et l'opérateur de disjonction "$\vee$" introduit à la section 1.1.2.

Notation abrégée

Comme pour la notation ensembliste, nous introduisons une notation abrégée de la quantification. En effet, il est fréquent que les expressions contenant des quantificateurs prennent les formes "$(\forall x \mid x \in T \Rightarrow \ldots)$" et "$(\exists x \mid x \in T \wedge \ldots)$". Dans les deux cas, l'ensemble T peut être considéré comme le type de la variable x. C'est pourquoi nous utilisons fréquemment les notations définies ci-dessous [15] :

Définition 1.2.2. *Notation abrégée des quantificateurs universel et existentiel*
Soit T un ensemble et $P(x)$ une expression booléenne qui dépend d'un élément $x \in T$. Alors :

$$\begin{array}{lll} \texttt{a}: & (\forall x \in T \mid P(x)\,) \stackrel{\text{def}}{=} (\forall x \mid x \in T \Rightarrow P(x)\,) & \textit{(Quantificateur universel)} \\ \texttt{b}: & (\exists x \in T \mid P(x)\,) \stackrel{\text{def}}{=} (\exists x \mid x \in T \wedge P(x)\,) & \textit{(Quantificateur existentiel)} \end{array}$$

14. L'opérateur arithmétique **modulo** " mod " retourne le reste de la division entière. On a donc $x \bmod 2 = 0$ si x est pair et $x \bmod 2 = 1$ si x est impair.

15. En informatique il arrive que les expressions de formes "$(\forall x \mid R(x) \Rightarrow P(x)\,)$" et "$(\exists x \mid R(x) \wedge P(x)\,)$" soient remplacées par "$(\forall x \mid R(x) : P(x)\,)$" et "$(\exists x \mid R(x) : P(x)\,)$". Nous n'utiliserons pas ces formes.

Il est ici **très important** de comprendre pourquoi dans le cas de $\forall$, c'est une implication ($\Rightarrow$) qui intervient alors que dans le cas du $\exists$, c'est une conjonction ($\wedge$). Confrontez cette définition à votre logique personnelle.

Ainsi, nous avons les équivalences suivantes :

$$\begin{aligned}(\forall x \mid x \in A \Rightarrow x < 10) &\Leftrightarrow (\forall x \in A \mid x < 10)\,,\\ (\exists x \mid x \in A \wedge x \bmod 2 = 0) &\Leftrightarrow (\exists x \in A \mid x \bmod 2 = 0)\,.\end{aligned}$$

Combinaison d'expressions et lois de De Morgan

Il est possible de combiner plusieurs expressions impliquant des quantificateurs universels et existentiels afin de construire des expressions plus complexes. Par exemple, l'expression qui suit équivaut à l'affirmation "*Il n'existe pas, dans les naturels, un nombre pair qui soit un nombre premier.*" :

$$\neg\,(\,\exists x \in \mathbb{N} \mid x \bmod 2 = 0 \wedge (\forall y \in \mathbb{N} \mid 1 < y < x \Rightarrow x \bmod y \neq 0)\,)\ .$$

Le domaine des mathématiques qui s'intéresse à ce type d'expressions s'appelle la **logique du premier ordre**[16].

Une propriété importante des deux quantificateurs présentés est la façon dont ils interagissent avec l'opérateur de négation ($\neg$) : on dit que $\forall$ est l'opération duale de $\exists$ et vice-versa, ce qui peut être écrit sommairement et intuitivement par : $\forall P = \neg\exists\neg P$. Une forme plus utile pour nous est simplement une généralisation des **lois de De Morgan** (voir la proposition 1.1.4 à la page 13).

Proposition 1.2.3. *Lois de De Morgan (généralisées aux quantificateurs).*
Soit T un ensemble et $P(x)$ une expression booléenne qui dépend de $x \in T$. On a :

$$\begin{aligned}&\texttt{a}: \quad \neg(\forall x \in T \mid P(x)) \Leftrightarrow (\exists x \in T \mid \neg P(x)) \qquad \textit{(Première loi de De Morgan)}\\ &\texttt{b}: \quad \neg(\exists x \in T \mid P(x)) \Leftrightarrow (\forall x \in T \mid \neg P(x)) \qquad \textit{(Deuxième loi de De Morgan)}\end{aligned}$$

Il est **très important** de bien comprendre ces lois, en les interprétant avec votre logique personnelle, en français. Les comprendre, c'est les mémoriser.

16. Voir http://fr.wikipedia.org/wiki/Calcul_des_pr%C3%A9dicats

1.2.5 Opérateurs ensemblistes

Similairement aux opérateurs booléens qui permettent de combiner des expressions booléennes atomiques, il existe des opérateurs sur les ensembles permettant de créer de nouveaux ensembles en combinant des ensembles existants. C'est le cas des opérateurs ensemblistes de complément "^{c}", d'union "$\cup$", d'intersection "$\cap$" et de différence "$\setminus$".

D'autres opérateurs ensemblistes permettent de créer des expressions booléennes répondant à la question : "*Est-ce qu'un ensemble est le sous-ensemble d'un autre ensemble ?*". Ce sont les opérateurs d'inclusion "$\subseteq$" et d'inclusion stricte "$\subset$".

Les sections suivantes sont consacrées à la présentation des définitions et des propriétés des opérateurs ensemblistes.

Les premiers opérateurs ensemblistes présentés permettent de créer de nouveaux ensembles en combinant des ensembles existants. La définition 1.2.4 repose sur les opérateurs booléens (voir définition 1.1.1), mais leur signification est très intuitive :

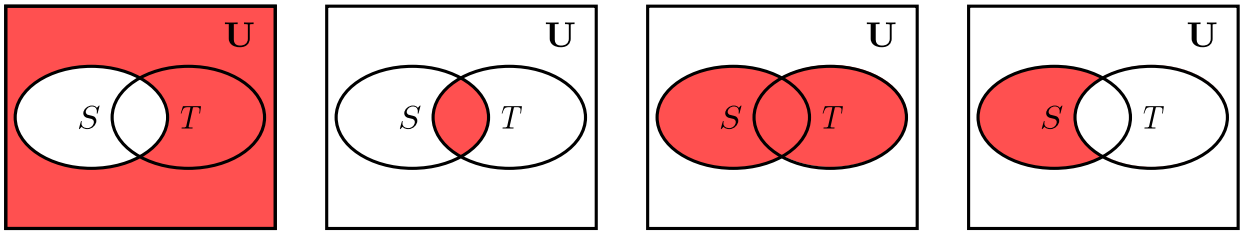
— Le **complément** "S^c" d'un ensemble S contient tous les éléments qui n'appartiennent pas à l'ensemble S, étant donné un contexte bien défini (c'est-à-dire qu'on doit connaître la nature de l'ensemble universel $\mathbf{U}$) ;
— L'**intersection** "$S \cap T$" des deux ensembles S et T contient les éléments qui appartiennent à la fois à l'ensemble S et à l'ensemble T ;
— L'**union** "$S \cup T$" des deux ensembles S et T contient les éléments qui appartiennent à l'ensemble S ou à l'ensemble T (ou encore aux deux ensembles simultanément) ;
— La **différence** "$S \setminus T$" de l'ensemble S par l'ensemble T contient les éléments qui appartiennent à l'ensemble S, mais qui n'appartiennent pas à l'ensemble T.

Définition 1.2.4. *Définitions des opérateurs sur les ensembles.*
Soit S et T des ensembles, alors :

$$\begin{array}{lllll}
\texttt{a}: & S^c & \stackrel{\text{def}}{=} & \{e \mid e \notin S\} & \textit{(Complément)} \\
\texttt{b}: & S \cap T & \stackrel{\text{def}}{=} & \{e \mid e \in S \wedge e \in T\} & \textit{(Intersection)} \\
\texttt{c}: & S \cup T & \stackrel{\text{def}}{=} & \{e \mid e \in S \vee e \in T\} & \textit{(Union)} \\
\texttt{d}: & S \setminus T & \stackrel{\text{def}}{=} & \{e \mid e \in S \wedge e \notin T\} & \textit{(Différence)}
\end{array}$$

La figure 1.3 illustre, par des diagrammes de Venn, les ensembles obtenus par l'application de ces opérateurs. Similairement aux tables de vérité énumérant les résultats de l'évaluation des opérateurs booléens (section 1.1.2), les diagrammes de Venn sont suffisamment explicites pour servir de définitions aux opérateurs. Nous verrons bientôt que les diagrammes de Venn peuvent aussi servir à démontrer l'équivalence entre des ensembles exprimés de manières

différentes. Cependant, comme il peut être fastidieux d'illustrer un grand nombre d'ensembles à l'aide d'un diagramme de Venn, ces démonstrations ne peuvent vraiment être utilisées que pour des cas simples.



(a) Complément S^c (b) Intersection $S \cap T$ (c) Union $S \cup T$ (d) Différence $S \setminus T$

FIGURE 1.3 – Diagrammes de Venn des opérateurs ensemblistes. Pour chaque opérateur, la zone du diagramme coloriée en rouge correspond au nouvel ensemble obtenu.

Opérateurs d'inclusion d'ensembles

Les deux opérateurs d'inclusions permettent de comparer deux ensembles afin de déterminer si un ensemble est un sous-ensemble d'un autre. Ils forment des expressions booléennes :

— L'**inclusion** "$T \subseteq S$" est évaluée à `vrai` lorsque tous les éléments de l'ensemble T appartiennent aussi à l'ensemble S (il s'agit de la situation illustrée par le diagramme de Venn de la figure 1.1a à la page 37). On dit que "l'ensemble T est inclus dans l'ensemble S" ou que "l'ensemble T est un sous-ensemble de l'ensemble S".

— L'**inclusion stricte** "$T \subset S$" est évaluée à `vrai` lorsque tous les éléments de l'ensemble T appartiennent aussi à l'ensemble S, mais que les deux ensembles ne sont pas égaux (il s'agit de la situation illustrée par le diagramme de Venn de la figure 1.2a à la page 37). On dit que "l'ensemble T est strictement inclus dans l'ensemble S" ou que "l'ensemble T est un sous-ensemble strict de l'ensemble S".

La définition 1.2.5 ci-bas formalise ces concepts :

Définition 1.2.5. *Définitions des opérateurs d'inclusions.*
Soit S et T des ensembles, alors :

$$\texttt{a}: \quad T \subseteq S \stackrel{\text{def}}{=} (\forall e \mid e \in T \Rightarrow e \in S) \qquad \textit{(Inclusion)}$$
$$\texttt{b}: \quad T \subset S \stackrel{\text{def}}{=} T \subseteq S \wedge (\exists e \mid e \in S \wedge e \notin T) \qquad \textit{(Inclusion stricte)}$$

Les opérateurs "$\supseteq$" et "$\supset$" désignent l'inclusion inverse et l'inclusion inverse stricte :

$$T \supseteq S \stackrel{\text{def}}{=} S \subseteq T \quad \text{et} \quad T \supset S \stackrel{\text{def}}{=} S \subset T\,.$$

De même, pour indiquer la négation d'une expression ensembliste d'inclusion, on peut apposer une barre oblique sur le symbole d'inclusion. Ainsi, nous obtenons les équivalences suivantes :

$$\begin{aligned} T \nsubseteq S &\stackrel{\text{def}}{=} \neg(T \subseteq S), \qquad T \not\subset S \stackrel{\text{def}}{=} \neg(T \subset S), \\ T \nsupseteq S &\stackrel{\text{def}}{=} \neg(T \supseteq S), \qquad T \not\supset S \stackrel{\text{def}}{=} \neg(T \supset S)\,. \end{aligned}$$

Ensemble puissance

L'**ensemble puissance** $\mathcal{P}(S)$ de l'ensemble S contient tous les sous-ensembles possibles de l'ensemble S. Dans la définition ci-dessous, il faut bien comprendre que l'élément E s'avère être un ensemble.

Définition 1.2.6. *Définition de l'ensemble puissance.*
Soit S un ensemble, alors :

$$\mathcal{P}(S) \stackrel{\text{def}}{=} \{E \mid E \subseteq S\}.$$

Voici des exemples d'ensembles puissances :

$$\begin{aligned} \mathcal{P}(\{1,2,3\}) &= \{\,\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\,\}\,, \\ \mathcal{P}(\{42\}) &= \{\,\emptyset, \{42\}\,\}\,, \\ \mathcal{P}(\emptyset) &= \{\,\emptyset\,\}\,. \end{aligned}$$

Remarquons que l'ensemble puissance de n'importe quel ensemble S contient l'ensemble vide $\emptyset$ comme élément, parce que l'ensemble vide est nécessairement sous-ensemble de l'ensemble S. De même, l'ensemble puissance de l'ensemble vide n'est pas égal à l'ensemble vide ($\mathcal{P}(\emptyset) \neq \emptyset$). Il s'agit plutôt d'un ensemble contenant un élément : $|\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1$.

Priorité des opérateurs

La table 1.3 présente la priorité des opérateurs qui est utilisée lors de la construction d'une expression ensembliste. Un opérateur ayant une priorité élevée est évalué avant un opérateur ayant une priorité faible, à moins que l'usage de parenthèses indique un autre ordre d'évaluation.

Insistons sur le fait que les opérateurs booléens possèdent une priorité plus faible que les

TABLE 1.3 – Priorité des opérateurs ensemblistes.

Symbole(s)	Nom(s)	
c	Complément	*(priorité élevée)*
$\setminus$	Différence	
$\cap \ \cup$	Intersection, Union	
$\subseteq \ \subset$	Inclusion, Inclusion stricte	
$\in \ =$	Appartenance, Égalité	
Opérateurs booléens (voir table 1.1, page 11)		*(priorité faible)*

opérateurs ensemblistes. Par exemple, les deux expressions suivantes sont équivalentes :

$$\begin{aligned} & A \subseteq B \cup C \Rightarrow e \in A \wedge (e \in T \vee e \in U) \\ \Leftrightarrow \quad & [\, A \subseteq (B \cup C)\,] \Rightarrow [\ (e \in A) \wedge (\,(e \in T) \vee (e \in U)\,)\ ]\,. \end{aligned}$$

1.2.6 Propriétés des opérateurs et démonstrations

Cette section présente plusieurs propriétés des opérateurs ensemblistes définis à la section précédente. De même, nous présentons les démonstrations de quelques-unes de ces propriétés. Nous verrons d'abord comment faire une démonstration par cas à l'aide de diagrammes de Venn. Les démonstrations par diagramme de Venn sont à la théorie des ensembles ce que les démonstrations par tables de vérité sont à algèbre booléenne. Ensuite, nous présenterons des démonstrations par succession d'équivalences. Cette technique sera très similaire à celle que nous avons vue dans la section 1.1.4 sur l'algèbre booléenne.

Lois de De Morgan et démonstration par diagrammes de Venn

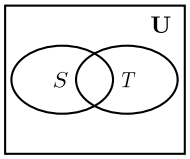
Les premières propriétés des opérateurs booléens que nous avons présentées sont les lois de De Morgan (proposition 1.1.4, page 13). Nous présentons maintenant les **lois de De Morgan** appliquées aux ensembles. Il est intéressant de remarquer que, dans cette nouvelle proposition, l'intersection "$\cap$" vient remplacer la conjonction "$\wedge$", l'union "$\cup$" vient remplacer la disjonction "$\vee$" et le complément "^{c}" vient remplacer la négation "$\neg$".

Proposition 1.2.7. *Lois de De Morgan (version ensembliste).*
Soit S un ensemble, alors les égalités suivantes sont vraies :

a :	$(S \cap T)^c$	$=$	$S^c \cup T^c$	*(Première loi de De Morgan)*
b :	$(S \cup T)^c$	$=$	$S^c \cap T^c$	*(Deuxième loi de De Morgan)*

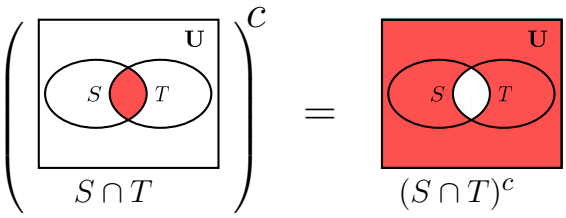
À la section 1.1.2, nous avons vu qu'il est possible de démontrer les propriétés des opérateurs booléens en énumérant toutes les possibilités à l'aide d'une table de vérité. Similairement, nous pouvons démontrer les propriétés des opérateurs ensemblistes à l'aide de diagrammes de Venn. Dans les deux contextes, il s'agit de la technique de **démonstration par cas**. Nous en donnons ici un exemple en démontrant la version ensembliste de la première loi de De Morgan.

Démonstration de la première loi de De Morgan. (Proposition 1.2.7-a)
Soit S et T deux ensembles. Démontrons "$(S \cap T)^c = S^c \cup T^c$" à l'aide de diagrammes de Venn. Considérons la représentation suivante des ensembles S et T :

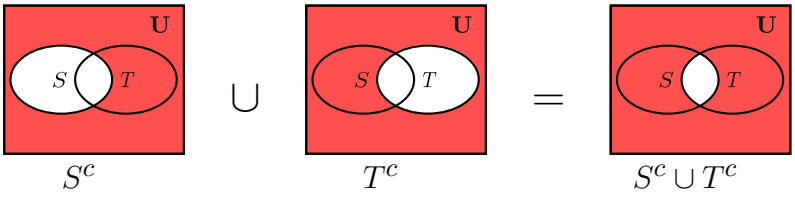


Il s'agit de la représentation la plus générale de deux ensembles, car elle contient tous les cas possibles[17], c'est-à-dire qu'un élément peut soit : appartenir simultanément à S et T, appartenir à S mais pas à T, appartenir à T mais pas à S ou n'appartenir ni à S et ni à T.

Bâtissons d'abord l'ensemble "$(S \cap T)^c$" :



Bâtissons ensuite l'ensemble "$S^c \cup T^c$" :



Les diagrammes de Venn obtenus montrent bien que les éléments appartenant à "$(S \cap T)^c$" sont les mêmes que les éléments appartenant à l'ensemble "$S^c \cup T^c$". **C.Q.F.D.**

17. Nous voyons ici qu'une démonstration par diagramme de Venn est, sous la forme d'un diagramme, une démonstration par cas, tout comme une démonstration par table de vérité est une démonstration par cas en algèbre booléenne.

Le lecteur est invité à démontrer la version ensembliste de la deuxième loi de De Morgan (proposition 1.2.7-b) à l'aide de la même technique.

Propriétés du complément, de l'intersection, de l'union et de la différence

Les prochaines propositions énumèrent les propriétés des quatre opérateurs ensemblistes présentés par la définition 1.2.4 (page 41). Remarquons que ces propriétés sont directement issues des opérateurs booléens que nous avons présentés à la section 1.1.3.

Proposition 1.2.8. *Propriétés du complément.*
Soit S un ensemble, alors les égalités suivantes sont vraies :

a :	$(S^c)^c$	$=$	S	*(Complémentarité)*
b :	$S \cup S^c$	$=$	$\mathbf{U}$	*(Tiers exclu)*
c :	$S \cap S^c$	$=$	$\emptyset$	*(Contradiction)*

Proposition 1.2.9. *Propriétés de l'intersection.*
Soit S, T et U des ensembles, alors les égalités suivantes sont vraies :

a :	$S \cap \mathbf{U}$	$=$	S	*(Élément neutre)*
b :	$S \cap \emptyset$	$=$	$\emptyset$	*(Élément absorbant)*
c :	$S \cap S$	$=$	S	*(Idempotence)*
d :	$S \cap T$	$=$	$T \cap S$	*(Commutativité)*
e :	$(S \cap T) \cap U$	$=$	$S \cap (T \cap U)$	*(Associativité)*
f :	$(S \cup T) \cap U$	$=$	$(S \cap U) \cup (T \cap U)$	*(Distributivité)*

Proposition 1.2.10. *Propriétés de l'union.*
Soit S, T et U des ensembles, alors les égalités suivantes sont vraies :

a :	$S \cup \emptyset$	$=$	S	*(Élément neutre)*
b :	$S \cup \mathbf{U}$	$=$	$\mathbf{U}$	*(Élément absorbant)*
c :	$S \cup S$	$=$	S	*(Idempotence)*
d :	$S \cup T$	$=$	$T \cup S$	*(Commutativité)*
e :	$(S \cup T) \cup U$	$=$	$S \cup (T \cup U)$	*(Associativité)*
f :	$(S \cap T) \cup U$	$=$	$(S \cup U) \cap (T \cup U)$	*(Distributivité)*

Proposition 1.2.11. *Propriétés de la différence.*
Soit S, T et U des ensembles, alors les égalités suivantes sont vraies :

a :	$S \setminus \emptyset$	$=$	S	*(Élément neutre)*
b :	$S \setminus T$	$=$	$S \cap T^c$	*(Réécriture de la différence)*
c :	$S \cup (T \setminus S)$	$=$	$S \cup T$	*(Union d'une différence)*
d :	$S \cap (T \setminus S)$	$=$	$\emptyset$	*(Intersection d'une différence)*
e :	$S \setminus (T \cup U)$	$=$	$(S \setminus T) \cap (S \setminus U)$	*(Différence d'une union)*
f :	$S \setminus (T \cap U)$	$=$	$(S \setminus T) \cup (S \setminus U)$	*(Différence d'une intersection)*

Démonstrations par succession d'équivalences

Étant donné que nous avons défini les opérateurs ensemblistes en nous basant sur les opérateurs booléens, les propriétés ci-haut se démontrent aisément en référant aux propriétés des opérateurs booléens déjà démontrées à la section 1.1.3. En guise d'exemple, nous présentons ci-bas la démonstration de la distributivité de l'intersection et la démonstration de la distributivité de l'union sous la forme d'une **démonstration par succession d'équivalences**.

La proposition suivante nous aidera à faire le pont entre les propriétés des opérateurs ensemblistes et les propriétés des opérateurs booléens. Les propriétés présentées à la proposition 1.2.12 découlent directement de la définition des opérateurs ensemblistes (définition 1.2.4, page 41) et de l'axiome d'extensionnalité (définition 1.2.1, page 33).

Proposition 1.2.12. *Appartenance d'un élément à un ensemble obtenu par opérations ensemblistes.*
Soit S et T des ensembles et soit e un élément, alors :

a :	$e \in S^c$	$\Leftrightarrow$	$\neg(e \in S)$	*(Complément)*
b :	$e \in S \cap T$	$\Leftrightarrow$	$e \in S \wedge e \in T$	*(Intersection)*
c :	$e \in S \cup T$	$\Leftrightarrow$	$e \in S \vee e \in T$	*(Union)*
d :	$e \in S \setminus T$	$\Leftrightarrow$	$e \in S \wedge \neg(e \in T)$	*(Différence)*

Nous allons maintenant démontrer deux propriétés en procédant par successions d'équivalences, en commençant par la propriété de distributivité de l'intersection. L'étape clé de cette démonstration est l'utilisation de la distributivité de la conjonction (propriété 1.1.6), un résultat déjà démontré (voir page 16). La deuxième démonstration est celle de la propriété de distributivité de l'union. La démarche employée est très semblable à celle de la démonstration de la distributivité de l'intersection. Il est donc intéressant ici de constater que le fait de bien comprendre la "mécanique" d'une démonstration d'un énoncé mathématique peut parfois nous aider à démontrer d'autres énoncés mathématiques similaires.

Démonstration de la distributivité de l'intersection. (Proposition 1.2.9-f)
Soit S, T et U des ensembles. Nous voulons démontrer "$(S \cup T) \cap U = (S \cap U) \cup (T \cap U)$". Par l'axiome d'extensionnalité (définition 1.2.1, avec $[S := (S \cup T) \cap U]$ et $[T := (S \cap U) \cup (T \cap U)]$), nous savons que cela est équivalent à démontrer :

$$(\forall e \mid e \in (S \cup T) \cap U \Leftrightarrow e \in (S \cap U) \cup (T \cap U)) .$$

Soit e un élément quelconque. [18]
Démontrons "$e \in (S \cup T) \cap U \Leftrightarrow e \in (S \cap U) \cup (T \cap U)$" :

$$\begin{array}{ll}
& e \in (S \cup T) \cap U \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-b – Intersection, avec } [S := S \cup T] \textit{ et } [T := U] \rangle \\
& e \in (S \cup T) \wedge e \in U \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-c – Union} \rangle \\
& (e \in S \vee e \in T) \wedge e \in U \\
\Leftrightarrow & \quad \left\langle \begin{array}{l} \textit{Prop 1.1.6-f – Distributivité de la conjonction, avec } [p := e \in S], [q := e \in T] \\ \textit{et } [r := e \in U] \end{array} \right\rangle \\
& (e \in S \wedge e \in U) \vee (e \in T \wedge e \in U) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-b – Intersection, 2 fois} \rangle \\
& e \in (S \cap U) \vee (e \in T \cap U) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-c – Union, avec } [S := S \cap U] \textit{ et } [T := T \cap U] \rangle \\
& e \in (S \cap U) \cup (T \cap U) .
\end{array}$$

C.Q.F.D.

Démonstration de la distributivité de l'union. (Proposition 1.2.10-f)
Soit S, T et U des ensembles. Nous voulons démontrer "$(S \cap T) \cup U = (S \cup U) \cap (T \cup U)$". Par l'axiome d'extensionnalité (définition 1.2.1, avec $[S := (S \cap T) \cup U]$ et $[T := (S \cup U) \cap (T \cup U)]$), nous savons que cela est équivalent à démontrer :

$$(\forall e \mid e \in (S \cap T) \cup U \Leftrightarrow e \in (S \cup U) \cap (T \cup U)) .$$

Soit e un élément quelconque.
Démontrons donc "$e \in (S \cap T) \cup U \Leftrightarrow e \in (S \cup U) \cap (T \cup U)$" :

$$\begin{array}{ll}
& e \in (S \cap T) \cup U \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-c – Union, avec } [S := S \cap T] \textit{ et } [T := U] \rangle \\
& e \in (S \cap T) \vee e \in U
\end{array}$$

18. Incursion dans le chapitre suivant. Oui, c'est comme ça qu'on démontre un énoncé qui commence par $\forall$, on se donne un e. Nous y reviendrons !

$\Leftrightarrow$ $\langle$ *Prop 1.2.12-b – Intersection* $\rangle$

$(e \in S \wedge e \in T) \vee e \in U$

$\Leftrightarrow$ $\left\langle \begin{array}{l} \textit{Prop 1.1.7-f – Distributivité de la disjonction, avec } [p := e \in S],\ [q := e \in T] \\ \textit{et } [r := e \in U] \end{array} \right\rangle$

$(e \in S \vee e \in U) \wedge (e \in T \vee e \in U)$

$\Leftrightarrow$ $\langle$ *Prop 1.2.12-c – Union, 2 fois* $\rangle$

$e \in (S \cup U) \wedge (e \in T \cup U)$

$\Leftrightarrow$ $\langle$ *Prop 1.2.12-b – Intersection, avec* $[S := S \cup U]$ *et* $[T := T \cup U]$ $\rangle$

$e \in (S \cup U) \cap (T \cup U)$.

C.Q.F.D.

La technique de démonstration par succession d'équivalences peut être utilisée pour démontrer toutes les propriétés des opérateurs ensemblistes rencontrées jusqu'à maintenant.

Propriétés des opérateurs d'inclusions

Les propriétés suivantes permettent de réécrire certaines expressions ensemblistes comprenant des opérateurs d'inclusion (voir la définition 1.2.5, page 42). Insistions sur la première propriété, qui stipule que l'ensemble vide $\emptyset$ est un sous-ensemble de tous les ensembles possibles.

Proposition 1.2.13. *Propriétés d'équivalences de l'inclusion.*
Soit S, T et U des ensembles, on a :

a :	$\emptyset \subseteq S$		*(Omniprésence de l'ensemble vide)*
b :	$S \subseteq S$		*(Réflexivité)*
c :	$\neg(S \subset S)$		*(Irréflexivité)*
d :	$S = T \Leftrightarrow$	$S \subseteq T \wedge T \subseteq S$	*(Antisymétrie)*
e :	$S \subseteq T \Leftrightarrow$	$S \subset T \vee S = T$	*(Réécriture de l'inclusion)*
f :	$S \subset T \Leftrightarrow$	$S \subseteq T \wedge T \neq S$	*(Réécriture de l'inclusion stricte)*

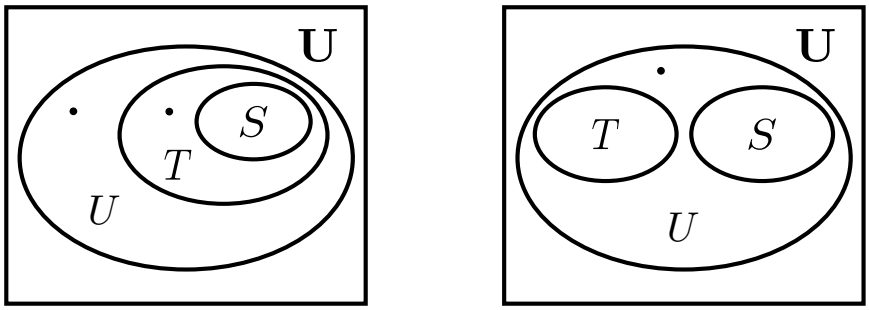
La propriété d'antisymétrie (proposition 1.2.13-d) sera démontrée à la section 1.3.6 (page 62) portant sur les techniques de démonstration.

Alors que la proposition 1.2.13 présente des propriétés d'équivalence entre des expressions ensemblistes, la proposition qui suit présente des implications. Ainsi, pour chacune de ces propriétés, le fait que l'expression à gauche de l'implication soit vraie permet de déduire le

terme à droite de l'implication. Par contre, si le terme de droite est vrai, on ne peut rien déduire du terme de gauche. La figure 1.4 illustre ce phénomène par deux diagrammes de Venn en prenant comme exemple la propriété de transitivité (proposition 1.2.14-h).

Proposition 1.2.14. *Propriétés d'implications de l'inclusion.*
Soit S, T et U des ensembles, alors les implications suivantes sont vraies :

`a :`	$S \subset T$	$\Rightarrow$	$S \subseteq T$	
`b :`	$S \subset T$	$\Rightarrow$	$T \nsubseteq S$	
`c :`	$S \subset T$	$\Rightarrow$	$T \not\subset S$	
`d :`	$S \subset T \wedge U \nsubseteq T$	$\Rightarrow$	$U \nsubseteq S$	
`e :`	$S \subseteq T \wedge T \subseteq U$	$\Rightarrow$	$S \subseteq U$	*(Transitivité (1))*
`f :`	$S \subseteq T \wedge T \subset U$	$\Rightarrow$	$S \subset U$	*(Transitivité (2))*
`g :`	$S \subset T \wedge T \subseteq U$	$\Rightarrow$	$S \subset U$	*(Transitivité (3))*
`h :`	$S \subset T \wedge T \subset U$	$\Rightarrow$	$S \subset U$	*(Transitivité (4))*



(a) $S \subset T \wedge T \subset U \Rightarrow S \subset U$ (b) $\neg(S \subset T \wedge T \subset U \Leftarrow S \subset U)$

FIGURE 1.4 – Le diagramme de gauche illustre la transitivité (prop. 1.2.14-h). Le diagramme de droite illustre un cas où cette propriété ne peut pas être inversée (le fait que $S \subset U \Leftrightarrow$ `vrai` n'implique pas que $S \subset T \Leftrightarrow$ `vrai`).

1.2.7 Exercices sur la logique du premier ordre

Exercice 1
Définissez des prédicats et fonctions appropriées (pensez-y d'abord sans l'indice [19]) et formalisez ensuite les phrases suivantes

1. Tout le monde aime Léo.
2. Léo aime quelqu'un.
3. Léo n'aime personne
4. Tout le monde aime tout le monde
5. Quelqu'un aime tout le monde
6. Tout le monde s'aime lui-même
7. Personne n'aime tout le monde
8. Quelqu'un n'aime personne

Exercice 2
Est-ce que les situations suivantes sont possibles ? Justifiez.

1. $(\forall x \in E \mid P(x))$ est vrai, mais $\neg(\exists x \in E \mid \neg P(x))$ est faux
2. $(\exists x \in E \mid P(x))$ est vrai, mais $\neg(\forall x \in E \mid \neg P(x))$ est faux
3. $(\forall x \in E \mid P(x)) \Rightarrow (\exists x \in E \mid P(x))$ est faux
4. $(\exists x \in E \mid P(x)) \Rightarrow (\forall x \in E \mid P(x))$ est vrai

Exercice 3
Trouvez un ensemble E et un prédicat P tel que $(\exists x \in E \mid P(x)) \Rightarrow \neg(\forall x \in E \mid P(x))$ est vrai. Est-ce que cette expression est toujours vraie ?

Exercice 4
Quelle est la différence entre chaque paire d'expressions suivante ? s'il y a une différence, trouver un exemple de phrase, en français, qui l'illustre

1. $(\forall x \in E \mid \neg P(x))$ et $\neg(\forall x \in E \mid P(x))$?
2. $(\exists x \in E \mid \neg P(x))$ et $\neg(\exists x \in E \mid P(x))$?
3. $(\forall x \mid x \in E \Rightarrow P(x))$ et $(\forall x \mid x \in E \wedge P(x))$?
4. $(\exists x \mid x \in E \Rightarrow P(x))$ et $(\exists x \mid x \in E \wedge P(x))$?

Confrontez 3 et 4 à la définition 1.2.2.

19. Prenons l'ensemble P des *Personnes*, précisons que Léo $\in P$ et prenons le prédicat à deux variables : $aime(x, y)$ qui pourrait aussi être écrit "x aime y"

Exercice 5

Éliminez les négations devant les parenthèses

1. $\neg(\forall x \in E \mid P(x))$
2. $\neg(\exists x \in E \mid \neg P(x))$
3. $\neg(\exists x \in E \mid x$ aime Léo$)$
4. $\neg((\forall x \in E \mid x > 3) \wedge (\exists x \in E \mid 5 - x > 0))$
5. $\neg(\forall x \in E \mid (\exists y \in F \mid x < y))$

Exercice 6

Écrivez en logique :

— Un nombre pair multiplié par un nombre impair donne un nombre pair. Vous pouvez utiliser les prédicats pair(z) et impair(z) suivants, pour $z \in \mathbb{Z}$:

$$\text{pair}(z) \stackrel{\text{def}}{=} (\exists k \in \mathbb{Z} \mid z = 2k)$$
$$\text{impair}(z) \stackrel{\text{def}}{=} (\exists k \in \mathbb{Z} \mid z = 2k + 1)$$

— Un truc bien connu pour savoir si un nombre se divise par 9 : additionner les chiffres de sa représentation en base 10 et évaluer si ce nombre se divise par 9. Écrivez cet énoncé pour les nombres positifs de 2 chiffres (par exemple 21, 34, 99), c'est-à-dire : un nombre est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. Ces nombres s'écrivent sous la forme $10d+u$ où $d, u \in \{0, 1, 2, \ldots, 9\}$ (la dizaine et l'unité). Rappelons la définition du modulo, pour 9 (c.-à-d. le reste de la division par 9), pour un $n \in \mathbb{N}$:

$$(n \bmod 9 = r) \stackrel{\text{def}}{=} (r \in \{0, 1, 2, \ldots, 8\}) \wedge (\exists k \in \mathbb{N} \mid n = 9k + r).$$

Un nombre n est donc divisible par 9 si $n \bmod 9 = 0$.

1.2.8 Exercices sur les ensembles

Exercice 1 : Définissez les ensembles suivants par compréhension :

a) l'ensemble des entiers non négatifs plus petits que 4 ;

b) l'ensemble des entiers strictement positifs divisibles par 3 et plus petits que 4 ;

c) l'ensemble des nombres impairs ;

d) l'ensemble des carrés dont la racine est située entre 10 et 22 ;

e) l'ensemble des puissances de 2.

Exercice 2 : Donnez une description en *langue française* des ensembles suivants :

a) $\{x \in \mathbb{Z} \mid 0 < x \wedge x \text{ est pair}\}$;

b) $\{x \in \mathbb{N}^* \mid 0 < x \wedge x \bmod 2 = 0\}$;

c) $\{p \mid q \in \mathbb{Z} \wedge r = 2 \wedge p > 0 \wedge p = q \cdot r\}$;

d) $\{z \in \mathbb{N}^* \mid (\exists y \in \mathbb{Z} \mid 2y = z)\}$;

e) $\{z \in \mathbb{Z} \mid -1 < z \wedge (\exists x \in \mathbb{Z} \mid z = x \cdot y) \wedge (y = 2 \vee y = 3)\}$;

f) $\{z \in \mathbb{Z} \mid -1 < x \wedge 1 < y < 4 \wedge z = x \cdot y\}$.

Exercice 3 :

a) Définissez l'ensemble suivant par compréhension. L'ensemble des nombres premiers compris entre 10 et 30. Vous pouvez utiliser la fonction booléenne premier(i) qui retourne la valeur de l'expression "i est un nombre premier", c'est-à-dire `vrai` si i est premier, `faux` sinon.

b) Décrivez l'ensemble suivant en français.

$$\{x \mid y \in \mathbb{N} \wedge z \in \{2, 3\} \wedge x = y^z\}$$

Exercice 4 : Soit l'ensemble de couleurs $C = \{\texttt{rouge}, \texttt{vert}, \texttt{bleu}\}$. Écrivez les ensembles suivants en extensions :

a) $\mathcal{P}(C)$;

b) $\mathcal{P}(C) \cap \emptyset$;

c) $\mathcal{P}(C) \cap \mathcal{P}(\emptyset)$;

d) $\{c \in \mathcal{P}(C) \mid 2 > |c|\}$;

e) $\{c \in \mathcal{P}(C) \mid c \subseteq \{\texttt{rouge}, \texttt{bleu}\}\}$;

f) $\{c \in \mathcal{P}(C) \mid \{\texttt{rouge}, \texttt{bleu}\} \subseteq c\}$.

Exercice 5 : Démontrez chacune des propriétés suivantes à l'aide des deux techniques de démonstration vues jusqu'à maintenant, c'est-à-dire (*i*) à l'aide de diagrammes de Venn (démonstration par cas) et (*ii*) par une succession d'équivalences :

a) Complémentarité (Proposition 1.2.8-a) : $(S^c)^c = S$;

b) Deuxième loi de De Morgan appliquée aux ensembles (Proposition 1.2.7-b) : $(S \cup T)^c = S^c \cap T^c$;

c) Réécriture de la différence (Proposition 1.2.11-b) : $S \setminus T = S \cap T^c$.

d) Différence d'une union (Proposition 1.2.11-e) : $S \setminus (T \cup U) = (S \setminus T) \cap (S \setminus U)$;

1.3 Techniques de démonstration

> Le logicien : Tous les chats sont mortels. Socrate est mortel. Donc Socrate est un chat.
> Le vieux monsieur : [...] Socrate était donc un chat !
> Le logicien : La logique vient de nous le révéler.
>
> Eugène Ionesco, *Rhinocéros (1959)*

Dans les sections précédentes, nous avons introduit certaines techniques de démonstration, principalement les démonstrations par cas (dans les situations particulières des démonstrations à l'aide des tables de vérité et des diagrammes de Venn) et les démonstrations par successions d'équivalences. Ces types de démonstrations sont très "mécaniques" (sauf peut-être celles par diagramme de Venn). En effet, on peut concevoir sans trop de difficultés des algorithmes permettant de vérifier si telle ou telle démonstration est valide ou non.

Les différentes démonstrations présentées dans cette section prennent davantage la forme d'un véritable texte français. Elles reposent sur les mêmes règles mathématiques que les démonstrations qu'on a vues jusqu'à maintenant, mais on y met davantage l'accent sur la signification des énoncés. Ainsi, ces démonstrations sont destinées à être lues (et comprises) par un humain plutôt qu'un ordinateur. Il s'agit d'une approche plus répandue en mathématique.

Les pages suivantes contiennent une série d'exemples et de stratégies pour effectuer une démonstration. Les démonstrations mathématiques consistent bien entendu en quelque chose de plus complexe que les exemples exposés ici. Cependant, ces derniers serviront de balises pour les démonstrations relativement simples qui seront demandées à l'intérieur de ce cours. Pour les démonstrations plus costaudes, vous n'aurez pas à les faire par vous-mêmes, mais seulement (et c'est déjà pas mal) à les comprendre.

L'approche présentée ici est basée principalement sur deux questions importantes :

1. Que faire si l'énoncé qu'on souhaite démontrer contient un quantificateur universel (c'est-à-dire un "$\forall$") ?
2. Que faire si l'énoncé qu'on souhaite démontrer contient un quantificateur existentiel (c'est-à-dire un "$\exists$") ?

Ce sont les idées les plus importantes, mais il faut quand même savoir quoi faire pour démontrer la conjonction "$\wedge$", la disjonction "$\vee$", l'implication "$\Rightarrow$" et le si et seulement si "$\Leftrightarrow$". Ces derniers se raisonnent plus intuitivement que "$\forall$" et "$\exists$".

Il importe d'être conscient qu'il n'existe pas de techniques de démonstration qui soient meilleures que d'autres, pourvu que toutes les démonstrations soient effectuées avec la même

rigueur mathématique. Pour un certain énoncé, il y aura parfois des démonstrations qu'on pourra juger plus "élégantes" que d'autres, parce qu'elles sont plus succinctes, plus faciles à comprendre ou qu'elles nous aident à comprendre le problème auquel on s'intéresse. Souvent, il s'agira d'une question de préférences personnelles. C'est à force de lire des démonstrations et d'en écrire soi-même qu'on développe un intérêt pour les "belles" démonstrations.

1.3.1 Structure des démonstrations d'un quantificateur universel "∀"

Supposons que nous devons démontrer une propriété de la forme suivante :

$$(\forall x \in X \mid P(x)\,).$$

Pour ce faire, il suffit de démontrer que pour une entité inconnue fixée x appartenant à l'ensemble X, on peut *déduire* que x satisfait P. Quand on dit une **entité inconnue**, on veut dire qu'on ne peut rien présumer sur elle (sauf le fait qu'elle appartient l'ensemble X). Quand on dit une **entité fixée**, on veut dire qu'on ne la changera pas en cours de route.

Ainsi, la démonstration d'un énoncé commençant par un quantificateur universel "∀" sera toujours structurée comme suit :

> **Démonstration de** $(\forall x \in X \mid P(x))$.
> Soit $x \in X$. $\langle$ *Montrons que* $P(x)$ *est vrai.* $\rangle$
> Alors pour telle raison *blablabla*. Ce qui implique *ceci et cela...*
> Et on peut finalement en conclure que $P(x)$ est vrai.
> **C.Q.F.D.**

Notez que la démonstration commence par une *"présentation" de la variable* x , de son type et, le cas échéant, de la ou les propriétés que nous savons que cette variable satisfait. C'est une étape essentielle. Dans une démonstration, on ne peut utiliser une variable qui n'a pas été "présentée", on doit d'abord s'entendre avec le lecteur sur ce qu'est cette inconnue. En échange, une fois cette étape faite, même si la valeur de la variable est inconnue, elle ne changera plus jusqu'à la fin de la démonstration. Autrement dit, une fois "présentée", une variable reste inconnue, mais ne varie plus. Vous verrez par la suite que le moment où on choisit ou prend une variable fait une différence. Les lettres **C.Q.F.D.** signifient "Ce qu'il fallait démontrer". Alors avant de les écrire, il est important de s'assurer que ce qu'on a fait est bien *ce qu'il fallait démontrer*.

Notez également que la démonstration se termine par le fait qu'après plusieurs étapes d'argumentation mathématiquement correctes, on en arrive à conclure que cette variable x

doit obligatoirement satisfaire la propriété P.

PENSEZ-Y!

Attention ! si le domaine d'un quantificateur universel est vide, l'énoncé est vrai ! C'est-à-dire que

$$(\forall x \in \emptyset \mid P(x)) \text{ est toujours vrai}$$

Un exemple serait : tous les chiens qui parlent sont noirs. Comme aucun chien ne parle, cette affirmation est vraie. Ça peut être bizarre, car c'est inutile de dire ça ; mais on peut convenir qu'on ne peut pas démontrer que c'est faux : si c'était faux, on pourrait trouver un chien qui parle, mais qui n'est pas noir. Notre intuition n'aime pas ça, car on s'est habitué à n'entendre que des affirmations utiles, donc non vides.

Une autre raison technique et mathématique pour l'encadré précédent est que l'élément neutre du ET (rappelons que le "pour tout" est un ET) est la constante `vrai`. Voici une analogie : l'élément neutre de la multiplication est 1, ce qui fait qu'on a choisi que $x^0 = 1$ (ne multiplier aucun x donne l'élément neutre de la multiplication) ; même principe pour l'addition avec l'élément neutre 0. Même principe pour le ET : faire le ET d'aucun élément, ça donne l'élément neutre.

Exemple 1.3.1. Démonstration de $(\forall x \in]0,1[\mid x^2 < x)$
Soit $x \in]0,1[$ $\langle$ *Montrons que* $x^2 < x$. $\rangle$
On a $x < 1$.
Comme $x > 0$, on peut multiplier de chaque côté de l'inégalité sans la changer.
Donc $x \cdot x < x$, c.-à-d. $x^2 < x$, comme voulu.
C.Q.F.D.

1.3.2 Structure des démonstrations d'un quantificateur existentiel "∃".

Supposons que nous voulons démontrer une expression de la forme suivante :

$$(\exists x \in X \mid P(x)\,).$$

Cela demande de trouver un élément x de l'ensemble X dont on est *sûr* de l'existence. Il

faut aussi choisir "intelligemment" ce x de telle sorte que ce x satisfasse aussi la propriété P.

Ainsi, la démonstration d'un énoncé commençant par un quantificateur existentiel "$\exists$" sera toujours structurée comme suit :

> **Démonstration de** $(\exists x \in X \mid P(x))$**.**
> Prenons x, choisi de *telle façon*. Un tel x existe et appartient à X car ...
> $\langle$ *Montrons que* $P(x)$ *est vrai.* $\rangle$
> Alors pour *telles et telles raisons*, on a donc *ceci et cela...*
> Ce qui nous permet de conclure que $P(x)$ est vrai.
> **C.Q.F.D.**

Notez qu'ici encore, on n'utilise pas une variable sans l'avoir préalablement *présentée*. Mais contrairement à la situation du quantificateur universel "$\forall$", on doit au moment de sa présentation *être sûr de l'existence* d'une telle variable (puisque l'affirmation est justement qu'elle *existe*). L'unique raison pour laquelle à la section 1.3.1 on ne se préoccupe pas de savoir si un tel x existe, c'est que s'il n'existe pas de $x \in X$, alors "$(\forall x \in X \mid P(x))$" est nécessairement vrai.

Exemple 1.3.2. Démonstration de $(\exists x \in \mathbb{N} \mid x^2 = 2x + 8)$
Prenons $x = 4$. Ce x existe, car $4 \in \mathbb{N}$. $\langle$ *Montrons que* $x^2 = 2x + 8$. $\rangle$
On a $4^2 = 16$ et $2 \cdot 4 + 8 = 16$.
Ainsi, $x^2 = 2x + 8$ comme désiré.
C.Q.F.D.

Voici un exemple de démonstration où on "oublie de vérifier que notre x est dans le bon ensemble". En fait l'énoncé est faux.

Exemple 1.3.3. Démonstration incorrecte de $(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$
Prenons $x = \frac{1}{2}$. On a bien que $\frac{1}{2}$ existe $\langle$ *Montrons que* $4x^2 = 4x - 1$. $\rangle$
On a $4(\frac{1}{2})^2 = 1$ et $4(\frac{1}{2}) - 1 = 1$.
Ainsi, $4x^2 = 4x - 1$.
C.Q.F.D. (INCORRECTE)

Ici, on a oublié de vérifier que notre x était dans le bon ensemble. Ce n'est pas le cas, $x \notin \mathbb{N}$. Une démonstration que cet énoncé est faux est demandée en exercice.

1.3.3 Démonstrations utilisant les propriétés de l'arithmétique

Dans ce cours, nous tiendrons toutes les **propriétés de l'arithmétique** pour acquises. Ainsi, les propriétés de base des opérateurs d'addition, de soustraction, de multiplication, de division sont supposées connues de tous et n'ont donc pas à être explicitement justifiées. Par exemple, nous savons tous que si n est un nombre naturel, $n+1$ est plus grand que n. Dans un tel cas, un simple commentaire de la forme "Propriété de l'arithmétique" suffira.

Il est toutefois important d'être rigoureux dans l'application de ces propriétés. Par exemple, attardons-nous à l'énoncé suivant :

$$(\forall n \in \mathbb{N} \mid (\exists m \in \mathbb{N} \mid m > n))\,.$$

Nous présentons une première tentative de démonstration incorrecte (qui peut sembler valide si on ne prend pas le temps d'y réfléchir suffisamment), puis une seconde démonstration qui est valide.

Démonstration (incorrecte) de $(\forall n \in \mathbb{N} \mid (\exists m \in \mathbb{N} \mid m > n))$.
Soit $n \in \mathbb{N}$. $\langle$ *Montrons* $(\exists m \in \mathbb{N} \mid m > n)$ $\rangle$
Soit m, un nombre qui est *plus grand que tout* nombre naturel. $\langle$ *Montrons* $m > n$ $\rangle$
Alors bien sûr, on a que $m > n$.
C.Q.F.D. (INCORRECTE)

Bien évidemment, ce qui cloche dans cette démonstration, c'est qu'il n'existe pas de tel nombre *magique* m. Cependant, si pour une raison ou une autre, on pouvait démontrer qu'un tel nombre existe, alors la démonstration deviendrait correcte. De façon similaire, il ne suffit pas de remplacer la deuxième ligne par "Soit m, un nombre plus grand que n" : c'est bien beau d'y croire, trouver que c'est évident ne le démontre pas, il faut exhiber ce nombre. Voici donc ce qu'il faut faire :

Démonstration (correcte) de $(\forall n \in \mathbb{N} \mid (\exists m \in \mathbb{N} \mid m > n))$**.**
Soit $n \in \mathbb{N}$. $\langle$ *Montrons* $(\exists m \in \mathbb{N} \mid m > n)$ $\rangle$
Prenons $m = n + 1$.[20] Par les propriétés de l'arithmétique, un tel m existe et $m \in \mathbb{N}$.
$\langle$ *Montrons* $m > n$ $\rangle$

20. On a écrit "Soit $m = n+1$" selon la façon habituelle en mathématiques, plutôt que "Soit $m := n+1$". Ici, il n'y a pas d'ambiguïté à le faire et le terme "Soit" indique que m reçoit une valeur (ce ne serait pas approprié mathématiquement d'écrire une expression comme $x = x+1$ puisque celle-ci serait toujours fausse) !

Alors bien sûr, on a que $m = n + 1 > n$. ⟨ *Propriété de l'arithmétique.* ⟩
C.Q.F.D.

Notez que le m qu'on a choisi ici est construit à partir du n qui avait préalablement été présenté, ce qui est tout à fait légal. On n'aurait cependant pas pu faire un tel argument si nous avions eu à démontrer "$(\exists m \in \mathbb{N} \mid (\forall n \in \mathbb{N} \mid m > n))$". D'ailleurs, ce dernier énoncé est faux, donc impossible à démontrer, nous nous en convaincrons plus loin.

1.3.4 Démonstrations avec un "$\neg\exists$" ou un "$\neg\forall$"

Que fait-on avec les énoncés contenant la négation d'un quantificateur existentiel "$\neg\exists$" ou la négation d'un quantificateur universel "$\neg\forall$" ? Il serait difficile de "présenter" une variable x qui "n'existe pas". La stratégie consiste à transformer la négation en énoncé positif, comme dans l'exemple qui suit. En fait, le raisonnement utilise une des lois de De Morgan généralisées, introduites à la proposition 1.2.3, page 40, que l'on rappelle ici :

$$\texttt{a}: \quad \neg(\forall x \in T \mid P(x)) \quad \Leftrightarrow \quad (\exists x \in T \mid \neg P(x)) \qquad \text{(Première loi de De Morgan)}$$
$$\texttt{b}: \quad \neg(\exists x \in T \mid P(x)) \quad \Leftrightarrow \quad (\forall x \in T \mid \neg P(x)) \qquad \text{(Deuxième loi de De Morgan)}$$

Débutons par une démonstration simple utilisant la première loi de De Morgan. Nous allons démontrer que l'énoncé suivant est faux :

"Tout nombre naturel au carré égale un."

Démonstration que $(\forall x \in \mathbb{N}^* \mid x^2 = 1)$ **est faux.**
On veut démontrer que le contraire de $(\forall x \in \mathbb{N}^* \mid x^2 = 1)$ est vrai.
Ainsi, on veut démontrer $\neg(\forall x \in \mathbb{N}^* \mid x^2 = 1)$.
Ce qui est équivalent à $(\exists x \in \mathbb{N}^* \mid x^2 \neq 1)$. ⟨ *Par la 1ere loi de De Morgan* ⟩
Prenons $x = 2$. Ce x existe, et $2 \in \mathbb{N}^*$. ⟨ *Montrons* $x^2 \neq 1$ ⟩
Comme $2^2 = 4$, on a $x^2 \neq 1$ comme voulu. **C.Q.F.D.**

L'objectif de la démonstration précédente est de montrer qu'un "pour tout" est faux. Dans ce cas, l'essentiel de la démonstration consiste à présenter un élément "x" qui appartient au domaine "$\mathbb{N}^*$", mais qui ne respecte pas l'expression "$x^2 = 1$". Insistons sur l'importance de *présenter* l'élément (ce que nous faisons en écrivant "Prenons $x = 2$"), comme dans toutes les démonstrations d'un "$\exists$", tel que vu à la section 1.3.2.

Présentons maintenant une démonstration utilisant la deuxième loi de De Morgan. Il s'agit de démontrer l'énoncé suivant :

> "Il n'est pas vrai qu'il existe un nombre naturel positif qui soit plus grand que son carré."

Notons que si ce naturel n'existe pas, c'est que tous les nombres naturels satisfont le contraire.

Démonstration de $\neg(\exists m \in \mathbb{N}^* \mid m > m^2)$.
Par la loi de De Morgan, on peut transformer l'énoncé en "$(\forall m \in \mathbb{N}^* \mid \neg(m > m^2))$", ou encore "$(\forall m \in \mathbb{N}^* \mid m \leq m^2)$. Démontrons donc ceci.

Soit $m \in \mathbb{N}^*$. ⟨ *on veut monter* $m \leq m^2$ ⟩
Alors on a $m \geq 1$. ⟨ *Par la définition de* $\mathbb{N}^*$ ⟩
En multipliant par m des deux côtés, on obtient $m \cdot m \geq 1 \cdot m$. ⟨ *Arithmétique* ⟩
Ce qui est équivalent à $m \leq m^2$.

C.Q.F.D.

Nous reverrons une démonstration similaire avec "$n \in \mathbb{N}$" (au lieu de "$n \in \mathbb{N}^*$"), quand nous verrons la technique de démonstration par cas, à la section 1.3.7, page 64.

Pour conclure cette section, voici une démonstration un peu plus complexe qui utilise à la fois la première et la deuxième loi de De Morgan.

Démonstration de $\neg(\exists m \in \mathbb{N} \mid (\forall n \in \mathbb{N} \mid m > n))$.
Nous devons démontrer $\neg(\exists m \in \mathbb{N} \mid (\forall n \in \mathbb{N} \mid m > n))$.
Ce qui est équivalent à démontrer $(\forall m \in \mathbb{N} \mid \neg(\forall n \in \mathbb{N} \mid n < m))$. ⟨ *De Morgan* ⟩
Ce qui est équivalent à démontrer $(\forall m \in \mathbb{N} \mid (\exists n \in \mathbb{N} \mid \neg(n < m)))$. ⟨ *De Morgan* ⟩
Ce qui est équivalent à démontrer $(\forall m \in \mathbb{N} \mid (\exists n \in \mathbb{N} \mid n \geq m))$. ⟨ *Arithmétique* ⟩
Démontrons donc $(\forall m \in \mathbb{N} \mid (\exists n \in \mathbb{N} \mid n \geq m))$.

Soit $m \in \mathbb{N}$. ⟨ *Pour ce* m *fixe, démontrons maintenant* $(\exists n \in \mathbb{N} \mid n \geq m)$. ⟩
Prenons $n = m + 1$. Un tel n existe et *est bien* un nombre de $\mathbb{N}$, car m l'est.
⟨ *Montrons* $n \geq m$ ⟩
Alors on a que $n = m + 1 \geq m$. ⟨ *Propriété de l'arithmétique* ⟩

C.Q.F.D.

Dans la démonstration précédente, on devait démontrer "$(\forall m \in \mathbb{N} \mid (\exists n \in \mathbb{N} \mid n \geq m))$" et on a :

1. Choisi un $m \in \mathbb{N}$ tout à fait quelconque (on a rien dit sur ce m hormis qu'il était dans $\mathbb{N}$) ;

2. Choisi un n, pas n'importe lequel, mais dont on était sûr de l'existence et de son appartenance à $\mathbb{N}$;
3. Grâce à une certaine séquence d'arguments mathématiquement corrects, on a réussi à démontrer que pour ce m et ce n, on a bien $n \geq m$.

Ce **Q**u'il **F**allait **D**émontrer.

1.3.5 Une démonstration avec une implication "⇒"

Pour démontrer "$P \Rightarrow Q$", il suffit de supposer que P est vrai et d'en déduire Q. Nous présentons un exemple d'une démonstration avec un quantificateur universel "∀".

Démonstration de "Pour tout (∀) ensemble S et T, on a $S \subseteq T \cup S$".
Soit S et T des ensembles.
On veut démontrer $(\forall e \mid e \in S \Rightarrow e \in T \cup S)$ ⟨ *Définition 1.2.5-a – Inclusion* ⟩
Soit e un élément quelconque. ⟨ *on veut montrer* $e \in S \Rightarrow e \in T \cup S$ ⟩
Supposons $e \in S$. ⟨ *montrons* $e \in T \cup S$ ⟩
Comme $e \in S$, alors "$e \in T$ ou $e \in S$" est vrai.
Donc on a $e \in T \cup S$. ⟨ *définition de* $T \cup S$ ⟩
C.Q.F.D.

Remarquez qu'au cours d'une démonstration il est très utile, et souvent essentiel pour ne pas s'embourber, d'*écrire* spécifiquement ce que nous sommes en train de démontrer dans cette étape. C'est ce qu'on fait ici lorsqu'on dit "on veut montrer $e \in S \Rightarrow e \in T \cup S$" et "montrons $e \in T \cup S$".

Une démonstration avec une implication inverse "⇐" se traite de la même façon, symétriquement : pour démontrer "$P \Leftarrow Q$", on suppose Q et on en déduit P.

1.3.6 Une démonstration avec un ssi "⇔" et en passant, un "∧"

Que fait-on avec les énoncés contenant un si et seulement si "⇔" ? Dans une démonstration par successions d'équivalences, ceci se démontre en une étape, mais, dans une démonstration plus "classique", il est commun de démontrer séparément "$P \Rightarrow Q$" et "$P \Leftarrow Q$". Nous basons notre technique de démonstration sur la définition de l'opérateur "si et seulement si"

(voir la définition 1.1.3 à la page 10) :

$$P \Leftrightarrow Q \quad \stackrel{\text{def}}{=} \quad (P \Rightarrow Q) \wedge (P \Leftarrow Q)\,.$$

La démonstration suivante est importante, car c'est cette propriété qui nous permet de démontrer que deux ensembles sont égaux ssi ils sont inclus l'un dans l'autre, ce qui rend souvent les démonstrations d'égalité d'ensembles plus faciles.

Démonstration de l'antisymétrie de l'inclusion. (Propriété 1.2.13-d)
Soit S et T des ensembles. Nous voulons démontrer $S \subseteq T \wedge T \subseteq S \;\Leftrightarrow\; S = T$.

$\boxed{\Rightarrow :}$ Supposons ($\heartsuit$) $S \subseteq T \wedge T \subseteq S$. ⟨ *on veut démontrer* $(\forall e \mid e \in S \Leftrightarrow e \in T)$ ⟩
Soit e. ⟨ *on veut démontrer* (†) $e \in S \Leftrightarrow e \in T$ ⟩
$\boxed{\Rightarrow :}$ Supposons que $e \in S$ alors par ($\heartsuit$) on a $S \subseteq T$
donc $e \in T$, comme voulu. ⟨ *le "⇒" de* (†) *est démontré* ⟩
$\boxed{\Leftarrow :}$ Supposons que $e \in T$ alors par ($\heartsuit$) on a $T \subseteq S$
donc $e \in S$. ⟨ *le "⇐" de* (†) *est démontré* ⟩

⟨ ⇒ *est démontré* ⟩

$\boxed{\Leftarrow :}$ Supposons $S = T$, c.-à-d., ($\heartsuit\heartsuit$) $(\forall e \mid e \in S \Leftrightarrow e \in T)$. ⟨ *on veut* $S \subseteq T \wedge T \subseteq S$ ⟩
Pour démontrer un ET, on démontre les deux composantes séparément.
— Démontrons $S \subseteq T$. ⟨ *c'est-à-dire* $(\forall e \mid e \in S \Rightarrow e \in T)$ ⟩
Soit e, et supposons $e \in S$.
Par ($\heartsuit\heartsuit$), on a $e \in T$, comme voulu.

— Démontrons $T \subseteq S$. ⟨ *c'est-à-dire* $(\forall e \mid e \in T \Rightarrow e \in S)$ ⟩
Soit e, et supposons $e \in T$.
Par ($\heartsuit\heartsuit$), on a $e \in S$, comme voulu.

⟨ ⇐ *est démontré* ⟩

Conclusion, nous avons bien démontré les 2 directions de ⇔.

C.Q.F.D.

Dans la 2e partie de la démonstration précédente, on veut démontrer $S \subseteq T \wedge T \subseteq S$. On y suit la technique de démonstration pour un "∧" qui est schématisée comme suit :

Démonstration de $P \wedge Q$
Démonstration P.
Démonstration de Q.

C.Q.F.D.

Dans la démonstration précédente, nous avons aussi utilisé des énoncés, (♡) et (♡♡) pour argumenter. On le fait pour des hypothèses qu'on se donne (ici en démontrant une implication) ou pour utiliser des théorèmes déjà démontrés. Ici encore, on fait une déduction en utilisant le syllogisme d'Aristote. Plus précisément, dans la démonstration précédente, nous avons, disons-le comme ceci : *utilisé un* $\forall$. En effet, par (♡♡), et par le fait que $e \in S$ nous avons déduit que $e \in T$.

1.3.7 Démonstration par cas, dont le "$\vee$"

Il arrive qu'on ne réussisse pas à démontrer l'énoncé "$(\forall x \in X \mid P(x))$", *d'un seul coup* pour tous les x. Alors, on peut faire une **démonstration par cas** : on choisit des ensembles $X_1, X_2, X_3, \ldots$ dont l'union est l'ensemble domaine X (il faut en être certain !) et on vérifie séparément chacune des expressions suivantes :

$$(\forall x \in X_1 \mid P(x)),\ (\forall x \in X_2 \mid P(x)),\ (\forall x \in X_3 \mid P(x)),\ \ldots$$

C'est le cas dans la démonstration suivante, dont nous avons démontré un seul cas à la section 1.3.4, en page 60. Notons que nous pouvons *séparer notre domaine* à tout moment d'une démonstration : il n'est pas nécessaire de réécrire toutes les expressions $(\forall x \in X_i \mid P(x)))$. Dans la démonstration suivante, on le voit par le fait que "Soit $m \in \mathbb{N}$" n'apparaît qu'une fois, au début, et les cas séparent ensuite le domaine. L'utilisation est similaire dans la démonstration qui suivra.

Démonstration de $\neg(\exists m \in \mathbb{N} \mid m > m^2)$**.**
Nous devons démontrer :

"Il n'est pas vrai qu'il existe un m naturel qui soit plus grand que son carré."

Si ce naturel n'existe pas, c'est que tous les nombres satisfont le contraire.
Par la loi de De Morgan, on peut transformer l'énoncé en "$(\forall m \in \mathbb{N} \mid \neg(m > m^2))$", ou encore "$(\forall m \in \mathbb{N} \mid m \leq m^2)$. Démontrons donc ceci.

Soit $m \in \mathbb{N}$. ⟨ *on veut monter* $m \leq m^2$ ⟩
Distinguons deux cas :
Cas 1 : $m = 0$.
On a bien $m \leq m^2$, puisque $0 \leq 0^2$. ⟨ *Cas 1 démontré* ⟩
Cas 2 : $m \in \mathbb{N}^*$.
Alors on a $m \geq 1$ ⟨ *Par la définition de* $\mathbb{N}^*$ ⟩

En multipliant par m des deux côtés, on obtient $m \cdot m \geq 1 \cdot m$ ⟨ *Arithmétique* ⟩
Ce qui est équivalent à $m \leq m^2$. ⟨ *Cas 2 démontré* ⟩

Puisque $\mathbb{N}^* \cup \{0\} = \mathbb{N}$, on a démontré que $m \leq m^2$ pour toutes les valeurs possibles de m.
C.Q.F.D.

Pourquoi a-t-on fait une démonstration par cas ici ? C'est que notre argument de multiplier par m chaque côté de "$0 \leq m$" n'aurait mené nulle part, ça aurait donné $0 \leq m^2$, ce n'est pas ce qu'on cherchait.

La démonstration par cas est aussi utile dans les circonstances suivantes : elle sert aussi à
— utiliser un OU donné par une hypothèse ou le domaine, comme dans la première partie de la démonstration suivante,
— démontrer un OU, comme dans la deuxième partie de la démonstration suivante.
Rappelons que nous avons déjà démontré cette propriété, la distributivité de l'union (propriété 1.2.10-f, page 46), en combinant des axiomes dans une série d'équivalences (voir la page 48). Bien que la démonstration présentée ici se révèle un peu plus longue, les démonstrations par cas sont parfois très concises.

Démonstration 2 de la distributivité de l'union. (Propriété 1.2.10-f)
Soit S et T des ensembles. Nous voulons démontrer :

$$S \cup (T \cap U) = (S \cup T) \cap (S \cup U)\,.$$

Utilisons l'antisymétrie de l'inclusion (propriété 1.2.13-d) et démontrons à tour de rôle chaque inclusion.

$\boxed{\subseteq :}$ Soit $s \in S \cup (T \cap U)$ ⟨ *on veut* $s \in (S \cup T) \cap (S \cup U)$ ⟩
Donc $s \in S$ ou $s \in (T \cap U)$: ce seront nos 2 cas, ils couvrent notre domaine :
Cas 1 $s \in S$:
alors $s \in S \cup T$ et $s \in S \cup U$ ⟨ *car* $S \subseteq S \cup T$ *et* $S \subseteq S \cup U$ *sont toujours vrais* ⟩
donc $s \in (S \cup T) \cap (S \cup U)$ ⟨ *1er cas démontré* ⟩
Cas 2 $s \in T \cap U$:
alors $s \in T$ et $s \in U$
donc $s \in S \cup T$ et $s \in S \cup U$ ⟨ *car* $T \subseteq S \cup T$ *et* $U \subseteq S \cup U$ ⟩
donc $s \in (S \cup T) \cap (S \cup U)$ ⟨ *2e cas démontré* ⟩

Les 2 cas ayant couvert toutes les possibilités, l'inclusion est démontrée [21].

21. Notez que pour le 2e cas, on aurait pu dire "$s \in (T \cap U) \setminus S$" pour avoir une vraie partition, mais c'est facultatif, puisque ce qui importe est que tous les s possibles soient vérifiés (ici certains le sont deux fois).

$\boxed{\supseteq :}$ Soit $s \in (S \cup T) \cap (S \cup U)$ $\langle$ *on veut* $s \in S \cup (T \cap U)$ $\rangle$
donc $s \in (S \cup T)$ et $s \in (S \cup U)$ $\langle$ *on veut* $s \in S$ *ou* $s \in T \cap U$ $\rangle$
Comme on veut démontrer un OU, allons-y en séparant le domaine selon $s \in S$.
Cas 1 $s \in S$:
alors $s \in S \cup (T \cap U)$ $\langle$ *1er cas démontré* $\rangle$
Cas 2 $s \notin S$:
alors $s \in T$ et $s \in U$ $\langle$ *Par hypothèse,* $s \in (S \cup T)$ *et* $s \in (S \cup U)$ $\rangle$
Donc $s \in T \cap U$.
alors $s \in S \cup (T \cap U)$ $\langle$ *2e cas démontré* $\rangle$

Comme $S \cup S^c$ donne l'ensemble universel $\mathbf{U}$, nous avons traité tous les cas. L'inclusion inverse est démontrée.

C.Q.F.D.

Vous trouvez que le 1er cas de $\boxed{\supseteq :}$ est trivial ? Eh oui, le 1er cas d'un OU à démontrer est toujours évident, c'est comme ça qu'on le choisit ! Dans la 2e partie de la démonstration précédente, on veut démontrer $s \in S \cup (T \cap U)$, ce qui est en fait équivalent à démontrer $s \in S \vee s \in (T \cap U)$. On y suit la technique de démonstration pour un "$\vee$" qui est schématisée comme suit :

Démonstration de $P \vee Q$.
Démonstration par cas
Cas 1, P est vrai Alors $P \vee Q$ est vrai (cas démontré).
Cas 2 : P est faux Alors pour telle et telle raison on déduit que Q est vrai.

C.Q.F.D.

1.3.8 Démonstrations par contradiction

Dans une démonstration, quand on arrive à une contradiction, on peut conclure que la *dernière* hypothèse qu'on a faite était fausse. Ceci arrive parfois dans une démonstration par cas (on conclut alors que le cas n'est pas possible et on passe au suivant). C'est ce même raisonnement qui nous permet de faire une **démonstration par contradiction** (aussi connue sous l'appellation *Reductio ad absurdum)* : on suppose que ce qu'on veut démontrer est faux, et on démontre que ça implique une contradiction. Ce genre de démonstration est basé sur l'équivalence (que vous pouvez vérifier par table de vérité) :

$$(\neg p \Rightarrow \texttt{faux}) \;\Leftrightarrow\; p\,.$$

Nous rencontrerons au fil de ces notes de cours quelques démonstrations importantes qui reposent sur cette technique, notamment la démonstration du théorème de Cantor dans la section sur les ensembles infinis (voir la section 1.5.6) et la démonstration du principe d'induction dans le chapitre sur les relations définies par récurrence (voir section 2.3).

Voici d'abord un premier exemple, plutôt simple, de démonstration par contradiction.

Démonstration : $(\forall x \in \mathbb{N}^* \mid x^2 \geq 1)$**.**
Démontrons l'énoncé par contradiction : supposons que le contraire est vrai.
Autrement dit, on suppose $\neg(\forall x \in \mathbb{N}^* \mid x^2 \geq 1)$, et on cherche une contradiction.
Ainsi, on a $(\exists x \in \mathbb{N}^* \mid x^2 < 1)$. ⟨ *Loi de De Morgan* ⟩
Soit $y \in \mathbb{N}^*$ choisi tel que $y^2 < 1$; Un tel y existe par la propriété énoncée à la ligne précédente.
Puisque $y \in \mathbb{N}^*$, on a nécessairement $y \geq 1$. ⟨ *Définition de l'ensemble* $\mathbb{N}^*$ ⟩
Donc, $y^2 \geq 1$. ⟨ *Propriété de l'arithmétique* ⟩
Nous avons à la fois $y^2 < 1$ et $y^2 \geq 1$, ce qui est une contradiction. Donc, on ne peut pas supposer $\neg(\forall x \in \mathbb{N}^* \mid x^2 \geq 1)$. **C.Q.F.D.**

Maintenant, illustrons la technique de démonstration par contradiction à l'aide d'un exemple plus compliqué, mais bien connu en mathématiques. Il s'agit de la démonstration que le nombre $\sqrt{2}$ est un nombre irrationnel, c'est-à-dire $\sqrt{2}$ ne peut pas s'écrire sous la forme d'une fraction $\frac{p}{q}$, où p et q sont deux entiers (avec q non nul). Autrement dit, $\sqrt{2} \notin \mathbb{Q}$, où $\mathbb{Q}$ est l'ensemble des nombres rationnels :

$$\mathbb{Q} \stackrel{\text{def}}{=} \left\{ \frac{x}{y} \mid x \in \mathbb{Z} \wedge y \in \mathbb{N}^* \right\}.$$

Démonstration : $\sqrt{2}$ **est un nombre irrationnel.**
Supposons le contraire, c'est-à-dire supposons que $\sqrt{2}$ est un nombre rationnel (autrement dit, $\sqrt{2} \in \mathbb{Q}$). ⟨ *Cherchons une contradiction* ⟩

Puisque $\sqrt{2}$ est rationnel, il peut être écrit comme une fraction irréductible.
⟨ *Propriétés de l'arithmétique* ⟩
Prenons $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $\frac{p}{q} = \sqrt{2}$ et tels que p et q n'ont aucun facteur commun autre que 1. ⟨ *De tels p et q existent par la définition d'irréductibilité d'une fraction* ⟩
Alors $\frac{p^2}{q^2} = 2$.
Ce qui implique $2 \cdot q^2 = p^2$. ⟨ *Arithmétique* ⟩
Donc p^2 est pair. ⟨ *Définition de "pair" et* q^2 *est un entier.* ⟩
Ce qui implique que $\underline{p \text{ est pair}}$. ⟨ *Comme démontré à l'exemple 1.3.5* ⟩

Prenons $p' \in \mathbb{Z}$ choisi tel que $p = 2 \cdot p'$. ⟨ *Un tel* p' *existe, car p est pair* ⟩

Alors $2 \cdot q^2 = (2 \cdot p')^2$.
Donc $2 \cdot q^2 = 4 \cdot (p')^2$.
Donc $q^2 = 2 \cdot (p')^2$. ⟨ *Arithmétique* ⟩
Donc q^2 est pair. ⟨ *Définition de "pair" et* $(p')^2$ *est un entier.* ⟩
Ce qui implique que q est pair. ⟨ *Comme démontré à l'exemple 1.3.5* ⟩

Puisque que p et q sont pairs, ils ont 2 comme facteur commun, ce qui est en *contradiction* avec nos choix initiaux de p et q (autrement dit, $\frac{p}{q}$ n'est pas une fraction irréductible).
Donc, on ne peut pas supposer que $\sqrt{2}$ est un nombre rationnel.
Ainsi, $\sqrt{2}$ est un nombre irrationnel. **C.Q.F.D.**

Pour finir cette section, nous allons démontrer qu'il existe une infinité de nombres premiers. Ce résultat mathématique est connu sous le nom de **théorème d'Euclide**. Bien que non récent (Euclide a vécu au 4e siècle avant notre ère), il s'agit d'un résultat impressionnant. Cela signifie, entre autres, qu'on ne pourra jamais répertorier tous les nombres premiers ; peu importe l'ordre de grandeur d'un nombre premier, il en existe toujours un autre plus grand ! Notons qu'il existe plusieurs démonstrations du théorème d'Euclide dans la littérature, utilisant des techniques variées[22]. Nous présentons ici une démonstration par contradiction similaire à la démonstration originale d'Euclide.

Nous aurons besoin de la propriété suivante :

> "Tout nombre naturel peut s'écrire comme un produit de nombre premier."

En effet, un nombre $x \in \mathbb{N}^*$ s'écrit comme le produit $1 \cdot x$ s'il est premier. Si x n'est pas premier, alors il existe deux nombres entiers y et z tels que $0 < y \leq z < x$ et $x = y \cdot z$. Si y et/ou z ne sont pas premier, il est possible de les exprimer à nouveau comme un produit de deux nombres, et ainsi de suite, jusqu'à n'obtenir que des nombres premiers.

Démonstration : il existe un nombre infini de nombres premiers.
Supposons le contraire, c'est-à-dire qu'il existe un nombre fini de nombres premiers.
⟨ *Cherchons une contradiction* ⟩
Posons P l'ensemble (fini) des nombres premiers.
Écrivons en extension ces nombres premiers :

$$P = \{p_1, p_2, \ldots, p_n\}, \quad \text{où } n = |P|.$$

22. Six de ces démonstrations, très différentes les unes des autres, sont présentées dans le livre *Proofs from THE BOOK* (Aigner et Ziegler, 2010), consacré aux démonstrations mathématiques qui se distinguent par leur élégance.

Considérons $k = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
On a que $k \notin P$, car k est strictement plus grand que tous les éléments de P.
Ainsi, k n'est pas un nombre premier.

⟨ *Car, par supposition, P contient tous les nombres premiers* ⟩

Donc il existe un nombre premier qui divise k.

⟨ *Car tout nombre naturel peut s'écrire comme un produit de nombre premier* ⟩

Soit $p_i \in P$ (où $i \in \{1, 2, \ldots, n\}$) un nombre premier qui divise k.

⟨ *Un tel nombre existe par l'argument précédent* ⟩

Par définition, le reste de la division de k par p_i est 0 (c'est-à-dire $k \bmod p_i = 0$).

Mais comme $k = p_i \cdot \big(p_1 \cdot p_2 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_n\big) + 1$,
on a également que le reste de la division de k par p_i est 1 (c'est-à-dire $k \bmod p_i = 1$).

Ce qui est une contradiction (le reste de la division de k par p_i ne peut être à la fois 0 et 1).

On ne peut donc supposer qu'il y a un nombre fini de nombres premiers,
c'est donc qu'il y en a un nombre infini. **C.Q.F.D.**

1.3.9 Autres façons d'attaquer une démonstration !

Comme dans les relations interpersonnelles, il n'est pas toujours recommandé d'attaquer une démonstration de front ! Il faut parfois user de ruse. Dans cette section, nous présentons quelques astuces qui s'appuient sur des propriétés déjà démontrées.

Affaiblissement de la conjonction

Soit p et q des expressions booléennes. Nous avons démontré par table de vérité que

$$p \wedge q \;\Rightarrow\; q \qquad \text{(Affaiblissement du } \wedge\text{, proposition 1.1.10-a).}$$

En revenant au syllogisme d'Aristote, on peut comprendre l'utilité de l'**affaiblissement de la conjonction** en constatant qu'il permet de faire le raisonnement suivant :

> $P \wedge Q \;\Rightarrow\; Q$ est un théorème
> Si on a une démonstration que $P \wedge Q$ est vrai
> Alors Q est vrai.

Il découle de ce résultat que si, lors d'une démonstration, nous supposons P, il nous est possible d'utiliser une propriété qui possède la forme $P \Rightarrow Q \wedge R$ pour déduire Q (et

simplement ignorer l'expression R lorsqu'elle nous est inutile). Nous avons effectivement utilisé ce résultat sans le mentionner précédemment, de même que dans l'exemple suivant.

Exemple 1.3.4. Nous voulons démontrer :

$$(\forall S, T, U \mid S \subseteq T \setminus U \;\Rightarrow\; S \subseteq U^c\,).$$

Démonstration. Soit S, T, U des ensembles.

Supposons $S \subseteq T \setminus U$ et démontrons $S \subseteq U^c$	$\langle$ *On veut* $(\forall e \in S \mid e \in U^c)$ $\rangle$
Soit un élément $e \in S$	$\langle$ *Démontrons* $e \in U^c$ $\rangle$
Donc, on a $e \in T \setminus U$	$\langle$ *par l'hypothèse de départ.* $\rangle$
Donc $e \in T$ **et** $e \notin U$	$\langle$ *Définition de "*$S \setminus T$*"* $\rangle$
Donc, on a bien $e \in U^c$	$\langle$ *Définition de "*U^c*"* $\rangle$
	C.Q.F.D.

Version contraposée d'une expression

La technique de **démonstration par contraposition** repose sur la proposition 1.1.9, page 18 :

$$(\forall p, q \mid p \Rightarrow q \;\Leftrightarrow\; \neg q \Rightarrow \neg p)\,.$$

On peut l'utiliser de deux façons. Au lieu de démontrer l'expression "p est vrai implique que q est vrai", on peut démontrer l'expression "q est faux implique que p est faux". Cela peut être plus facile dans certains contextes et, puisque les deux expressions sont équivalentes, démontrer la deuxième expression équivaut à démontrer la première. Voici un tel exemple :

Exemple 1.3.5. On veut démontrer que si un nombre naturel a un carré pair, alors il est pair, c.-à-d. : $(\forall n \in \mathbb{N} \mid n^2 \text{ est pair } \Rightarrow n \text{ est pair })$. Nous aurons besoin des définitions suivantes.

$$\begin{aligned} n \text{ est pair} &\stackrel{\text{def}}{=} (\exists k \in \mathbb{N} \mid n = 2k) \\ n \text{ est impair} &\stackrel{\text{def}}{=} (\exists k \in \mathbb{N} \mid n = 2k+1) \end{aligned}$$

Démonstration de $(\forall n \in \mathbb{N} \mid n^2 \text{ est pair } \Rightarrow n \text{ est pair })$**.**
Démontrons plutôt la contraposition suivante :

$$(\forall n \in \mathbb{N} \mid n \text{ est impair } \Rightarrow n^2 \text{ est impair })$$

Soit $n \in \mathbb{N}$.	$\langle$ *On veut démontrer* n *est impair* $\Rightarrow n^2$ *est impair* $\rangle$
Supposons que n est impair.	$\langle$ *Montrons que* n^2 *est impair, c.-à-d.* $(\exists k \in \mathbb{N} \mid n^2 = 2k+1)$ $\rangle$

Soit $i \in \mathbb{N}$ choisi tel que $n = 2i + 1$. ⟨ *Un tel i existe par la définition de "impair"* ⟩
On a $n^2 = (2i+1)^2 = 4i^2 + 4i + 1 = 2(2i^2 + 2i) + 1$ ⟨ *Propriétés de l'arithmétique* ⟩
En posant $j := 2i^2 + 2i$, on obtient $n^2 = 2j + 1$.
Comme $i \in \mathbb{N}$, on a $j \in \mathbb{N}$. ⟨ *Arithmétique* ⟩
Comme voulu, n^2 est impair, puisque nous avons montré $(\exists k \in \mathbb{N} \mid n^2 = 2k + 1)$.
C.Q.F.D.

Une autre façon d'utiliser la contraposition apparaît dans la démonstration suivante.

Exemple 1.3.6. Nous voulons démontrer : $(\forall S, T, U \mid S \subseteq T \wedge \neg(U \subseteq T) \Rightarrow \neg(U \subseteq S))$. Pour comprendre l'idée de la démonstration, dessinez un diagramme de Venn qui illustre cette expression.

Démonstration. Soit S, T, U des ensembles.
Supposons $S \subseteq T \wedge \neg(U \subseteq T)$ et démontrons $\neg(U \subseteq S)$. ⟨ *on veut* $\neg(\forall u \in U \mid u \in S)$ ⟩
⟨ *par De Morgan, on veut* $(\exists u \in U \mid u \notin S)$ ⟩
Prenons $u \in U$ choisi tel que $u \notin T$. Ce u existe car, par hypothèse, $\neg(U \subseteq T)$, c'est-à-dire $(\exists u \in U \mid u \notin T)$. ⟨ *il reste à montrer* $u \notin S$ ⟩

Par hypothèse, on a $S \subseteq T$, c.-à-d. $(\forall x \mid x \in S \Rightarrow x \in T)$. Ça ne nous aide pas directement, car nous avons $u \notin T$; par contre, voyons la contraposition de cette hypothèse :

$$(\forall x \mid x \notin T \Rightarrow x \notin S).$$

Ainsi, comme $u \notin T$, nous avons $u \notin S$, et c'est bien ce qu'on voulait. **C.Q.F.D.**

Utiliser l'*existence d'un élément* dans une démonstration

Il arrive que nous ayons une hypothèse qui affirme l'existence d'un élément. Il faut souvent, pour démontrer la suite, prendre cet élément en le fixant. Les deux démonstrations de la section 1.3.8 le font :

- Dans la démonstration que $\sqrt{2}$ est irrationnel, quand on écrit "Soit p... q... tels que....", on utilise l'hypothèse que $\sqrt{2}$ serait rationnel (puisqu'on fait une démonstration par contradiction), ce qui dit exactement qu'il existe de tels p et q. On continue alors la démonstration avec ces éléments p et q, comme s'ils existaient, ce qui nous permet de déduire des affirmations sur ces éléments.
- Dans la démonstration qu'il existe un nombre infini de nombres premiers, après avoir supposé qu'il en existe un nombre fini, on nomme ces nombres et on les utilise.

Ces deux démonstrations sont par contradiction, mais on peut *utiliser* une affirmation d'existence à chaque fois qu'une telle affirmation est vraie ou mise en hypothèse. Par exemple, nous pouvons démontrer

$$(\exists x \in \mathbb{N} \mid x^2 = x).$$

Ensuite, nous pouvons utiliser un tel x dans une démonstration si ça nous est utile.

1.3.10 Exercices sur les techniques de démonstration

Pour cette série d'exercices, vous devez écrire vos démonstrations sous la forme d'un texte français, similairement aux démonstrations présentées tout au long de la section 1.3. Nous vous encourageons cependant à vous former une intuition en utilisant les diagrammes de Venn si les énoncés concernent des ensembles.

Exercice 1 :

a) Vous venez de démontrer qu'un élément quelconque d'un ensemble X est aussi élément d'un ensemble Y. Écrivez la phrase logique que vous venez de démontrer.

b) Étant donnés deux ensembles A et B. En vous inspirant du numéro a), expliquez comment "classiquement" on démontrerait l'énoncé : A=B

c) Étant donné deux ensembles U et V. Vous venez de démontrer qu'un élément quelconque de l'ensemble V est aussi élément d'un ensemble U. Puis vous avez démontré qu'il existe un élément de l'ensemble U qui n'appartient pas à l'ensemble V. Écrivez la phrase logique que vous venez de démontrer.

Exercice 2 : Soit S et T des ensembles quelconques. Démontrez $S \setminus T = S \cap T^c$ à l'aide de l'antisymétrie de l'inclusion (Propriété 1.2.13-d) : ($\star\star$) $S = T \;\Leftrightarrow\; S \subseteq T \wedge T \subseteq S$.

Exercice 3 : Supposons que S et T sont deux ensembles quelconques. Démontrez :

a) $S \cap T \subseteq T$

b) $S \setminus T \subseteq S$.

c) Transitivité de $\subseteq$: $\quad S \subseteq T \wedge T \subseteq U \Rightarrow S \subseteq U$;

d) $(\forall x \mid P(x) \Rightarrow Q(x)) \;\Leftrightarrow\; \{x \mid P(x)\} \subseteq \{x \mid Q(x)\}$

Exercice 4 : Supposons que S et T sont deux ensembles quelconques. Démontrez :

a) $S \subseteq T \;\Leftrightarrow\; S \cap T = S$;

b) $S \subseteq T \;\Leftrightarrow\; S \cup T = T$

Exercice 5 : Donnez les grandes étapes d'une démonstration d'un énoncé qui se lirait comme suit :

$$\neg\big(\forall x \in X \mid P(x) \Rightarrow Q(x)\big).$$

Exercice 6 : Démontrez

1. $(\exists x \in \mathbb{N} \mid x^2 = x)$.
2. $(\exists x \in \mathbb{N} \mid x^2 = -1) \Rightarrow (\forall y \in \mathbb{N} \mid (\exists x \in \mathbb{N} \mid x^2 y + y = 0))$ [23].

Exercice 7 : Démontrez que $(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$ est toujours faux. C'est-à-dire, démontrez $\neg(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$. Faites-le par contradiction.

Exercice 8
Soit PAIRS $= \{i \in \mathbb{Z} \mid (\exists j \in \mathbb{Z} \mid i = 2j)\}$ et IMPAIRS $= \{i \in \mathbb{Z} \mid (\exists j \in \mathbb{Z} \mid i = 2j + 1)\}$. Démontrez

1. $(\forall x \in \text{PAIRS} \mid x^2 + 1 \in \text{IMPAIRS})$.
2. $(\forall x, y \in \mathbb{Z} \mid x \in \text{PAIRS} \Rightarrow xy \in \text{PAIRS})$.

Une note sur l'opérateur modulo. Le modulo est très important en informatique pour toutes les données cycliques. Un exemple courant : si un événement arrive tous les 16 jours, pour connaître le jour de la semaine associé à la prochaine occurrence, il suffit de calculer "16 mod 7", c'est-à-dire le reste de division de 16 par 7. Ce nombre est 2. Ainsi, il suffit d'ajouter 2 jours : si l'événement s'est produit un lundi, la prochaine occurrence sera un mercredi, puis ensuite un vendredi, etc. Les exercices suivants vous obligent à maîtriser le modulo...

Exercice 9 : Démontrons que la définition du modulo par 9 qui suit est correcte,

$$(n \bmod 9 = r) \stackrel{\text{def}}{=} (r \in \{0, 1, 2, \ldots, 8\}) \wedge (\exists k \in \mathbb{N} \mid n = 9k + r).$$

C'est-à-dire démontrez que le "r" est unique :

$$\begin{aligned}(\forall n, r_1, r_2 \in \mathbb{N} \mid [&(r_1 \in \{0, 1, 2, \ldots, 8\} \wedge (\exists k \in \mathbb{N} \mid n = 9k + r_1)) \\ &\wedge (r_2 \in \{0, 1, 2, \ldots, 8\} \wedge (\exists k \in \mathbb{N} \mid n = 9k + r_2)) \Rightarrow r_1 = r_2]\end{aligned}$$

Exercice 10 : Un truc bien connu pour savoir si un nombre se divise par 9 : additionner les chiffres de sa représentation en base 10 et évaluer si ce nombre se divise par 9. Démontrons cet énoncé pour les nombres positifs de 2 chiffres (par exemple 21, 34, 99). Ces nombres s'écrivent sous la forme $10d + u$ où $d, u \in \{0, 1, 2, \ldots, 9\}$ (la dizaine et l'unité). Ainsi, démontrez :

$$\big(\forall d, u \in \{0, 1, 2, \ldots, 9\} \;\big|\; (10d + u) \bmod 9 = 0 \Leftrightarrow (d + u) \bmod 9 = 0\big).$$

23. Relisez la section sur l'utilisation de $\exists$, page 71. Bien sûr l'hypothèse est fausse, mais on s'amuse : à partir d'une hypothèse fausse, on peut démontrer n'importe quoi. Morale : gare aux démagogues !

1.4 Relations et fonctions

> Je suis à la recherche d'une relation qui soit totale et déterministe.
>
> Anonyme (Probablement un mathématicien.)

À la section 1.2, nous avons défini un ensemble comme étant une collection d'éléments non ordonnée qui ne contient pas de répétitions. Les ensembles seront le concept de base pour définir les relations. Une relation entre deux ensembles permet de lier des éléments du premier ensemble avec les éléments du deuxième.

Les relations ont beaucoup en commun avec les bases de données souvent utilisées dans les systèmes informatiques. Par exemple, on peut imaginer qu'une base de données contient un ensemble de noms de réalisateurs et un ensemble de titres de film, et qu'une relation lie chaque réalisateur aux films dont il est l'artisan.

Nous verrons aussi que les relations permettent d'étudier les fonctions mathématiques (telle, par exemple, "$f(x) = x^2$") et d'introduire un ordre dans un ensemble (si $a \in \mathbb{N}$ et $b \in \mathbb{N}$, on pourra évaluer la valeur de vérité de l'expression "$a \leq b$").

1.4.1 n-uplet et produit cartésien

Un **n-uplet** consiste en une liste contenant n éléments. Nous écrivons les éléments d'un n-uplet entre les symboles "$\langle$" et "$\rangle$". Par exemple, le 5-uplet qui suit contient les nombres entiers de 1 à 5 inclusivement en ordre croissant :

$$u \;:=\; \langle 1, 2, 3, 4, 5 \rangle \,.$$

Contrairement aux ensembles, les éléments d'un n-uplet sont ordonnés et peuvent contenir des répétitions. Ainsi :

$$\langle 1, 2, 3, 4, 5 \rangle \;\neq\; \langle 5, 1, 3, 2, 4 \rangle \;\neq\; \langle 1, 1, 2, 3, 4, 5 \rangle \,.$$

Comme pour un ensemble, les **éléments** d'un n-uplet peuvent être de type quelconque (nombres, mots, phrases, expressions booléennes...). Généralement, on utilise le terme **couple** ou le terme **paire** pour désigner un 2-uplet (par exemple le couple "$\langle \texttt{vrai}, \texttt{faux} \rangle$") et le terme **triplet** pour désigner un 3-uplet (par exemple le triplet "$\langle \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \rangle$").

L'opérateur de **produit cartésien** "$\times$" entre deux ensembles permet de créer l'ensemble des couples réunissant un élément du premier ensemble et un élément du deuxième ensemble.

Définition 1.4.1. *Produit cartésien de deux ensembles*
Soit S et T des ensembles, alors :

$$S \times T \stackrel{\text{def}}{=} \{\langle a, b\rangle \mid a \in S \wedge b \in T\}\,.$$

Voici un exemple de produit cartésien entre deux ensembles :

$$\{1, 2\} \times \{\mathtt{a}, \mathtt{b}, \mathtt{c}\} \;=\; \{\langle 1, \mathtt{a}\rangle, \langle 1, \mathtt{b}\rangle, \langle 1, \mathtt{c}\rangle, \langle 2, \mathtt{a}\rangle, \langle 2, \mathtt{b}\rangle, \langle 2, \mathtt{c}\rangle\}\,.$$

Insistons sur le fait que $\{1, 2\} \times \{\mathtt{a}, \mathtt{b}, \mathtt{c}\} \;\neq\; \{\mathtt{a}, \mathtt{b}, \mathtt{c}\} \times \{1, 2\}$, puisque les éléments d'un couple sont ordonnés.

La définition qui suit présente le produit cartésien entre plusieurs ensembles. Notez qu'il s'agit d'une généralisation de la définition 1.4.1, c'est-à-dire que cette nouvelle définition est compatible avec la définition du produit cartésien de deux ensembles. Ainsi le produit cartésien des ensembles S et T est l'ensemble de toutes les paires dont le premier membre est un élément de S et le second un élément de T. On peut facilement généraliser cette définition à $S \times T \times U$ comme un ensemble de triplets, à $S \times T \times U \times V$ comme un ensemble de quadruplets, etc.

Définition 1.4.2. *Produit cartésien d'un nombre arbitraire d'ensembles*
Soit un nombre n d'ensembles désignés par les variables $S_1, S_2, \ldots, S_n$, on a :

$$S_1 \times S_2 \times \ldots \times S_n \stackrel{\text{def}}{=} \{\langle e_1, e_2, \ldots, e_n\rangle \mid e_1 \in S_1 \wedge e_2 \in S_2 \wedge \ldots \wedge e_n \in S_n\}\,.$$

Pour désigner un produit cartésien de n fois le même ensemble S par lui même, on utilise la notation S^n :

$$S^n \stackrel{\text{def}}{=} \underbrace{S \times S \times \ldots \times S}_{n \text{ fois}}\,.$$

En accord avec cette notation, on désigne les coordonnées du **plan cartésien** par $\mathbb{R}^2$ et l'**espace tridimensionnel** par $\mathbb{R}^3$. Tel qu'illustré par la figure 1.5, le plan cartésien est constitué de l'ensemble des couples $\langle x, y\rangle$ tels que $x \in \mathbb{R}$ et $y \in \mathbb{R}$. Similairement, l'espace tridimensionnel est constitué de l'ensemble des triplets $\langle x, y, z\rangle$ tels que $x, y, z \in \mathbb{R}$.

La proposition suivante présente certaines propriétés du produit cartésien.

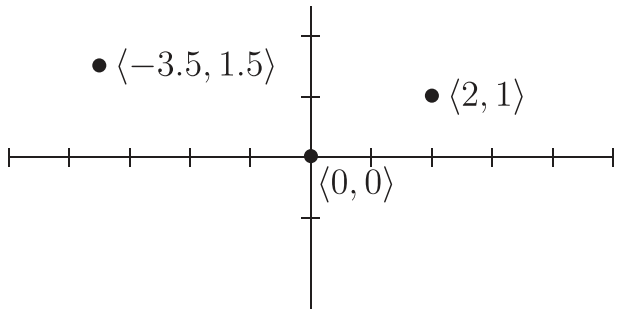


FIGURE 1.5 – Les points d'un plan cartésien correspondent à l'ensemble de couples $\{\langle x, y\rangle \mid x \in \mathbb{R} \wedge y \in \mathbb{R}\} = \mathbb{R}^2$. Les trois points illustrés sur cette figure forment le sous-ensemble $\{\langle -3.5, 1.5\rangle, \langle 0, 0\rangle, \langle 2, 1\rangle\} \subset \mathbb{R}^2$.

Proposition 1.4.3. *Propriétés du produit cartésien*
Soit S, T, U et V des ensembles, alors les expressions suivantes sont vraies :

a :	$S \times T = T \times S$	$\Leftrightarrow$	$S = \emptyset \vee T = \emptyset \vee S = T$	
b :	$S \times (T \cup U)$	$=$	$(S \times T) \cup (S \times U)$	*(Distributivité sur l'union)*
c :	$S \times (T \cap U)$	$=$	$(S \times T) \cap (S \times U)$	*(Distributivité sur l'intersection)*
d :	$S \times (T \setminus U)$	$=$	$(S \times T) \setminus (S \times U)$	*(Distributivité sur la différence)*
e :	$S \subseteq U \wedge T \subseteq V$	$\Rightarrow$	$S \times T \subseteq U \times V$	
f :	$S \times T \subseteq S \times U$	$\Rightarrow$	$S = \emptyset \vee T \subseteq U$	
g :	$(S \cap T) \times (U \cap V)$	$=$	$(S \times U) \cap (T \times V)$	
h :	$\lvert S \times T\rvert$	$=$	$\lvert S\rvert \cdot \lvert T\rvert$ *si S et T sont des ensembles finis.*	

Nous présentons maintenant la démonstration de deux propriétés du produit cartésien. La première démonstration (distributivité de l'union) est effectuée par une série d'équivalences, en appliquant "mécaniquement" (et adéquatement) les définitions et propriétés déjà énoncées. La deuxième démonstration (distributivité de la différence) est écrite dans un style "textuel" et fait davantage appel à la compréhension du lecteur. On y voit un aspect important des démonstrations qui impliquent des *ensembles de paires*.

Démonstration de la distributivité de "$\times$" sur l'union. (Proposition 1.4.3-b)
Soit S, T et U des ensembles. Nous voulons démontrer "$S \times (T \cup U) = (S \times T) \cup (S \times U)$". Par l'axiome d'extensionnalité (définition 1.2.1, avec $[e := \langle a, b\rangle]$, $[S := S \times (T \cup U)]$ et $[T := (S \times T) \cup (S \times U)]$), nous savons que cela est équivalent à démontrer :

$$(\forall\, e \mid e \in S \times (T \cup U) \Leftrightarrow e \in (S \times T) \cup (S \times U)\,)\,.$$

Toutefois, les éléments e ici sont des *paires*, donc e est nécessairement de la forme $< a, b >$. C'est pourquoi on peut plutôt écrire qu'on veut démontrer :

$$(\forall\, \langle a,b\rangle \mid \langle a,b\rangle \in S \times (T \cup U) \Leftrightarrow \langle a,b\rangle \in (S \times T) \cup (S \times U)\,)\,.$$

Soit $\langle a,b\rangle$ une paire.
Démontrons "$\langle a,b\rangle \in S \times (T \cup U) \Leftrightarrow \langle a,b\rangle \in (S \times T) \cup (S \times U)$" :

$$\begin{aligned}
& \langle a,b\rangle \in S \times (T \cup U) \\
\Leftrightarrow \quad & \langle \textit{ Def 1.4.1 – Produit cartésien, avec } [T := T \cup U] \,\rangle \\
& a \in S \wedge (b \in T \cup U) \\
\Leftrightarrow \quad & \langle \textit{ Prop 1.2.12-c – Union } \rangle \\
& a \in S \wedge (b \in T \vee b \in U) \\
\Leftrightarrow \quad & \langle \textit{ Prop 1.1.6-b – Distributivité de la conjonction } \rangle \\
& (a \in S \wedge b \in T) \vee (a \in S \wedge b \in U) \\
\Leftrightarrow \quad & \langle \textit{ Def 1.4.1 – Produit cartésien, 2 fois } \rangle \\
& (\langle a,b\rangle \in S \times T) \vee (\langle a,b\rangle \in S \times U) \\
\Leftrightarrow \quad & \langle \textit{ Prop 1.2.12-c – Union, avec } [S := S \times T] \textit{ et } [T := S \times U] \,\rangle \\
& \langle a,b\rangle \in (S \times T) \cup (S \times U)\,.
\end{aligned}$$

C.Q.F.D.

Démonstration de la distributivité de "×" sur la différence. (Proposition 1.4.3-d)
Soit S, T et U des ensembles. Nous voulons démontrer "$S \times (T \setminus U) = (S \times T) \setminus (S \times U)$".
Utilisons l'antisymétrie de l'inclusion (propriété 1.2.13-d) et démontrons chaque inclusion.

$\boxed{\subseteq :}$ Soit $\langle a,b\rangle \in S \times (T \setminus U)$. $\langle$ *on veut* $\langle a,b\rangle \in (S \times T) \setminus (S \times U)$ $\rangle$
Alors par définition de $\times$, on sait que $a \in S$, $b \in T$ et $b \notin U$.
Donc $\langle a,b\rangle \in S \times T$, mais $\langle a,b\rangle \notin S \times U$.
Donc $\langle a,b\rangle \in (S \times T) \setminus (S \times U)$. $\langle$ *"⊆" démontré* $\rangle$

$\boxed{\supseteq :}$ Soit $\langle a,b\rangle \in (S \times T) \setminus (S \times U)$. $\langle$ *on veut* $\langle a,b\rangle \in S \times (T \setminus U)$ $\rangle$
Alors on sait que $\langle a,b\rangle \in S \times T$ et que $\langle a,b\rangle \notin S \times U$.
Donc $a \in S$, $b \in T$ et $\neg(a \in S \wedge b \in U)$.
Donc $a \in S$, $b \in T$ et $\neg(a \in S) \vee \neg(b \in U)$. $\langle$ *De Morgan* $\rangle$
Comme $a \in S$, on a nécessairement $\neg(b \in U)$.
$\langle$ *Pour que $p \vee q$ soit vrai alors que p est faux, il faut que q soit vrai.* $\rangle$
Autrement dit $a \in S$ et $b \in T \setminus U$. $\langle$ *Car $a \in S$, $b \in T$, $b \notin U$* $\rangle$
Ainsi, par définition de $\times$, $\langle a,b\rangle \in S \times (T \setminus U)$. $\langle$ *"⊇" démontré* $\rangle$

C.Q.F.D.

1.4.2 Définitions et représentations des relations

Les relations permettent de lier entre eux les éléments de plusieurs ensembles. Deux notations sont utilisées largement pour les relations, la lettre R sous forme majuscule ou calligraphique $\mathcal{R}$, de même que les lettres minuscules de l'**alphabet grec** [24]. Nous utiliserons les deux. Dans les énoncés des définitions et des propositions, nous utilisons souvent les lettres "$\mathcal{R}$", "$\mathcal{L}$", "rhô" ρ, "sigma" σ et "thêta" θ pour désigner des relations, au même titre que nous utilisons, depuis le début de ce document, les lettres p, q et r pour désigner des expressions booléennes et les lettres S, T et U pour désigner des ensembles. Bien sûr, ceci n'est qu'une convention. Tout pictogramme (et non seulement une lettre) peut représenter une variable ; il suffit de bien expliquer le choix qu'on fait.

Considérons n ensembles $S_1, S_2, \ldots, S_n$. Une **relation n-aire $\mathcal{R}$** sur ces ensembles est un ensemble de n-uplets tel que :

$$\mathcal{R} \subseteq S_1 \times S_2 \times \ldots \times S_n \,.$$

Dans ce cours, le mot **relation** est utilisé pour désigner **relation binaire**, qui est notre principal objet d'étude. Ainsi, une relation $\mathcal{R} \subseteq S \times T$ est un ensemble de couples (c'est-à-dire de 2-uplets) qui associent certains éléments de S à certains éléments de T.

Voici quatre exemples de relations binaires :

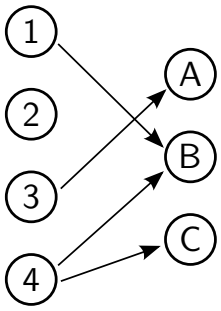
1. Soit R l'ensemble des réalisateurs d'Hollywood et F l'ensemble des films, la relation "bêta" $\beta \subseteq R \times F$ est telle que $\langle r, f \rangle \in \beta$ si le réalisateur $r \in R$ a réalisé le film $f \in F$:

$$\beta := \left\{ \begin{array}{l} \langle \text{Spielberg, Jaws} \rangle, \langle \text{Spielberg, Indiana Jones} \rangle, \langle \text{Spielberg, E.T.} \rangle, \ldots, \\ \langle \text{Jackson, Braindead} \rangle, \langle \text{Jackson, Lord of the Rings} \rangle, \langle \text{Jackson, King Kong} \rangle, \ldots, \\ \langle \text{Mendes, American Beauty} \rangle, \langle \text{Mendes, Road to Perdition} \rangle, \langle \text{Mendes, Jarhead} \rangle, \ldots \end{array} \right\}.$$

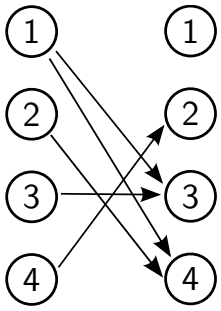
2. Soit E l'ensemble des étudiants d'un cours et $N = \{A+, A, A-, B+, B, B-, \ldots\}$ l'ensemble des cotes possibles, la relation "gamma" $\gamma \subseteq E \times N$ associe chaque étudiant à la cote qu'il a obtenue pour ce cours.

$$\gamma := \{\langle e, n \rangle \in E \times N \mid \text{L'étudiant } e \text{ a obtenu la cote } n \text{ pour ce cours}\} \,.$$

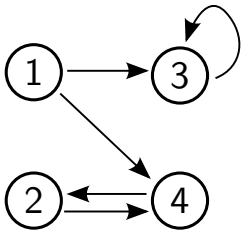
24. En mathématiques et en sciences, il est fréquent d'utiliser des lettres grecques pour nommer des variables. Bien que cela soit souvent rébarbatif au premier abord, il ne faut pas se laisser intimider par les lettres $\alpha, \beta, \gamma, \ldots$ davantage que par les lettres x, y, z ! Le lecteur est invité à se référer à l'annexe A (page 255) pour connaître la prononciation en français de chacune des lettres de l'alphabet grec.



(a) Graphe de la relation ρ sous forme biparti.



(b) Graphe de la relation σ sous forme biparti.



(c) Graphe de la relation σ sous forme fusionné.

FIGURE 1.6 – Exemples de représentations d'une relation à l'aide d'un graphe. On considère les ensembles $K = \{1, 2, 3, 4\}$ et $L = \{A, B, C\}$, ainsi que les relations "rhô" $\rho = \{\langle 1, B\rangle, \langle 3, A\rangle, \langle 4, B\rangle, \langle 4, C\rangle\} \subset K \times L$ et "sigma" $\sigma = \{\langle 1, 3\rangle, \langle 1, 4\rangle, \langle 2, 4\rangle, \langle 3, 3\rangle, \langle 4, 2\rangle\} \subset K^2$. Les figures (b) et (c) illustrent la relation σ de deux manières différentes, ce qui est possible, car l'ensemble de départ est le même que l'ensemble d'arrivée.

3. La relation "thêta" $\theta \subseteq \mathbb{R}^2$ suivante contient les points d'un cercle de rayon unitaire et centré à l'origine du plan cartésien :

$$\theta \;:=\; \{\langle x, y\rangle \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}\,.$$

4. On peut aussi voir l'opérateur "plus petit ou égal" comme une relation (on définit ici l'opérateur sur les entiers relatifs $\mathbb{Z}$ seulement) :

$$\leq \;:=\; \{\langle a, b\rangle \in \mathbb{Z}^2 \mid (b - a) \in \mathbb{N}\}\,.$$

Représentation par un graphe

Un **graphe** est un ensemble de sommets dont certains sont reliés entre eux par des arêtes ou des arcs [25]. Nous désignons par le terme **graphe de relation** un diagramme qui représente une relation à l'aide d'un graphe. On peut imaginer plusieurs légères variantes dans la manière de dessiner ces diagrammes. Dans le cadre de ce cours, nous utilisons les termes "graphe de relation sous forme biparti" et "graphe de relation sous forme fusionné" pour distinguer les deux variantes auxquelles nous avons recours.

Considérons d'abord une relation $\mathcal{R} \subseteq S \times T$ sur deux ensembles possiblement distincts S et T. Les sommets du **graphe de relation sous forme biparti** $\mathcal{R}$ sont regroupés en

25. Le chapitre 3 de ce document est consacré à la théorie des graphes.

deux groupes, celui de gauche représentant les éléments de l'ensemble de départ S et celui de droite représentant les éléments de l'ensemble d'arrivée T. Les arêtes relient entre eux les éléments qui forment un couple dans la relation $\mathcal{R}$. Autrement dit, il y a une arête entre $a \in S$ et $b \in T$ lorsque $\langle a, b\rangle \in \mathcal{R}$. Les figures 1.6a et 1.6b présentent deux exemples de graphes de relations sous forme bipartis.

Considérons maintenant une relation $\mathcal{R} \subseteq S \times S$ partageant le même ensemble de départ et d'arrivée S. Dans ce cas, le **graphe de relation sous forme fusionné** σ représente une seule fois chaque sommet de S. Les arêtes relient entre eux les éléments qui forment un couple dans la relation $\mathcal{R}$. Notez que l'orientation des arêtes est ici importante. La figure 1.6c présente un exemple de graphe de relation sous forme fusionné.

Relation vide et relation triviale

Considérons le produit cartésien $S \times T$. La **relation triviale** $\mathcal{R} := S \times T$ désigne la relation où chaque élément de l'ensemble de départ S forme un couple avec chaque élément de l'ensemble d'arrivée T.

L'ensemble vide $\emptyset$ est une relation constituée d'aucun couple. Il s'agit de la **relation vide**. Rappelons que pour n'importe quels ensembles S et T, nous avons $\emptyset \subseteq S \times T$.

Notation infixe pour les relations

Nous souhaiterons souvent vérifier l'**appartenance** d'un couple à une relation. Conformément à la définition de l'opérateur d'appartenance "$\in$" présentée à la section 1.2.2, l'expression booléenne "$\langle a, b\rangle \in \mathcal{R}$" est évaluée à `vrai` si le couple $\langle a, b\rangle$ appartient à la relation $\mathcal{R}$, sinon l'expression est évaluée à `faux`. Par souci de concision, nous utilisons souvent la notation "$a \ \mathcal{R} \ b$" (appelée "notation infixe") :

Définition 1.4.4. *Notation infixe pour les relations*
Soit S et T deux ensembles, soit $\mathcal{R} \subseteq S \times T$ une relation et soit $\langle a, b\rangle$ un couple tel que $a \in S$ et $b \in T$. On écrit :

$$a \ \mathcal{R} \ b \quad \stackrel{\text{def}}{=} \quad \langle a, b\rangle \in \mathcal{R}\,.$$

En considérant les exemples de relations "bêta" β, "thêta" θ et "plus petit ou égal" $\leq$, on a :

Spielberg β Jaws	est vrai,	Spielberg β Jarhead	est faux,
$\sqrt{0.5}\ \theta\ \sqrt{0.5}$	est vrai,	$1.0\ \theta\ 1.0$	est faux,
$1 \leq 2$	est vrai,	$2 \leq 1$	est faux.

PENSEZ-Y!

Il peut sembler étrange à première vue d'écrire une expression telle "$a \mathcal{R} b$" afin d'exprimer la phrase "Le couple $\langle a, b\rangle$ appartient à la relation $\mathcal{R}$". La notation correspond plutôt à : "a est en relation $\mathcal{R}$ avec b".

D'ailleurs, il est naturel à tous d'écrire l'expression "$a \leq b$", ce que nous pouvons exprimer par la phrase "Le couple $\langle a, b\rangle$ appartient à la relation *plus petit ou égal*". Dans ce cas-ci, la notation "$\langle a, b\rangle \in \leq$" peut sembler contre-intuitive, quoiqu'elle soit tout aussi appropriée.

Il faut bien comprendre ici que la lettre "$\mathcal{R}$", une lettre grecque θ ou le symbole mathématique "$\leq$" sont seulement des pictogrammes que nous avons choisis pour représenter des relations. Ce sont nos habitudes qui nous font préférer une notation plutôt qu'une autre dépendamment du pictogramme utilisé.

Ensemble de départ et domaine / Ensemble d'arrivée et image

Considérons une relation $\mathcal{R} \subseteq S \times T$. On dit que S est l'**ensemble de départ** et que l'ensemble T est l'**ensemble d'arrivée**[26].

La définition suivante établit que le **domaine** d'une relation est l'ensemble des éléments figurant comme premier membre d'un couple dans cette relation. De même, l'**image** d'une relation est l'ensemble des éléments y figurant comme deuxième membre d'un couple. Le domaine d'une relation est inclus dans son ensemble de départ. De même, l'image d'une relation est incluse dans son ensemble d'arrivée.

Définition 1.4.5. *Domaine et image d'une relation*
Soit S et T deux ensembles et soit $\mathcal{R} \subseteq S \times T$ une relation. On a :

$$\texttt{a}: \quad \mathrm{Dom}(\mathcal{R}) \stackrel{\text{def}}{=} \{a \in S \mid (\exists b \in T \mid a \mathcal{R} b)\} \quad \textit{(Domaine de la relation } \mathcal{R}\textit{)}$$
$$\texttt{b}: \quad \mathrm{Im}(\mathcal{R}) \stackrel{\text{def}}{=} \{b \in T \mid (\exists a \in S \mid a \mathcal{R} b)\} \quad \textit{(Image de la relation } \mathcal{R}\textit{)}$$

26. Certains livres de mathématiques nomment "co-domaine" ce que nous désignons ici par "ensemble d'arrivée".

En considérant les quatre exemples de relations donnés précédemment, on obtient :

1. Pour la relation β :
   — L'ensemble de départ est le même que le domaine. Notez qu'ici, on considère que chaque réalisateur a au moins un film à son actif (car sinon, il ne pourrait pas porter le titre de réalisateur !) ;
   — L'ensemble d'arrivée est le même que l'image, en supposant que tous les films sont associés à au moins un réalisateur.
   — $\mathrm{Dom}(\beta) = \{\text{Spielberg, Jackson, Mendes, } \ldots\}$;
   — $\mathrm{Im}(\beta) = \{\text{Jaws, Indiana Jones, E.T., Braindead, Lord of the Rings, } \ldots\}$;
2. Pour la relation γ :
   — L'ensemble de départ est E ;
   — L'ensemble d'arrivée est N ;
   — $\mathrm{Dom}(\gamma) = E$, en supposant que tous les étudiants ont assisté à l'examen final ;
   — $\mathrm{Im}(\gamma) \subseteq N$, car on ne sait pas si toutes les cotes possibles ont été attribuées. En effet, il est envisageable que tous les étudiants de la classe aient obtenu A+.
3. Pour la relation θ :
   — L'ensemble des nombres réels $\mathbb{R}$ est à la fois l'ensemble de départ et l'ensemble d'arrivée ;
   — $\mathrm{Dom}(\theta) = \mathrm{Im}(\theta) = [-1, 1] \subset \mathbb{R}$. Notez que l'intervalle des nombres entre x_1 et x_2 est noté $[x_1, x_2]$ et correspond à l'ensemble $\{y \in \mathbb{R} \mid x_1 \leq y \leq x_2\}$
4. Pour la relation $\leq$:
   — L'ensemble de départ, le domaine, l'ensemble d'arrivée et l'image sont tous égaux ;
   — $\mathrm{Dom}(\leq) = \mathrm{Im}(\leq) = \mathbb{Z}$.

1.4.3 Opérateurs sur les relations

La **relation identité** "$\mathbf{I}_S$" associée à l'ensemble S est une relation particulière où chaque couple associe un élément de S avec lui-même.

Définition 1.4.6. *Relation identité*
Soit S un ensemble. On a :

$$\mathbf{I}_S \stackrel{\text{def}}{=} \{\langle a, a\rangle \in S^2 \mid a \in S\},$$

ou, de manière équivalente :

$$\langle a, a\rangle \in \mathbf{I}_S \;\Leftrightarrow\; a \in S\,.$$

Remarquez que, conformément à la définition 1.4.5, on a $\mathrm{Dom}(\mathbf{I}_S) = \mathrm{Im}(\mathbf{I}_S) = S$.

Composition de relations

La définition suivante présente l'opérateur de **composition** "$\circ$" qui permet de regrouper deux relations en une seule. La composition des relations $\mathcal{R}$ et $\mathcal{L}$ s'écrit "$\mathcal{R}\circ\mathcal{L}$", et se prononce "$\mathcal{R}$ composé avec $\mathcal{L}$" ou plus succinctement "$\mathcal{R}$ rond $\mathcal{L}$".

Définition 1.4.7. *Composition de deux relations*[27]
Soit S, T et U trois ensembles et soit $\mathcal{R} \subseteq S \times T$ et $\mathcal{L} \subseteq T \times U$ deux relations binaires. On a :

$$\mathcal{R} \circ \mathcal{L} \stackrel{\text{def}}{=} \{\langle a, c\rangle \in S \times U \mid (\exists b \in T\, \langle a, b\rangle \in \mathcal{R} \wedge \langle b, c\rangle \in \mathcal{L})\}\,.$$

On peut donc écrire, en utilisant la notation infixe :

$$a\ (\mathcal{R} \circ \mathcal{L})\ c \ \Leftrightarrow\ (\exists b \in T \mid a\ \mathcal{R}\ b \wedge b\ \mathcal{L}\ c)\,.$$

À titre d'exemple, si la relation "bêta" $\beta \subseteq R \times F$ associe les réalisateurs aux films qu'ils ont réalisés et la relation "alpha" $\alpha \subseteq F \times \mathbb{N}$ associe les films à leur année de parution, la relation $\beta \circ \alpha \subseteq R \times \mathbb{N}$ associe les réalisateurs aux années de parution de leurs films :

$$\beta \circ \alpha \ = \ \left\{ \begin{array}{l} \langle \text{Spielberg}, 1975\rangle, \langle \text{Spielberg}, 1981\rangle, \langle \text{Spielberg}, 1982\rangle, \ldots, \\ \langle \text{Jackson}, 1992\rangle, \langle \text{Jackson}, 2001\rangle, \langle \text{Jackson}, 2005\rangle, \ldots, \\ \langle \text{Mendes}, 1999\rangle, \langle \text{Mendes}, 2002\rangle, \langle \text{Mendes}, 2005\rangle, \ldots \end{array} \right\}.$$

La figure 1.7 illustre un autre exemple de composition de relations.

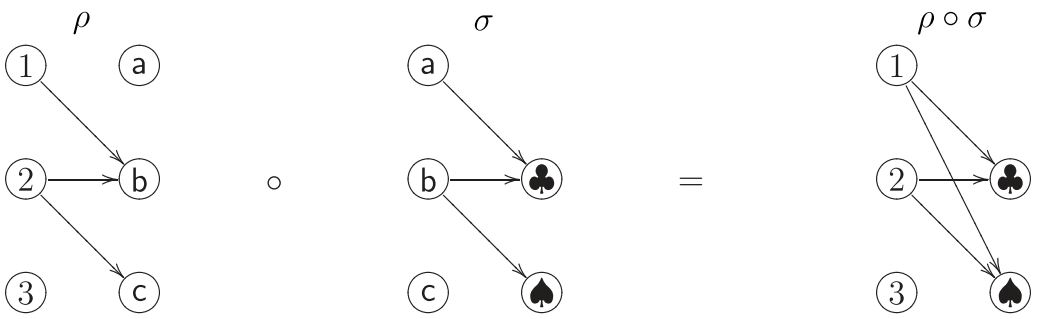
La proposition 1.4.8 énonce quelques propriétés de l'opérateur de composition. La première propriété utilise la relation identité "$\mathbf{I}_S$" présentée par la définition 1.4.6.

Proposition 1.4.8. *Propriétés de la composition*
Soit $\mathcal{R}$, $\mathcal{R}_1$, $\mathcal{L}$ des relations. On pose $S = \text{Dom}(\mathcal{R})$ et $T = \text{Im}(\mathcal{R})$. Les expressions suivantes sont vraies :

a :	$\mathbf{I}_S \circ \mathcal{R}$	$=$	$\mathcal{R} \circ \mathbf{I}_T$	$=$	$\mathcal{R}$	*(Élément neutre)*
b :	$\emptyset \circ \mathcal{R}$	$=$	$\mathcal{R} \circ \emptyset$	$=$	$\emptyset$	*(Élément absorbant)*
c :	$(\mathcal{R} \circ \mathcal{R}_1) \circ \mathcal{L}$			$=$	$\mathcal{R} \circ (\mathcal{R}_1 \circ \mathcal{L})$	*(Associativité)*
d :	$\mathcal{R} \subseteq \mathcal{R}_1$			$\Rightarrow$	$\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{R}_1 \circ \mathcal{L}$	*(Monotonie)*

27. Il existe plusieurs notations pour désigner la *compostion* de deux relations. La définition adoptée ici diffère légèrement de celle utilisée habituellement en mathématiques, qui est plutôt :

$$\mathcal{L} \circ \mathcal{R} \stackrel{\text{def}}{=} \{\langle a, c\rangle \in S \times U \mid (\exists b \in T\, \langle a, b\rangle \in \mathcal{R} \wedge \langle b, c\rangle \in \mathcal{L})\}\,.$$



$$\{\langle 1, \mathsf{b}\rangle, \langle 2, \mathsf{b}\rangle, \langle 2, \mathsf{c}\rangle\} \quad \circ \quad \{\langle \mathsf{a}, \clubsuit\rangle, \langle \mathsf{b}, \clubsuit\rangle, \langle \mathsf{b}, \spadesuit\rangle\} \quad = \quad \{\langle 1, \clubsuit\rangle, \langle 1, \spadesuit\rangle, \langle 2, \clubsuit\rangle, \langle 2, \spadesuit\rangle\}$$

FIGURE 1.7 – Exemple illustrant la composition de deux relations ρ et σ.

Comme l'opérateur de composition est associatif (propriété 1.4.8-c), l'ordre d'évaluation des opérateurs de composition consécutifs n'a pas d'influence sur le résultat final. On peut donc omettre les parenthèses lors de l'écriture. Autrement dit, on a :

$$\mathcal{R} \circ \mathcal{R}_1 \circ \mathcal{L} = (\mathcal{R} \circ \mathcal{R}_1) \circ \mathcal{L} = \mathcal{R} \circ (\mathcal{R}_1 \circ \mathcal{L}).$$

Puissance d'une relation

On utilise la notation "$\mathcal{R}^n$" pour désigner la **puissance** d'une relation[28], c'est-à-dire l'application de l'opérateur de composition n fois consécutives sur la relation $\mathcal{R}$. La définition suivante établit la convention que la **puissance zéro** "$\mathcal{R}^0$" d'une relation $\mathcal{R} \in S^2$ donne la relation identité $\mathbf{I}_S$.

Définition 1.4.9. *Puissance d'une relation*
Soit S un ensemble, $\mathcal{R} \subseteq S^2$ une relation et n un nombre entier positif ou nul ($n \in \mathbb{N}$).
Si $n \geq 1$, on a :

$$\mathcal{R}^n \stackrel{\text{def}}{=} \underbrace{\mathcal{R} \circ \mathcal{R} \circ \ldots \circ \mathcal{R}}_{n \text{ fois}},$$

sinon ($n = 0$), on a :

$$\mathcal{R}^0 \stackrel{\text{def}}{=} \mathbf{I}_S\,.$$

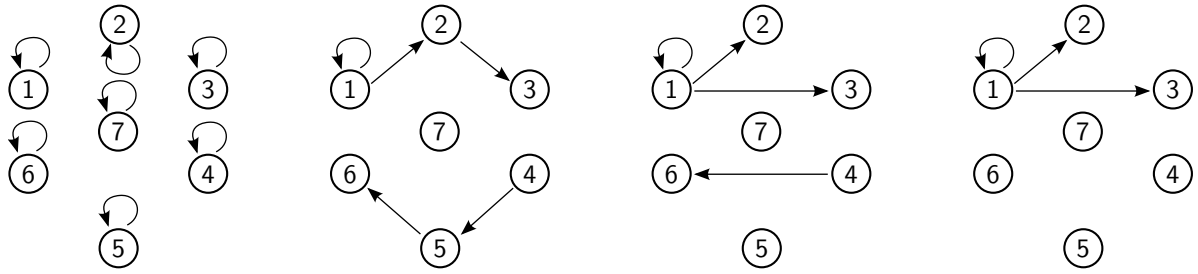
En guise d'exemple, considérons la relation "delta" :

$$\delta \;:=\; \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 4,5\rangle, \langle 5,6\rangle\} \;\subset\; \{1,2,3,4,5,6,7\}^2.$$

28. Notons ici que nous utilisons la même notation (l'exposant n) pour désigner à la fois la puissance "à la n" d'une relation (définition 1.4.9) et le produit cartésien "n fois" d'un ensemble par lui-même (définition 1.4.2). Bien que cela pourrait porter à confusion (une relation étant définie comme un ensemble), le contexte d'utilisation de cette notation empêche habituellement toute ambiguïté.

Nous avons, tel qu'illustré par des graphes dans la figure 1.8 :

$$\begin{aligned}
\delta^0 &= \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 4,4\rangle, \langle 5,5\rangle, \langle 6,6\rangle, \langle 7,7\rangle\}, \\
\delta^1 &= \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 4,5\rangle, \langle 5,6\rangle\}, \\
\delta^2 &= \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 4,6\rangle\}, \\
\delta^n &= \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle\} \quad \text{pour tout } n \geq 3.
\end{aligned}$$



(a) Relation δ^0. (b) Relation δ^1. (c) Relation δ^2. (d) Relation δ^n, pour tout $n \geq 3$.

FIGURE 1.8 – Graphes de relation sous formes fusionnés illustrant les relations obtenues en appliquant l'opérateur puissance sur la relation $\delta = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 4,5\rangle, \langle 5,6\rangle\}$ pour différentes valeurs d'exposant.

La proposition qui suit présente deux propriétés de l'opérateur puissance qu'il est relativement facile de déduire de l'associativité de la composition (propriété 1.4.8-c).

Proposition 1.4.10. *Propriétés de la puissance d'une relation*
Soit $\mathcal{R}$ une relation et soit m et n deux entiers positifs, alors les expressions suivantes sont vraies :

$$\begin{aligned}
&\texttt{a}: \quad \mathcal{R}^m \circ \mathcal{R}^n = \mathcal{R}^{m+n} && \textit{(Somme des exposants)} \\
&\texttt{b}: \quad (\mathcal{R}^m)^n = \mathcal{R}^{m \cdot n} && \textit{(Produit des exposants).}
\end{aligned}$$

Clôture d'une relation

À partir de la définition de la puissance d'une relation, on définit les concepts de **clôture transitive** et de **clôture transitive et réflexive**[29]. Dans ce document, la clôture transitive d'une relation $\mathcal{R}$ est notée "$\mathcal{R}^+$" et la clôture transitive et réflexive de $\mathcal{R}$ est notée "$\mathcal{R}^*$".

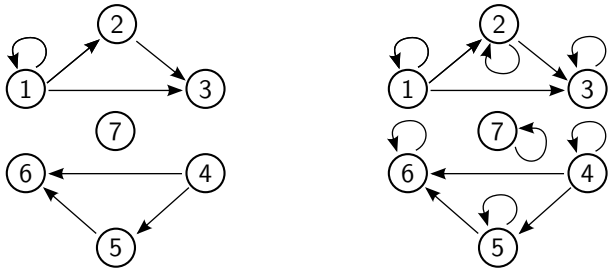
29. Certains auteurs utilisent le terme "fermeture" au lieu de "clôture".

Définition 1.4.11. *Clôtures d'une relation*
Soit $\mathcal{R}$ une relation. On a :

$$\texttt{a}: \quad \mathcal{R}^{+} \stackrel{\text{def}}{=} \mathcal{R}^{1} \cup \mathcal{R}^{2} \cup \mathcal{R}^{3} \cup \ldots \qquad \textit{(Clôture transitive)}$$
$$\texttt{b}: \quad \mathcal{R}^{*} \stackrel{\text{def}}{=} \mathcal{R}^{0} \cup \mathcal{R}^{1} \cup \mathcal{R}^{2} \cup \mathcal{R}^{3} \cup \ldots \qquad \textit{(Clôture transitive et réflexive)}$$

Nous verrons à la section 1.4.4 que les relations $\mathcal{R}^{+}$ et $\mathcal{R}^{*}$ appartiennent nécessairement à la famille des relations transitives, ce qui explique le choix du terme "clôture transitive". De même, la relation $\mathcal{R}^{*}$ appartient également à la famille des relations réflexives.

La figure 1.9 illustre les deux types de clôtures sur la relation δ donnée en exemple à la figure 1.8.



(a) Relation δ^{+}. (b) Relation δ^{*}.

FIGURE 1.9 – Graphes de relation sous formes fusionnés illustrant la clôture transitive δ^{+} et la clôture transitive et réflexive δ^{*} de la relation $\delta = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 4,5\rangle, \langle 5,6\rangle\}$.

Inverse d'une relation

L'**inverse** d'une relation $\mathcal{R}$, noté "$\mathcal{R}^{-1}$", est obtenu simplement en inversant l'ordre des éléments de chaque couple appartenant à $\mathcal{R}$. Autrement dit, "$\langle b,a\rangle \in \mathcal{R}^{-1} \Leftrightarrow \langle a,b\rangle \in \mathcal{R}^{1}$", ce qui est exprimé dans la définition suivante :

Définition 1.4.12. *Inverse d'une relation*
Soit S et T deux ensembles et soit $\mathcal{R} \subseteq S \times T$ une relation. On a :

$$\mathcal{R}^{-1} \stackrel{\text{def}}{=} \{\langle b,a\rangle \in T \times S \mid \langle a,b\rangle \in \mathcal{R}\}\,.$$

Ainsi, l'ensemble de départ d'une relation $\mathcal{R}$ devient l'ensemble d'arrivée de la relation inverse $\mathcal{R}^{-1}$ et l'ensemble d'arrivée de $\mathcal{R}$ devient l'ensemble de départ de $\mathcal{R}^{-1}$. Autrement dit, si $\mathcal{R} \subseteq S \times T$, alors on a $\mathcal{R}^{-1} \subseteq T \times S$.

En guise d'exemple, considérons la relation $\delta = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 4,5\rangle, \langle 5,6\rangle\} \subseteq \mathbb{N}^2$. Nous avons :

$$\delta^{-1} \quad = \quad \{\langle 1,1\rangle, \langle 2,1\rangle, \langle 3,2\rangle, \langle 5,4\rangle, \langle 6,5\rangle\}\,.$$

La proposition suivante présente quelques propriétés qu'il est possible de démontrer à partir de la définition de la relation inverse.

Proposition 1.4.13. *Propriétés de la relation inverse*
Soit $\mathcal{R}$ et $\mathcal{L}$ deux relations, alors les expressions suivantes sont vraies :

a :	$\mathrm{Dom}(\mathcal{R}^{-1})$	$=$	$\mathrm{Im}(\mathcal{R})$	*(Domaine d'une relation inverse)*
b :	$\mathrm{Im}(\mathcal{R}^{-1})$	$=$	$\mathrm{Dom}(\mathcal{R})$	*(Image d'une relation inverse)*
c :	$\emptyset^{-1}$	$=$	$\emptyset$	*(Inverse de la relation vide)*
d :	$(\mathcal{R} \circ \mathcal{L})^{-1}$	$=$	$\mathcal{L}^{-1} \circ \mathcal{R}^{-1}$	*(Inverse de la composition)*
e :	$(\mathcal{R} \cup \mathcal{L})^{-1}$	$=$	$\mathcal{L}^{-1} \cup \mathcal{R}^{-1}$	*(Inverse de l'union)*
f :	$(\mathcal{R} \cap \mathcal{L})^{-1}$	$=$	$\mathcal{L}^{-1} \cap \mathcal{R}^{-1}$	*(Inverse de l'intersection).*

1.4.4 Familles de relations

Nous allons maintenant définir plusieurs propriétés des relations auxquelles nous ferons régulièrement référence par la suite. Ces propriétés nous aideront à caractériser la "famille" à laquelle une relation appartient.

Réflexivité, symétrie et transitivité

Les premières propriétés présentées s'appliquent aux relations dont l'ensemble de départ est le même que l'ensemble d'arrivée.

Définition 1.4.14. *Relation réflexive, irréflexive, symétrique, asymétrique, antisymétrique et transitive*
Soit $\mathcal{R} \subseteq S^2$ une relation. Alors :

a :	$\mathcal{R}$ *est réflexif*	$\stackrel{\text{def}}{=}$	$(\forall a \in S \mid a\ \mathcal{R}\ a\,)$
b :	$\mathcal{R}$ *est irréflexif*	$\stackrel{\text{def}}{=}$	$(\forall a \in S \mid \neg(a\ \mathcal{R}\ a)\,)$
c :	$\mathcal{R}$ *est symétrique*	$\stackrel{\text{def}}{=}$	$(\forall a \in S, b \in S \mid a\ \mathcal{R}\ b \Rightarrow b\ \mathcal{R}\ a\,)$
d :	$\mathcal{R}$ *est asymétrique*	$\stackrel{\text{def}}{=}$	$(\forall a \in S, b \in S \mid a\ \mathcal{R}\ b \Rightarrow \neg(b\ \mathcal{R}\ a)\,)$
e :	$\mathcal{R}$ *est antisymétrique*	$\stackrel{\text{def}}{=}$	$(\forall a \in S, b \in S \mid a\ \mathcal{R}\ b \wedge b\ \mathcal{R}\ a \Rightarrow a = b\,)$
f :	$\mathcal{R}$ *est transitif*	$\stackrel{\text{def}}{=}$	$(\forall a \in S, b \in S, c \in S \mid a\ \mathcal{R}\ b \wedge b\ \mathcal{R}\ c \Rightarrow a\ \mathcal{R}\ c\,).$

À titre d'exemple, examinons les propriétés de trois relations bien connues sur l'ensemble des nombres relatifs $\mathbb{Z}$:

Propriétés	$\leq$	$<$	$=$
Réflexivité	$\surd$		$\surd$
Irréflexive		$\surd$	
Symétrie			$\surd$
Asymétrie		$\surd$	
Antisymétrie	$\surd$	$\surd$	$\surd$
Transitivité	$\surd$	$\surd$	$\surd$

Si certaines affirmations de ce tableau vous semblent bizarres (comme l'antisymétrie de $<$), retournez à la table de vérité de l'implication : quand la précondition (partie gauche) d'une implication est fausse, l'implication est... vraie !

La proposition suivante montre qu'il est possible d'exprimer les propriétés énoncées par la définition 1.4.14 à l'aide des opérateurs ensemblistes.

Proposition 1.4.15. *Définitions équivalentes d'une relation réflexive, irréflexive, symétrique, asymétrique, antisymétrique et transitive*
Soit $\mathcal{R} \subseteq S^2$ une relation. Alors :

a :	$\mathcal{R}$ *est réflexif*	$\Leftrightarrow$	$\mathbf{I}_S \subseteq \mathcal{R}$
b :	$\mathcal{R}$ *est irréflexif*	$\Leftrightarrow$	$\mathbf{I}_S \cap \mathcal{R} = \emptyset$
c :	$\mathcal{R}$ *est symétrique*	$\Leftrightarrow$	$\mathcal{R}^{-1} = \mathcal{R}$
d :	$\mathcal{R}$ *est asymétrique*	$\Leftrightarrow$	$\mathcal{R} \cap \mathcal{R}^{-1} = \emptyset$
e :	$\mathcal{R}$ *est antisymétrique*	$\Leftrightarrow$	$\mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathbf{I}_S$
f :	$\mathcal{R}$ *est transitif*	$\Leftrightarrow$	$\mathcal{R}^2 \subseteq \mathcal{R}$

Il est formateur de bien comprendre que les énoncés de la dernière proposition et de la définition 1.4.14 sont deux manières équivalentes d'exprimer les mêmes concepts. Nous démontrons ici que les deux manières d'exprimer la transitivité sont équivalentes. Rappelons qu'une technique pour démontrer un si et seulement si "$\Leftrightarrow$" consiste à démontrer d'abord l'implication "$\Rightarrow$", puis à démontrer l'implication inverse "$\Leftarrow$". Nous avons déjà présenté cette technique de démonstration à la section 1.3.6 (page 62).

Démonstration de la "définition équivalente de la transitivité". (Prop. 1.4.15-f)
Soit S un ensemble et $\mathcal{R} \subseteq S^2$.
Nous voulons démontrer "$\mathcal{R}^2 \subseteq \mathcal{R} \;\Leftrightarrow\; (\forall a \in S, b \in S, c \in S \mid a \;\mathcal{R}\; b \wedge b \;\mathcal{R}\; c \Rightarrow a \;\mathcal{R}\; c)$".

$\boxed{\Rightarrow:}$ Supposons $\mathcal{R}^2 \subseteq \mathcal{R}$ (c.-à-d. : $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$) et démontrons :

$$(\forall a \in S, b \in S, c \in S \mid a \mathcal{R} b \wedge b \mathcal{R} c \Rightarrow a \mathcal{R} c)$$

Soit $a, b, c \in S$, et supposons $a \mathcal{R} b$ et $b \mathcal{R} c$. ⟨ *Montrons* $a \mathcal{R} c$. ⟩
Puisque $(\exists b \in S \mid a \mathcal{R} b \wedge b \mathcal{R} c)$, on a $a (\mathcal{R} \circ \mathcal{R}) c$. ⟨ *Par définition 1.4.7.* ⟩
Donc, on a $a \mathcal{R}^2 c$. ⟨ *Définition de* $\mathcal{R}^2$. ⟩
C'est-à-dire $\langle a, c \rangle \in \mathcal{R}^2$.
Donc, on a $\langle a, c \rangle \in \mathcal{R}$. ⟨ *Car par hypothèse, on a* $\mathcal{R}^2 \subseteq \mathcal{R}$. ⟩
Et donc $a \mathcal{R} c$. ⟨ *"⇒" est démontré.* ⟩

$\boxed{\Leftarrow:}$ Supposons "$(\forall a \in S, b \in S, c \in S \mid a \mathcal{R} b \wedge b \mathcal{R} c \Rightarrow a \mathcal{R} c)$" et démontrons $\mathcal{R}^2 \subseteq \mathcal{R}$, c.-à-d., par définition, démontrons :

$$(\forall \langle a, c \rangle \mid \langle a, c \rangle \in \mathcal{R}^2 \Rightarrow \langle a, c \rangle \in \mathcal{R}).$$

Soit $\langle a, c \rangle$, et supposons $\langle a, c \rangle \in \mathcal{R}^2$. ⟨ *Montrons* $\langle a, c \rangle \in \mathcal{R}$. ⟩
Alors on a $\langle a, c \rangle \in \mathcal{R} \circ \mathcal{R}$. ⟨ *Définition de* $\mathcal{R}^2$. ⟩
Prenons b choisi tel que $a \mathcal{R} b$ et $b \mathcal{R} c$. ⟨ *Un tel* b *existe, car* $\langle a, c \rangle \in \mathcal{R} \circ \mathcal{R}$ *(déf. 1.4.7).* ⟩
Alors on a $a \mathcal{R} c$. ⟨ *Car par hypothèse :* $a \mathcal{R} b \wedge b \mathcal{R} c \Rightarrow a \mathcal{R} c$ ⟩
Et donc, on a $\langle a, c \rangle \in \mathcal{R}$. ⟨ *"⇐" est démontré.* ⟩
C.Q.F.D.

Totalité, surjectivité, déterminisme et injectivité

Cette section, ainsi que la suivante, présente (entre autres choses) une des notions les plus importantes en mathématiques, soit la notion de fonction. En effet, comme nous le verrons, une fonction peut être vue comme une relation ayant deux propriétés particulières, soient celle de totalité et celle de déterminisme.

Considérons une relation $\mathcal{R} \subseteq S \times T$, où S est l'ensemble de départ et T est l'ensemble d'arrivée. On dit que :

— $\mathcal{R}$ est une **relation totale** lorsque chaque élément de l'ensemble de départ S est associé à au moins un élément de l'ensemble d'arrivée T (c'est-à-dire que $\mathrm{Dom}(\mathcal{R}) = S$) ;
— $\mathcal{R}$ est une **relation surjective** lorsque chaque élément de l'ensemble d'arrivée T est associé à au moins un élément de l'ensemble de départ S (c'est-à-dire que $\mathrm{Im}(\mathcal{R}) = T$) ;
— $\mathcal{R}$ est une **relation déterministe** lorsque chaque élément de l'ensemble de départ S est associé à au plus un élément de l'ensemble d'arrivée T ;
— $\mathcal{R}$ est une **relation injective** lorsque chaque élément de l'ensemble d'arrivée T est

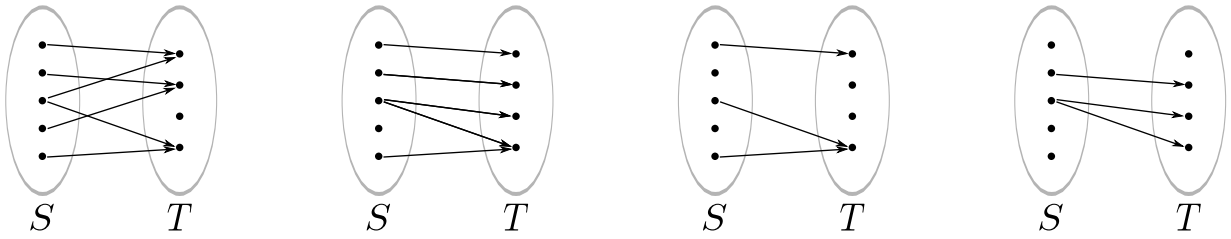
associé à au plus un élément de l'ensemble de départ S .

De plus, on dit que :

— $\mathcal{R}$ est une **relation bijective** lorsqu'elle est à la fois surjective et injective ;

— $\mathcal{R}$ est une **fonction** lorsqu'elle est à la fois totale et déterministe. La section 1.4.5 s'intéresse plus particulièrement à ce type de relations.

La définition 1.4.16 énonce formellement les quatre propriétés de totalité, surjectivité, déterminisme et injectivité. La figure 1.10 illustre ces mêmes propriétés par des exemples.



(a) Totalité (b) Surjectivité (c) Déterminisme (d) Injectivité

FIGURE 1.10 – Exemples de graphes de relation sous forme bipartis respectant une seule des propriétés énoncées par la définition 1.4.16.

Définition 1.4.16. *Relation totale, surjective, déterministe, injective*
Soit $\mathcal{R} \subseteq S \times T$ une relation. Alors :

a :	$\mathcal{R}$ *est total*	$\stackrel{\text{def}}{=}$	$(\forall a \in S \mid (\exists b \in T \mid a \mathcal{R} b))$
b :	$\mathcal{R}$ *est surjectif*	$\stackrel{\text{def}}{=}$	$(\forall b \in T \mid (\exists a \in S \mid a \mathcal{R} b))$
c :	$\mathcal{R}$ *est déterministe*	$\stackrel{\text{def}}{=}$	$(\forall a \in S, b \in T, b' \in T \mid a \mathcal{R} b \wedge a \mathcal{R} b' \Rightarrow b = b')$
d :	$\mathcal{R}$ *est injectif*	$\stackrel{\text{def}}{=}$	$(\forall a \in S, a' \in S, b \in T \mid a \mathcal{R} b \wedge a' \mathcal{R} b \Rightarrow a = a')$.
e :	$\mathcal{R}$ *est bijectif*	$\stackrel{\text{def}}{=}$	$\mathcal{R}$ *est injectif et surjectif.*

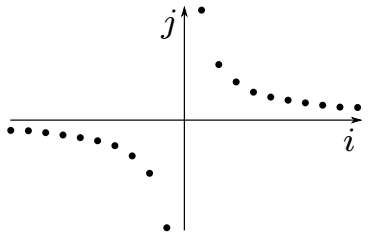
Remarque : Les propriétés de déterminisme et d'injectivité sont peut-être plus faciles à comprendre quand on considère leur contraposition :

c :	$\mathcal{R}$ est déterministe	$\Leftrightarrow$	$(\forall a \in S, b \in T, b' \in T \mid b \neq b' \Rightarrow \neg(a \mathcal{R} b \wedge a \mathcal{R} b'))$
d :	$\mathcal{R}$ est injectif	$\Leftrightarrow$	$(\forall a \in S, a' \in S, b \in T \mid a \neq a' \Rightarrow \neg(a \mathcal{R} b \wedge a' \mathcal{R} b))$.

C'est plus facile à comprendre, mais plus difficile à utiliser dans les démonstrations !

Face à une nouvelle relation, on désirera souvent connaître ses propriétés, c'est-à-dire savoir à quelles familles de relations elle appartient et à quelles familles elle n'appartient pas. À titre d'exemple, considérons la relation "tau" $\tau \subseteq \mathbb{Z} \times \mathbb{R}$ définie par l'ensemble suivant (la figure de droite illustre 20 couples appartenant à l'ensemble τ) :

$$\tau \;=\; \left\{ \langle i, j\rangle \in \mathbb{Z}\times\mathbb{R} \;\middle|\; j = \frac{1}{i} \right\}.$$



Avant de se lancer dans la démonstration des propriétés d'une relation, il convient de l'étudier afin d'avoir une idée (au moins intuitive) de ce que nous voulons démontrer. En jetant un coup d'oeil à la représentation de la relation sur un plan cartésien, on est porté à croire que la relation τ est déterministe et injective (car à chaque i est associé au plus un j, et à chaque j est associé au plus un i), mais non totale et non surjective (car la valeur 0 ne fait pas partie du domaine ni de l'image de τ).

Ces intuitions sont confirmées par la démonstration suivante. Remarquons que pour démontrer qu'une relation *ne possède pas* une propriété (dans ce cas-ci, la totalité et la surjectivité), il faut trouver un **contre-exemple**.

Démonstration :
la relation τ est déterministe, injective, non totale et non surjective.

A **La relation τ est déterministe.**

Démontrons que $(\forall a \in \mathbb{Z}, b \in \mathbb{R}, b' \in \mathbb{R} \mid a\ \tau\ b \wedge a\ \tau\ b' \Rightarrow b = b')$.
Soit $a \in \mathbb{Z}$, $b \in \mathbb{R}$ et $b' \in \mathbb{R}$ et supposons $a\ \tau\ b$ et $a\ \tau\ b'$ ⟨ *démontrons* $b = b'$ ⟩
Comme $a\ \tau\ b$, par définition de τ, on a $b = \frac{1}{a}$.
Comme $a\ \tau\ b'$, par définition de τ, on a $b' = \frac{1}{a}$.
Alors on a $b = b'$. ⟨ *Arithmétique – Transitivité de "="* ⟩
τ est donc une relation déterministe. ⟨ *Point* **A** *démontré.* ⟩

B **La relation τ est injective.**

Démontrons que $(\forall a \in \mathbb{Z}, a' \in \mathbb{Z}, b \in \mathbb{R} \mid a\ \tau\ b \wedge a'\ \tau\ b \Rightarrow a = a')$.
Soit $a \in \mathbb{Z}$, $a' \in \mathbb{Z}$ et $b \in \mathbb{R}$ et supposons $a\ \tau\ b$ et $a'\ \tau\ b$ ⟨ *montrons* $a = a'$ ⟩
Comme $a\ \tau\ b$, par définition de τ, on a $b = \frac{1}{a}$.
Comme $a'\ \tau\ b$, par définition de τ, on a $b = \frac{1}{a'}$.
Alors on a $\frac{1}{a} = \frac{1}{a'}$. ⟨ *Arithmétique – Transitivité de "="* ⟩
Alors on a $a = a'$. ⟨ *Arithmétique* ⟩
τ est bien une relation injective. ⟨ *Point* **B** *démontré.* ⟩

C **La relation τ n'est pas totale.**

Nous devons démontrer que $\neg(\forall a \in \mathbb{Z} \mid (\exists b \in \mathbb{R} \mid a \ \tau \ b)\,)$.
Ce qui est équivalent à démontrer que $(\exists a \in \mathbb{Z} \mid \neg(\exists b \in \mathbb{R} \mid a \ \tau \ b)\,)$.
⟨ *Proposition 1.2.3-a (page 40) – De Morgan, avec* $[P(x) := (\exists b \in \mathbb{R} \mid a \ \tau \ b)]$. ⟩
Ce qui est équivalent à démontrer que $(\exists a \in \mathbb{Z} \mid (\forall b \in \mathbb{R} \mid \neg(a \ \tau \ b))\,)$.
⟨ *Proposition 1.2.3-b (page 40) – De Morgan, avec* $[P(x) := a \ \tau \ b]$. ⟩

Démontrons que $(\exists a \in \mathbb{Z} \mid (\forall b \in \mathbb{R} \mid \neg(a \ \tau \ b))\,)$.
Prenons $a = 0$. ⟨ *Un tel a existe, et* $0 \in \mathbb{Z}$. ⟩
Soit $b \in \mathbb{R}$.
Comme $\frac{1}{0}$ n'est pas un élément de $\mathbb{R}$, on ne peut pas avoir $b = \frac{1}{0}$. ⟨ *Arithmétique* ⟩
Par la définition de τ, on ne peut pas avoir $a \ \tau \ b$.
On a donc $\neg(a \ \tau \ b)$.
τ n'est donc pas une relation totale. ⟨ *Point* **C** *démontré.* ⟩

D **La relation τ n'est pas surjective.**

Nous devons démontrer que $\neg(\forall b \in \mathbb{R} \mid (\exists a \in \mathbb{Z} \mid a \ \tau \ b)\,)$.
Ce qui est équivalent à démontrer que $(\exists b \in \mathbb{R} \mid \neg(\exists a \in \mathbb{Z} \mid a \ \tau \ b)\,)$. ⟨ *De Morgan* ⟩
Ce qui est équivalent à démontrer que $(\exists b \in \mathbb{R} \mid (\forall a \in \mathbb{Z} \mid \neg(a \ \tau \ b))\,)$. ⟨ *De Morgan* ⟩

Démontrons que $(\exists b \in \mathbb{R} \mid (\forall a \in \mathbb{Z} \mid \neg(a \ \tau \ b))\,)$.
Prenons $b = 0$. ⟨ *Un tel b existe, et* $0 \in \mathbb{R}$. ⟩
Soit $a \in \mathbb{Z}$.
On a que $\frac{1}{a} \neq 0$ quelle que soit la valeur de a. ⟨ *Arithmétique* ⟩
On ne peut donc pas avoir $b = \frac{1}{a}$.
On a donc $\neg(a \ \tau \ b)$.
τ n'est donc pas une relation surjective. ⟨ *Point* **D** *démontré.* ⟩
C.Q.F.D.

Pour approfondir la maîtrise de ce type de démonstration, le lecteur est invité à démontrer que la relation $\tau' = \left\{\langle i, j\rangle \in \mathbb{Z} \times \mathbb{R} \mid j = |\frac{1}{i}|\right\}$ n'est pas injective et que la relation $\tau'' = \left\{\langle i, j\rangle \in \mathbb{Z} \times \mathbb{R} \mid j = \frac{1}{i}\right\} \cup \{\langle 0, 42\rangle\}$ est totale.

Propriétés d'une relation inverse

Le théorème suivant fait grandement ressortir la relation de dualité qu'il y a entre la totalité et la surjectivité et entre le déterminisme et l'injectivité. Cependant pour bien comprendre ce qui se passe ici, il est important de bien comprendre la signification de chacune

des phrases qui composent cette démonstration et non seulement de s'assurer formellement que c'est bien une démonstration correcte.

Théorème 1.4.17. *Dualité totalité–surjectivité et dualité déterminisme–injectivité*
Soit $\mathcal{R}$ une relation. Alors :

a :	$\mathcal{R}$ *est total*	$\Leftrightarrow$	$\mathcal{R}^{-1}$ *est surjectif ;*
b :	$\mathcal{R}$ *est déterministe*	$\Leftrightarrow$	$\mathcal{R}^{-1}$ *est injectif ;*
c :	$\mathcal{R}$ *est injectif*	$\Leftrightarrow$	$\mathcal{R}^{-1}$ *est déterministe ;*
d :	$\mathcal{R}$ *est surjectif*	$\Leftrightarrow$	$\mathcal{R}^{-1}$ *est total.*

Démonstration. Soit $\mathcal{R} \subseteq S \times T$.

a : $\mathcal{R}$ est total $\Leftrightarrow$ $\mathcal{R}^{-1}$ est surjectif.

$\mathcal{R}$ est total.
$\Leftrightarrow (\forall a \in S \mid (\exists b \in T \mid a \ \mathcal{R} \ b)\,).$ ⟨ *déf. totalité de $\mathcal{R}$* ⟩
$\Leftrightarrow (\forall a \in S \mid (\exists b \in T \mid b \ (\mathcal{R}^{-1}) \ a)\,).$ ⟨ *déf. $\mathcal{R}^{-1}$* ⟩
$\Leftrightarrow \mathcal{R}^{-1}$ est surjectif. ⟨ *déf. surjectivité de $\mathcal{R}^{-1}$* ⟩

b : $\mathcal{R}$ est déterministe $\Leftrightarrow$ $\mathcal{R}^{-1}$ est injectif.

$\mathcal{R}$ est déterministe.
$\Leftrightarrow (\forall a \in S, b \in T, b' \in T \mid a \ \mathcal{R} \ b \wedge a \ \mathcal{R} \ b' \Rightarrow b = b').$ ⟨ *déf. déterminisme de $\mathcal{R}$* ⟩
$\Leftrightarrow (\forall a \in S, b \in T, b' \in T \mid b \ (\mathcal{R}^{-1}) \ a \wedge b' \ (\mathcal{R}^{-1}) \ a \Rightarrow b = b').$ ⟨ *définition de $\mathcal{R}^{-1}$* ⟩
$\Leftrightarrow (\forall b \in T, b' \in T, a \in S \mid b \ (\mathcal{R}^{-1}) \ a \wedge b' \ (\mathcal{R}^{-1}) \ a \Rightarrow b = b')$
$\Leftrightarrow \mathcal{R}^{-1}$ est injectif. ⟨ *définition de l'injectivité de $\mathcal{R}^{-1}$* ⟩

c : $\mathcal{R}$ est injectif $\Leftrightarrow$ $\mathcal{R}^{-1}$ est déterministe.

$\mathcal{R}$ est injectif.
$\Leftrightarrow (\forall a \in S, a' \in S, b \in T \mid a \ \mathcal{R} \ b \wedge a' \ \mathcal{R} \ b \Rightarrow a = a')$ ⟨ *définition de l'injectivité de $\mathcal{R}$* ⟩
$\Leftrightarrow (\forall a \in S, a' \in S, b \in T \mid b \ (\mathcal{R}^{-1}) \ a \wedge b \ (\mathcal{R}^{-1}) \ a' \Rightarrow a = a')$ ⟨ *définition de $\mathcal{R}^{-1}$* ⟩
$\Leftrightarrow (\forall b \in T, a \in S, a' \in S \mid b \ (\mathcal{R}^{-1}) \ a \wedge b \ (\mathcal{R}^{-1}) \ a' \Rightarrow a = a')$
$\Leftrightarrow \mathcal{R}^{-1}$ est déterministe. ⟨ *déf. déterminisme de $\mathcal{R}^{-1}$* ⟩

d : $\mathcal{R}$ est surjectif $\Leftrightarrow$ $\mathcal{R}^{-1}$ est total.

$\mathcal{R}$ est surjectif.
$\Leftrightarrow (\forall b \in T \mid (\exists a \in S \mid a \ \mathcal{R} \ b)\,).$ ⟨ *définition de la surjectivité de $\mathcal{R}$* ⟩
$\Leftrightarrow (\forall b \in T \mid (\exists a \in S \mid b \ (\mathcal{R}^{-1}) \ a)\,).$ ⟨ *définition de $\mathcal{R}^{-1}$* ⟩
$\Leftrightarrow \mathcal{R}^{-1}$ est total. ⟨ *définition de la totalité de $\mathcal{R}^{-1}$* ⟩

C.Q.F.D.

Propriétés d'une relation composée

Le théorème suivant stipule que les quatre propriétés des relations énoncées par la définition 1.4.16 (page 91) se conservent lors de la composition de deux relations.

Pour bien comprendre ce théorème, il peut être utile de réviser la définition de l'opérateur de composition "$\circ$" (définition 1.4.7, page 84). Ainsi, si $\mathcal{R} \subseteq S \times T$ et $\mathcal{L} \subseteq T \times U$ sont deux relations, la relation composée $(\mathcal{R} \circ \mathcal{L}) \subseteq S \times U$ sera telle que :

$$a\ (\mathcal{R} \circ \mathcal{L})\ c \ \Leftrightarrow\ (\exists b \in T \mid a\ \mathcal{R}\ b \wedge b\ \mathcal{L}\ c)\,.$$

Théorème 1.4.18. *Composition de relations totales, surjectives, déterministes et injectives.*

Soit $\mathcal{R} \subseteq S \times T$ et $\mathcal{L} \subseteq T \times U$ deux relations. Alors :

a :	$\mathcal{R}$ *et* $\mathcal{L}$ *sont totaux*	$\Rightarrow$	$\mathcal{R} \circ \mathcal{L}$ *est total ;*
b :	$\mathcal{R}$ *et* $\mathcal{L}$ *sont déterministes*	$\Rightarrow$	$\mathcal{R} \circ \mathcal{L}$ *est déterministe ;*
c :	$\mathcal{R}$ *et* $\mathcal{L}$ *sont injectifs*	$\Rightarrow$	$\mathcal{R} \circ \mathcal{L}$ *est injectif ;*
d :	$\mathcal{R}$ *et* $\mathcal{L}$ *sont surjectifs*	$\Rightarrow$	$\mathcal{R} \circ \mathcal{L}$ *est surjectif.*

Nous présentons ici la démonstration des deux premiers points du théorème, soit la composition de relations totales et la composition de relations déterministes. Le lecteur est encouragé à compléter la démonstration des deux derniers points de l'énoncé. Il est possible de s'inspirer grandement du travail déjà fait, considérant que, comme nous en informe le théorème 1.4.17 (page 94) il y a dualité entre les notions de totalité et de surjectivité ainsi qu'entre les notions de déterminisme et d'injectivité.

Démonstration (partielle) du théorème 1.4.18 .
Soit $\mathcal{R} \subseteq S \times T$ et $\mathcal{L} \subseteq T \times U$.

a : $\mathcal{R}$ et $\mathcal{L}$ sont totaux $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est total

En supposant	$(\heartsuit)$	$(\forall a \in S \mid (\exists b \in T \mid a\ \mathcal{R}\ b)\ )$
et	$(\heartsuit\heartsuit)$	$(\forall b \in T \mid (\exists c \in U \mid b\ \mathcal{L}\ c)\ )$
Démontrons		$(\forall a \in S \mid (\exists c \in U \mid a\ (\mathcal{R} \circ \mathcal{L})\ c)\ )$

Soit $a \in S$. ⟨ *Montrons* $(\exists c \in U \mid a\ (\mathcal{R} \circ \mathcal{L})\ c)$. ⟩
Prenons $b \in T$ choisi tel que $a\ \mathcal{R}\ b$. ⟨ *Par* $(\heartsuit)$ *un tel b appartenant à T existe bien pour a.* ⟩
Prenons $c \in U$ choisi tel que $b\ \mathcal{L}\ c$. ⟨ *Par* $(\heartsuit\heartsuit)$ *un tel c appartenant à U existe bien pour b.* ⟩
Alors on a bien que $a\ (\mathcal{R} \circ \mathcal{L})\ c$. ⟨ *Par la définition de* $\circ$*, car* $a\ \mathcal{R}\ b$ *et* $b\ \mathcal{L}\ c$. ⟩
$\mathcal{R} \circ \mathcal{L}$ est donc une relation totale. ⟨ *Point "a" démontré* ⟩

b : $\mathcal{R}$ et $\mathcal{L}$ sont déterministes $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est déterministe

En supposant	$(\star)$	$(\forall a \in S, b \in T, b' \in T \mid a \ \mathcal{R}\ b \wedge a \ \mathcal{R}\ b' \Rightarrow b = b')$
et	$(\star\star)$	$(\forall b \in T, c \in U, c' \in U \mid b \ \mathcal{L}\ c \wedge b \ \mathcal{L}\ c' \Rightarrow c = c')$
Démontrons		$(\forall a \in S, c \in U, c' \in U \mid a \ (\mathcal{R} \circ \mathcal{L})\ c \wedge a \ (\mathcal{R} \circ \mathcal{L})\ c' \Rightarrow c = c')$

Soit $a \in S, c \in U, c' \in U$ et supposons $a \ (\mathcal{R} \circ \mathcal{L})\ c$ et $a \ (\mathcal{R} \circ \mathcal{L})\ c'$ ⟨ *Montrons que* $c = c'$. ⟩

Prenons $b \in T$ choisi tel que $a \ \mathcal{R}\ b \wedge b \ \mathcal{L}\ c$

⟨ *Comme* $a \ (\mathcal{R} \circ \mathcal{L})\ c$, *par la définition de* $\circ$, *un tel* b *existe.* ⟩

Prenons $b' \in T$ choisi tel que $a \ \mathcal{R}\ b' \wedge b' \ \mathcal{L}\ c'$

⟨ *Comme* $a \ (\mathcal{R} \circ \mathcal{L})\ c'$, *par la définition de* $\circ$, *un tel* b' *existe.* ⟩

Notons qu'il est a priori possible que b' soit différent de b.

Comme on a $a \ \mathcal{R}\ b$ et $a \ \mathcal{R}\ b'$, on a donc $b = b'$. ⟨ *Voir* $(\star)$. ⟩

Ce dernier fait, combiné avec $b' \ \mathcal{L}\ c'$, nous donne $b \ \mathcal{L}\ c'$.

Ainsi, on a à la fois $b \ \mathcal{L}\ c$ et $b \ \mathcal{L}\ c'$.

On a donc $c = c'$ ⟨ *Voir* $(\star\star)$. ⟩

$\mathcal{R} \circ \mathcal{L}$ est donc une relation déterministe. ⟨ *Point "b" démontré* ⟩

c : $\mathcal{R}$ et $\mathcal{L}$ sont injectifs $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est injectif

Cette partie de la démonstration est laissée en exercice au lecteur.

d : $\mathcal{R}$ et $\mathcal{L}$ sont surjectifs $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est surjectif

Cette partie de la démonstration est laissée en exercice au lecteur.

C.Q.F.D.

1.4.5 Fonctions (totales) et fonctions partielles

Une relation est appelée une **fonction** (ou **fonction totale**) si elle est à la fois totale et déterministe[30]. Autrement dit, une relation $f \subseteq X \times Y$ est une fonction lorsque pour chaque $x \in X$ il existe *un et un seul* $y \in Y$ tel que $\langle x, y \rangle \in f$. En effet :

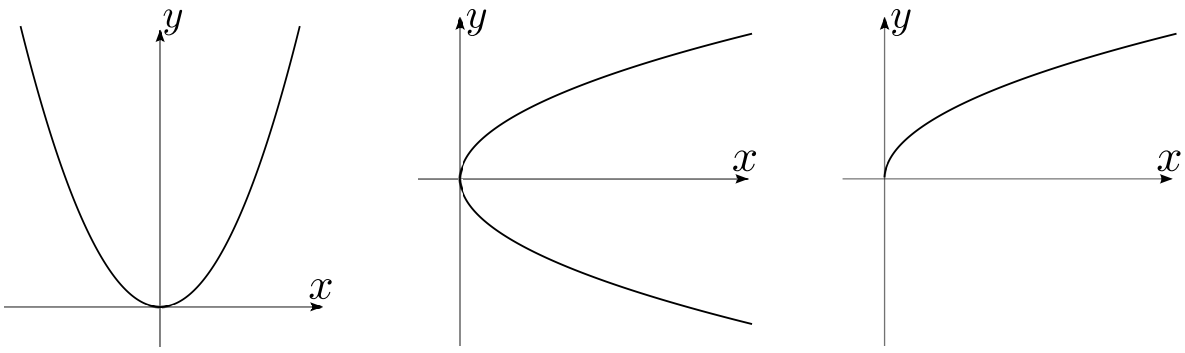
- le fait que pour chaque $x \in X$ il existe *un* $y \in Y$ établit que f est une relation totale ;
- le fait que pour chaque $x \in X$ il n'existe qu'*un seul* $y \in Y$ établit que f est une relation déterministe.

Nous utilisons le terme **fonction partielle** pour désigner une relation déterministe qui n'est pas totale. Autrement dit, une relation $f \subseteq X \times Y$ est une fonction partielle lorsque

30. Il s'agit d'une convention que nous adoptons pour ce cours et qui est fréquemment utilisée en mathématiques. Notez cependant que certains auteurs utilisent plutôt le terme "**application**" pour désigner une relation totale et déterministe. Dans ce cas, le terme "fonction" désigne une relation déterministe (et pas nécessairement totale).

pour chaque $x \in X$ il y a *au plus* un $y \in Y$ tel que $\langle x, y\rangle \in f$ et il existe un $x \in X$ tel que $(\forall y \in Y \mid x \notin Y)$.

À titre d'exemple, la figure 1.11 présente trois relations dans le plan cartésien ($\mathbb{R}^2$). La parabole ($y = x^2$) est une fonction, la racine carrée ($y = \sqrt{x}$) est une fonction partielle et l'inverse de la parabole ($y^2 = x$) n'est ni une fonction ni une fonction partielle. En fait, l'inverse de la parabole est une relation bijective.



(a) $\{\langle x, y\rangle \in \mathbb{R}^2 \mid y = x^2\}$ (b) $\{\langle x, y\rangle \in \mathbb{R}^2 \mid x = y^2\}$ (c) $\{\langle x, y\rangle \in \mathbb{R}^2 \mid y = \sqrt{x}\}$

FIGURE 1.11 – Exemples d'une fonction (a), d'une relation non déterministe (b) et d'une fonction partielle (c). Notez que le graphique de l'exemple (c) peut aussi représenter une fonction si on considère plutôt la relation totale et déterministe $\{\langle x, y\rangle \in \mathbb{R}^+ \times \mathbb{R} \mid y = \sqrt{x}\}$ avec $\mathbb{R}^+ \stackrel{\text{def}}{=} \{x \in \mathbb{R} \mid x \geq 0\}$.

Notation et règle de correspondance

Lorsqu'une relation f est une fonction, l'expression "$\langle x, y\rangle \in f$" pourra être remplacée par "$f(x) = y$" (la notation "$f.x = y$" est aussi utilisée à l'occasion, mais la notation infixe "$x\ f\ y$" n'est utilisée que lorsqu'on ne voit f que comme une relation). Ainsi :

$$f(x) = y \quad \stackrel{\text{def}}{=} \quad \langle x, y\rangle \in f\,.$$

Contrairement au cas où la relation f n'est pas une fonction, cette nouvelle notation ne comporte ici aucune ambiguïté puisque que chaque "x" de l'ensemble de départ est en relation avec *un* et *un seul* "y" de l'ensemble d'arrivée.

On utilise le terme **règle de correspondance** pour désigner la règle qui permet de savoir à quel élément y de l'ensemble d'arrivée correspond chacun des éléments x de l'ensemble de départ. Dans le cadre de ce cours, pour démontrer qu'une relation définie par règle de correspondance est une fonction, il sera suffisant de dire que cette règle de correspondance

est bien définie (c'est-à-dire que cette règle associe bien à chaque élément de l'ensemble de départ *un* et *un seul* élément de l'ensemble d'arrivé.)

Il y a plusieurs notations permettant de bien définir une fonction, nous utiliserons souvent la suivante, puisqu'elle met clairement en évidence les trois notions nécessaires pour "connaître complètement" une fonction (ensemble de départ, ensemble d'arrivée et règle de correspondance) :

$$\begin{array}{rccc} f: & X & \longrightarrow & Y \\ & a & \longmapsto & [\ldots] \end{array}$$

Cette notation signifie : f est une fonction d'ensemble de départ X, d'ensemble d'arrivée Y, qui est définie par la règle de correspondance "$f(a) = [\ldots]$". Par exemple, on définit la parabole sur le plan cartésien (fréquemment représentée par l'équation " $y = x^2$ ") par :

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^2 \end{array}$$

Ce qui est équivalent à :

$$f \;=\; \{\langle x, y\rangle \in \mathbb{R}^2 \mid y = x^2\}\,.$$

PENSEZ-Y!

Il ne faut pas perdre de vue qu'une fonction est un ensemble. Ainsi, toutes les notations utilisées jusqu'ici pour définir un ensemble sont également valides. Comme discuté à la section 1.2.2 (page 33), on peut toujours définir un ensemble par compréhension ou par extension.

Par exemple, une fonction d qui associe un nombre relatif avec le double de sa valeur (c'est-à-dire $d(x) = 2x$) peut-être écrite des manières suivantes :

(1) $$\begin{array}{rccc} d: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & 2x\,, \end{array}$$

(2) $d \;=\; \{\langle a, b\rangle \in \mathbb{Z}^2 \mid b = 2a\}$,

(3) $d \;=\; \{\ldots, \langle -3, -6\rangle, \langle -2, -4\rangle, \langle -1, -2\rangle, \langle 0, 0\rangle, \langle 1, 2\rangle, \langle 2, 4\rangle, \langle 3, 6\rangle, \ldots\}$.

Les équations (1) et (2) définissent l'ensemble d par compréhension, tandis que l'équation (3) définit l'ensemble d par extension. Rappelons qu'il n'y a *aucune distinction* entre les ensembles obtenus par les trois définitions.

Cette dernière constatation peut paraître dérangeante à un informaticien, qui conçoit que pour programmer une telle "fonction", il est beaucoup plus efficace de multiplier une variable par 2 que de parcourir une liste pour trouver la réponse désirée. Ici, il importe de distinguer le concept d'une fonction dans la théorie des ensembles et le concept d'une fonction du point de vue d'un langage de programmation. Bien qu'il s'agisse d'un problème important, le "temps de calcul" d'une fonction ne nous intéresse pas pour l'instant, et nous travaillons consciemment avec des outils qui en font abstraction.

Dans les énoncés énoncés mathématiques et les démonstrations qui suivent, nous écrirons souvent "*Soit une fonction* $f : S \longrightarrow T$*...*" pour présenter une relation $f \subseteq S \times T$ qui est à la fois déterministe et totale.

Fonctions surjectives, injectives et bijectives

Les deux prochaines propositions montrent que, lorsqu'une relation f est une fonction, la notation "$f(a) = b$" permet de réécrire les définitions d'injectivité et de surjectivité.

Proposition 1.4.19. *Définitions équivalentes d'une fonction surjective*
Soit une fonction $f : S \longrightarrow T$*. Les deux expressions suivantes sont équivalentes :*

a : $(\forall b \in T \mid (\exists a \in S \mid a \ f \ b))$
b : $(\forall b \in T \mid (\exists a \in S \mid f(a) = b))$

La proposition 1.4.19-a correspond à la définition originale d'une relation surjective (définition 1.4.16-b, page 91), tandis que la proposition 1.4.19-b est obtenue en utilisant la notation "$f(a) = b$" propre aux fonctions.

Proposition 1.4.20. *Définitions équivalentes d'une fonction injective*
Soit une fonction $f : S \longrightarrow T$*. Les trois expressions suivantes sont équivalentes :*

a : $(\forall a \in S, a' \in S, b \in T \mid a \ f \ b \wedge a' \ f \ b \Rightarrow a = a')$
b : $(\forall a \in S, a' \in S \mid f(a) = f(a') \Rightarrow a = a')$
c : $(\forall a \in S, a' \in S \mid a \neq a' \Rightarrow f(a) \neq f(a'))$

La proposition 1.4.20-a correspond à la définition originale d'une relation injective (définition 1.4.16-d, page 91) et la proposition 1.4.20-b est obtenue en utilisant la notation "$f(a) = b$" propre aux fonctions. À partir de cette dernière, on obtient la proposition 1.4.20-c en appliquant la propriété de contraposition (Proposition 1.1.9, page 18).

Les propositions 1.4.19 et 1.4.20 sont bien sûr utiles pour démontrer qu'une fonction possède (ou non) la propriété de surjectivité ou d'injectivité. À titre d'exemple, considérons la fonction suivante :

$$\begin{array}{rccc} k: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & 2x \end{array}$$

Intuitivement, la fonction k semble être une relation injective (car chaque élément de l'image "$2x$" semble associé à un seul élément du domaine "x") mais non surjective (car les nombres impairs ne semblent pas faire partie de l'image). Pour en être certain, en voici la démonstration.

Démonstration : la fonction k est injective, mais non surjective.

A La fonction k est injective.

Comme k est une fonction, nous allons démontrer :

$$(\forall x \in \mathbb{Z}, x' \in \mathbb{Z} \mid k(x) = k(x') \Rightarrow x = x')\,.$$

Soit $x \in \mathbb{Z}$ et $x' \in \mathbb{Z}$ et supposons $k(x) = k(x')$. ⟨ *Montrons* $x = x'$ ⟩
Alors on a $2x = 2x'$. ⟨ *Définition de* k ⟩
Alors on a $\frac{2x}{2} = \frac{2x'}{2}$. ⟨ *Arithmétique* ⟩
Alors on a $x = x'$. ⟨ *Arithmétique* ⟩
k est bien une fonction injective. ⟨ *Point* **A** *démontré.* ⟩

B La fonction k est non surjective

Nous devons donc démontrer :

$$\neg(\forall y \in \mathbb{Z} \mid (\exists x \in \mathbb{Z} \mid k(x) = y))\,.$$

Ce qui est équivalent à démontrer $(\exists y \in \mathbb{Z} \mid \neg(\exists x \in \mathbb{Z} \mid k(x) = y))$. ⟨ *De Morgan* ⟩
Ce qui est équivalent à démontrer $(\exists y \in \mathbb{Z} \mid (\forall x \in \mathbb{Z} \mid k(x) \neq y))$. ⟨ *De Morgan* ⟩

Démontrons donc $(\exists y \in \mathbb{Z} \mid (\forall x \in \mathbb{Z} \mid k(x) \neq y))$.
Prenons $y = 3$. ⟨ *Un tel* y *existe et* $\in \mathbb{Z}$*, car* $3 \in \mathbb{Z}$. ⟩
Soit $x \in \mathbb{Z}$. ⟨ *Montrons* $k(x) \neq y$ ⟩
Alors clairement, $k(x) = 2x \neq 3$, car 3 n'est pas un nombre pair. ⟨ *Arithmétique* ⟩
k n'est pas une fonction surjective. ⟨ *Point* **B** *démontré.* ⟩

C.Q.F.D.

Fonctions inverses

Considérons une fonction $f : S \longrightarrow T$. La **fonction inverse** de f est une fonction $g : T \longrightarrow S$ telle que, pour tout $\langle a, b\rangle \in S \times T$, on a $f(\,g(b)\,) = b$ et $g(\,f(a)\,) = a$. Notons qu'il est toujours possible de calculer la relation inverse f^{-1} d'une fonction f (voir la définition 1.4.12), mais que la relation f^{-1} n'est pas nécessairement une fonction. Plus précisément, les résultats suivants découlent directement du théorème 1.4.17.

Corollaire 1.4.21. *Inverses de fonctions et de relations*
Soit f une relation.

a :	*f est une fonction*	$\Leftrightarrow$	*f^{-1} est une relation bijective ;*
b :	*f est une fonction injective*	$\Leftrightarrow$	*f^{-1} est une relation bijective et déterministe ;*
c :	*f est une fonction surjective*	$\Leftrightarrow$	*f^{-1} est une relation bijective et totale ;*
d :	*f est une fonction bijective*	$\Leftrightarrow$	*f^{-1} est une fonction bijective.*

Le théorème suivant établit le lien entre les notions de composition de relations et de fonctions inverses.

Théorème 1.4.22. *Composition de fonctions inverses*
Soit $\mathcal{R} \subseteq S \times T$ et $\mathcal{L} \subseteq T \times S$ deux relations. On a que $\mathcal{R}$ et $\mathcal{L}$ sont deux fonctions bijectives et $\mathcal{R}^{-1} = \mathcal{L}$ si et seulement si :

$$\mathcal{R} \circ \mathcal{L} \;=\; \mathbf{I}_S \quad \textit{et} \quad \mathcal{L} \circ \mathcal{R} \;=\; \mathbf{I}_T\,.$$

1.4.6 Exercices sur les relations et fonctions

Exercice 1 : (*Vous pouvez faire cet exercice en représentant vos relations par des graphes.*)

Étant données les trois relations $\rho, \sigma, \theta \subseteq \{1,2,3,4\} \times \{1,2,3,4\}$ suivantes :
- $\rho = \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 3,4\rangle, \langle 4,1\rangle\}$
- $\sigma = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,1\rangle, \langle 3,1\rangle, \langle 4,1\rangle\}$
- $\theta = \{\langle x,y\rangle \mid x \leq y\}$

1. Calculez $\rho \circ \sigma$, ρ^2, θ^c et θ^{-1}.
2. Déterminez la (ou les) propriété(s) que la relation ρ satisfait parmi les suivantes :
   (a) réflexivité (b) irréflexivité (c) symétrie
   (d) asymétrie (e) antisymétrie (f) transitivité
3. Même question pour la relation σ.
4. Même question pour la relation θ.
5. Existe-t-il un n pour lequel $\rho^n = \{1,2,3,4\} \times \{1,2,3,4\}$? Si oui, trouvez le plus petit de ces n.
6. Même question pour la relation σ.
7. Même question pour la relation θ.

Exercice 2 : (*Pour ce numéro, aucune justification n'est demandée.*)

Étant données les deux relations $\rho, \theta \subseteq \mathbb{Z} \times \mathbb{Z}$ suivantes :
- $\rho = \{\langle i,j\rangle \mid i+1 = j\}$
- $\theta = \{\langle x,y\rangle \mid (\exists z \in \mathbb{Z} \mid 2z = x - y)\}$

a) Donnez ρ^2, θ^c et θ^{-1}.

b) Déterminez la (ou les) propriété(s) que la relation ρ satisfait parmi les suivantes :
   (a) réflexivité (b) irréflexivité (c) symétrie
   (d) asymétrie (e) antisymétrie (f) transitivité

c) Même question pour la relation θ.

Exercice 3 : Quelles propriétés parmi : *réflexivité, irréflexivité, symétrie, asymétrie, antisymétrie et transitivité* les relations suivantes possèdent-elles ?

a) $b \mathcal{R} c$ ssi b et c sont des entiers tous deux négatifs ou tous deux positifs.

b) $b \mathcal{R} c$ ssi b et c sont des entiers tels que $b - c$ est un multiple de 5.

c) $\emptyset$, où $\emptyset$ est une relation sur un ensemble non vide B.

d) $\mathbf{I}_B$, la relation identité sur un ensemble non vide B.

e) $B \times B$ où B est un ensemble non vide contenant au moins deux éléments.

f) $=$ sur $\mathbb{Z}$.

g) $<$ sur $\mathbb{Z}$.

h) $\leq$ sur $\mathbb{Z}$.

i) $b \ \rho \ c$ ssi b est le père de c.

j) $b \ \rho \ c$ ssi b est le père de c ou vice-versa.

k) $b \ \rho \ c$ ssi b est c ou le père de c.

Exercice 4 : Démontrez la définition équivalente de l'antisymétrie (Proposition 1.4.15-e) :

$$(\forall a, b \in S \mid a \,\mathcal{R}\, b \wedge b \,\mathcal{R}\, a \Rightarrow a = b) \ \Leftrightarrow \ \mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathbf{I}_S \,.$$

Exercice 5 : (*Pour cet exercice, aucune réponse n'a à être justifiée.*) Dites si chacune des relations suivantes est (*i*) déterministe, (*ii*) totale, (*iii*) injective, (*iv*) surjective, (*v*) une fonction, (*vi*) une fonction injective, (*vii*) une fonction surjective ou (*viii*) une fonction bijective.

a) $\rho = \{\langle i, j\rangle \in \mathbb{R}^2 \mid i + 1 = j\}$;

b) $\sigma = \{\langle i, j\rangle \in \mathbb{N}^2 \mid i + 1 = j\}$;

c) $\theta = \{\langle i, j\rangle \in \mathbb{N}^2 \mid i - 1 = j\}$;

d) $d : \mathbb{R} \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $d(x) = x^2$;

e) la relation inverse de la relation d définie en d) ;

f) $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $f(x) = x^2$;

g) $g : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$, définie par la règle de correspondance : $g(x) = x^2$;

h) $h : \mathbb{R} \longrightarrow [-1, 1]$, définie par la règle de correspondance : $h(x) = sin(x)$;

i) $i : \mathbb{R} \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $i(x) = x^3$;

j) la relation inverse de la relation i définie en i) ;

k) $k : \mathbb{R} \longrightarrow \mathbb{R}^+$, définie par la règle de correspondance : $k(x) = 2^x$;

l) $l : \mathbb{R} \longrightarrow \mathbb{R}^+$, définie par la règle de correspondance : $l(x) = log_2(x)$;

m) $m : \mathbb{R}^+ \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $m(x) = log_2(x)$.

Exercice 6 : (*Pour ce numéro, seuls le c) et le g) nécessitent quelques justifications et vous pouvez définir toute relation par une représentation graphique.*)

a) Construisez une relation $\rho \subseteq A \times B$ qui soit une fonction bijective.

b) Construisez une relation $\theta \subseteq C \times D$ qui ne soit ni totale, ni déterministe, ni injective, ni surjective.

c) Dans votre réponse en a), est-ce que $|A| = |B|$? Si oui, recommencez la question a) de telle sorte que $|A| \neq |B|$. Si vous n'y arrivez pas, expliquez pourquoi.

d) Soit $E = \{1, 2, 3\}$. Construisez une fonction $f : E \longrightarrow \mathcal{P}(E)$.

e) À partir de la fonction f que vous avez fabriquée en d), construisez l'ensemble $T = \{e \in E \mid e \notin f(e)\}$.

f) Étant donné le f et le T que vous avez construits, est-ce que T appartient à l'ensemble d'arrivée de f ?

g) Étant donné le f et le T que vous avez construits, est-ce que $T \in \mathrm{Im}(f)$?
Si vous avez répondu non, refaites les numéros d) et e) de telle sorte que $T \in \mathrm{Im}(f)$.
Si vous n'y arrivez pas, expliquez brièvement pourquoi.

Exercice 7 : (*Pour cet exercice, toute réponse doit être pleinement justifiée.*)
Soit les cinq relations :

— $\rho \subseteq \mathbb{N} \times \mathbb{N}$, définie par : $\rho = \{\langle i, j\rangle \mid i + 1 = j\}$
— $\theta \subseteq \mathbb{Z} \times \mathbb{Z}$, définie par : $\theta = \{\langle x, y\rangle \mid (\exists z \in \mathbb{Z} \mid 2z = x - y)\}$
— $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, définie par la règle de correspondance : $f(x) = x + 3$
— $g : \mathbb{N} \longrightarrow \mathbb{N}$, définie par la règle de correspondance : $g(x) = x + 3$
— $h : \mathbb{Z} \longrightarrow \mathbb{Z}$, définie par la règle de correspondance : $h(x) = x^2$

A) Pour chacune d'elle, déterminez si oui ou non, il s'agit :

1) d'une relation déterministe
2) d'une fonction (c.-à-d. : déterministe et totale) ;
3) d'une fonction injective (c.-à-d. : déterministe, totale et injective) ;
4) d'une fonction surjective (c.-à-d. : déterministe, totale et surjective) ;
5) d'une fonction bijective (c.-à-d. : déterministe, totale, injective et surjective).

B) Donnez la fonction inverse de chacune des fonctions bijectives trouvées en A5).

Exercice 8 : Étant donnée une fonction $h : \mathbb{Z} \longrightarrow \mathbb{Z}$

- h est strictement croissante $\stackrel{\text{def}}{=} (\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow h(x) < h(x'))$
- h est strictement décroissante $\stackrel{\text{def}}{=} (\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow h(x) > h(x'))$

(A) Démontrez que la composition de deux fonctions est encore une fonction (B) Démontrez l'énoncé suivant :

Si $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ et $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ sont deux fonctions strictement décroissantes alors $f \circ g$ est une fonction strictement croissante.

(C) Démontrez l'énoncé suivant :

Si $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ et $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ sont deux fonctions strictement croissantes alors $f \circ g$ est une fonction strictement croissante.

Exercice 9 : On désire modéliser une base de données contenant des informations sur les étudiants et les cours de l'université à l'aide de relations. On considère les trois ensembles suivants :

— L'ensemble ETUDIANTS contenant les noms des étudiants de l'université.
— L'ensemble ENSEIGNANTS contenant les noms des enseignants.
— L'ensemble COURS contenant les sigles des cours offerts par l'université.

De plus, on modélise les tables de la base de données à l'aide des deux relations suivantes :

— La relation EtudCo $\subseteq$ ETUDIANTS $\times$ COURS qui associe les étudiants aux cours qu'ils suivent.
— La relation EnsCo $\subseteq$ ENSEIGNANTS $\times$ COURS qui associe les enseignants aux cours qu'ils donnent.

a) Écrivez l'ensemble des étudiants

1. inscrits au cours `MAT1919`. Bien sûr, on suppose ici que `MAT1919` $\in$ COURS.
2. qui ne sont inscrits qu'au cours `MAT1919`.
3. qui ne sont inscrits à aucun cours
4. qui sont inscrits à au moins un cours

b) Que retournent les ensembles suivants ?

1. $\{e \in \text{ETUDIANTS} \mid (\forall y \in \text{COURS} \mid \langle e, y\rangle \in \text{EtudCo} \Rightarrow y = \texttt{MAT1919})\}$
2. $\{e \in \text{ETUDIANTS} \mid (\forall y \in \text{COURS} \mid \langle e, y\rangle \in \text{ETUDIANTS} \times \text{COURS} \Rightarrow y = \texttt{MAT1919})\}$
3. $\{e \in \text{ETUDIANTS} \mid (\exists \texttt{MAT1919} \in \text{COURS} \mid \langle e, \texttt{MAT1919}\rangle \in \text{EtudCo})\}$

c) Dites à quoi correspond la relation EnsCo^{-1}.

d) En combinant les relations EnsCo et EtudCo à l'aide des opérateurs de relations appropriés, écrivez la définition d'une nouvelle relation qui associe les étudiants aux enseignants qu'ils subissent à cette session. Vous devez définir cette relation à partir de ces deux relations

seulement (vous ne pouvez pas définir une relation intermédiaire).

e) Dites quelle interprétation possède l'expression suivante :

$$(\exists x \in \text{ENSEIGNANTS} \mid (\forall y \in \text{COURS} \mid \neg(x \,\text{EnsCo}\, y)))\,.$$

Comment écrirait-on qu'il en existe plusieurs (au moins 2) ?

Exercice 10 : Sans justifier vos réponses, dites si les énoncés suivants sont VRAIS ou FAUX.

a) une relation asymétrique est toujours antisymétrique et irréflexive. _____.

b) Si $\rho = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x < y\}$, alors $\rho^{-1} = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x > y\}$ et $\rho^c = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x \geq y\}$. _____.

c) Si $\theta = \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N})^2 \mid A \subset B\}$, alors $\theta^{-1} = \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N})^2 \mid A \supset B\}$ et $\theta^c = \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N})^2 \mid A \supseteq B\}$. _____.

Exercice 11 : (*Pour fin de réflexion et de discussion*) Un hôtel a un nombre infini de chambres (pour chaque entier $i > 0$, il y a une chambre portant le numéro i). L'hôtel est plein (il y a un voyageur dans chaque chambre). Arrive un nouveau voyageur qui voudrait bien dormir à l'hôtel lui aussi. Alors l'hôtelier lui dit qu'il va lui trouver une chambre. Il ne mettra à la porte aucun voyageur, il ne mettra pas deux voyageurs dans une même chambre et il ne fera pas construire une nouvelle chambre. Alors comment l'hôtelier fera-t-il ?

Exercice 12 : (*Pour fin de réflexion et de discussions*) Une charrue enlève la neige le long d'une route qui s'étend jusqu'à l'infini. Tout au long de la route, il y a 15cm de neige. La pelle de la charrue laisse écouler un quinzième de la neige qui entre dans sa pelle (c.-à-d. : 1cm de neige sur les 15). Supposant que la pelle a une capacité infinie et que les flocons qu'elle laisse écouler sortent selon un principe "premier entré, premier sorti", quelle quantité de neige restera dans la pelle une fois le travail terminé ?

Exercice 13 : (*Pour fin de réflexion et de discussions*) Vous avez deux ensembles infinis, comment savoir lequel des deux a le plus grand nombre d'éléments ?

1.5 Ensembles infinis

> Only two things are infinite, the universe and human stupidity and I'm not sure about the former.
>
> Albert Einstein (1879 – 1955)

Dans cette dernière partie du chapitre, nous nous intéressons aux ensembles de taille infinie. Même en informatique, nous sommes confrontés à de telles structures, entre autres lorsque l'on se demande quelles sont les possibilités et les limites de l'informatique. Par exemple, lorsqu'on se pose des questions telles que :

— *Qu'est-ce qui est calculable en informatique ?*
— *Étant donné un problème, peut-on toujours décider si ce problème a une solution ou non ?*

Dans un autre ordre d'idées, si on souhaite développer un système qui aura à interagir avec le monde réel, on est confronté à la notion d'infini. En effet, ce monde réel, la plupart du temps, fait appel à des paramètres continus, telles la distance, la température, la vitesse. Ces paramètres peuvent prendre une infinité de valeurs différentes.

Les structures infinies sont en général beaucoup plus difficiles à étudier que les structures finies. Notre intuition, généralement solide face aux structures finies, est grandement mise à l'épreuve devant l'infini. À titre d'exemple :

> *Une charrue enlève la neige le long d'une route qui s'étend jusqu'à l'infini. Tout au long de la route, il y a 15 cm de neige. La pelle de la charrue laisse écouler un quinzième de la neige qui entre dans sa pelle (c.-à-d. : 1cm de neige sur les 15). Supposant que la pelle a une capacité infinie et que les flocons qu'elle laisse écouler sortent selon le principe du premier arrivé, premier servi, quelle quantité de neige restera dans la pelle pour toujours ?*

Cet exemple est bien sûr irréalisable dans notre monde. Si on fait cependant abstraction de ce petit détail et qu'on analyse le problème selon la théorie des ensembles, on est obligé de constater que chaque flocon qui entre dans la pelle finira par en sortir, donc "qu'une fois le travail terminé", il ne restera plus rien dans la pelle.

Dans ce chapitre, nous nous intéresserons plus particulièrement au problème de la cardinalité des ensembles. Nous savons déjà que calculer la **cardinalité d'un ensemble fini** revient à compter le nombre d'éléments que cet ensemble contient. Il est évident que dans le

cas des ensembles infinis, cette approche n'est pas envisageable. Pour les ensembles infinis, nous ne pourrons faire mieux que de comparer les ensembles infinis les uns avec les autres. Nous aurons donc des résultats du type :

- un ensemble A *a autant d'éléments* qu'un ensemble B, ce que nous traduirons par : *la cardinalité de A est égale à celle de B* ;

ou encore :

- un ensemble A *a moins d'éléments* qu'un ensemble B,
  ce que nous traduirons par : *la cardinalité de A est plus petite que celle de B.*

Encore une fois, dans le cas des ensembles finis, dire qu'un ensemble A a moins, autant, ou plus d'éléments qu'un ensemble B n'est pas compliqué. Il nous suffit de savoir "compter jusque-là". Dans le cas des ensembles infinis, on *ne sait clairement pas* "compter jusque-là". Il nous faudra donc développer une autre méthode pour arriver à nos fins.

En plus, quelques surprises nous attendent. L'exemple suivant nous en donne un avant-goût :

Le problème de l'hôtel de Hilbert :

> *Un hôtel a un nombre infini de chambres (pour chaque entier $i > 0$, il y a une chambre portant le numéro i). L'hôtel est plein (il y a un voyageur dans chaque chambre). Arrive un nouveau voyageur qui voudrait bien dormir à l'hôtel lui aussi. Alors l'hôtelier lui dit qu'il va lui trouver une chambre. Il ne mettra à la porte aucun voyageur, il ne mettra pas deux voyageurs dans une même chambre et il ne fera pas construire une nouvelle chambre. Alors comment l'hôtelier fera-t-il ?*

Si on énumère par $\mathbb{N}^* = \{1, 2, 3, 4, \ldots\}$ l'ensemble des numéros de porte des chambres de l'hôtel, qu'on donne au nouveau voyageur l'étiquette "0" et à chaque voyageur déjà dans une chambre l'étiquette correspondant au numéro de sa chambre, voici ce que l'hôtelier peut faire :

— *Installer le voyageur "0" dans la chambre "1" ;*
— *Déménager le voyageur "1" dans la chambre "2" ;*
— *Déménager le voyageur "2" dans la chambre "3" ;*
— *Déménager le voyageur "3" dans la chambre "4" ;*
— *etc.*

Cette solution va bien sûr déranger beaucoup de monde. Mais, en fin de compte, chaque voyageur dormira seul dans une chambre !

Le fait qu'il y ait une solution à ce problème choque notre intuition. Ce choc vient du fait que, logiquement, il nous faut conclure qu'*il y a autant d'éléments* dans $\mathbb{N}^*$ que dans $\mathbb{N}$,

alors que le premier ensemble est *strictement inclus* dans le second ; la notion d'avoir autant d'éléments semble être plutôt élastique dans le cas des ensembles infinis.

Il devient donc de plus en plus évident que le problème du calcul de la cardinalité d'un ensemble infini sera un problème difficile à résoudre. En fait, comme il a déjà été dit auparavant, on ne répondra pas directement à la question "combien tel ensemble infini a-t-il d'éléments ?". On comparera plutôt deux à deux les ensembles, en se demandant s'ils ont autant d'éléments l'un que l'autre ou si l'un en a plus que l'autre. De ces éléments de comparaison, on pourra déduire une hiérarchie des cardinalités des différents ensembles infinis.

1.5.1 "Avoir autant d'éléments"

À la recherche d'une définition

Si on veut arriver à bien définir cette notion d'ensemble infini ayant **autant d'éléments** qu'un autre, il nous faut trouver une méthode qui, dans le cas fini, permet d'établir si oui ou non deux ensembles ont le "même nombre d'éléments". Toutefois, cette méthode ne doit pas reposer sur notre capacité de compter les éléments des ensembles finis. On est en effet en droit d'espérer qu'une telle méthode soit applicable aux ensembles infinis. Nous sommes donc face à ce problème un peu comme un jeune enfant qui a dans une main des pierres blanches et dans l'autre des pierres noires, et qui se demande si, oui ou non, chaque main a autant de pierres.

Voici une solution qui convient au niveau des capacités de l'enfant (en fait cette solution a vraiment été proposée à un enfant de trois ans) :

> *Prends une pierre blanche et une pierre noire et place-les côte à côte, puis prends une autre pierre blanche et une autre pierre noire et place-les côte à côte, juste en dessous de celles que tu as déjà placées, continue ce processus tant qu'il reste de pierres de chacun des deux tas. Si les deux tas se finissent en même temps, c'est que tu en avais autant dans chaque main, sinon c'est le tas dans lequel il reste encore des pierres qui en avait le plus.*

L'enfant fabrique, par ce procédé, une *relation* entre le tas de pierres blanches et celui de pierres noires. Si nous sommes dans la situation où les deux tas sont épuisés en même temps, c'est que la relation fabriquée est une **fonction bijective** (voir la définition à la section 1.4.5). Autrement dit, dans le cas fini, nous avons le résultat suivant :

Théorème 1.5.1. *Deux ensembles finis A et B ont le même nombre d'éléments si et seulement s'il existe une fonction bijective $f : A \longrightarrow B$.*

Rappelons-nous que pour l'instant, la notion avoir "**autant d'éléments**" n'a toujours pour les ensembles infinis aucune signification. Pour remédier à ce problème, nous pourrions nous baser sur ce dernier théorème et *décider* (comme Cantor !) que deux ensembles (finis ou infinis) ont "autant d'éléments" si on peut trouver une fonction bijective de l'un vers l'autre. Autrement dit :

Définition 1.5.2. *Soit A et B, deux ensembles. A et B* ont autant d'éléments *(ou* ont la même cardinalité*) ssi il existe une fonction bijective de A vers B.*

Comme nous l'avons vu à la section 1.2.2 la phrase "la cardinalité de A est égale à la cardinalité de B" est notée "$|A| = |B|$".

Notre définition est-elle correcte ?

À la base, cette définition d'avoir "autant d'éléments" est un choix que nous faisons ici. On aurait pu retenir une autre définition qui, dans le cas fini, aurait coïncidé avec notre définition.

Donc, avant d'accepter cette nouvelle définition, il serait bon de nous demander si elle correspond bien à une notion élargie de la notion d'**égalité** entre le nombre d'éléments d'un ensemble et le nombre d'éléments d'un autre ensemble. Car une fois qu'on se l'est donnée, elle devient un axiome de notre théorie et on doit vivre avec et accepter tous les résultats que nous démontrerons à partir de cette définition, même si parfois ceci pourrait heurter l'intuition que nous avons de ce concept d'avoir "autant d'éléments".

Concrètement, une bonne définition de cette notion "d'égalité" de cardinalités devrait posséder les trois grandes propriétés :

- **la réflexivité** Est-ce qu'avec cette définition, un ensemble A a toujours la même cardinalité que lui-même ?
  Autrement dit, est-ce que pour tout ensemble A, on a $|A| = |A|$?
- **la symétrie** Avec cette définition, le fait qu'un ensemble A ait la même cardinalité qu'un ensemble B implique-t-il toujours que B a la même cardinalité que A ?
  Autrement dit, est-ce que pour tout A, B, on a $|A| = |B| \Rightarrow |B| = |A|$?
- **la transitivité** Est-ce qu'avec cette définition, le fait qu'un ensemble A ait la même cardinalité qu'un ensemble B combiné au fait que ce B ait la même cardinalité qu'un

troisième ensemble C implique toujours que A a la même cardinalité que C ?
Autrement dit, est-ce que pour tout A, B, C,
on a $(|A| = |B|) \wedge (|B| = |C|) \Rightarrow (|A| = |C|)$?

Nous démontrerons à la section 1.7.2 (page 142) que la notre définition d'avoir "autant d'éléments" possède bien les trois propriétés ci-haut, lorsque nous présenterons le concept de **relation d'équivalence** (une relation d'équivalence étant justement un relation qui est à la fois réflexive, symétrique et transitive). Bien qu'un lecteur curieux est libre d'aller consulter la section 1.7 immédiatement, nous tiendrons pour l'instant ce fait pour acquis afin de se concentrer sur les concepts clés des ensembles infinis.

1.5.2 "Autant" d'éléments que $\mathbb{N}$: Les ensembles infinis dénombrables

Parmi les ensembles infinis, une certaine classe est plus intéressante que les autres, c'est celle des **ensembles infinis dénombrables** :

Définition 1.5.3. *Un ensemble A est dit* dénombrable *s'il est fini ou de la même cardinalité que l'ensemble* $\mathbb{N}$.

Établir une bijection f entre l'ensemble des **nombres naturels** $\mathbb{N}$ et un ensemble A donne une énumération des éléments de A. On peut ainsi analyser A en regardant un à un les éléments de A en commençant par l'élément $f(0)$, puis en regardant l'élément $f(1)$, etc. Pour cette raison, les ensembles infinis dénombrables auront sur plusieurs aspects un comportement très semblable à celui des ensembles finis. Très souvent, il sera facile de généraliser un théorème défini sur des structures finies aux structures infinies dénombrables, alors qu'une généralisation aux structures non dénombrables sera très difficile, voire impossible.

D'autre part, il est très souvent possible de définir en extension une fonction bijective dont le domaine est $\mathbb{N}$. Contrairement à la forme en compréhension qui nécessite l'élaboration d'une règle de correspondance, la forme en extension permet de montrer la **dénombrabilité** de certains ensembles d'une façon intuitive et visuelle. Une fonction bijective $f : \mathbb{N} \longrightarrow A$ qui est ainsi définie est souvent appelée une **énumération** de l'ensemble A puisque cela consiste à énumérer un à un les différents éléments de l'ensemble d'arrivée ; $f(0)$ est le $0^{\text{ième}}$ élément de cette énumération, $f(1)$ est le 1^{er} élément de cette énumération, $f(2)$ est le $2^{\text{ième}}$ élément de cette énumération, etc. En fait, on se convainc intuitivement (ou se convainc entre amis... !) qu'un ensemble est dénombrable en écrivant la liste de ses éléments, c'est-à-dire en montrant qu'on peut les écrire un à un sur une feuille (ceci est flou pour l'instant, mais ça s'éclaircira

dans la démonstration que $\mathbb{N} \times \mathbb{N}$ est dénombrable). Dans les faits, nous utiliserons une représentation visuelle de cette énumération, plutôt que de la présenter comme un ensemble en extension. Ceci nous permettra de définir correctement (et de façon convaincante) les fonctions bijectives *sans démontrer la bijectivité de façon formelle* (oui ici, on se dispense d'une démonstration !).

Proposition 1.5.4. *L'ensemble $\mathbb{Z}$ est dénombrable.*

Démonstration Démontrons la dénombrabilité de $\mathbb{Z}$, en construisant la fonction bijective $f : \mathbb{N} \longrightarrow \mathbb{Z}$, qui est définie en extension par :

$$\begin{array}{ccccccccccc} \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots \\ & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \\ \cdots & f(8) & f(6) & f(4) & f(2) & f(0) & f(1) & f(3) & f(5) & f(7) & \cdots \end{array}$$

On a donc que $|\mathbb{N}| = |\mathbb{Z}|$.
$\mathbb{Z}$ est donc un ensemble dénombrable.

C.Q.F.D.

Notez qu'aucun des mots de cette démonstration n'est superflu.

Dans cette démonstration, on a donné une représentation visuelle d'une définition de f en extension. Avec une définition en extension habituelle, on aurait plutôt écrit : $f = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, -1\rangle, \langle 3, 2\rangle, \langle 4, -2\rangle, \langle 5, 3\rangle, \ldots\}$. Ce n'est pas convaincant, ce n'est pas facile à lire. En compréhension, on aurait pu définir f par règle de correspondance comme suit :

$$f(n) := \begin{cases} -n/2 & \text{si } n \text{ est pair} \\ (n+1)/2 & \text{si } n \text{ est impair} \end{cases}$$

Ainsi définie par une règle de correspondance, on argumenterait que f est bien une fonction en disant que pour chaque n il y a une et une seule image possible, c'est assez rapide. Par contre, il resterait à démontrer que f est injective et surjective ; il faut alors passer par la définition de chacune de ces propriétés et faire une démonstration comme celle qui a été faite sur la fonction τ de la page 91. C'est ici qu'on comprend l'avantage de la représentation visuelle que nous adoptons dans ce cours. En effet, même si cette façon visuelle d'exhiber une fonction bijective est un peu moins rigoureuse que la forme en compréhension, on comprend clairement comment f est définie ; pour se convaincre que f satisfait les 4 propriétés nécessaires, on doit voir graphiquement ces propriétés, comme suit :

1. f est totale : tous les $n \in \mathbb{N}$ ont une image, c.-à-d. on voit pour tout $n \in \mathbb{N}$ les symboles "$f(n) \rightarrow$" quelque part dans la représentation. On voit $f(0) \rightarrow$, $f(1) \rightarrow$, $f(2) \rightarrow$, etc. (aucun n'est oublié)

2. f est déterministe : on ne voit pas plus d'une fois ces $f(n)$. On ne voit pas, par exemple $f(8) \to 2$ et $f(8) \to 3$.
3. f est injective : on ne voit pas 2 n différents pointer vers le même nombre, ou ce qui arrive souvent dans les copies d'étudiants quelque chose comme $f(3) \to 4$ de même que $f(5) \to 32/8$ (ici les deux valeurs 3 et 5 sont envoyées sur le même élément, 4) ;
4. f est surjective : on "voit" que "tous" les éléments de l'ensemble d'arrivée sont la cible d'une flèche. Si l'ensemble a été "bien énuméré", bien écrit, ceci se fait bien.

Ainsi, une définition en extension visuelle qui a été bien définie est toujours une fonction bijective. Attention ! assurez-vous que votre représentation visuelle respecte bien les 4 points ci-haut.

Proposition 1.5.5. *L'ensemble* $\mathbb{N} \times \mathbb{N}$ *est dénombrable.*

Démonstration Pour montrer la dénombrabilité de $\mathbb{N} \times \mathbb{N}$, nous allons construire une fonction bijective $k : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ en la définissant en extension de la manière suivante :

$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 0,2\rangle$	$\langle 0,3\rangle$	$\langle 0,4\rangle$	
$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\cdots$
$k(0)$	$k(2)$	$k(5)$	$k(9)$	$k(14)$	
$\langle 1,0\rangle$	$\langle 1,1\rangle$	$\langle 1,2\rangle$	$\langle 1,3\rangle$	$\langle 1,4\rangle$	
$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\cdots$
$k(1)$	$k(4)$	$k(8)$	$k(13)$	$k(19)$	
$\langle 2,0\rangle$	$\langle 2,1\rangle$	$\langle 2,2\rangle$	$\langle 2,3\rangle$	$\langle 2,4\rangle$	
$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\cdots$
$k(3)$	$k(7)$	$k(12)$	$k(18)$	$k(25)$	
$\langle 3,0\rangle$	$\langle 3,1\rangle$	$\langle 3,2\rangle$	$\langle 3,3\rangle$	$\langle 3,4\rangle$	
$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\cdots$
$k(6)$	$k(11)$	$k(17)$	$k(24)$	$k(32)$	
$\langle 4,0\rangle$	$\langle 4,1\rangle$	$\langle 4,2\rangle$	$\langle 4,3\rangle$	$\langle 4,4\rangle$	
$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\cdots$
$k(10)$	$k(16)$	$k(23)$	$k(31)$	$k(40)$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

On a donc que $\left|\mathbb{N}\right| = \left|\mathbb{N} \times \mathbb{N}\right|$.
$\mathbb{N} \times \mathbb{N}$ est donc un ensemble dénombrable.

C.Q.F.D.

Vérifiez les 4 propriétés d'une fonction bijective dans l'exemple ci-haut. Notons encore une fois que nous n'avons pas formellement démontré que f est une fonction bijective, mais nous l'avons écrite de sorte que les 4 points à vérifier sont faciles à vérifier. Cette démonstration illustre bien comment **l'énumération judicieuse** des éléments de l'ensemble d'arrivée est

importante et comment la représentation visuelle nous aide à trouver une fonction bijective qui fait l'affaire. Ici on a écrit les éléments de $\mathbb{N}\times\mathbb{N}$ dans le plan selon leurs coordonnées (grosso modo). Ils sont tous là (donc notre fonction a de bonnes chances d'être déjà surjective!!!). Ils ne sont pas répétés (ce qui évitera de donner à deux n différents la même image qui apparaîtrait à 2 endroits différents, donc notre fonction sera sûrement injective).

Remarquons que, étant donné que la relation "avoir autant d'éléments" est transitive (voir le théorème 1.7.4), si nous avons déjà démontré la dénombrabilité d'un ensemble A, nous pouvons alors démontrer la dénombrabilité d'un nouvel ensemble B en utilisant le lemme suivant :

Lemme 1.5.6. *Étant donné un ensemble infini B. Alors,*
B est dénombrable $\Leftrightarrow$ $(\exists A \mid A$ est dénombrable et $|A| = |B|)$.

1.5.3 "Avoir au moins autant d'éléments"

La notion "d'avoir autant d'éléments" nous a jusqu'ici permis d'explorer un peu l'univers des ensembles infinis, mais notre exploration serait certainement meilleure si on pouvait raffiner cette notion "d'égalité" entre les cardinalités en une notion "d'inégalité". Avec une telle notion, on pourrait, comme dans le cas fini, bâtir une hiérarchie des cardinalités d'ensembles infinis.

À la recherche d'une définition

Lorsque nous avons eu à choisir une définition "d'égalité" de cardinalités, nous avons eu principalement à tenir compte de deux critères. Il fallait que notre définition (1) coïncide dans le cas fini avec la définition déjà existante et (2) ne nécessite aucunement notre habileté à compter les éléments d'un ensemble fini. Dans le cas présent, nous sommes également confrontés à ces deux mêmes critères avec, en plus, le besoin que cette nouvelle notion "d'inégalité" des cardinalités soit compatible avec la notion "d'égalité" des cardinalités qu'on vient de se donner. Ceci implique que, pour définir la notion de "la cardinalité de A *est plus petite ou égale à* la cardinalité de B", on a essentiellement deux possibilités : soit on dit que c'est équivalent au fait qu'il existe une fonction injective de A vers B, soit on dit que c'est équivalent au fait qu'il existe une fonction surjective de B vers A.

Dans le cas fini, ces deux définitions seraient équivalentes, car la première signifie que A a autant ou moins d'éléments que B et la seconde que B a autant ou plus d'éléments que A. Le théorème suivant montre que c'est vrai en général.

Théorème 1.5.7. *Soit A et B, deux ensembles non vides. Alors,*
$\exists$ fonction injective $f : A \longrightarrow B$ ssi $\exists$ fonction surjective $g : B \longrightarrow A$.

Démonstration.

$\Rightarrow$: Supposons qu'il existe une fonction injective de A vers B et démontrons qu'il existe une fonction surjective de B vers A.

Soit $f : A \longrightarrow B$, une fonction injective. On veut définir $g : B \longrightarrow A$.

Prenons $a_0 \in A$ et $g_0 = \{\langle b, a_0\rangle \mid b \in B \setminus \mathrm{Im}(f)\}$. $\langle$ *a_0 existe, car $A \neq \emptyset$; g_0 existe.* $\rangle$

Posons $g = f^{-1} \cup g_0$ $\langle$ *$f^{-1} \subseteq B \times A$ et $g_0 \subseteq B \times A$, donc $g \subseteq B \times A$ et il existe.* $\rangle$

Montrons que g est une fonction surjective.

1. $g \subseteq B \times A$ **est total.** C'est-à-dire $(\forall b \in B \mid (\exists a \in A \mid b\ g\ a))$.

   Soit $b \in B$. $\langle$ *Montrons* $(\exists a \in A \mid b\ g\ a)$ $\rangle$

   Alors, il y a deux cas à considérer :

   Cas 1 : $b \in \mathrm{Im}(f)$.

   Prenons $a \in A$ choisi tel que $f(a) = b$ $\langle$ *Un tel a existe – définition de* $\mathrm{Im}(f)$ $\rangle$

   Alors on a $\langle a, b\rangle \in f$, donc $\langle b, a\rangle \in f^{-1}$

   donc $\langle b, a\rangle \in g$, comme voulu $\langle$ *car $f^{-1} \subseteq g$* $\rangle$

   Cas 2 : $b \notin \mathrm{Im}(f)$.

   Alors on sait que $\langle b, a_0\rangle \in g_0 \subseteq g$. $\langle$ *Définition de g_0 et g.* $\rangle$

   Donc $(\exists a \in A \mid b\ g\ a)$, tel que voulu $\langle$ *Car $a_0 \in A$ et $\langle b, a_0\rangle \in g$.* $\rangle$

   Donc g est total.

2. $g \subseteq B \times A$ **est déterministe**, c.-à-d. $(\forall b \in B, a, a' \in A \mid b\ g\ a \wedge b\ g\ a' \Rightarrow a = a')$.

   Soit $b \in B$ et a, $a' \in A$ et supposons $b\ g\ a \wedge b\ g\ a'$. $\langle$ *Montrons $a = a'$* $\rangle$

   Ici aussi, il y a deux cas à considérer :

   Cas 1 : $b \in \mathrm{Im}(f)$.

   On a $\langle b, a\rangle \in g$, par hypothèse, mais $\langle b, a\rangle \notin g_0$ $\langle$ *car $b \in \mathrm{Im}(f)$* $\rangle$

   De même, on a $\langle b, a'\rangle \in g$, mais $\langle b, a'\rangle \notin g_0$

   Donc $\langle b, a\rangle \in f^{-1}$ et $\langle b, a'\rangle \in f^{-1}$

   Donc $\langle a, b\rangle \in f$ et $\langle a', b\rangle \in f$.

   Ce qui implique que $a = a'$, comme voulu. $\langle$ *Car f est injectif.* $\rangle$

   Cas 2 : $b \notin \mathrm{Im}(f)$.

   On a $\langle b, a\rangle \in g$, par hypothèse, mais $\langle b, a\rangle \notin f^{-1}$ $\langle$ *car $b \notin \mathrm{Im}(f)$* $\rangle$

   De même, on a $\langle b, a'\rangle \in g$ mais $\langle b, a'\rangle \notin f^{-1}$

   Donc $\langle b, a\rangle \in g_0$ et $\langle b, a'\rangle \in g_0$.

   Cela implique que $a = a_0$ et $a' = a_0$.

   On a donc que $a = a'$. $\langle$ *Transitivité de* $=$ $\rangle$

Comme les 2 cas couvrent toutes les possibilités, $a = a'$ est démontré : g est donc déterministe.

Comme g est aussi totale, g est donc une fonction de B vers A (et on pourrait continuer la démonstration en utilisant ce fait, donc la définition de surjectivité pour les fonctions, mais ce n'est pas utile cette fois-ci).

3. $g : B \longrightarrow A$ **est surjectif.** C'est-à-dire $(\forall a \in A \mid (\exists b \in B \mid b\ g\ a))$.

   Soit $a \in A$. $\langle$ *Montrons* $(\exists b \in B \mid b\ g\ a)$ $\rangle$
   Prenons $b = f(a)$, c.-à-d. $\langle a, b\rangle \in f$.
   $\langle$ *Un tel* b *existe et appartient à* B*, car* f *est total.* $\rangle$
   Alors $\langle b, a\rangle \in f^{-1} \subseteq g$, donc on a bien $b\ g\ a$.

La démonstration de $\Rightarrow$ est donc complète.

$\Leftarrow$: Supposons qu'il existe une fonction surjective de B vers A et démontrons qu'il existe une fonction injective de A vers B.

Soit $g : B \longrightarrow A$, une fonction surjective.
Par définition, ceci implique que pour tout $a \in A$, il existe un $b \in B$ tel que $g(b) = a$.
Pour *chacun* des $a \in A$, nous allons choisir[31] un tel $b \in B$ que nous noterons b_a.
Ainsi on a que pour tout $a \in A$, $(\star)$ $g(b_a) = a$ et que $(\star\star)$ $b_a \in B$.
Soit $f : A \longrightarrow B$ défini par la règle de correspondance $f(a) = b_a$.

Alors cette fonction est bien définie, car $(\star)$ et $(\star\star)$ impliquent que pour tout $a \in A$, il existe un et un seul élément qui est en f-relation avec a, c'est b_a. Et ce b_a appartient bien à B, l'ensemble d'arrivée de f. La relation f est donc bien totale et déterministe.

Il ne reste qu'à démontrer que f est injectif, c'est-à-dire que :

$$(\forall a, a' \in A \mid f(a) = f(a') \Rightarrow a = a')\,.$$

Soit $a, a' \in A$ et supposons $f(a) = f(a')$. $\langle$ *Montrons* $a = a'$. $\rangle$
Alors on a que $b_a = b_{a'}$. $\langle$ *Définition de* f. $\rangle$
Et donc que $g(b_a) = g(b_{a'})$. $\langle$ *Car* g *est une fonction.* $\rangle$
Et donc que $a = a'$. $\langle$ *Voir* $(\star)$. $\rangle$

f est bien une fonction injective.

C.Q.F.D.

31. en supposant l'axiome du choix. Voir la remarque à ce propos à la fin de cette sous-section.

Nous pouvons donc maintenant définir notre notion de "cardinalité plus petite ou égale à" :

Définition 1.5.8. *Soit A et B, deux ensembles.*
On dit que A a une cardinalité plus petite ou égale à *la cardinalité de B, noté "$|A| \leq |B|$",*

- *ssi il existe une fonction injective de A vers B.*

Ou, ce qui est équivalent,

- *ssi il existe une fonction surjective de B vers A.*

Remarque : Dans la partie "$\Leftarrow$:" de la démonstration du théorème 1.5.7 nous avons tenu pour acquis qu'il était possible de choisir un élément b_a pour chaque élément a, et ce en une seule étape. En fait, ceci n'est pas aussi évident qu'il y paraît. Ceci utilise un nouvel axiome, *l'axiome du choix* qui, en gros, dit que si vous avez une quantité infinie d'ensembles non vides devant vous et que vous souhaitez choisir un élément dans chacun de ces ensembles, vous pouvez supposer que vous savez le faire en une seule étape, même si dans les faits vous ne pourrez jamais faire cette opération puisqu'elle nécessite une infinité d'étapes. Plus formellement :

Axiome du choix 1.5.9. *Soit $(A_i)_{i\in I}$, une famille infinie d'ensembles non vides. Alors il existe une famille d'éléments $(a_i)_{i\in I}$ telle que pour chaque $i \in I$, $a_i \in A_i$.*

Nous n'utiliserons pas explicitement cet axiome dans les démonstrations et problèmes de ce cours. Notez tout de même que nous en ferons encore une fois une utilisation implicite dans la démonstration du théorème 1.5.11.

Notre définition est-elle correcte ?

D'une façon similaire à ce que nous avons fait à la section 1.5.1 pour la notion "=", nous allons nous demander si notre notion de "$\leq$" correspond bien au concept "plus petit ou égal" tel qu'on le connaît.

Pour que ce soit le cas, notre définition de "$\leq$" devrait posséder les trois grandes propriétés suivantes :

- **la réflexivité.** Est-ce qu'avec cette définition, un ensemble A a toujours une cardinalité plus petite ou égale à elle-même ?
  Autrement dit est que pour tout ensemble A, on a $|A| \leq |A|$?
- **l'antisymétrie.** Est-ce qu'avec cette définition, le fait qu'un ensemble A ait une cardinalité plus petite ou égale à celle d'un ensemble B combiné avec le fait que B ait une

cardinalité plus petite ou égale à celle d'un ensemble A implique toujours que B a la même cardinalité que A ?
Autrement dit, est-ce que pour tout A, B, on a $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |B| = |A|$?

- **la transitivité.** Est-ce qu'avec cette définition, le fait qu'un ensemble A ait une cardinalité plus petite ou égale à celle d'un ensemble B combiné au fait que ce B ait une cardinalité plus petite ou égale à celle d'un troisième ensemble C implique toujours que A a une cardinalité plus petite ou égale à celle de C ?
Autrement dit, est-ce que pour tout A, B, C, on a $|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$?

Nous verrons à la section 1.7.4 (page 147) que la notre définition de "$\leq$" possède bien les trois propriétés ci-haut, lorsque nous présenterons le concept de **relation d'odre**.

De plus, nous verrons que notre notion "$\leq$" se comporte comme une relation d'**ordre complet**, c'est-à-dire qu'étant donné n'importe quelle paire d'ensembles A et B, on a toujours ou bien que A a une cardinalité plus petite que celle de B, ou bien que A a une cardinalité plus grande que celle de B, ou bien que A a une cardinalité égale à celle de B.

Autrement dit, pour tout A, B, on a $(|A| < |B|) \vee (|A| > |B|) \vee (|A| = |B|)$. Ce comportement est souhaitable pour qu'une notion de type "plus petit ou égale" satisfasse notre intuition.

La relation "cardinalité $\leq$" est-elle compatible avec $\subseteq$?

Il est aussi intéressant de noter que notre notion de "$\leq$" est compatible avec la notion de sous-ensemble. En effet, si un ensemble A est inclus dans un ensemble B, nous aurons toujours que la cardinalité de A est plus petite ou égale à celle de B.

Autrement dit, pour tout A, B, on a $(A \subseteq B) \Rightarrow (|A| \leq |B|)$. Ce fait est une conséquence directe de la proposition suivante.

Proposition 1.5.10. *Soit A et B deux ensembles.*
Si $A \subseteq B$ alors la fonction $I_{A\subseteq B} : \begin{array}{ccc} A & \longrightarrow & B \\ a & \longmapsto & a \end{array}$ *est bien définie et est injective.*

Démonstration Exercice.

1.5.4 $|\mathbb{N}|$ est la plus petite cardinalité infinie

Intuitivement, on ne voit pas comment un ensemble infini pourrait avoir une cardinalité plus petite que $|\mathbb{N}|$. Cette intuition est effectivement juste, en voici la démonstration.

Théorème 1.5.11. *Soit A un ensemble infini. Alors $|A| \geq |\mathbb{N}|$.*

Démonstration.
Soit A un ensemble infini. Alors, nous devons démontrer que $|A| \geq |\mathbb{N}|$ et pour ce faire, nous allons montrer qu'il existe une fonction injective de $\mathbb{N}$ vers A.
Construisons la fonction $f : \mathbb{N} \longrightarrow A$ récursivement de la façon suivante :

Prenons $a_0 \in A$. ⟨ *Un tel a_0 existe, car l'ensemble infini A est non vide.* ⟩
Définissons $f(0) = a_0$.
Prenons $a_1 \in A \backslash \{a_0\}$. ⟨ *Un tel a_1 existe, car l'ensemble infini A contient plus d'un élément.* ⟩
Définissons $f(1) = a_1$.
Prenons $a_2 \in A \backslash \{a_0, a_1\}$. ⟨ *Un tel a_2 existe, car A est infini et contient donc plus de 2 éléments.* ⟩
Définissons $f(2) = a_2$.
Prenons $a_3 \in A \setminus \{a_0, a_1, a_2\}$.
⟨ *Un tel a_3 existe, car A infini, contient plus de trois éléments.* ⟩ Définissons $f(3) = a_3$.
Continuant cette construction, ad infinitum, on aura défini $f(n)$, pour tout $n \in \mathbb{N}$.

Comme $\forall n \in \mathbb{N}$, n est en relation f avec *un et un seul* élément de A (c.-à-d. l'élément a_n), f est bien une fonction de $\mathbb{N}$ vers A.

Il ne reste qu'à démontrer que f est injective. C'est-à-dire que

$$(\forall n, n' \in \mathbb{N} \mid n \neq n' \Rightarrow f(n) \neq f(n')) .$$

Soit n, $n' \in \mathbb{N}$ et supposons $n \neq n'$ ⟨ *Montrons $f(n) \neq f(n')$* ⟩
On a alors $n < n'$ ou $n' < n$.
Les 2 cas étant symétriques, sans perte de généralité, supposons que $n < n'$.
Ainsi, $f(n)$ a été choisi avant $f(n')$, ce qui implique que $a_n \in \{a_0, a_1, \ldots, a_{n'-1}\}$.
Ce qui implique que $a_n \neq a_{n'}$. ⟨ *Car par construction, $a_{n'} \in A \setminus \{a_0, a_1, \ldots, a_{n'-1}\}$.* ⟩

Comme en plus on a $a_n = f(n)$ et $a_{n'} = f(n')$. ⟨ *Voir la définition de f.* ⟩
On a donc que $f(n) \neq f(n')$.

f est donc une fonction injective.

C.Q.F.D.

1.5.5 Donnons-nous des outils

Dans cette section, nous allons énoncer plusieurs résultats qui pourront être utiles lorsque viendra le temps de démontrer si deux ensembles ont la même cardinalité ou si un des deux

a une cardinalité plus petite que l'autre.

Les deux premiers résultats sont des conséquences directes des définitions de "même cardinalité" et "cardinalité plus petite ou égale" et des théorèmes 1.7.3, 1.5.7 et 1.7.7 et de l'axiome du choix 1.5.9.

Théorème 1.5.12. *Soit A et B, deux ensembles, alors les énoncés suivants sont équivalents :*

1. $|A| = |B|$.
2. $\exists$ *fonction bijective* $f : A \longrightarrow B$.
3. $\exists$ *fonction bijective* $g : B \longrightarrow A$.
4. $|A| \leq |B|$ *et* $|A| \geq |B|$.
5. $\exists$ *fonction injective* $f : A \longrightarrow B$ *et* $\exists$ *fonction injective* $g : B \longrightarrow A$.
6. $\exists$ *fonction injective* $f : A \longrightarrow B$ *et* $\exists$ *fonction surjective* $h : A \longrightarrow B$.
7. $\exists$ *fonction surjective* $k : B \longrightarrow A$ *et* $\exists$ *fonction surjective* $h : A \longrightarrow B$.
8. $\exists$ *fonction surjective* $k : B \longrightarrow A$ *et* $\exists$ *fonction injective* $g : B \longrightarrow A$.

Théorème 1.5.13. *Soit A et B, deux ensembles, alors les énoncés suivants sont équivalents :*

1. $|A| < |B|$.
2. $|A| \leq |B|$ *et* $|A| \neq |B|$.
3. $\exists$ *fonction injective,* $f : A \longrightarrow B$ *mais* $\nexists$ *fonction bijective* $g : B \longrightarrow A$.
4. $|A| \leq |B|$ *et* $|A| \ngeq |B|$.
5. $\exists$ *fonction injective,* $f : A \longrightarrow B$ *mais* $\nexists$ *fonction injective* $g : B \longrightarrow A$.
6. $\exists$ *fonction injective,* $f : A \longrightarrow B$ *mais* $\nexists$ *fonction surjective* $g : A \longrightarrow B$.
7. $|A| \ngeq |B|$.
8. $\nexists$ *fonction injective* $g : B \longrightarrow A$.
9. $\nexists$ *fonction surjective* $g : A \longrightarrow B$.

Les deux résultats suivants portent sur la notion de dénombrabilité. Ils découlent essentiellement des théorèmes 1.5.12 et 1.5.13 et du fait que $|\mathbb{N}|$ est "la plus petite cardinalité infinie" (le théorème 1.5.11).

Théorème 1.5.14. *Soit A un ensemble. Alors les résultats suivants sont équivalents :*

1. *A est dénombrable.*
2. *$|A| \leq |\mathbb{N}|$*
3. *$\exists$ fonction surjective $f : \mathbb{N} \longrightarrow A$.*
4. *$\exists$ fonction injective $f : A \longrightarrow \mathbb{N}$.*
5. *$|A| < |\mathbb{N}|$ ou $|A| = |\mathbb{N}|$*
6. *A est fini ou $\exists$ fonction bijective $f : A \longrightarrow \mathbb{N}$.*
7. *A est fini ou $\exists$ fonction bijective $f : \mathbb{N} \longrightarrow A$.*

Corollaire 1.5.15. *Soit A un ensemble. Alors les résultats suivants sont équivalents :*

1. *A est non dénombrable*[32].
2. *$|A| > |\mathbb{N}|$.*
3. *$\nexists$ fonction surjective $f : \mathbb{N} \longrightarrow A$.*
4. *$\nexists$ fonction injective $f : A \longrightarrow \mathbb{N}$.*
5. *A est infini et $|A| \neq |\mathbb{N}|$.*
6. *A est infini et $\nexists$ fonction bijective $f : A \longrightarrow \mathbb{N}$.*
7. *A est infini et $\nexists$ fonction bijective $f : \mathbb{N} \longrightarrow A$.*

Théorème 1.5.16. *Soit A et B, deux ensembles dénombrables (finis ou infinis). Alors*

1. *$A \cup B$ est dénombrable,*
2. *$A \times B$ est dénombrable.*

Démonstration du théorème 1.5.16.
Soit A et B, deux ensembles dénombrables. Prenons $f : \mathbb{N} \longrightarrow A$ et $g : \mathbb{N} \longrightarrow B$, deux fonctions surjectives

⟨ *De tels f et g existent, voir Théorème 1.5.14.* ⟩

1. Démontrons que $A \cup B$ est dénombrable.

Soit $h : \mathbb{N} \longrightarrow A \cup B$

$$n \longmapsto \begin{cases} f(\frac{n}{2}) & \text{si } n \text{ est pair} \\ g(\frac{n-1}{2}) & \text{si } n \text{ est impair} \end{cases}$$

La fonction h est bien définie, car chaque $n \in \mathbb{N}$ est en h-relation avec **un** et **un seul** élément de $A \cup B$ qui est **ou bien** $f(\frac{n}{2}) \in A$, si n est pair, **ou bien** $g(\frac{n-1}{2}) \in B$ si n est impair.

32. Dans la prochaine section, nous verrons qu'il existe des ensembles qui sont non dénombrables.

Donc, pour démontrer que $A \cup B$ est dénombrable, il suffit de montrer que h est surjectif. ⟨ *Voir Théorème 1.5.14.* ⟩

Montrons donc que $(\forall y \in A \cup B \mid (\exists n \in \mathbb{N} \mid h(n) = y))$.

Soit $y \in A \cup B$. ⟨ *Il faut montrer* $(\exists n \in \mathbb{N} \mid h(n) = y)$ ⟩

Il y a deux cas (non nécessairement mutuellement exclusifs) à considérer.

Cas 1 : $y \in A$

Prenons $i \in \mathbb{N}$ choisi tel que $f(i) = y$.

⟨ *Un tel i existe, car $f : \mathbb{N} \longrightarrow A$ est surjectif.* ⟩

Prenons $n = 2i$.

⟨ *Un tel n existe et appartient à* $\mathbb{N}$. ⟩

Alors, on a bien
$h(n) = h(2i) = f(\frac{2i}{2}) = f(i) = y$.

Cas 2 : $y \in B$

Prenons $j \in \mathbb{N}$ choisi tel que $g(j) = y$.

⟨ *Un tel j existe, car $g : \mathbb{N} \longrightarrow A$ est surjectif.* ⟩

Prenons $n = 2j + 1$.

⟨ *Un tel n existe et appartient à* $\mathbb{N}$. ⟩

Alors, on a bien
$h(n) = h(2j + 1) = g(\frac{(2j+1)-1}{2}) = g(j) = y$.

Dans chacun des deux cas on a bien qu'il existe un $n \in \mathbb{N}$ tel que $h(n) = y$. h est donc une fonction surjective. $A \cup B$ est donc dénombrable.

2. Démontrons que $A \times B$ est dénombrable.

Nous avons démontré à la proposition 1.5.5 que $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Par le théorème 1.5.14, il est donc suffisant de montrer que $\big|A \times B\big| \leq \big|\mathbb{N} \times \mathbb{N}\big|$. Pour démontrer la dénombrabilité de $A \times B$, il suffit donc de montrer qu'il existe une fonction surjective de $\mathbb{N} \times \mathbb{N}$ vers $A \times B$.

Soit la fonction H suivante :

$$\begin{array}{rccc} H & : & \mathbb{N} \times \mathbb{N} & \longrightarrow & A \times B \\ & & \langle i,j \rangle & \longmapsto & \langle f(i), g(j) \rangle \end{array}$$

On note que H est bien définie (c'est-à-dire, elle est bien une relation totale et déterministe), car pour tout couple $\langle i, j \rangle \in \mathbb{N} \times \mathbb{N}$, $H(\langle i, j \rangle) = \langle f(i), g(j) \rangle$ est bien un élément de $A \times B$ puisque $f(i)$ est bien un élément de A et $g(j)$ est bien un élément de B.

Il existe donc pour chaque couple $\langle i, j \rangle \in \mathbb{N} \times \mathbb{N}$, *un et un seul* élément de $A \times B$ qui est en H-relation avec $\langle i, j \rangle$. On peut donc dire que H est bien une fonction.

Démontrons que H est surjectif.

Il faut démontrer que $\Big(\forall \langle \alpha, \beta \rangle \in A \times B \mid \Big(\exists \langle i, j \rangle \in \mathbb{N} \times \mathbb{N} \mid H(\langle i, j \rangle) = \langle \alpha, \beta \rangle\Big)\Big)$.

Soit $\langle \alpha, \beta \rangle \in A \times B$.

Prenons $i \in \mathbb{N}$ choisi tel que $f(i) = \alpha$

$\langle$ *Un tel i existe, car $f : \mathbb{N} \longrightarrow A$ est une fonction surjective et $\alpha \in A$.* $\rangle$

Prenons $j \in \mathbb{N}$ choisi tel que $g(j) = \beta$

$\langle$ *Un tel j existe, car $g : \mathbb{N} \longrightarrow B$ est une fonction surjective et $\beta \in B$.* $\rangle$

Alors, on a bien que $\langle i, j \rangle \in \mathbb{N} \times \mathbb{N}$ et que $H(\langle i, j \rangle) = \langle \alpha, \beta \rangle$.

H est donc surjectif.

On a donc que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}| \geq |A \times B|$.

Par le théorème 1.5.14–$(2 \Rightarrow 1)$, $A \times B$ est donc un ensemble dénombrable.

C.Q.F.D.

1.5.6 "Plus d'éléments" que $\mathbb{N}$: Les ensembles non dénombrables

En terminant ce chapitre, nous allons essayer de trouver des **ensembles infinis non dénombrables**. À première vue, on aurait pu croire que tous les ensembles étaient dénombrables puisque $\mathbb{Z}$ est dénombrable et même $\mathbb{Q}$ l'est. Cependant, nous allons voir que $\mathbb{R}$, lui, ne l'est pas. Nous verrons même comment on peut fabriquer des ensembles de cardinalité toujours plus grande.

Le prochain théorème est dû à Cantor, le père de la théorie des ensembles.

Théorème 1.5.17. (Cantor) *Pour tout ensemble A,* $|A| < |\mathcal{P}(A)|$.

Ce théorème est démontré à l'aide de la technique de **démonstration par contradiction**. Comme expliqué à la section 1.3.8 (page 66), ce type de démonstration est basé sur l'équivalence :

$$(\neg p \Rightarrow \text{faux}) \;\Leftrightarrow\; p,$$

c'est-à-dire : *pour démontrer que p est vrai, on peut démontrer que la négation de p nous mène à une contradiction.*

Démonstration du théorème 1.5.17 (Cantor)

Il faut démontrer l'énoncé suivant : $(\star)$ Pour tout ensemble A, on a $|A| < |\mathcal{P}(A)|$.

Supposons le contraire, c'est-à-dire qu'il existe un ensemble A tel que $|A| \geq |\mathcal{P}(A)|$. Et cherchons une contradiction.

Soit donc A un tel ensemble.
Prenons $f : A \longrightarrow \mathcal{P}(A)$, une fonction surjective. $\langle$ *Une telle fonction existe, voir Déf. 1.5.8.* $\rangle$

Soit $T = \{a \in A \mid a \notin f(a)\}$.
Remarquons que $T \subseteq A$ et donc que $T \in \mathcal{P}(A)$.

Prenons $a_0 \in A$, choisi tel que $f(a_0) = T$ ⟨ *Un tel a_0 existe, car f est surjectif.* ⟩

Alors il y a deux cas à considérer.

Cas 1 : $a_0 \in T$.
Alors $a_0 \notin f(a_0)$. ⟨ *Définition de T.* ⟩
Ce qui implique que $a_0 \notin T$. ⟨ *Car $f(a_0) = T$.* ⟩
On a donc à la fois que $a_0 \in T$ et que $a_0 \notin T$, ce qui est une **contradiction**.

Cas 2 : $a_0 \notin T$.
Alors $\neg(a_0 \notin f(a_0))$. ⟨ *Définition de T.* ⟩
Ce qui implique que $(a_0 \in f(a_0))$. ⟨ *Définition de $\notin$ et Prop 1.1.5-a (Double négation)* ⟩
Ce qui implique que $a_0 \in T$. ⟨ *Car $f(a_0) = T$.* ⟩
Dans ce deuxième et dernier cas on a aussi à la fois que $a_0 \in T$ et que $a_0 \notin T$,
ce qui est donc ici aussi une **contradiction**.

Le fait que nous obtenions une contradiction dans chacun des deux cas nous permet de conclure que notre hypothèse est fausse, c'est-à-dire que l'énoncé $(\star)$ est vrai.

C.Q.F.D.

Nous verrons que $\mathbb{R}$ est aussi un ensemble non dénombrable, cependant, avant d'énoncer ce résultat, nous devons faire un bref rappel sur les **nombres réels**.

Rappel 1.5.18. La représentation base 10 d'un nombre réel est de la forme

$$b_n\, b_{n-1} \ldots b_1\, b_0,\ \ a_0\, a_1\, a_2\, a_3\, a_4 \ldots$$

où les b_j et les a_i sont des chiffres de 0 à 9.

Exemple : $\frac{8}{3} = 2,\, 666\ldots$

Cependant, cette représentation n'est pas unique. En effet, le nombre $0,\, 213$ par exemple peut être représenté par "$0,\, 213000\ldots$" et par "$0,\, 212999\ldots$". Pour éviter toute ambiguïté, nous allons supposer ici que nous ne représenterons jamais un nombre réel par une représentation base 10 qui se terminerait par une séquence infinie de 9.

En particulier, **chacun** des nombres de l'intervalle $[0, 1[$ aura une **unique** représentation base 10 de la forme $0, a_0\, a_1\, a_2\, a_3\, a_4\, a_5 \ldots$, où chacun des a_i est un chiffre de 0 à 9 et qui ne se termine pas par une séquence infinie de 9.

Histoire de bien comprendre ce problème de la non-unicité de la représentation en base 10, voici la démonstration que $0,\,9999\ldots = 1$ et la démonstration que $0,\,212999\ldots = 0,\,213000\ldots$:

Démontrons que $0,\,9999\ldots = 1$**.**

Posons $x = 0,\,9999\ldots$.

Alors on a
$$\begin{array}{rcl} 10\,x & = & 9,\,9999\ldots \\ -\,x & = & -\,0,\,9999\ldots \\ \hline 9\,x & = & 9 \end{array}$$

Ce qui implique bien que $x = 1$.

C.Q.F.D.

Démontrons que $0,\,212999\ldots = 0,\,213000\ldots$ **.**

Posons $y = 0,\,212999\ldots$.

Alors on a
$$\begin{array}{rcl} 10\,000\,y & = & 2129,\,9999\ldots \\ -\,1\,000\,y & = & -\;212,\,9999\ldots \\ \hline 9000\,y & = & 1917 \end{array}$$

Ce qui implique que $y = \frac{1917}{9000}$.

Et on vérifie facilement que $\frac{1917}{9000} = 0,\,213$

C.Q.F.D.

Théorème 1.5.19. $\mathbb{R}$ *est non dénombrable.*

Démonstration.

Étape 1 : Nous allons démontrer que l'intervalle $[0,1[$ est non dénombrable.

Nous allons démontrer que $\big|\mathbb{N}\big| \ngeq \big|[0,1[\big|$.

Pour ce faire, nous allons démontrer

$$\neg(\exists f : \mathbb{N} \longrightarrow [0,1[|\ f \text{ est surjective}),$$

ce qui est équivalent à démontrer

$$(\forall f : \mathbb{N} \longrightarrow [0,1[|\ f \text{ est non-surjective}).$$

Soit $f : \mathbb{N} \longrightarrow [0,1[$ une telle fonction.

$\langle$ *Démontrons qu'il existe* $b \in [0,1[$ *tel que* $b \notin Im(f)$ $\rangle$

Nous allons maintenant représenter f en extension, en représentant en base 10 chacun des $f(n)$, comme justifié par le rappel 1.5.18.

Soit $\left(a_{\langle n,i\rangle}\right)_{n,i\in\mathbb{N}}$, une famille[33] de chiffres de 0 à 9, qui satisfont :

$$\begin{aligned}
f(0) &= 0,\ a_{\langle 0,0\rangle}\, a_{\langle 0,1\rangle}\, a_{\langle 0,2\rangle}\, a_{\langle 0,3\rangle}\, a_{\langle 0,4\rangle}\, a_{\langle 0,5\rangle}\ldots\\
f(1) &= 0,\ a_{\langle 1,0\rangle}\, a_{\langle 1,1\rangle}\, a_{\langle 1,2\rangle}\, a_{\langle 1,3\rangle}\, a_{\langle 1,4\rangle}\, a_{\langle 1,5\rangle}\ldots\\
f(2) &= 0,\ a_{\langle 2,0\rangle}\, a_{\langle 2,1\rangle}\, a_{\langle 2,2\rangle}\, a_{\langle 2,3\rangle}\, a_{\langle 2,4\rangle}\, a_{\langle 2,5\rangle}\ldots\\
f(3) &= 0,\ a_{\langle 3,0\rangle}\, a_{\langle 3,1\rangle}\, a_{\langle 3,2\rangle}\, a_{\langle 3,3\rangle}\, a_{\langle 3,4\rangle}\, a_{\langle 3,5\rangle}\ldots\\
f(4) &= 0,\ a_{\langle 4,0\rangle}\, a_{\langle 4,1\rangle}\, a_{\langle 4,2\rangle}\, a_{\langle 4,3\rangle}\, a_{\langle 4,4\rangle}\, a_{\langle 4,5\rangle}\ldots\\
\vdots\quad &\quad \vdots\qquad\qquad\qquad\qquad \vdots
\end{aligned}$$

Prenons $\left(b_i\right)_{i\in\mathbb{N}}$, une famille de chiffres choisis de sorte que[34] pour chaque $i\in\mathbb{N}$ $b_i\in\{0,1,2,3,4,5,6,7,8\}\setminus\{a_{\langle i,i\rangle}\}$; par exemple, prenons[35] :

$$b_i = \begin{cases} 4 & \text{si } a_{\langle i,i\rangle}\neq 4\\ 5 & \text{si } a_{\langle i,i\rangle}=4\end{cases}$$

Ces b_i existent. Soit maintenant $b=0,\ b_0\, b_1\, b_2\, b_3\, b_4\, b_5\ldots$.

Clairement, b est un nombre de l'intervalle $[0,1[$, représenté en base 10 par une famille de chiffres qui ne se termine pas par une séquence infinie de 9.
Alors $b_i\neq a_{\langle i,i\rangle}$ pour tout $i\in\mathbb{N}$, par définition :
donc $b\neq f(i)$ pour tout $i\in\mathbb{N}$, par unicité de la représentation en base 10 ;
donc $b\notin Im(f)$, comme voulu.

Ainsi, $[0,1[$ n'est pas dénombrable.

Étape 2 : Nous allons maintenant démontrer que $\mathbb{R}$ est non dénombrable.
Comme $[0,1[\subseteq\mathbb{R}$ par la proposition 1.5.10, on a $\left|[0,1[\right|\leq\left|\mathbb{R}\right|$.
Ceci, combiné avec l'étape 1, implique que $\left|\mathbb{N}\right|<\left|[0,1[\leq\left|\right|\mathbb{R}\right|$.

$\mathbb{R}$ est donc non dénombrable. **C.Q.F.D.**

33. Cette façon de nommer les éléments avec 2 indices peut sembler compliquée, mais elle est naturelle, si on y pense un peu... nous avons beaucoup d'éléments à "nommer".
34. Ces b_i sont choisis en utilisant la "diagonale", c'est-à-dire les éléments $a_{\langle i,i\rangle}$, dans le but de construire le b suivant qui ne sera égal à aucun $f(n)$.
35. Ceci sert à fixer des b_i possibles, mais n'est pas nécessaire dans la démonstration, c'est pour donner un exemple...

1.5.7 Exercices sur les ensembles infinis

Exercice 1

Démontrez que les ensembles suivants sont infinis dénombrables (c.-à-d. : qu'ils ont la même cardinalité que $\mathbb{N}$). *Pour ce numéro, vous pouvez, tout comme dans les notes de cours, donner des définitions en extension visuelle de toute fonction bijective dont le domaine est* $\mathbb{N}$*, et dans ce cas, vous n'avez pas à démontrer qu'il s'agit effectivement d'une fonction bijective.*

a) $\mathbb{N} \times \{5, 12, 789\}$.

b) $\mathbb{N} \setminus \{5, 12, 789\}$.

c) $\mathbb{N} \times \mathbb{N}$.

d) $\mathbb{Z} \times \mathbb{Z}$.

e) l'ensemble de toutes les puissances de 2.

f) l'ensemble de tous les mots qu'on peut construire avec un alphabet qui soit composé uniquement des lettres "a", "b" et "c".

Exercice 2

a) Démontrez que la fonction $f : \mathbb{N} \longrightarrow \mathbb{N} \times \{2, 3\}$,

définie par la règle de correspondance $f(i) = \begin{cases} \langle \frac{i}{2}, 2 \rangle & \text{si } i \text{ est pair} \\ \langle \frac{i-1}{2}, 3 \rangle & \text{si } i \text{ est impair} \end{cases}$

est surjective.

b) En déduire que $\mathbb{N} \times \{2, 3\}$ est dénombrable.

Exercice 3 : (*Pour ce numéro, aucune justification n'est demandée.*)
Étant donnés les ensembles A, B, C et D, que peut-on conclure sur leurs cardinalités ?

a) — il existe une fonction bijective de A vers C ;
— il existe une fonction surjective de A vers B ;
— il existe une fonction injective de A vers D.

b) — il existe une fonction bijective de A vers C ;
— il existe une fonction surjective de A vers B ;
— il existe une fonction injective de A vers D ;
— il existe une fonction surjective de B vers D.

c) — il existe une fonction surjective de A vers B ;
— il existe une fonction surjective de B vers C ;
— il existe une fonction surjective de C vers D ;
— il existe une fonction surjective de D vers $\mathbb{N}$.

d) — il existe une fonction surjective de A vers B,
— il existe une fonction bijective de B vers C,
— il n'existe pas de fonction injective de C vers $\mathbb{N}$.

Exercice 4
Rappel : *L'ensemble* $\mathbb{Q} \stackrel{\text{def}}{=} \left\{ \frac{x}{y} \;\middle|\; x \in \mathbb{Z}, y \in \mathbb{Z}^* \right\}$ *est l'ensemble des nombres rationnels.*

a) Démontrez que $\mathbb{Z} \times \mathbb{Z}^*$ est dénombrable en construisant en extension une fonction bijective entre $\mathbb{N}$ et cet ensemble..

b) Démontrez que la relation F suivante est une fonction surjective :

$$\begin{array}{rccc} F: & \mathbb{Z} \times \mathbb{Z}^* & \longrightarrow & \mathbb{Q} \\ & \langle x, y \rangle & \longmapsto & \frac{x}{y} \end{array}$$

c) En utilisant a) et b), démontrez que $\mathbb{Q}$ est dénombrable.

Exercice 5 : Complétez et justifiez brièvement.

a) S'il n'existe pas de fonction surjective de A vers $\mathbb{N}$, alors A est _____.

b) S'il n'existe pas de fonction surjective de $\mathbb{N}$ vers A, alors A est _____.

c) Soit $(A_i)_{i\in\mathbb{N}}$, une famille d'ensembles finis, alors l'union de tous les ensembles de cette famille (notée $\bigcup_{i\in\mathbb{N}} A_i$) est _____.

d) Soit $(A_i)_{i\in\mathbb{N}}$, une famille d'ensembles infinis dénombrables, alors $\bigcup_{i\in\mathbb{N}} A_i$ est _____.

Exercice 6
Démontrez que l'ensemble de tous les sous-ensembles finis de $\mathbb{N}$ est dénombrable alors que l'ensemble de tous les sous-ensembles de $\mathbb{N}$ ne l'est pas.

Exercice 7 : Soit la fonction f, définie par $\begin{array}{rccc} f: & [1,100] & \longrightarrow & [0,1] \\ & x & \longmapsto & \frac{x-1}{100} \end{array}$

a) Démontrez que f est injective, mais pas surjective.
b) Peut-on conclure de a) que $\left|[1,100]\right| \leq \left|[0,1]\right|$? Pourquoi ?
c) Peut-on conclure de a) que $\left|[1,100]\right| < \left|[0,1]\right|$? Pourquoi ?
d) Est-ce que $[1,100]$ est dénombrable ? Justifiez.

1.6 Ensembles de fonctions

Dans cette section, nous étudions les ensembles dont les éléments sont des fonctions. Rappelons qu'une **fonction** est une relation déterministe et totale. Nous adoptons la notation B^A pour représenter l'**ensemble de toutes les fonctions** dont l'ensemble de départ est A et l'ensemble d'arrivé est B.

Définition 1.6.1. *Étant donnés deux ensembles A et B, on définit B^A comme étant l'ensemble de **toutes** les fonctions de A vers B.*

Autrement dit : $B^A = \{f : A \longrightarrow B \mid \ \}$.

Par exemple, comme illustré par la figure 1.12, l'ensemble de toutes les fonctions dont l'ensemble de départ est $\{1, 2\}$ et l'ensemble d'arrivé est $\{5, 6\}$ est formé de quatre éléments.

$$\{5,6\}^{\{1,2\}} \ = \ \Big\{\{\langle 1,5\rangle, \langle 2,5\rangle\},\ \{\langle 1,5\rangle, \langle 2,6\rangle\},\ \{\langle 1,6\rangle, \langle 2,5\rangle\},\ \{\langle 1,6\rangle, \langle 2,6\rangle\}\Big\}.$$

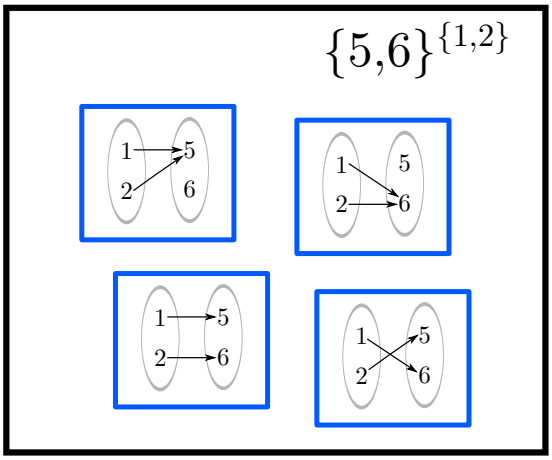


FIGURE 1.12 – Représentation visuelle de l'ensemble de fonctions $\{5, 6\}^{\{1,2\}}$.

PENSEZ-Y!

La notation "ensemble B exposant ensemble A" n'est pas très intuitive. La raison pour laquelle elle a été adoptée est que, si A et B sont des ensembles finis, la cardinalité de l'ensemble B^A est la même que la cardinalité de l'ensemble B exposant la cardinalité de l'ensemble A, c'est-à-dire :

$$|B^A| \ = \ \underbrace{|B| \times |B| \times \ldots \times |B|}_{|A| \text{ fois}} \ = \ |B|^{|A|}.$$

1.6.1 Fonctions à valeur de sortie binaire

En programmation informatique, on a souvent recours à des fonctions dont la valeur de sortie est `faux` ou `vrai`. Ainsi, pour une fonction f dont tous les arguments possibles sont représentés par l'ensemble A, nous avons

$$f \in \{0,1\}^A\,,$$

où `faux` et `vrai` ont été remplacés par 0 et 1 pour être plus concis.

Par exemple, la figure 1.13 illustre l'ensemble des fonctions à valeur de sortie binaire dont l'ensemble de départ est $\{0,1,2\}$. Notons que cet ensemble comporte $2^3 = 8$ éléments, car chacun des 3 nombres de l'ensemble de départ est associé à soit 0 ou 1.

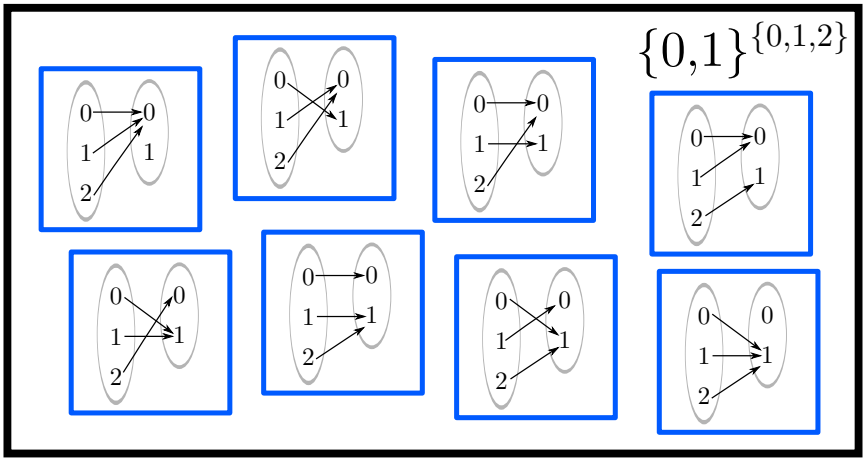


FIGURE 1.13 – Représentation visuelle de l'ensemble de fonctions $\{0,1\}^{\{0,1,2\}}$.

Comme nous le verrons bientôt, il existe une forte similitude entre l'ensemble de fonctions à valeur de sortie binaire $\{0,1\}^A$ et l'ensemble de tous les sous-ensembles de A (c'est-à-dire l'ensemble puissance $\mathcal{P}(A)$). Nous allons introduire cette similitude à l'aide d'un exemple inspiré de la programmation.

Examinons un exemple concret !

Supposons qu'on gère un site web possédant une banque de données d'utilisateurs. Le profil de chaque utilisateur contient une liste de sujets qui l'intéressent. Nous avons les intérêts suivants [36] :

36. Fournies par Somabec dans son profil utilisateur en mars 2014.

FIGURE 1.14 – Des choix de listes de courriel

Ainsi l'ensemble des intérêts est

> `INTERETS` := { Agroalimentaire, Arts langue et littératures, Dictionnaire, Droit, Économie et gestion, Géographie et histoire, Informatique, Ingénierie urbanisme, Loisirs, Medecine, Médecine vétérinaire, Psychiatrie - psychologie, Sciences de la vie, Sciences infirmières, Sciences physiques, Sciences sociales, Sport, Tous les vient de paraitre }.

Lorsqu'un utilisateur est connecté au site web, nous avons (en tant que programmeur du site web) accès à une fonction `interesse_par`(x), qui prend un sujet $x \in$ `INTERETS` en argument et qui retourne `vrai` si le sujet x intéresse l'utilisateur courant, `faux` sinon. Nous avons donc

$$\texttt{interesse\_par} \in \{0,1\}^{\texttt{INTERETS}}. \tag{1.1}$$

Demandons-nous maintenant quelle structure de données utiliser pour représenter les intérêts d'un utilisateur. Une première possibilité serait d'utiliser un ensemble :

$$\texttt{interets\_utilisateur} \in \mathcal{P}\big(\texttt{INTERETS}\big). \tag{1.2}$$

Dans ce cas, lorsqu'un utilisateur se connecte à son profil, le système initialiserait une variable contenant les sujets qui intéressent l'utilisateur. Par exemple :

$$\texttt{interets\_utilisateur} := \big\{\text{Informatique, Loisirs, Sciences physiques}\big\}. \tag{1.3}$$

On constate donc qu'une fonction à valeur de sortie binaire `interesse_par` (ligne (1.1)) correspond à un et un seul ensemble de sujets (ligne (1.2)). Sans être le même "objet" mathématique, ces deux concepts peuvent représenter la même chose.

En programmation, il est fréquent d'utiliser un tableau de valeurs binaires (c'est-à-dire une suite de 0 et de 1) pour représenter un sous-ensemble. Dans notre exemple, on peut associer

chacun des sujets de la figure 1.14 à un index (un nombre de 0 à 17). Ainsi, l'ensemble de la ligne (1.3) serait représenté, dans la mémoire de l'ordinateur, par

$$\texttt{interets\_utilisateur} := 000000\ 101000\ 001000\,. \tag{1.4}$$

Les blocs sont ici de longueur 6 pour aider la lecture (conformément aux colonnes de la figure 1.14). Il y a "1" à chaque fois que le sujet est choisi par l'utilisateur et un "0" sinon. Ainsi, pour un utilisateur qui choisit tous les sujets, on enregistrerait :

$$\texttt{interets\_de\_curieux} := 111111\ 111111\ 111111\,,$$

ce qui est beaucoup moins long que l'ensemble des titres de tous les sujets. Notons qu'on peut effacer et ajouter un choix facilement en utilisant cette représentation.

Ainsi, l'ensemble de tous les tableaux binaires de tailles 18 possède la même cardinalité (2^{18}) que l'ensemble puissance de l'ensemble `INTERETS`, ainsi que la même cardinalité que l'ensemble de fonctions $\{0,1\}^{\texttt{INTERETS}}$. Cette constatation est la clé de la compréhension de la proposition 1.6.2.

Cardinalité des ensembles de fonctions à valeur de sortie binaire

Dans l'exemple précédent, nous avons déduit que $\left|\mathcal{P}(\texttt{INTERETS})\right| = \left|\{0,1\}^{\texttt{INTERETS}}\right|$. Nous allons maintenant voir que cela est vrai pour tous les ensembles, qu'ils soient finis ou infinis, en démontrant la proposition suivante :

Proposition 1.6.2. *Pour tout ensemble A, on a* $\left|\mathcal{P}(A)\right| = \left|\{0,1\}^A\right|$.

Remarquons que pour que notre démonstration soit valide pour les ensembles infinis, nous devons avoir recours à la notion d'avoir "**autant d'éléments**" introduite à la section 1.5.1 (voir la définition 1.5.2, page 110). Autrement dit, nous allons démontrer que, pour tout ensemble A, il existe une fonction bijective entre l'ensemble $\{0,1\}^A$ et l'ensemble $\mathcal{P}(A)$.

Démonstration de la proposition 1.6.2.
Soit la fonction G suivante :

$$\begin{array}{rccc} G & : & \{0,1\}^A & \longrightarrow & \mathcal{P}(A) \\ & & f{:}A\longrightarrow\{0,1\} & \longmapsto & \{a\in A \mid f(a)=1\} \end{array}$$

On note que G est bien définie (c'est-à-dire, elle est bien une relation totale et déterministe), car pour toute fonction $f \in \{0,1\}^A$, $G(f) = \{a \in A \mid f(a) = 1\}$ est bien un élément de

$\mathcal{P}(A)$ puisque c'est un sous-ensemble de A.
Il existe donc pour chaque fonction $f \in \mathrm{Dom}(G)$, **un** et **un seul** élément de $\mathcal{P}(A)$ qui est en G-relation avec f.
G est donc une fonction.

Démontrons que G est injectif et surjectif.

Injectivité. Il faut démontrer que $\Big(\forall f_1, f_2 \in \{0,1\}^A \mid f_1 \neq f_2 \Rightarrow G(f_1) \neq G(f_2)\Big)$.

Soit $f_1, f_2 \in \{0,1\}^A$, et supposons $f_1 \neq f_2$. ⟨ *Démontrons* $G(f_1) \neq G(f_2)$ ⟩
Prenons $x \in A$ choisi tel que $f_1(x) \neq f_2(x)$ ⟨ *Un tel* x *existe, car* $f_1 \neq f_2$ ⟩

Comme l'ensemble d'arrivée de f_1 et celui de f_2 sont tous deux égaux à $\{0,1\}$,
sans perte de généralité nous pouvons supposer que $f_1(x) = 0$ et $f_2(x) = 1$.
Ce qui implique que $x \notin \{a \in A \mid f_1(a) = 1\}$ et que $x \in \{a \in A \mid f_2(a) = 1\}$.
On a donc $x \notin G(f_1)$ et $x \in G(f_2)$.
Ce qui implique $G(f_1) \neq G(f_2)$. ⟨ *Car* $G(f_1)$ *et* $G(f_2)$ *sont deux ensembles et ils n'ont pas exactement les mêmes éléments.* ⟩
G est donc injectif.

Surjectivité Il faut démontrer que $(\forall B \in \mathcal{P}(A) \mid (\exists f_{_B} \in \{0,1\}^A \mid G(f_{_B}) = B))$. On aurait pu écrire "$\exists f$", mais ce nom, f_B, nous rappellera que son image doit être B.

Soit $B \in \mathcal{P}(A)$. ⟨ *Notons que* $B \subseteq A$. ⟩
Posons $f_{_B} : A \longrightarrow \{0,1\}$

$$a \longmapsto \begin{cases} 0 & \text{si } a \notin B. \\ 1 & \text{si } a \in B. \end{cases}$$

La fonction $f_{_B}$ est bien définie, car pour chaque élément a, ou bien $a \in B$ ou bien $a \notin B$. Ce qui ici implique que a est en $f_{_B}$-relation avec *un et un seul* élément de $\{0,1\}$.
$f_{_B}$ est donc bien une fonction (c.-à-d. : totale et déterministe).

De plus,

$$\begin{aligned} & G(f_{_B}) \\ &= \{a \in A \mid f_{_B}(a) = 1\} && \langle \textit{ Définition de } G. \rangle \\ &= \{a \in A \mid a \in B\} && \langle \textit{ Définition de } f_{_B}. \rangle \\ &= B. && \langle \textit{ Car } B \subseteq A. \rangle \end{aligned}$$

G est donc surjectif.

G est donc une fonction bijective de $\{0,1\}^A$ vers $\mathcal{P}(A)$.
Ce qui implique que $\Big|\{0,1\}^A\Big| = \Big|\mathcal{P}(A)\Big|$. **C.Q.F.D.**

Il est important de bien comprendre la fonction G construite au début de la démonstration précédente. Sa construction n'est pas si compliquée qu'elle peut le paraître au premier abord. Pour vous en convaincre, voici un petit exemple.

Posons $A := \{0, 1, 2\}$. Alors, l'ensemble de fonctions binaires $\{0, 1\}^A$ est celui illustré par la figure 1.13 au début de cette section (page 130). De même, l'ensemble de tous les sous-ensembles de A est :

$$\mathcal{P}(A) \;=\; \Big\{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{1, 2\}, \{0, 2\}, \{0, 1, 2\}\Big\}\,.$$

Dans cet exemple, la fonction $G : \{0, 1\}^A \longrightarrow \mathcal{P}(A)$ sera (en extension) :

$$\begin{array}{lcllcl}
G\Big(\{\langle 0,0\rangle, \langle 1,0\rangle, \langle 2,0\rangle\}\Big) & = & \emptyset\,, & G\Big(\{\langle 0,1\rangle, \langle 1,1\rangle, \langle 2,0\rangle\}\Big) & = & \{0,1\}\,,\\
G\Big(\{\langle 0,1\rangle, \langle 1,0\rangle, \langle 2,0\rangle\}\Big) & = & \{0\}\,, & G\Big(\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,1\rangle\}\Big) & = & \{1,2\}\,,\\
G\Big(\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,0\rangle\}\Big) & = & \{1\}\,, & G\Big(\{\langle 0,1\rangle, \langle 1,0\rangle, \langle 2,1\rangle\}\Big) & = & \{0,2\}\,,\\
G\Big(\{\langle 0,0\rangle, \langle 1,0\rangle, \langle 2,1\rangle\}\Big) & = & \{2\}\,, & G\Big(\{\langle 0,1\rangle, \langle 1,1\rangle, \langle 2,1\rangle\}\Big) & = & \{0,1,2\}\,.
\end{array}$$

PENSEZ-Y!

Dans un langage de programmation qui accepte que les arguments des fonctions soient eux-mêmes des fonctions, la fonction G s'implémente en quelques lignes. Reprenons l'exemple ci-haut et illustrons ces dires dans à l'aide d'un interpréteur Python.

```
>>> A = set([0,1,2])
>>> def G(f):
...     resultat = set()
...     for a in A:
...         if f(a) == 1:
...             resultat.add(a)
...     return resultat
...
>>> def modulo_2(x):
...     return x % 2
...
>>> G(modulo_2)
```

```
{1}
>>> def trivial(x):
...     return 1
...
>>> G(trivial)
{0, 1, 2}
```

Notez qu'un programmeur avancé peut écrire la fonction G en une seule ligne de Python, grâce aux *expressions lambda* et aux *ensembles par compréhensions* :

```
>>> G = lambda f: {a for a in A if f(a) == 1}
```

Bien sûr, vous n'avez pas à apprendre cela dans le cadre du cours. Cela dit, rien ne vous empêche de vous amuser avec ces concepts dans vos temps libres ! Voici quelques références vers la documentation officielle de Python (en anglais) pour ceux qui désirent en savoir plus :

– https://docs.python.org/3/tutorial/datastructures.html#sets
– https://docs.python.org/3/tutorial/controlflow.html#lambda-expressions
– https://docs.python.org/3/tutorial/datastructures.html#tut-listcomps

1.6.2 Dénombrabilité des ensembles de fonctions

À la section 1.5.2, nous avons défini les ensembles infinis dénombrables comme étant les ensembles qui ont une cardinalité égale à l'ensemble $\mathbb{N}$. Conséquemment, comme vu à la section 1.5.6, un **ensemble infini non dénombrable** a une cardinalité strictement supérieure à $\mathbb{N}$. À la lumière de nos nouvelles connaissances, étudions la (non-)dénombrabilité des ensembles de fonctions.

Corollaire 1.6.3. $\{0,1\}^{\mathbb{N}}$ *est un ensemble non dénombrable.*

Démonstration. Par la proposition 1.6.2, on a $|\{0,1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$.
De même, par le théorème de Cantor (théorème 1.5.17, page 123), on a $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$.
Ainsi, $|\{0,1\}^{\mathbb{N}}| > |\mathbb{N}|$. **C.Q.F.D.**

Le résultat précédent se généralise au résultat suivant :

Théorème 1.6.4. *Soit A un ensemble ayant au moins deux éléments et B un ensemble infini.*
Alors A^B est un ensemble non dénombrable.

Nous ne ferons pas la démonstration du théorème 1.6.4, mais nous allons illustrer l'essentiel des idées qui lui sont rattachées en démontrant la proposition suivante :

Proposition 1.6.5. $\{0,1,2\}^{\mathbb{N}}$ *est un ensemble non dénombrable.*

Avant d'effectuer la démonstration en détail, remarquons que toute fonction qui est *élément de* $\{0,1\}^{\mathbb{N}}$ (*l'ensemble de toutes les fonctions dont le domaine est* $\mathbb{N}$ *et l'image est incluse dans* $\{0,1\}$) peut aussi être interprétée comme un *élément de* $\{0,1,2\}^{\mathbb{N}}$ (*l'ensemble de toutes les fonctions dont le domaine est* $\mathbb{N}$ *et l'image est incluse dans* $\{0,1,2\}$).

Autrement dit, il y a une fonction injective "canonique" de $\{0,1\}^{\mathbb{N}}$ vers $\{0,1,2\}^{\mathbb{N}}$. Ce qui implique que $\left|\{0,1\}^{\mathbb{N}}\right| \leq \left|\{0,1,2\}^{\mathbb{N}}\right|$. Comme en plus on vient de démontrer que $\{0,1\}^{\mathbb{N}}$ est non dénombrable, cette idée nous "convainc" que $\{0,1,2\}^{\mathbb{N}}$ est également non dénombrable. C'est ce que la démonstration suivante fait de façon rigoureuse.

Démonstration de la proposition 1.6.5.
Nous allons démontrer $\left|\{0,1\}^{\mathbb{N}}\right| \leq \left|\{0,1,2\}^{\mathbb{N}}\right|$ en construisant explicitement une fonction injective de $\{0,1\}^{\mathbb{N}}$ vers $\{0,1,2\}^{\mathbb{N}}$, et comme on sait par le corollaire 1.6.3 que l'ensemble $\{0,1\}^{\mathbb{N}}$ est non dénombrable, nous aurons le résultat.

Pour démontrer $\left|\{0,1\}^{\mathbb{N}}\right| \leq \left|\{0,1,2\}^{\mathbb{N}}\right|$, nous allons construire une fonction injective H de $\{0,1\}^{\mathbb{N}}$ vers $\{0,1,2\}^{\mathbb{N}}$ de la manière suivante :

$$\begin{array}{ccccc} H & : & \{0,1\}^{\mathbb{N}} & \longrightarrow & \{0,1,2\}^{\mathbb{N}} \\ & & \left(\begin{array}{ccccc} f & : & \mathbb{N} & \longrightarrow & \{0,1\} \\ & & n & \longmapsto & f(n) \end{array}\right) & \longmapsto & \left(\begin{array}{ccccc} H(f) & : & \mathbb{N} & \longrightarrow & \{0,1,2\} \\ & & n & \longmapsto & f(n) \end{array}\right) \end{array}$$

Autrement dit, étant donné une fonction f de $\mathbb{N}$ vers $\{0,1\}$, $H(f)$ est la fonction de $\mathbb{N}$ vers $\{0,1,2\}$ qui a ***la même règle de correspondance*** *que f.*

On note que H est bien définie (c'est-à-dire, elle est bien une relation totale et déterministe), car il existe pour chaque fonction $f \in \mathrm{Dom}(H)$, *un et un seul* élément de $\{0,1,2\}^{\mathbb{N}}$ qui est en H-relation avec f.

H est donc une fonction, il ne reste qu'à démontrer qu'elle est injective.

Il faut donc démontrer que $\Big(\forall f_1, f_2 \in \{0,1\}^{\mathbb{N}} \mid f_1 \neq f_2 \Rightarrow H(f_1) \neq H(f_2)\Big)$.

Soit $f_1, f_2 \in \{0,1\}^{\mathbb{N}}$, et supposons $f_1 \neq f_2$.
Prenons $x \in \mathbb{N}$ choisi tel que $f_1(x) \neq f_2(x)$. ⟨ *Un tel x existe, car $f_1 \neq f_2$.* ⟩
Alors $H(f_1)(x) = f_1(x)$ ⟨ *Par la définition de H.* ⟩
Et $H(f_2)(x) = f_2(x)$ ⟨ *Par la définition de H.* ⟩
On a donc $H(f_1)(x) \neq H(f_2)(x)$ ⟨ *Puisque $f_1(x) \neq f_2(x)$.* ⟩
On a donc $H(f_1) \neq H(f_2)$

La fonction H est donc injective, ce qui complète la démonstration que $\{0,1,2\}^{\mathbb{N}}$ est non dénombrable.

C.Q.F.D.

1.6.3 Exercices sur les ensembles de fonctions

Exercice 1
Sans justifier vos réponses, dites si les énoncés suivants sont VRAIS ou FAUX.

a) Tous les ensembles de fonctions non-dénombrables. _____.

b) $\left|\mathbb{N}^{\{0,1\}}\right| = \left|\{0,1\}^{\mathbb{N}}\right|$. _____.

c) $\mathbb{N}^{\mathbb{Z}}$ est dénombrable. _____.

Exercice 2

a) Démontrez que l'ensemble de tous les mots *finis* sur l'alphabet {"a", "b"} est dénombrable alors que l'ensemble de tous les mots *infinis* sur ce même alphabet ne l'est pas.

b) Est-ce que l'ensemble de tous les mots (*finis et infinis*) sur l'alphabet {"a", "b"} est dénombrable ? Justifiez brièvement.

Exercice 3

a) Les données d'entrée et de sortie d'un programme sont des séquences de bits. On peut donc considérer une séquence de bits comme un nombre naturel exprimé en binaire (en ajoutant un bit "1" au début de la séquence, de sorte que les "0" initiaux du programme soient significatifs). Donc un programme calcule une fonction de $\mathbb{N}$ vers $\mathbb{N}$.

L'ensemble de toutes les fonctions de $\mathbb{N}$ vers $\mathbb{N}$ est-il dénombrable ?

b) Un programme en JAVA est construit à partir d'un nombre fini de symboles et est de longueur finie. On peut donc considérer un programme comme un mot écrit à l'aide d'un certain alphabet.

L'ensemble de tous les programmes en JAVA est-il dénombrable ?

c) Si on suppose qu'on n'a aucun problème de mémoire, est-ce que n'importe quelle fonction de $\mathbb{N}$ vers $\mathbb{N}$ peut-être calculée en JAVA ? (Justifiez brièvement.)

Exercice 4
Expliquez brièvement pourquoi $\{0,1,2\}^{\mathbb{N}}$ est non dénombrable.

Exercice 5

En construisant en extension une fonction bijective appropriée, démontrez la dénombrabilité de l'ensemble $\mathbb{Z}^{\{1,2\}}$. Notez que des théorèmes des notes de cours permettent de démontrer la dénombrabilité de cet ensemble, mais vous ne pouvez les utiliser pour cet exercice.

Astuce : *La difficulté est de représenter les éléments de cet ensemble. Écrivez $f_{i,j}$ pour la fonction qui envoie 1 sur le nombre i et 2 sur le nombre j (il faut toutefois définir cette nouvelle notation dans votre réponse avant de l'utiliser)*

1.7 Relations d'équivalences et ordres

Lorsque nous avons introduit les ensembles, nous avons insisté sur le fait que les éléments de ces ensembles ne sont pas ordonnés. Dans cette section, nous verrons que certaines relations permettent de comparer les éléments d'un ensemble. Nous parlerons de relations d'équivalence (qui peuvent être vues comme une généralisation de l'égalité "=") et d'ordres (qui peuvent être vus comme une généralisation du plus petit ou égal "$\leq$"). Ces concepts reposent sur les propriétés de réflexivité, de transitivité et de symétrie dont nous avons discuté à la section 1.4.4 (voir la définition 1.4.14, page 88).

1.7.1 Relations d'équivalences

Il arrive que l'on veuille regrouper des éléments d'ensembles selon certaines particularités. Deux éléments d'un ensemble sont équivalents lorsqu'ils possèdent une certaine caractéristique en commun. Cette caractéristique dépend du contexte dans lequel on travaille. Voici quelques idées d'éléments qu'on peut vouloir considérer comme équivalents :

- Deux personnes sont équivalentes si elles ont le même nom de famille ;
- Deux nombres entiers sont équivalents s'ils possèdent la même parité (pair ou impair) ;
- Deux nombres naturels sont équivalents si leur représentation binaire requiert de même nombre de bits (le nombre de bit requis pour $x \in \mathbb{N}$ étant donné par $\lfloor \log_2 x \rfloor + 1$) ;
- Deux fonctions C++ sont équivalentes si elles ont toujours la même valeur de retour. Par exemple, les trois fonctions suivantes sont équivalentes selon cette définition :

```
int bleu(int a)
{
    return 2*a;
}
```

```
int blanc(int b)
{
    int x = b+b;
    return x;
}
```

```
int rouge(int c)
{
    if (c==5) return 10;
    else return bleu(c);
}
```

Une relation sur un ensemble S peut être appelée **relation d'équivalence** si elle se comporte comme la relation "=" en arithmétique. Plus formellement, elle doit satisfaire la définition suivante.

Définition 1.7.1. *Relation d'équivalence*
Une relation $\mathcal{R} \subseteq S^2$ est une **relation d'équivalence** *si elle est réflexive, symétrique et transitive.*

Nous utilisons souvent le symbole "$\simeq$" pour désigner une relation d'équivalence. Dans ce contexte, l'expression "$a \simeq b$" signifie "l'élément a est équivalent à l'élément b". Ainsi, la relation $\mathcal{R} \subseteq S^2$ est une relation d'équivalence si elle possède les propriétés suivantes :

– **Réflexivité** (Déf 1.4.14-a) : $a \simeq a$, pour tout $a \in S$;
– **Symétrie** (Déf 1.4.14-c) : Si $a \simeq b$ alors $b \simeq a$, pour tout $a, b \in S$;
– **Transitivité** (Déf 1.4.14-f) : Si $a \simeq b$ et $b \simeq c$ alors $a \simeq c$, pour tout $a, b, c \in S$.

Considérons un ensemble de personnes P, l'ensemble des nombres naturels $\mathbb{N}$ et l'ensemble F des fonctions programmables en langage C++. Voici quelques exemples de relations d'équivalences pour chacun de ces trois ensembles :

— $\simeq_1 := \{\langle a, b\rangle \in P^2 \mid a$ a le même nom de famille que $b\}$ est une relation d'équivalence sur P. On a :

$$\text{“Réjean Tremblay”} \simeq_1 \text{“Elvis Tremblay”}\,.$$

— $\simeq_2 := \{\langle x, y\rangle \in \mathbb{N}^2 \mid x \bmod 2 = y \bmod 2\}$ est une relation d'équivalence sur $\mathbb{N}$. On a :

$$\neg(8 \simeq_2 11) \quad \text{et} \quad 8 \simeq_2 42\,.$$

— $\simeq_3 := \{\langle x, y\rangle \in \mathbb{N}^2 \mid \lfloor \log_2 x \rfloor = \lfloor \log_2 y \rfloor\}$ est une relation d'équivalence sur $\mathbb{N}$. On a :

$$8 \simeq_3 11 \quad \text{et} \quad \neg(8 \simeq_3 42)\,.$$

— $\simeq_4 := \{\langle f_1, f_2\rangle \in F^2 \mid f_1$ et f_2 ont toujours la même valeur de retour $\}$ est une relation d'équivalence sur F. On a :

$$\texttt{bleu()} \simeq_4 \texttt{blanc()}, \quad \texttt{blanc()} \simeq_4 \texttt{rouge()} \quad \text{et} \quad \texttt{rouge()} \simeq_4 \texttt{bleu()}\,.$$

Le lecteur est encouragé à démontrer que les relations ci-dessus sont bien des relations d'équivalences. Pour ce faire, il faut démontrer qu'elles possèdent chacune des trois propriétés de réflexivité, de symétrie et de transitivité.

Étant donné une relation d'équivalence $\simeq$ sur un ensemble S, une **classe d'équivalence** est un sous ensemble qui regroupe tous les éléments de S qui sont équivalents entre eux. Remarquons que chaque élément de S appartient à *une et une seule* classe d'équivalence. De même, l'union de toutes les classes d'équivalences de S égale l'ensemble S lui-même.

À titre d'exemple, les ensembles N_1 et N_2 ci dessous sont les deux classes d'équivalence de la relation $\simeq_2 := \{\langle x, y\rangle \in \mathbb{N}^2 \mid x \bmod 2 = y \bmod 2\}$ sur l'ensemble $\mathbb{N}$ (On a bien $N_1 \cup N_2 = \mathbb{N}$.) :

$$\begin{aligned} N_1 &:= \{0, 2, 4, 6, 8, \ldots\}\,, \\ N_2 &:= \{1, 3, 5, 7, 9, \ldots\}\,. \end{aligned}$$

Enfin, remarquons pour compléter que la relation d'égalité "=" est une relation d'équivalence sur $\mathbb{N}$. Cette relation d'équivalence est très stricte, car chaque élément n'est équivalent qu'à lui-même (c'est une relation à la fois symétrique et antisymétrique !). Autrement dit, toutes les classes d'équivalences de la relation "=" ne contiennent qu'un seul élément. Par contre, la relation = sur les expressions algébrique est une relation d'équivalence plus complexe, avec des équivalences comme $(x-\pi)(x+\pi) = x^2 - \pi^2$, et combien d'autres... !

1.7.2 "Autant d'éléments" est une relation d'équivalence

À la section 1.5.1 sur les ensembles infinis, nous avons défini la notion ensembliste "**autant d'éléments**". En bref, nous avons choisi que les ensembles A et B sont de même cardinalité ($|A| = |B|$) si et seulement si il existe une fonction bijective entre A et B (voir la définition 1.5.2, page 110). Nous allons maintenant démontrer que cette notion d'égalité entre ensembles se comporte comme une relation d'équivalence, telle que présentée par la définition 1.7.1 ci-haut. Pour ce faire, démontrons que notre relation "autant d'éléments" est réflexive, symétrique et transitive.

La réflexivité de notre relation "autant d'éléments"

Pour démontrer la réflexivité, il faut démontrer que pour tout ensemble A, il existe une fonction bijective de A vers A. La réflexivité est donc une conséquence de la proposition suivante :

Proposition 1.7.2. *Soit A un ensemble, la relation $\boldsymbol{I}_A$ est une fonction bijective.*

Démonstration.
Rappelons que $\mathbf{I}_A : A \longrightarrow A$ est défini par la règle de correspondance $\mathbf{I}_A(x) = x$, $\forall x \in A$. Le fait que $\mathbf{I}_A$ soit une fonction (c.-à-d. : totale et déterministe) découle directement du fait que la relation est définie par une règle de correspondance où, pour chaque élément x de l'ensemble de départ, ne correspond qu'un et un seul élément de l'ensemble d'arrivée, soit x lui-même.

- Démontrons l'injectivité, c.-à-d. : $(\forall x, x' \in A \mid \mathbf{I}_A(x) = \mathbf{I}_A(x') \Rightarrow x = x')$.
  Soit $x, x' \in A$, et supposons $\mathbf{I}_A(x) = \mathbf{I}_A(x')$. $\langle$ *Montrons* $x = x'$ $\rangle$
  Alors on a immédiatement $x = x'$. $\langle$ *Car* $\mathbf{I}_A(x) = x$ *et* $\mathbf{I}_A(x') = x'$. $\rangle$
  $\mathbf{I}_A$ est bien une fonction injective.

- Démontrons la surjectivité, c.-à-d. : $(\forall y \in A \mid (\exists x \in A \mid \mathbf{I}_A(x) = y))$.
  Soit $y \in A$. $\langle$ *Montrons* $(\exists x \in A \mid \mathbf{I}_A(x) = y)$ $\rangle$
  Et prenons $x = y$. $\left\langle$ *Un tel x existe et appartient bien à A, car l'ensemble de départ coïncide avec l'ensemble d'arrivée.* $\right\rangle$
  Alors on a bien $\mathbf{I}_A(x) = y$. $\langle$ *Car* $\mathbf{I}_A(x) = x$ *et* $x = y$. $\rangle$
  $\mathbf{I}_A$ est bien une fonction surjective.

$\mathbf{I}_A$ est bien une fonction bijective. **C.Q.F.D.**

La symétrie de notre relation "autant d'éléments"

Pour montrer la symétrie, il faut montrer que pour toute paire d'ensembles A et B : s'il existe une fonction bijective de A vers B, alors il existe une fonction bijective de B vers A.

La symétrie est une conséquence du théorème suivant :

Théorème 1.7.3. *Soit A et B, deux ensembles, et $f \subseteq A \times B$. Alors*

la relation f est une fonction bijective ssi la relation inverse $f^{-1} \subseteq B \times A$ est une fonction bijective.

Démonstration.
Rappelons que la relation inverse de la relation f est : $f^{-1} = \{\langle b, a\rangle \in B \times A \mid \langle a, b\rangle \in f\}$.

Soit $f \subseteq A \times B$.
Pour démontrer f est une fonction bijective $\Leftrightarrow$ f^{-1} est une fonction bijective, il suffirait de démontrer :

$$\begin{cases} 1.- & f \text{ est total} \Leftrightarrow f^{-1} \text{ est surjectif}; \\ 2.- & f \text{ est déterministe} \Leftrightarrow f^{-1} \text{ est injectif}; \\ 3.- & f \text{ est injectif} \Leftrightarrow f^{-1} \text{ est déterministe}; \\ 4.- & f \text{ est surjectif} \Leftrightarrow f^{-1} \text{ est total}. \end{cases}$$

Or, nous avons déjà fait cette démonstration (Voir le théorème 1.4.17 à la page 94).

C.Q.F.D.

La transitivité de notre relation "autant d'éléments"

Pour démontrer la transitivité, il faut démontrer que, pour tout triplet d'ensembles A, B et C, s'il existe une fonction bijective de A vers B et une fonction bijective de B vers C, alors il existe une fonction bijective de A vers C.

La transitivité est une conséquence du théorème suivant :

Théorème 1.7.4. *Soit A, B et C, trois ensembles, et soit $f \subseteq A \times B$ et $g \subseteq B \times C$.*

Si f et g sont deux fonctions bijectives, alors $f \circ g$ sera une fonction bijective de A vers C.

Démonstration.
Ce théorème est une conséquence directe de la définition d'une fonction bijective et du théorème 1.4.18 présenté à la page 95. **C.Q.F.D.**

1.7.3 Relations d'ordres

Un **ordre** est une relation qui permet d'ordonner les éléments d'un ensemble. Le critère d'ordre dépend du problème étudié. Voici quelques idées de critères :

— Un mot qui en précède un autre selon l'ordre alphabétique ;
— Une personne qui est l'ancêtre d'une autre ;
— Une tâche qui est préalable à une autre pour assembler une voiture sur une chaîne de montage.

Ordre partiel

Définition 1.7.5. *Ordre partiel*
Une relation $\mathcal{R} \subseteq S^2$ est un **ordre partiel** *sur l'ensemble S si elle est réflexive, antisymétrique et transitive.*

Nous utiliserons souvent le symbole "$\preceq$" pour désigner une relation d'ordre. Dans ce contexte, l'expression "$a \preceq b$" signifie que l'élément a précède l'élément b selon une relation d'ordre donnée. Nous utiliserons parfois la notation "$b \succeq a$" pour désigner l'expression "$a \preceq b$".

Ainsi, une relation $\preceq \subseteq S^2$ est un **ordre partiel** sur l'ensemble S si elle possède les trois propriétés suivantes :

– **Réflexivité** (Déf 1.4.14-a) : $a \preceq a$, pour tout $a \in S$;
– **Antisymétrie** (Déf 1.4.14-e) : Si $a \preceq b$ et $b \preceq a$ alors $a = b$, pour tout $a, b \in S$;
– **Transitivité** (Déf 1.4.14-f) : Si $a \preceq b$ et $b \preceq c$ alors $a \preceq c$, pour tout $a, b, c \in S$.

Voici deux exemples de relations qui sont des ordres partiels, même si ceci demande un peu de réflexion (ou une démonstration) pour s'en convaincre :

— Considérons l'ensemble puissance des naturels $\mathcal{P}(\mathbb{N})$. Nous pouvons redéfinir l'opérateur ensembliste d'inclusion comme un ordre partiel sur $\mathcal{P}(\mathbb{N})$:

$$\subseteq \stackrel{\text{def}}{=} \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \mid e \in A \Rightarrow e \in B\}\,.$$

— Considérons l'ensemble des nombres naturels non nuls $\mathbb{N}^*$ et définissons l'ordre partiel "est un diviseur de" que nous définissons ainsi :

$$\preceq_{\mathcal{D}} \stackrel{\text{def}}{=} \{\langle a, b\rangle \in \mathbb{N}^* \times \mathbb{N}^* \mid b \bmod a = 0\}\,.$$

Selon cet ordre partiel, on a entre autres que : $1 \preceq_{\mathcal{D}} 3 \preceq_{\mathcal{D}} 9 \preceq_{\mathcal{D}} 27 \preceq_{\mathcal{D}} 270\ldots$

Ordre complet

Une relation $\preceq$ sur un ensemble S est un **ordre complet**[37] lorsque, en plus d'être un ordre partiel (c'est-à-dire d'être réflexive, antisymétrique et transitive), elle respecte la propriété suivante :

$$(\forall a \in S, b \in S \mid a \preceq b \vee b \preceq a)\,.$$

Autrement dit, $\preceq$ est un ordre complet si et seulement si tous les éléments de l'ensemble S sont comparables entre eux.

L'ordre partiel "est un diviseur de", que l'on note "$\preceq_{\mathcal{D}}$", présenté en exemple plus haut n'est pas un ordre complet sur $\mathbb{N}^*$. En effet, on n'a ni $2 \preceq_{\mathcal{D}} 3$ ni $3 \preceq_{\mathcal{D}} 2$. De même, l'ordre partiel d'inclusion $\subseteq$ n'est pas un ordre complet, car $\{1, 2\} \nsubseteq \{2, 3\}$ et $\{2, 3\} \nsubseteq \{1, 2\}$.

Un ordre complet bien connu est la relation "plus petit ou égal" $\leq$. De même, l'ordre alphabétique sur l'ensemble des mots du dictionnaire est un ordre complet.

Ordre partiel strict

Un **ordre strict** est un ordre qui *ne contient pas* les couples formés du même élément.

Définition 1.7.6. *Ordre partiel strict*
Une relation $\mathcal{R} \subseteq S^2$ est un **ordre partiel strict** *sur l'ensemble S si elle est irréflexive, aymétrique et transitive.*

Nous utilisons souvent le symbole "$\prec$" pour désigner une relation qui est un ordre strict. Contrairement à un ordre, un ordre strict n'admet jamais "$a \prec a$", pour tout a appartenant

37. Plusieurs auteurs utilisent plutôt le terme "ordre total". Dans ce texte, on utilise le terme "ordre complet" pour éviter toute confusion possible avec le concept de "relation totale", qui désigne une relation qui possède la propriété de totalité.

à l'ensemble sur lequel est définie la relation.

Ainsi, une relation $\prec$ est un **ordre partiel strict** sur l'ensemble S si elle possède les trois propriétés suivantes :

- **Irréflexivité** (Déf 1.4.14-b) : $\neg(a \prec a)$, pour tout $a \in S$;
- **Asymétrie** (Déf 1.4.14-d) : Si $a \prec b$ alors $\neg(b \prec a)$, pour tout $a, b \in S$;
- **Transitivité** (Déf 1.4.14-f) : Si $a \prec b$ et $b \prec c$ alors $a \prec c$, pour tout $a, b, c \in S$.

Nous pouvons redéfinir l'opérateur ensembliste d'inclusion stricte comme un ordre partiel strict sur $\mathcal{P}(\mathbb{N})$:

$$\subset \stackrel{\text{def}}{=} \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \mid A \neq B \wedge (e \in A \Rightarrow e \in B)\}.$$

Ordre complet strict

Une relation $\prec$ sur un ensemble S est un **ordre complet strict** lorsque, en plus d'être un ordre partiel strict, tous les éléments de l'ensemble S sont comparables entre eux :

$$(\forall a \in S, b \in S \mid a \prec b \vee b \prec a \vee a = b).$$

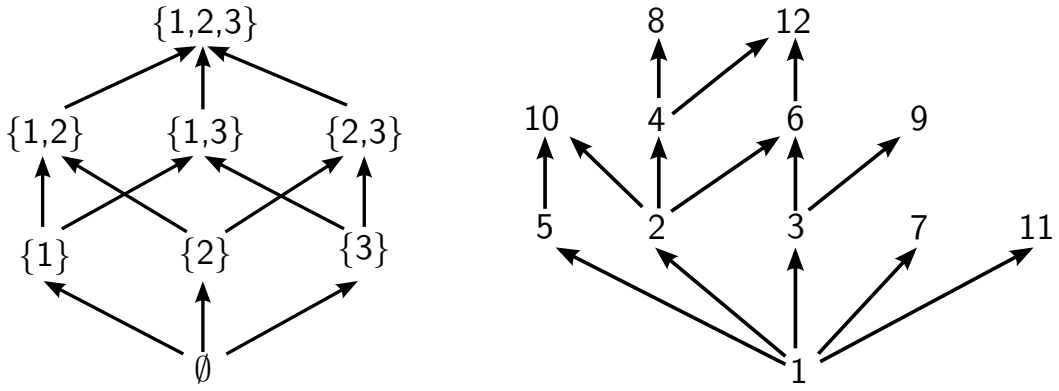
La relation "strictement plus petit" $<$ est un exemple bien connu d'ordre complet strict.

Notez que pour passer d'un ordre (partiel ou complet) à un ordre strict, il suffit d'enlever tous les couples de la forme $\langle a, a\rangle$ de la relation. Inversement, pour passer d'un ordre strict à un ordre, il suffit d'ajouter tous les couples de la forme $\langle a, a\rangle$ à la relation.

Diagrammes de Hasse

On peut représenter un ordre $\preceq$ sur un ensemble S par un **diagramme de Hasse** (en autant que la cardinalité de S ne soit pas trop grande). Ce diagramme prend la forme d'un graphe dont les sommets correspondent aux éléments de S. Si a et b sont deux éléments distincts de S et que $a \preceq b$, alors le sommet a est placé plus bas que le sommet b. S'il n'existe pas d'élément $e \in S \setminus \{a, b\}$, tel que $a \preceq e \preceq b$, alors une arête relie les sommets a et b.

La figure 1.15 présente les diagrammes de Hasse des deux ordres partiels donnés en exemple plus haut.



(a) Ordre $\subseteq$ sur $\mathcal{P}(\{1,2,3\})$. (b) Ordre $\preceq_{\mathcal{D}}$ sur $\{1,2,\ldots,12\}$.

FIGURE 1.15 – Diagrammes de Hasse des ordres partiels d'inclusion $\subseteq$ (figure de gauche) et "est un diviseur de" $\prec_{\mathcal{D}}$ (figure de droite).

1.7.4 "Au moins autant d'éléments" est un ordre complet

Revenons aux ensembles infinis. À la section 1.5.3, nous avons défini la notion ensembliste "**au moins autant d'éléments**". Nous avons déclaré que l'ensemble A a une cardinalité plus petite ou égale à l'ensemble B ($|A| \leq |B|$) si et seulement si il existe une fonction injective de A vers B (voir la définition 1.5.8, page 117). Nous verrons maintenant que cette notion "$\leq$" se comporte comme une relation d'ordre complet. Nous ne ferons pas toutes les démonstrations dans le cadre de ce cours, mais voyons ce qu'on peut faire...

Rappelons qu'un ordre complet satisfait les exigences d'un ordre partiel (définition 1.7.5), c'est-à-dire qu'il s'agit d'une relation réflexive, antisymétrique et transitive.

La réflexivité de notre relation "cardinalité $\leq$"

Cette propriété est clairement vérifiée puisque, comme on l'a vu à la section 1.7.2 (voir la proposition 1.7.2, page 142), pour tout ensemble A il existe toujours une fonction bijective de A vers A. Cette fonction étant par conséquent injective, nous avons bien que pour tout ensemble A, $|A| \leq |A|$.

L'antisymétrie de notre relation "cardinalité $\leq$"

Cette propriété découle du théorème suivant :

Théorème 1.7.7. (Bernstein-Schröder) *Soit A et B, deux ensembles.*
S'il existe une fonction injective de A vers B et une fonction injective de B vers A, alors il existera une fonction bijective de A vers B.
Autrement dit : $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$.

Cependant, nous ne ferons pas cette démonstration dans le cadre de ce cours.

La transitivité de notre relation "cardinalité $\leq$"

Pour démontrer la transitivité, il faut montrer que, pour tout triplet d'ensembles A, B et C, s'il existe une fonction injective de A vers B et une fonction injective de B vers C, alors il existe une fonction injective de A vers C. Or, nous savons déjà que c'est le cas, grâce au théorème 1.4.18-c (page 95).

La "cardinalité $\leq$" est un ordre complet

Nous n'allons pas faire cette démonstration. Il est intéressant de savoir tout de même qu'il a été démontré que pour démontrer

pour toute paire d'ensembles A et B, on a $(|A| < |B|) \vee (|A| > |B|) \vee (|A| = |B|)$

il faut absolument supposer l'axiome du choix.

1.7.5 Exercices sur les relations d'équivalences et ordres

Exercice 1 : Étant donné le tableau suivant, qui donne les propriétés de relations fictives, mais plausibles (toute ressemblance avec une relation existante est purement spéculative), dites lesquelles sont des relations d'équivalence, des ordres partiels, des ordres partiels stricts.

	réflexivité	irréflexivité	symétrie	asymétrie	antisymétrie	transitivité
a	x		x			x
b	x			x		x
c		x	x	x	x	x
d	x		x		x	x
e	x		x		x	x
f		x		x	x	x
g	x				x	x
h		x		x	x	
i		x	x			
j	x				x	

Exercice 2

Soit la relation suivante, qui est un ordre partiel sur l'ensemble de fonctions $\{0,1\}^{\{1,2,3\}}$.

$$\left\{ \langle f, g\rangle \in \{0,1\}^{\{1,2,3\}} \times \{0,1\}^{\{1,2,3\}} \;\middle|\; \big(\forall i \in \{1,2,3\} \mid f(i) \leq g(i)\big) \right\}.$$

Tracez le diagramme de Hasse de cet ordre.

Chapitre 2

Relations définies par récurrence

2.1 Suites

Dans ce chapitre, nous étudierons des problèmes reliés à la notion de suite. Une **suite** est une séquence infinie de nombres réels. Un élément de cette suite est appelé un **terme** de la suite.

Par exemple, $\langle 0, 2, 4, 6, 8, \ldots \rangle$ est la représentation en extension de la suite des entiers naturels pairs ou encore $\langle 0, 1, 4, 9, 16, \ldots \rangle$, celle des carrés parfaits. Voici un exemple plus complexe, connu sous le nom de suite de Fibonacci : $\langle 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots \rangle$. Chaque terme de la suite de Fibonacci est la somme des deux termes précédents.

De façon générale, la suite $\langle a_0, a_1, a_2, a_3, a_4, \ldots \rangle$ se note $\langle a_n \rangle_{n \in \mathbb{N}}$. Une telle suite est en fait une fonction de $\mathbb{N}$ vers $\mathbb{R}$, on peut donc représenter $\langle a_n \rangle_{n \in \mathbb{N}}$ en utilisant la notation introduite à la section 1.4.5 :

$$\begin{array}{rccc} f & : & \mathbb{N} & \longrightarrow & \mathbb{R} \\ & & n & \longmapsto & a_n \end{array}$$

Une suite ne commence pas nécessairement par l'indice 0, elle peut commencer par tout autre élément $n_0 \in \mathbb{Z}$. La suite $\langle a_{n_0}, a_{n_0+1}, a_{n_0+2}, a_{n_0+3} \ldots \rangle$ peut être représentée par la fonction :

$$\begin{array}{rccc} f & : & \{n \in \mathbb{Z} \mid n \geq n_0\} & \longrightarrow & \mathbb{R} \\ & & n & \longmapsto & a_n \end{array}$$

De même, la suite $\langle a_1, a_2, a_3, a_4, \ldots \rangle$ débutant à l'indice 1 se note $\langle a_n \rangle_{n \in \mathbb{N}^*}$.

Une suite peut donc être définie en **extension** (par exemple, $\langle 0, 2, 4, 6, 8, \ldots \rangle$) ou (de façon plus rigoureuse) en **compréhension** :

$$\begin{array}{rccc} f & : & \mathbb{N} & \longrightarrow & \mathbb{R} \\ & & n & \longmapsto & 2n. \end{array}$$

2.1.1 Définition par terme général et par récurrence

La définition en compréhension d'une suite est appelée **définition par terme général**. Plutôt que d'utiliser le formalisme des fonctions, on présente généralement une définition par terme général d'une suite en donnant simplement la formule générique permettant de calculer *directement* n'importe quel terme de la suite ainsi que l'ensemble des indices pour lesquels la formule est valide. Par exemple, le terme général de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ des entiers naturels pairs est

$$b_n \;=\; 2n \qquad \forall n \in \mathbb{N}\,. \tag{2.1}$$

À part la définition en extension et celle par terme général, il y a une autre façon (tout aussi rigoureuse que celle par terme général) de définir une suite : la **définition par récurrence**, qui consiste à donner directement la valeur du premier terme (ou les valeurs des quelques premiers termes) de la suite ainsi qu'une méthode pour calculer la valeur de n'importe quel terme de la suite en fonction de son (ou ses) prédécesseur(s). Ainsi, la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ des entiers naturels pairs peut se définir récursivement par

$$\left\{ \begin{array}{rcll} b_0 & = & 0 & \\ b_n & = & b_{n-1} + 2 & \forall n \in \mathbb{N}^*\,. \end{array} \right. \tag{2.2}$$

La **suite de Fibonacci**[1] $\langle f_n \rangle_{n\in\mathbb{N}}$ se définit récursivement par

$$\left\{ \begin{array}{rcll} f_0 & = & 0 & \\ f_1 & = & 1 & \\ f_n & = & f_{n-1} + f_{n-2} & \forall n \in \mathbb{N} \setminus \{0,1\}\,. \end{array} \right. \tag{2.3}$$

Nous verrons au cours de ce chapitre que le terme général de la suite de Fibonacci est :

$$f_n \;=\; \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n \qquad \forall n \in \mathbb{N}\,.$$

1. Dans la littérature, la suite de Fibonacci est la plupart du temps définie pour $n \geq 1$, c'est-à-dire : $f_1 = 1$, $f_2 = 1$ et $f_n = f_{n-1} + f_{n-2} \quad \forall n \in \mathbb{N}^* \setminus \{1,2\}$.

2.1.2 Notation sigma "Σ"

En mathématiques, on représente fréquemment une somme de plusieurs termes en utilisant la **notation sigma**. À l'aide de cette notation, la somme des nombres entiers entre 1 et 5 inclusivement s'écrit :

$$\sum_{i=1}^{5} i \;=\; 1+2+3+4+5\,.$$

De manière plus générale, la somme des nombres entiers entre 1 et n inclusivement s'écrit :

$$\sum_{i=1}^{n} i \;=\; 1+2+3+\ldots+(n-1)+n\,.$$

La définition suivante met en évidence que la notation sigma permet de présenter de façon concise une somme définie en extension.

Définition 2.1.1. *Notation sigma*
Soit $n, n_0 \in \mathbb{Z}$ tels que $n \geq n_0$ et une fonction $g : \{i \in \mathbb{Z} \mid n_0 \leq i \leq n\} \longrightarrow \mathbb{R}$. On écrit :

$$\sum_{i=n_0}^{n} g(i) \;\stackrel{\text{def}}{=}\; g(n_0)+g(n_0+1)+g(n_0+2)+\ldots+g(n)\,.$$

Ainsi, on peut écrire la définition en extension de la suite des entiers naturels pairs $\langle b_n \rangle_{n\in\mathbb{N}}$, dont le terme général est donné par l'équation (2.1), en utilisant la notation sigma :

$$b_n \;=\; \sum_{i=1}^{n} 2 \;=\; \underbrace{2+2+\ldots+2}_{n \text{ fois}}\,. \tag{2.4}$$

De même, la suite $\langle c_n \rangle_{n\in\mathbb{N}}$ de la somme des n premiers entiers naturels mis au carré s'écrit :

$$c_n \;=\; \sum_{i=0}^{n} i^2 \;=\; 0^2+1^2+2^2+3^2+\ldots+n^2\,. \tag{2.5}$$

La proposition 2.1.2 présente quelques propriétés des sommes qui permettent, dans certaines circonstances, de trouver le terme général d'une suite à partir d'une définition utilisant la notation sigma.

Proposition 2.1.2. *Propriétés arithmétiques des sommes en notation sigma.*
Soit $n, n_0 \in \mathbb{Z}$ tels que $n \geq n_0$, deux fonctions $g, h : \{i \in \mathbb{Z} \mid n_0 \leq i \leq n\} \longrightarrow \mathbb{R}$ et une constante $k \in \mathbb{R}$. On a :

$$\texttt{a}: \quad \sum_{i=n_0}^{n} 1 = n - n_0 + 1 \qquad \textit{(En particulier, } \sum_{i=1}^{n} 1 = n\textit{)}$$

$$\texttt{b}: \quad \sum_{i=n_0}^{n} k \cdot g(i) = k \cdot \sum_{i=n_0}^{n} g(i) \qquad \textit{(En particulier, } \sum_{i=1}^{n} k = k \cdot n\textit{)}$$

$$\texttt{c}: \quad \sum_{i=n_0}^{n} g(i) + h(i) = \sum_{i=n_0}^{n} g(i) + \sum_{i=n_0}^{n} h(i)$$

$$\texttt{d}: \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$$\texttt{e}: \quad \sum_{i=1}^{n} i^2 = \frac{(2n+1)(n+1)n}{6}$$

Par exemple, on retrouve l'expression du terme général des suites $\langle b_n \rangle_{n\in\mathbb{N}}$ et $\langle c_n \rangle_{n\in\mathbb{N}}$ que nous avons définies plus haut à l'aide de la notation sigma par les équations (2.4) et (2.5) :

$$b_n = \sum_{i=1}^{n} 2 = 2 \cdot n \qquad \langle \textit{ Prop 2.1.2-b, cas particulier avec } [k := 2] \rangle$$

$$c_n = \sum_{i=0}^{n} i^2 = 0^2 + \sum_{i=1}^{n} i^2$$

$$= \sum_{i=1}^{n} i^2 = \frac{(2n+1)(n+1)n}{6} \qquad \langle \textit{ Prop 2.1.2-e } \rangle$$

2.1.3 Temps d'exécution d'un algorithme

Le concept de suite se retrouve au centre de l'analyse de plusieurs problèmes en mathématiques et en informatique. On le retrouve entre autres lorsque l'on cherche à calculer le **temps d'exécution** t_n d'un programme en fonction d'un certain paramètre n qui est généralement relié à la taille des données fournies en entrée au programme.

En **analyse d'algorithmes**, on mesure typiquement le temps d'exécution en calculant le nombre de fois que sera exécutée une **instruction baromètre**, c'est-à-dire une instruction qui est exécutée au moins aussi souvent que n'importe quelle autre instruction du programme (à une constante près). Cette unité de mesure possède l'avantage de ne pas reposer sur la vitesse de l'ordinateur sur lequel est exécuté un programme, mais évalue seulement la

complexité de l'algorithme [2].

À titre d'exemple, le temps d'exécution d'un algorithme triant les n éléments d'un tableau en ordre croissant dépend généralement de la taille n du tableau (c'est-à-dire le nombre d'éléments à trier). L'instruction baromètre utilisée est le nombre de comparaisons entre deux éléments du tableau. Nous présenterons un exemple de calcul du temps d'exécution d'un algorithme de tri à la section 2.2.2.

Les algorithmes itératifs

Lorsqu'un algorithme est constitué de boucles (possiblement imbriquées), il est souvent naturel de calculer son temps d'exécution en utilisant la notation sigma "Σ". Considérons par exemple l'algorithme suivant :

```
Algo_Jouet_Un ( n )
  l ← 0
  Pour i = 1 à n Faire
      Pour j = 1 à i Faire
          l ← l + 1
      Fin Pour
  Fin Pour
  Retourner l
```

Ici, se demander quel sera (en fonction du paramètre n) le temps d'exécution de l'algorithme revient en gros à calculer le nombre de fois que sera exécutée l'instruction baromètre "$l \leftarrow l + 1$". Dans ce cas précis, cela est équivalent à se demander quelle sera la valeur retournée par l'algorithme, en fonction du paramètre n. Soit $\langle d_n \rangle_{n\in\mathbb{N}}$ la suite qui, pour chaque n, donne cette valeur finale. En utilisant la notation sigma "Σ", on peut traduire facilement les boucles "**Pour**" en sommes :

$$d_n \;=\; \sum_{i=1}^{n} \sum_{j=1}^{i} 1\,.$$

En appliquant successivement les propriétés arithmétiques des sommes énoncées par la pro-

2. Il s'agit ici d'une présentation très sommaire de l'analyse d'algorithmes. Le cours dédié entièrement à ce sujet vous en apprendra beaucoup plus !

position 2.1.2, on parvient à la définition par terme général de d_n :

$$\begin{aligned} d_n &= \sum_{i=1}^{n}\sum_{j=1}^{i} 1 &&= \sum_{i=1}^{n} i && \langle\ \textit{Prop 2.1.2-a}\ \rangle \\ &&&= \frac{n(n+1)}{2} && \langle\ \textit{Prop 2.1.2-d}\ \rangle \end{aligned}$$

On peut aussi exprimer d_n en définissant la suite par récurrence. En utilisant la convention appropriée[3], on remarque facilement que :

$$\begin{cases} d_0 &= 0 \\ d_n &= d_{n-1} + n \quad \forall n \in \mathbb{N}^* . \end{cases} \tag{2.6}$$

Les algorithmes récursifs

Pour analyser l'exemple précédent (l'algorithme `Algo_Jouet_Un`), la notation sigma semble plus appropriée que la définition par récurrence de la suite. Il existe cependant plusieurs cas où la définition par récurrence est la plus naturelle. C'est particulièrement le cas des algorithmes récursifs, comme dans l'exemple suivant :

```
Algo_Jouet_Deux ( n )
  Si n < 1 alors
      Retourner 1
  Sinon
      Retourner 2 × Algo_Jouet_Deux(n − 1)
  Fin Si
```

Désignons par $\langle b_n \rangle_{n\in\mathbb{N}}$ la suite qui, pour chaque n, donne la valeur retournée par la fonction décrite dans ce dernier exemple. Ici, il est facile de comprendre ce que sera la valeur de b_n si on connaît celle de b_{n-1} :

$$\begin{cases} b_0 &= 1; \\ b_n &= 2 \cdot b_{n-1} \quad \forall n \in \mathbb{N}^* . \end{cases} \tag{2.7}$$

Bien que la définition par récurrence soit une définition tout à fait rigoureuse, elle n'est pas très pratique. En effet, pour calculer b_{100} dans l'exemple précédent, il nous faut d'abord

3. Nous adoptons ici la convention que si $n = 0$, il n'y a pas d'erreur d'exécution, mais que les instructions à l'intérieur de la première boucle "Pour" ne sont tout simplement pas exécutées.

calculer b_{99} et pour calculer b_{99}, on a besoin de connaître b_{98}, etc. Donc, si on souhaite utiliser la suite $\langle a_n \rangle_{n \in \mathbb{N}}$ pour analyser notre petit algorithme "`Algo_Jouet_Deux`", pour chacune des valeurs de n, on serait mieux de travailler avec la définition par terme général de la suite (malheureusement plus difficile à obtenir) au lieu de la définition par récurrence.

Dans cet exemple simple, on peut "deviner" que le terme général de la suite est $b_n = 2^n$ en calculant les premiers termes de la suite :

n	0	1	2	3	4	$\cdots$	n
b_n	1	2	4	8	16	$\cdots$	2^n

La section 2.2 présente la méthode de la substitution à rebours qui nous aidera, dans certaines circonstances, à déduire le terme général d'une suite à partir de sa définition par récurrence. Ensuite, la section 2.3 présente la technique de démonstration par induction mathématique, qui permettra de démontrer que la définition par terme général que nous avons déduite ou devinée est bien équivalente à sa définition par récurrence.

2.1.4 Exercices sur les suites

Exercice 1 : Évaluez la valeur de la somme suivante :

$$s \;=\; \sum_{i=1}^{3}\sum_{j=1}^{2}(\, i^2 + j\,)\,.$$

Exercice 2 : En vous servant de la notation en extension des sommes, illustrez les égalités suivantes (la réponse du premier exercice vous est donnée à titre d'exemple) :

a) $\displaystyle\sum_{i=1}^{n} i \;=\; 1 + \sum_{i=2}^{n} i$

Solution :

$$\begin{aligned}\sum_{i=1}^{n} i &= 1 + 2 + 3 + \ldots + n \\ &= 1 + (2 + 3 + \ldots + n) \\ &= 1 + \sum_{i=2}^{n} i\end{aligned}$$

b) $\displaystyle\sum_{i=0}^{n} i \;=\; \sum_{i=1}^{n} i$

c) $\displaystyle\sum_{i=1}^{n}(n-i) \;=\; \sum_{i=1}^{n-1} i$

d) $\displaystyle\sum_{i=1}^{n} k\sqrt{i} \;=\; k \cdot \sum_{i=1}^{n} \sqrt{i}\;,$ pour tout $k \in \mathbb{R}$

e) $\displaystyle\sum_{i=0}^{n-1} 2i + 1 \;=\; \sum_{i=1}^{n} 2i - 1$

f) $\displaystyle\sum_{i=1}^{n-1}\sum_{j=1}^{n}\sum_{k=1}^{n} 1 \;=\; n^3 - n^2$

Exercice 3 : Soit la suite $\langle v_n \rangle_{n \in \mathbb{N}^*}$ dont le $n$ième terme correspond à la valeur retournée par l'algorithme suivant exécuté avec le paramètre n en entrée (avec $n \geq 1$).

```
Algo_Jouet_Trois ( n )
  v ← 0
  Pour i = 1 à n Faire
      Pour j = i + 1 à n Faire
          v ← v + 1
      Fin Pour
  Fin Pour
  Retourner v
```

a) À l'aide de la notation sigma, donnez l'expression permettant de calculer un terme v_n quelconque (avec $n \in \mathbb{N}^*$).

b) À partir de la réponse précédente, calculez le terme général de la suite $\langle v_n \rangle_{n \in \mathbb{N}^*}$. Pour ce faire, utilisez les propriétés arithmétiques des sommes en notation sigma.

c) Donnez la définition par récurrence de la suite $\langle v_n \rangle_{n \in \mathbb{N}^*}$.

d) Calculez les 5 premiers termes de la suite $\langle v_n \rangle_{n \in \mathbb{N}^*}$ à l'aide de chacune des trois expressions trouvées en (a), (b) et (c). Assurez-vous que les réponses sont identiques.

2.2 Méthode des substitutions à rebours

La **méthode des substitutions à rebours** présentée dans cette section est une "recette" qui nous permet, dans certains cas, de *déduire* le terme général d'une suite à partir de sa définition par récurrence. Précisons dès le départ que cette méthode ne permet pas de démontrer hors de tout doute l'équivalence entre la définition par récurrence d'une suite et le terme général déduit. Dans le cadre de ce cours, nous considérons cependant que, lorsque la méthode des substitutions à rebours est appliquée rigoureusement, elle est suffisamment convaincante pour qu'on puisse tenir son résultat pour acquis.

2.2.1 Description de la méthode

Pour illustrer les différentes étapes de la méthode des substitutions à rebours, considérons l'exemple (très simple) de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ dont nous avons donné la définition par récurrence à l'équation (2.7) :

$$\begin{cases} b_0 &= 1 \\ b_n &= 2 \cdot b_{n-1} \quad \forall n \in \mathbb{N}^* \,. \end{cases}$$

Les équations ci-dessous présentent les étapes de la méthode de la substitution à rebours appliquée à la suite $\langle b_n \rangle_{n\in\mathbb{N}}$. Nous discuterons ensuite de chacune des étapes.

$$\begin{aligned}
b_n &= 2 \cdot b_{n-1} && \langle\ \textit{Définition par récurrence de } b_n\ \rangle \\
&= 2 \cdot 2 \cdot b_{n-2} && \langle\ \textit{Car } b_{n-1} = 2b_{n-2}\ \rangle \\
&= 2 \cdot 2 \cdot 2 \cdot b_{n-3} && \langle\ \textit{Car } b_{n-2} = 2b_{n-3}\ \rangle \\
&= 2 \cdot 2 \cdot 2 \cdot 2 \cdot b_{n-4} && \langle\ \textit{Car } b_{n-3} = 2b_{n-4}\ \rangle \\
&= \ldots \\
&= \underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{i \text{ fois}} \cdot b_{n-i} && \langle\ \textit{Pour tout } i \in \{1, \ldots, n\}\ \rangle \\
&= \underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{n \text{ fois}} \cdot b_0 && \langle\ \textit{En utilisant } [i := n]\ \rangle \\
&= \underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{n \text{ fois}} \cdot 1 && \langle\ \textit{Car } b_0 = 1\ \rangle \\
&= 2^n \,. && \langle\ \textit{Arithmétique}\ \rangle
\end{aligned}$$

(A) Substituer à rebours

(B) Déduire l'expression après i subtitutions

(C) Substituer la valeur du cas de base

(D) Calculer le terme général

Nous avons donc divisé la démarche en quatre étapes clés :

(A) Substituer à rebours.
Nous débutons en considérant la récurrence "$b_n = 2 \cdot b_{n-1}$" et en substituant "b_{n-1}" par sa définition, c'est-à-dire par la même expression récursive. Nous répétons cette opération quelques fois, en substituant successivement les valeurs de "b_{n-2}", "b_{n-3}", ...

(B) Déduire l'expression après i subtitutions.
Après quelques substitutions à rebours, on voit apparaître une structure dans le développement de l'expression. Cela nous permet de déduire l'expression (en extension) de b_n après avoir effectué un nombre quelconque i de substitutions.

(C) Substituer la valeur du cas de base.
Maintenant que nous connaissons l'expression obtenue après i substitutions, nous calculons l'expression qui fait apparaître le cas de base de la récurrence. Ici, le cas de base "$b_0 = 1$" apparaitra après n substitutions. Cela nous permet d'obtenir une expression de b_n qui n'est plus récursive.

(D) Calculer le terme général
Nous transformons finalement l'expression en extension de b_n en une expression en compréhension. Dans l'exemple de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$, cette transformation est obtenue par une simple propriété arithmétique.

Notez que l'étape (D) ne sera pas toujours réalisable. En effet, déduire le terme général d'une suite à partir d'une expression en extension (ou en notation sigma) est souvent très difficile et parfois impossible.

2.2.2 Quelques exemples

Exemple 1 : La récurrence de l'équation (2.6)

Commençons par calculer, par la méthode des substitutions à rebours, le terme général de la récurrence $\langle d_n \rangle_{n\in\mathbb{N}}$ présentée par l'équation (2.6) :

$$\begin{cases} d_0 &= 0 \\ d_n &= d_{n-1} + n \quad \forall n \in \mathbb{N}^* . \end{cases}$$

Rappelons que nous avons obtenu cette expression après l'analyse de l'algorithme `Algo_Jouet_Un` de la page 154.

$$
\begin{array}{rcll}
d_n & = & d_{n-1} + n & \langle\ \textit{Définition par récurrence de } b_n\ \rangle \\
& = & d_{n-2} + (n-1) + n & \langle\ \textit{Car } d_{n-1} = d_{n-2} + (n-1)\ \rangle \\
& = & d_{n-3} + (n-2) + (n-1) + n & \langle\ \textit{Car } d_{n-2} = d_{n-3} + (n-2)\ \rangle \\
& = & d_{n-4} + (n-3) + (n-2) + (n-1) + n & \langle\ \textit{Car } d_{n-3} = d_{n-4} + (n-3)\ \rangle \\
& = & \ldots & \\
& = & d_{n-i} + (n-(i-1)\,) + (n-(i-2)\,) + \ldots + (n-1) + n & \langle\ \forall i \in \{1, \ldots, n\}\ \rangle \\
& = & d_0 + (n-(n-1)\,) + (n-(n-2)\,) + \ldots + (n-1) + n & \langle\ \textit{Avec } [i := n]\ \rangle \\
& = & (n-(n-1)\,) + (n-(n-2)\,) + \ldots + (n-1) + n & \langle\ \textit{Car } d_0 = 0\ \rangle \\
& = & 1 + 2 + \ldots + (n-1) + n & \langle\ \textit{Arithmétique}\ \rangle \\
& = & \displaystyle\sum_{j=1}^{n} j & \langle\ \textit{Réécriturre en notation sigma}\ \rangle \\
& = & \dfrac{n(n+1)}{2}\,. & \langle\ \textit{Proposition 2.1.2-d}\ \rangle
\end{array}
$$

Dans cet exemple, la méthode de la substitution à rebours nous a permis de réécrire en extension la suite $\langle d_n \rangle_{n \in \mathbb{N}}$. Nous avons ensuite constaté que l'expression obtenue correspondait à une somme en notation sigma dont nous connaissions le terme général (grâce à la proposition 2.1.2). Les propriétés des sommes sont en général très utiles lorsqu'on applique la méthode des substitutions à rebours sur des suites où la règle de récurrence comporte une addition.

Exemple 2 : Le tri par sélection

Le **tri par sélection** est un algorithme de tri simple et intuitif. Dans le pseudo-code ci-dessous, on considère que l'algorithme reçoit en entrée un tableau T contenant n nombres réels à trier en ordre croissant. Les éléments du tableau sont indexés de 1 à n. Ainsi, $T[1]$ réfère au premier élément du tableau et $T[n]$ au dernier élément.

Pour calculer le temps d'exécution de l'algorithme `Tri_Sélection` en fonction du nombre n d'éléments à trier, nous choisissons la comparaison "$T[j] < T[i\_min]$" en guise d'instruction baromètre, car cette instruction est exécutée au moins aussi souvent que n'importe quelle autre instruction de l'algorithme.

```
Tri_Sélection ( T[1,...,n] )
  Pour i = 1 à n Faire
      i_min ← i

      Pour j = i + 1 à n Faire
          Si T[j] < T[i_min] alors
              i_min ← j
          Fin Si
      Fin Pour

      échanger le contenu de T[i] et T[i_min]
  Fin Pour
  Retourner T
```

Désignons par $\langle s_n \rangle_{n \in \mathbb{N} \setminus \{0,1\}}$ la suite dont le $n$ième terme correspond au nombre d'exécutions de l'instruction baromètre pour un tableau de taille n. Nous considérons $n \geq 2$, car il est inutile de trier un tableau de moins de deux éléments. Puisque l'algorithme est de type itératif, il serait possible de définir la suite à l'aide de la notation sigma et de calculer le terme général associé en appliquant les propriétés de la proposition 2.1.2 (pourquoi ne pas le faire en exercice !). Cependant, nous allons ici définir la valeur du terme s_n par une règle de récurrence :

$$\begin{cases} s_2 &= 1 \\ s_n &= s_{n-1} + (n-1) \quad \forall n \in \mathbb{N} \setminus \{0,1,2\}\,. \end{cases}$$

L'expression de la récurrence est obtenue grâce aux deux constatations suivantes :

— Pour un tableau de taille 2, l'instruction baromètre est exécutée une seule fois (c'est notre cas de base) ;
— Pour un tableau de taille $n > 2$, la boucle interne est d'abord exécutée $(n-1)$ fois (il en va donc de même pour le nombre d'exécutions de l'instruction baromètre). Ensuite, le nombre d'exécutions de l'instruction est le même que si on exécute l'algorithme sur un tableau de taille $(n-1)$.

Utilisons donc la méthode des substitutions à rebours pour trouver le terme général de la suite $\langle s_n \rangle_{n \in \mathbb{N} \setminus \{0,1\}}$:

$$
\begin{aligned}
s_n &= s_{n-1} + (n-1) && \langle \textit{ Définition par récurrence de } s_n \rangle \\
&= s_{n-2} + (n-2) + (n-1) && \langle \textit{ Car } s_{n-1} = s_{n-2} + (n-2) \rangle \\
&= s_{n-3} + (n-3) + (n-2) + (n-1) && \langle \textit{ Car } s_{n-2} = s_{n-3} + (n-3) \rangle \\
&= s_{n-4} + (n-4) + (n-3) + (n-2) + (n-1) && \langle \textit{ Car } s_{n-3} = s_{n-4} + (n-4) \rangle \\
&= \ldots \\
&= s_{n-i} + (n-i) + (n-(i-1)) + \ldots + (n-2) + (n-1) && \langle\, \forall i \in \{1, \ldots, n-2\} \,\rangle \\
&= s_2 + (n-(n-2)) + (n-(n-3)) + \ldots + (n-2) + (n-1) && \langle \textit{ Avec } [i := n-2] \rangle \\
&= s_2 + 2 + 3 + \ldots + (n-2) + (n-1) && \langle \textit{ Arithmétique} \rangle \\
&= 1 + 2 + 3 + \ldots + (n-2) + (n-1) && \langle \textit{ Car } s_2 = 1 \rangle \\
&= \sum_{j=1}^{n-1} j && \langle \textit{ Réécriturre en notation sigma} \rangle \\
&= \frac{(n-1) \cdot ((n-1)+1)}{2} && \langle \textit{ Prop 2.1.2-d, avec } [n := n-1] \rangle \\
&= \frac{n \cdot (n-1)}{2} \,. && \langle \textit{ Arithmétique} \rangle
\end{aligned}
$$

Exemple 3 : Le problème des tours de Hanoï

Le problème des tours de Hanoï est un jeu de logique qui a été imaginé par le mathématicien français Édouard Lucas (1842 – 1891). Le jeu est constitué de trois tiges (que nous désignons par les tiges A, B et C) et de n disques. Tous les disques possèdent des diamètres distincts. Au début du jeu, les disques sont empilés sur la tige A en ordre de taille, de manière à ce que le disque de plus grand diamètre soit à la base de la pile et que le disque de plus petit diamètre soit au sommet de la pile (tel qu'illustré à la figure 2.1).

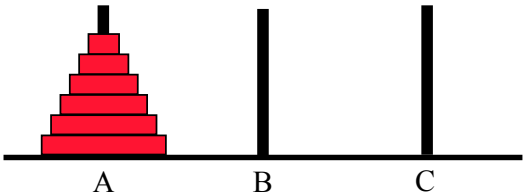


FIGURE 2.1 – Le problème des tours de Hanoï (à $n = 6$ disques).

Le but du jeu est de transférer tous les disques sur la tige C en respectant les contraintes suivantes :

— On ne peut déplacer qu'un seul disque à la fois. Les déplacements se font d'une tige à une autre, et donc du sommet d'une pile au sommet d'une autre pile ;
— Un disque peut seulement être déplacé sur un disque de diamètre supérieur ou encore sur une tige vide. Autrement dit, il est interdit de déplacer un disque sur une pile possédant des disques de tailles inférieures à lui même.

Examinons d'abord la stratégie qui permet de résoudre le problème des tours de Hanoï. Nous procédons en débutant par le cas le plus simple (c'est-à-dire déplacer une pile d'un seul disque) et en déduisant la méthode pour le cas général (c'est-à-dire déplacer une pile constituée d'un nombre quelconque de disques).

(1) Méthode pour déplacer un seul disque de la tige A vers la tige C. ($n = 1$)

— Déplacer l'unique disque de la tige A vers la tige C.

(2) Méthode pour déplacer deux disques de la tige A vers la tige C. ($n = 2$)

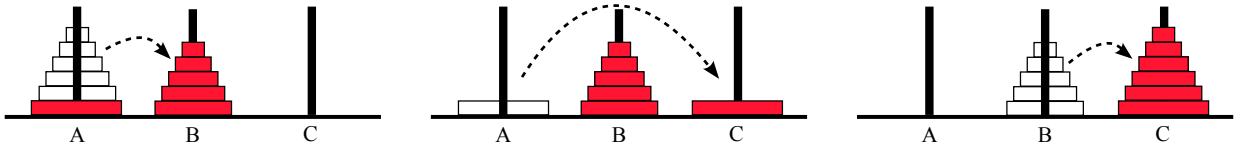
— Déplacer le petit disque de la tige A vers la tige B ;
— Déplacer le grand disque de la tige A vers la tige C ;
— Déplacer un petit disque de la tige B vers la tige C ;

(3) Méthode pour déplacer trois disques de la tige A vers la tige C. ($n = 3$)

— Déplacer deux disques de la tige A vers la tige B ;
⟨ *Appliquer la méthode* **(2)** *avec* [A := A] *et* [C := B]. ⟩
— Déplacer le grand disque de la tige A vers la tige C ;
— Déplacer deux disques de la tige B vers la tige C ;
⟨ *Appliquer la méthode* **(2)** *avec* [A := B] *et* [C := C]. ⟩

(⋯) Méthode pour déplacer n disques de la tige A vers la tige C. ($n \in \mathbb{N}^*$)

— Déplacer $n - 1$ disques de la tige A vers la tige B ; ⟨ *Voir figure 2.2a* ⟩
— Déplacer l'unique disque de la tige A vers la tige C ; ⟨ *Voir figure 2.2b* ⟩
— Déplacer $n - 1$ disques de la tige B vers la tige C ; ⟨ *Voir figure 2.2c* ⟩



(a) Déplacer $n-1$ disques de A vers B. (b) Déplacer 1 disque de A vers C. (c) Déplacer $n-1$ disques de B vers C.

FIGURE 2.2 – Illustration de la méthode à employer pour déplacer n disques de la tige A vers la tige C. Les étapes (a) et (c) se font par appels récursifs.

La stratégie permettant de résoudre le problème des tours de Hanoï s'exprime donc naturellement par un algorithme récursif. Le pseudo-code ci-dessous présente cet algorithme. Pour résoudre une instance du problème à n disques, l'appel initial à l'algorithme doit être :

```
Déplacer_Disques(n, A, C, B)
```

Prenez note que cette formulation de l'algorithme considère que le cas de base correspond à la situation où aucun disque n'est déplacé ($n = 0$). Il aurait été aussi valable de considérer le cas où un seul disque est déplacé ($n = 1$).

```
Déplacer_Disques(nbDisques, tigeDépart, tigeArrivée, tigeAuxiliare)
  Si nbDisques > 0 alors
      (1) Déplacer_Disques(nbDisques−1, tigeDépart, tigeAuxiliare, tigeArrivée)
      (2) Déplacer le disque de "tigeDépart" à "tigeArrivée"
      (3) Déplacer_Disques(nbDisques−1, tigeAuxiliare, tigeArrivée, tigeDépart)
  Fin Si
```

On désire maintenant connaître le nombre de déplacements de disques que l'on doit effectuer pour résoudre le problème des tours de Hanoï à n disques. Autrement dit, on désire calculer le nombre de fois que sera exécutée la ligne (2) dans l'algorithme `Déplacer_Disques` en fonction de la valeur initiale du paramètre "nbDisques". La suite correspondante $\langle h_n \rangle_{n \in \mathbb{N}}$ se définit naturellement par la récurrence suivante :

$$\begin{cases} h_0 &= 0 \\ h_n &= 2 \cdot h_{n-1} + 1 \quad \forall n \in \mathbb{N}^*. \end{cases} \tag{2.8}$$

Tentons de déduire le terme général de la suite $\langle h_n \rangle_{n\in\mathbb{N}}$ à l'aide de la méthode des substitutions à rebours :

$$
\begin{aligned}
h_n &= 2 \cdot h_{n-1} + 1 && \langle \textit{ Définition par récurrence de } h_n \rangle \\
&= 2 \cdot (2 \cdot h_{n-2} + 1) + 1 && \langle \textit{ Car } h_{n-1} = 2 \cdot h_{n-2} + 1 \rangle \\
&= 2 \cdot 2 \cdot h_{n-2} + 2 + 1 && \langle \textit{ Arithmétique} \rangle \\
&= 2 \cdot 2 \cdot (2 \cdot h_{n-3} + 1) + 2 + 1 && \langle \textit{ Car } h_{n-2} = 2 \cdot h_{n-3} + 1 \rangle \\
&= 2 \cdot 2 \cdot 2 \cdot h_{n-3} + 2 \cdot 2 + 2 + 1 && \langle \textit{ Arithmétique} \rangle \\
&= 2 \cdot 2 \cdot 2 \cdot (2 \cdot h_{n-4} + 1) + 2 \cdot 2 + 2 + 1 && \langle \textit{ Car } h_{n-3} = 2 \cdot h_{n-4} + 1 \rangle \\
&= 2 \cdot 2 \cdot 2 \cdot 2 \cdot h_{n-4} + 2 \cdot 2 \cdot 2 + 2 \cdot 2 + 2 + 1 && \langle \textit{ Arithmétique} \rangle \\
&= 2^4 \cdot h_{n-4} + 2^3 + 2^2 + 2^1 + 2^0 && \langle \textit{ Arithmétique} \rangle \\
&= \dots \\
&= 2^i \cdot h_{n-i} + 2^{i-1} + \dots + 2^2 + 2^1 + 2^0 && \langle\ \forall i \in \{1, \dots, n\}\ \rangle \\
&= 2^n \cdot h_0 + 2^{n-1} + \dots + 2^2 + 2^1 + 2^0 && \langle \textit{ Avec } [i := n] \rangle \\
&= 2^{n-1} + \dots + 2^2 + 2^1 + 2^0 && \langle \textit{ Car } h_0 = 0 \rangle \\
&= \sum_{j=0}^{n-1} 2^j && \langle \textit{ Réécriturre en notation sigma} \rangle \\
&= \dots \textbf{?} && \langle \textit{ À suivre...} \rangle
\end{aligned}
$$

À ce moment-ci, nous ne pouvons pas aller plus loin dans la transformation de l'expression h_n. La méthode des substitutions à rebours nous a permis de déduire une somme en notation sigma. Pour l'instant, nous ne connaissons aucune propriété qui nous permet d'exprimer cette somme sous la forme d'un terme général [4]. Cela met en évidence que cette méthode ne peut pas à elle seule résoudre n'importe quelles récurrences. Nous avons besoin d'outils supplémentaires !

4. Le lecteur avide de savoir peut se référer directement à la page 190, où nous calculons le terme général de la suite $\langle h_n \rangle_{n\in\mathbb{N}}$. Nous verrons en effet à la section 2.4.3 que le terme h_n correspond à la somme des n premiers termes d'une suite géométrique de raison 2.

2.2.3 Exercices sur la méthode des substitutions à rebours

Exercice 1 : Calculez le terme général des récurrences suivantes à l'aide de la méthode des substitutions à rebours :

a) $\begin{cases} x_1 &= 0 \\ x_n &= x_{n-1} + 5 \quad \forall n \in \mathbb{N}^* \setminus \{1\} \end{cases}$

b) $\begin{cases} y(1) &= 4 \\ y(n) &= 3 \cdot y(n-1) \quad \forall n \in \mathbb{N}^* \setminus \{1\} \end{cases}$

c) $\begin{cases} z(0) &= 0 \\ z(n) &= z(n-1) + 2n - 1 \quad \forall n \in \mathbb{N}^* \end{cases}$

2.3 Induction mathématique

Supposons que nous connaissons la définition par récurrence d'une suite $\langle a_n \rangle_{n\in\mathbb{N}}$ et que nous désirons trouver sa définition par terme général. Dans plusieurs cas de récurrences complexes, la façon la plus simple de procéder est de calculer les premiers termes de la suite à l'aide de l'expression de la récurrence et de "deviner" le terme général. Dans cette situation, il faut ensuite démontrer que l'expression que nous avons "devinée" est valide pour tous les termes de la suite. Pour ce faire, nous avons souvent recours au principe d'induction mathématique.

Notons que, bien que nous concentrons ici nos efforts sur l'étude des récurrences, le principe d'induction mathématique s'applique à un éventail de problèmes beaucoup plus large.

2.3.1 Induction mathématique faible

Le principe d'**induction mathématique** s'énonce de plusieurs façons, la forme la plus couramment utilisée étant :

Théorème 2.3.1. *Principe d'induction mathématique faible.*
Soit un prédicat P. Alors,

$$\texttt{a}: \quad \Big[\, P(0) \wedge \big(\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1)\big) \,\Big] \;\Rightarrow\; \big(\forall n \in \mathbb{N} \mid P(n)\big)$$

$$\texttt{b}: \quad \Big[\, P(0) \wedge \big(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n)\big) \,\Big] \;\Rightarrow\; \big(\forall n \in \mathbb{N} \mid P(n)\big)$$

Dans ce document, nous utiliserons surtout la deuxième formulation du théorème (2.3.1-b), car c'est celle qui se prête le mieux aux démonstrations reliées aux résolutions de récurrences telles que nous les avons définies. Le prédicat "$P(n)$" du théorème correspondra à l'énoncé "Le $n$ième terme de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ obtenu par le terme général est égal au $n$ième terme obtenu par la relation de récurrence".

Structure d'une démonstration par induction

Une démonstration utilisant le principe d'induction débute nécessairement par la présentation du prédicat "$P(n)$". Ensuite, la démonstration s'effectue en deux étapes distinctes, le cas de base et le pas d'induction.

(A) Cas de base : démonstration de $P(0)$.

On démontre que P est vrai pour la valeur 0 (seulement). Ce cas est presque toujours

très facile, mais il est essentiel.

(B) Pas d'induction : démonstration de $(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n))$**.**

Cette démonstration se fait comme d'habitude lorsqu'on a quantificateur universel "∀" qui s'applique à une implication "⇒" (relire au besoin la section 1.3.5) :

— On présente un $n \in \mathbb{N}^*$ pour lequel on ne suppose qu'une chose, c'est que le prédicat $P(n-1)$ est vrai pour cette valeur de n. Cette hypothèse s'appelle l'*hypothèse d'induction*.

— Puis on montre que ceci implique que pour cette valeur de n, le prédicat $P(n)$ est lui aussi vrai.

Une fois ces deux étapes démontrées, on peut conclure :

(A) et (B) impliquent $(\forall n \in \mathbb{N} \mid P(n))$**.**

L'exemple suivant devrait rendre cette idée plus précise.

Exemple de la suite des carrés parfaits

Soit $\langle c_n \rangle_{n\in\mathbb{N}}$ une suite définie par récurrence par

$$\begin{cases} c_0 &= 0 \\ c_n &= c_{n-1} + 2n - 1 \qquad \forall n \in \mathbb{N}^* . \end{cases}$$

Nous allons démontrer que cette suite correspond à la **suite des carrés parfaits**, c'est-à-dire que le terme général de la suite $\langle c_n \rangle_{n\in\mathbb{N}}$ est :

$$c_n \;=\; n^2 \quad \forall n \in \mathbb{N} .$$

Démonstration. La suite $\langle c_n \rangle_{n\in\mathbb{N}}$ est la suite des carrés parfaits.
Prenons le prédicat $P(n)$: $c_n = n^2$.
Alors nous devons démontrer que $(\forall n \in \mathbb{N} \mid P(n))$.
Et par le principe d'induction mathématique (théorème 2.3.1-b), il suffit de démontrer que

$$P(0) \;\wedge\; (\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n)) .$$

Cas de base : démontrons $P(0)$**.** ⟨ *C'est-à-dire, montrons* $c_0 = 0^2$. ⟩

$c_0 \;=\; 0 \;=\; 0^2$.

Pas d'induction : démontrons $(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n))$**.**

Soit $n \in \mathbb{N}^*$, et supposons $P(n-1)$. $\quad \langle$ *i.e., supposons* (HI) $c_{n-1} = (n-1)^2$ $\rangle$ [5]

Démontrons $P(n)$, c'est à dire $c_n = n^2$:

$$\begin{array}{rcll} c_n & = & c_{n-1} + 2n - 1 & \langle \textit{ Définition de } \langle c_n \rangle_{n\in\mathbb{N}} \rangle \\ & = & (n-1)^2 + 2n - 1 & \langle \textit{ Par } (HI) \textit{ hypothèse d'induction. } \rangle \\ & = & (n^2 - 2n + 1) + 2n - 1 & \langle \textit{ Développement d'un trinôme carré parfait } \rangle \\ & = & n^2 \,. & \langle \textit{ Simplification algébrique. } \rangle \end{array}$$

On a démontré $\big(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n)\big)$.

Conclusion : On a bien $\big(\forall n \in \mathbb{N} \mid P(n)\big)$, c'est-à-dire : $c_n = n^2 \quad \forall n \in \mathbb{N}$.

C.Q.F.D.

Démonstration du principe d'induction faible

Nous allons maintenant démontrer le principe d'induction faible. Pour ce faire, nous utilisons la technique de démonstration par contradiction (voir section 1.3.8). Nous aurons aussi besoin de l'axiome suivant :

Axiome : $\mathbb{N}$, accompagné de la relation $\leq$, est un ensemble *bien ordonné*. (C'est-à-dire : tout sous-ensemble non vide de l'ensemble $\mathbb{N}$ a un plus petit élément, en fonction de $\leq$.)

Démonstration du théorème 2.3.1-a (Principe d'induction mathématique faible)

Soit un prédicat $P(n)$, défini pour $n \in \mathbb{N}$.
Le plan est de faire une démonstration par contradiction. Supposons que P ne satisfait pas le principe d'induction :

$$\big[\ P(0) \wedge \big(\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1)\big)\ \big] \ \Rightarrow\ \big(\forall n \in \mathbb{N} \mid P(n)\big)$$

c'est-à-dire, nous avons les 3 affirmations suivantes :

$$\begin{array}{ll} P(0) & (\diamondsuit) \\ \big(\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1)\big) & (\spadesuit) \\ \neg\big(\forall n \in \mathbb{N} \mid P(n)\big). & (\heartsuit) \end{array}$$

5. Notons qu'il faut lire cet énoncé ainsi : « supposons que c_{n-1} (*celui qui est défini par la récurrence ci-haut*) est bien égal à $(n-1)^2$. » C'est l'hypothèse d'induction, notée (HI).

Cherchons une contradiction.
Soit A, l'ensemble des éléments de $\mathbb{N}$ pour lesquels $P(n)$ est faux.
Selon notre hypothèse ($\heartsuit$), $A \neq \emptyset$.

Soit n_A, le plus petit élément de A.
$\langle$ *Un tel n_A existe, car $\mathbb{N}$ est bien ordonné et A est un sous-ensemble non vide de $\mathbb{N}$.* $\rangle$

Comme, par hypothèse ($\diamondsuit$) on a que $P(0)$ est vrai, on a donc que $n_A \neq 0$.
Donc $n_A - 1 \in \mathbb{N}$.
Et comme n_A est le plus petit élément de A, on a que $P(n_A - 1)$ est vrai.
Donc $P(n_A)$ est lui aussi vrai. $\langle$ *Par l'hypothèse* ($\spadesuit$) *avec* $[n := n_A - 1]$. $\rangle$
Donc $n_A \notin A$.
Le nombre naturel n_A est donc à la fois le plus petit élément de A et pas un élément de A.
Contradiction.
Ainsi, on ne peut supposer le contraire. C'est donc que l'énoncé à démontrer est vrai.

C.Q.F.D.

Remarquons que la deuxième forme du théorème (2.3.1-b) est en fait une simple réécriture de la première forme (2.3.1-a). En effet, nous avons :

$$\big(\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1)\big) \;\Leftrightarrow\; \big(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n)\big)\,.$$

Induction faible avec un indice de base quelconque

La démonstration par induction mathématique faible telle que nous l'avons présentée jusqu'à maintenant peut ne pas être utilisable dans certains cas, notamment lorsque l'énoncé à démontrer n'est vrai qu'à partir d'une valeur de n plus élevée que 0. En particulier, lorsqu'une suite définie par récurrence ne commence pas à l'indice 0. Voici donc une des nombreuses autres variantes du principe d'induction mathématique faible.

Théorème 2.3.2. *Principe d'induction mathématique faible sur* $\{n_0,\, n_0+1,\, n_0+2,\, \ldots\}$.
Soit un prédicat P et un entier $n_0 \in \mathbb{N}$. Alors,

$$\Big[\; P(n_0) \;\wedge\; \big(\forall n \in \mathbb{I}\backslash\{n_0\} \mid P(n-1) \Rightarrow P(n)\big) \;\Big] \;\Rightarrow\; \big(\forall n \in \mathbb{I} \mid P(n)\big)\,,$$

où $\mathbb{I} \stackrel{\text{def}}{=} \{n_0,\, n_0+1,\, n_0+2,\, \ldots\}$.

Remarquons que, si on réécrit le théorème 2.3.2 précédent en substituant $[n_0 := 0]$, on

a $[\mathbb{I} := \mathbb{N}]$ et on retrouve exactement l'énoncé du théorème 2.3.1-b, c'est-à-dire le principe d'induction mathématique faible que nous utilisons lorsqu'une suite définie par récurrence commence à l'indice 0. Il est donc possible de démontrer le théorème 2.3.2 en adaptant légèrement la démonstration du théorème 2.3.1 que nous avons présenté plus haut. Le lecteur est d'ailleurs encouragé à faire cette démonstration en exercice.

De même, comme le met en évidence l'exemple suivant, les démonstrations se basant sur les théorèmes 2.3.1 et 2.3.2 sont très semblables, la différence principale étant qu'elles débutent en montrant la véracité prédicat $P(0)$ et $P(n_0)$ respectivement.

Exemple de la somme des nombres entiers positifs consécutifs

Nous allons maintenant démontrer la propriété 2.1.2-d (page 153), qui donne le terme général permettant de calculer la somme des n premiers nombres entiers positifs :

$$1 + 2 + 3 + \ldots + n \quad = \quad \sum_{i=1}^{n} i \quad = \quad \frac{n(n+1)}{2} \,.$$

Pour cette démonstration, il sera plus naturel d'utiliser l'indice 1 pour désigner le cas de base (plutôt que 0). C'est pourquoi nous allons utiliser le principe d'induction faible avec un indice de base quelconque.

Démonstration de la propriété 2.1.2-d (Somme des nombres entiers positifs consécutifs)
Prenons le prédicat $P(n) : \quad \sum_{i=1}^{n} i \;=\; \frac{n(n+1)}{2}$.
Alors nous devons démontrer que $(\forall n \in \mathbb{N}^* \mid P(n))$.
Et par le principe d'induction mathématique (théorème 2.3.2, avec $[n_0 := 1]$ et donc $[\mathbb{I} := \mathbb{N}^*]$), il suffit de démontrer que

$$P(1) \;\wedge\; (\forall n \in \mathbb{N}^* \backslash \{1\} \mid P(n-1) \Rightarrow P(n)) \,.$$

Cas de base : démontrons $P(1)$. $\left\langle$ *C'est-à-dire, démontrons* $\sum_{i=1}^{1} i \;=\; \frac{1 \cdot (1+1)}{2}$. $\right\rangle$

$\frac{1 \cdot (1+1)}{2} \;=\; \frac{2}{2} \;=\; 1$, ce qui est bien égal à $\sum_{i=1}^{1} i$.

Pas d'induction : démontrons $(\forall n \in \mathbb{N}^* \backslash \{1\} \mid P(n-1) \Rightarrow P(n))$.

Soit $n \in \mathbb{N}^* \backslash \{1\}$, et supposons $P(n-1)$, c'est-à-dire :

$$\sum_{i=1}^{n-1} i \;=\; \frac{(n-1)(\,(n-1)+1\,)}{2} \;=\; \frac{n(n-1)}{2} \qquad (HI)\,.$$

Démontrons $P(n)$, c'est à dire $\displaystyle\sum_{i=1}^{n} i \;=\; \frac{n(n+1)}{2}$:

$$\begin{aligned}
&\sum_{i=1}^{n} i \\
&= \quad 1+2+3+\ldots+(n-1)+n && \langle\ \textit{Réécriture de la somme de } 1 \textit{ à } n\ \rangle \\
&= \quad \left[\ \sum_{i=1}^{n-1} i\ \right] + n && \langle\ \textit{Réécriture de la somme de } 1 \textit{ à } (n-1)\ \rangle \\
&= \quad \frac{n(n-1)}{2} + n && \langle\ \textit{Par } (HI) \textit{ hypothèse d'induction.}\ \rangle \\
&= \quad \frac{n(n-1)+2n}{2} && \langle\ \textit{Arithmétique (dénominateur commun).}\ \rangle \\
&= \quad \frac{n(\,(n-1)+2\,)}{2} && \langle\ \textit{Arithmétique (mise en évidence de } n).\ \rangle \\
&= \quad \frac{n(n+1)}{2}\,. && \langle\ \textit{Arithmétique.}\ \rangle
\end{aligned}$$

On a démontré $\big(\forall n \in \mathbb{N}^* \setminus \{1\} \mid P(n-1) \Rightarrow P(n)\,\big)$.

Conclusion : On a bien $\big(\,\forall n \in \mathbb{N}^* \mid P(n)\,\big)$, c'est-à-dire : $\displaystyle\sum_{i=1}^{n} i \;=\; \frac{n(n+1)}{2}\,.$ **C.Q.F.D.**

2.3.2 Principe d'induction mathématique à deux cas de base

Lorsqu'une suite $\langle a_n \rangle_{n\in\mathbb{N}}$ est définie par récurrence, il arrive parfois que le calcul du terme a_n repose plusieurs de ses prédécesseurs (et non seulement de son prédécesseur immédiat a_{n-1}). Nous présentons maintenant une autre variante du principe d'induction qui est utile lorsque le terme a_n d'une suite est défini en fonction de ses deux prédécesseurs a_{n-1} et a_{n-2}.

Théorème 2.3.3. *Principe d'induction mathématique à deux cas de base.*
Soit un prédicat P. Alors,

$$\Big[\ P(0) \,\wedge\, P(1) \,\wedge\, \big(\forall n \in \mathbb{N} \setminus \{0,1\} \mid P(n-2) \wedge P(n-1) \Rightarrow P(n)\,\big)\ \Big] \;\Rightarrow\; \big(\forall n \in \mathbb{N} \mid P(n)\,\big)\,.$$

Comme nous le verrons dans l'exemple qui suit, une démonstration se basant sur ce dernier théorème doit donc débuter en démontrant la véracité des deux prédicats $P(0)$ et $P(1)$.

Exemple de la suite de Fibonacci

À la section 2.1.1, nous avons défini ainsi la **suite de Fibonacci** $\langle f_n \rangle_{n\in\mathbb{N}}$ par récurrence :

$$\begin{cases} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \qquad \forall n \in \mathbb{N} \setminus \{0,1\}\,. \end{cases}$$

Nous avons ensuite affirmé que le terme général de cette suite est :

$$f_n \;=\; \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}\,.$$

Nous allons maintenant démontrer la validité de cette définition par terme général en utilisant le principe d'induction à deux cas de base (théorème 2.3.3).

Démonstration. Terme général de la suite de Fibonacci.

Prenons le prédicat $P(n)$: $f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}$.

Alors nous devons démontrer que $(\forall n \in \mathbb{N} \mid P(n))$.

Par le principe d'induction mathématique à deux cas de base, il suffit de démontrer que :

$$P(0) \;\wedge\; P(1) \;\wedge\; \big(\forall n \in \mathbb{N} \setminus \{0,1\} \mid P(n-1) \wedge P(n-2) \Rightarrow P(n)\big)\,.$$

Pour démontrer cet énoncé, nous avons besoin de la remarque suivante :

Remarque (∗) : Les deux nombres $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$ sont les deux zéros[6] du polynôme $y = x^2 - x - 1$. Donc, $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$ sont les deux seuls nombres réels satisfaisant l'équation $0 = x^2 - x - 1$, et donc l'équation $x + 1 = x^2$. Autrement dit, additionner 1 à l'un de ces deux nombres est équivalent à l'élever au carré.

Cas de base 1 : démontrons $P(0)$**.** $\Big\langle$ *i.e., démontrons* $f_0 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^0 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^0$. $\Big\rangle$

$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^0 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^0 = \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}} = 0$, ce qui est bien égal à f_0 par définition.

Cas de base 2 : démontrons $P(1)$**.** $\Big\langle$ *i.e., démontrons* $f_1 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^1 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^1$. $\Big\rangle$

6. Rappelons que les zéros du polynôme $y = ax^2 + bx + c$, sont donnés par la formule $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

$$\begin{aligned}
\tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^1 - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^1 &= \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right) - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right) \\
&= \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2} - \tfrac{1-\sqrt{5}}{2}\right) \\
&= \tfrac{1}{\sqrt{5}}\left(\tfrac{2\sqrt{5}}{2}\right) \\
&= 1, \quad \text{et on a bien } f_1 = 1 \text{ par définition.}
\end{aligned}$$

Pas d'induction : démontrons $\big(\forall n \in \mathbb{N}\setminus\{0,1\} \mid P(n-1) \wedge P(n-2) \Rightarrow P(n)\big)$**.**

Soit $n \in \mathbb{N}\setminus\{0,1\}$, et supposons $P(n-1)$ et $P(n-2)$.

C'est-à-dire, supposons (ce sont nos hypothèses d'induction) :

- $f_{n-1} = \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-1} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-1}$,
- $f_{n-2} = \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-2} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-2}$.

Démontrons $P(n)$, c'est-à-dire $f_n = \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n}$:

$$\begin{aligned}
& f_n \\
= & \qquad \langle \textit{ Définition de } \langle f_n\rangle_{n\in\mathbb{N}\setminus\{0,1\}}. \rangle \\
& f_{n-1} + f_{n-2} \\
= & \qquad \langle \textit{ Hypothèses d'induction. } \rangle \\
& \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-1} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-1} + \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-2} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-2} \\
= & \\
& \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-1} + \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-2} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-1} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-2} \\
= & \qquad \langle \textit{ Mise en évidence double. } \rangle \\
& \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-2}\left(\tfrac{1+\sqrt{5}}{2}+1\right) - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-2}\left(\tfrac{1-\sqrt{5}}{2}+1\right) \\
= & \qquad \langle \textit{ Remarque } (*)\textit{, deux fois. } \rangle \\
& \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n-2}\left(\tfrac{1+\sqrt{5}}{2}\right)^{2} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n-2}\left(\tfrac{1-\sqrt{5}}{2}\right)^{2} \\
= & \qquad \langle \textit{ Propriété des exposants. } \rangle \\
& \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n}.
\end{aligned}$$

On a démontré $\big(\forall n \in \mathbb{N}\setminus\{0,1\} \mid P(n-1) \wedge P(n-2) \Rightarrow P(n)\big)$.

Conclusion : On a bien $\big(\forall n \in \mathbb{N} \mid P(n)\big)$,

c'est-à-dire : $f_n = \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^{n} - \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^{n} \quad \forall n \in \mathbb{N}$.

C.Q.F.D.

Nous sommes maintenant certains que le terme général de la suite de Fibonacci est

$$f_n \;=\; \tfrac{1}{\sqrt{5}}\left(\tfrac{1+\sqrt{5}}{2}\right)^n \;-\; \tfrac{1}{\sqrt{5}}\left(\tfrac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}\,.$$

Mais si ce terme général ne nous avait pas été donné gratuitement, nous aurions été tous incapables de le deviner. La méthode des séries génératrices présentée plus loin nous permettra de calculer le terme général de la suite de Fibonacci.

Pour votre culture générale, il est intéressant de constater que le nombre $\frac{1+\sqrt{5}}{2} \approx 1,618$ est une constante bien connue que l'on appelle le **nombre d'or**. Le nombre d'or possède plusieurs propriétés intéressantes. Il est présent dans plusieurs théories mathématiques et il est même utilisé en architecture[7].

2.3.3 Induction mathématique forte

Nous présentons maintenant la variante du principe d'induction connue sous le nom d'**induction mathématique forte**, que nous formulons ainsi :

Théorème 2.3.4. *Principe d'induction mathématique forte.*
Soit un prédicat P. Alors,

$$\left[\, P(0) \;\wedge\; \left(\forall n \in \mathbb{N}^* \;\middle|\; \Big(\forall k \in \{0,1,2,\ldots,n-1\} \;\Big|\; P(k)\Big) \Rightarrow P(n)\right)\right] \;\Rightarrow\; \big(\forall n \in \mathbb{N} \mid P(n)\big)\,.$$

Rappelons que l'idée principale du principe d'induction faible (voir le théorème 2.3.1 à la page 168) est de supposer que le prédicat $P(n-1)$ est vrai et de montrer que cela implique que le prédicat $P(n)$ est vrai. C'est ce que signifie l'expression suivante du théorème 2.3.1-b :

$$\big(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n)\big)\,.$$

Dans l'énoncé du principe d'induction forte (théorème 2.3.4), cette expression est remplacée par une expression plus générale, c'est-à-dire :

$$\left(\forall n \in \mathbb{N}^* \;\middle|\; \Big(\forall k \in \{0,1,2,\ldots,n-1\} \;\Big|\; P(k)\Big) \Rightarrow P(n)\right).$$

7. Pour en connaître davantage sur le nombre d'or, voir : http://fr.wikipedia.org/wiki/Nombre_d%27or

Cette dernière expression pourrait aussi se réécrire ainsi :

$$\Big(\forall n \in \mathbb{N}^* \;\Big|\; \big[P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(n-1)\big] \Rightarrow P(n)\Big)\,.$$

Autrement dit, lors de l'utilisation du principe d'induction forte, on suppose que, pour tout entier positif k plus petit que n, les prédicats $P(k)$ sont vrais. Ensuite, on montre que cela implique que le prédicat $P(n)$ est vrai.

Bien que le terme "principe d'induction forte" peut donner la fausse indication que cette nouvelle formulation permet de démontrer plus de résultats que le "principe d'induction faible", les deux principes sont dans les faits équivalents. Toutefois, le principe d'induction forte facilite grandement certaines démonstrations. Dans le cas qui nous intéresse (celui des suites définies par récurrence), nous utiliserons le principe d'induction forte lorsque la définition par récurrence du $n$ième terme d'une suite n'est pas donnée en fonction du terme précédent (le terme d'indice $n-1$) mais d'un autre terme d'indice inférieur à n.

Induction forte avec un indice de base quelconque

À la section 2.3.1, nous avons généralisé le principe d'induction faible (théorème 2.3.1-b) aux cas débutant par un indice quelconque (théorème 2.3.2). Le prochain théorème applique la même généralisation au principe d'induction forte.

Théorème 2.3.5. *Principe d'induction mathématique forte sur* $\{n_0,\, n_0+1,\, n_0+2,\, \ldots\}$. *Soit un prédicat* P *et un entier* $n_0 \in \mathbb{N}$. *Alors,*

$$\left[P(n_0) \wedge \left(\forall n \in \mathbb{I}\backslash\{n_0\} \;\middle|\; \Big(\forall k \in \{n_0, n_0+1, \ldots, n-1\} \;\Big|\; P(k)\Big) \Rightarrow P(n)\right)\right] \;\Rightarrow\; \big(\forall n \in \mathbb{I} \mid P(n)\big)\,,$$

où $\quad \mathbb{I} \stackrel{\text{def}}{=} \{n_0,\, n_0+1,\, n_0+2,\, \ldots\}\,.$

Exemple de démonstration utilisant le principe d'induction forte

Considérons la suite $\langle\, D(n)\,\rangle_{n\in\mathbb{N}^*}$ définie par la récurrence suivante :

$$\begin{cases} D(1) \;=\; 1 \\ D(n) \;=\; D(\,\lfloor \frac{n}{2} \rfloor\,) + D(\,\lceil \frac{n}{2} \rceil\,) + 1 \quad \forall n \in \mathbb{N} \setminus \{0,1\}\,. \end{cases}$$

Nous allons démontrer que le terme général de la suite $\langle\, D(n)\,\rangle_{n\in\mathbb{N}^*}$ est :

$$D(n) \;=\; 2n-1 \quad \forall n \in \mathbb{N}^*\,.$$

Démonstration Terme général de la suite $\langle\, D(n)\,\rangle_{n\in\mathbb{N}^*}$
Prenons le prédicat $P(n)$: $D(n) = 2n-1$.
Alors nous devons démontrer que $(\forall n \in \mathbb{N}^* \mid P(n))$.
Par le principe d'induction mathématique (théorème 2.3.5, avec $[n_0 := 1]$ et donc $[\mathbb{I} := \mathbb{N}^*]$), il suffit de démontrer que

$$P(1) \wedge \Big(\forall n \in \mathbb{N}\setminus\{0,1\} \;\Big|\; \Big(\forall k \in \{1,2,\ldots,n-1\} \;\Big|\; P(k)\Big) \Rightarrow P(n)\Big)\,.$$

Cas de base : démontrons $P(1)$. $\langle$ *C'est-à-dire, montrons* $D(1) = 2\cdot 1 - 1$. $\rangle$
$2\cdot 1 - 1 \;=\; 1$, ce qui est bien égal à $D(1)$.

Pas d'induction : démontrons $\big(\forall n \in \mathbb{N}\setminus\{0,1\} \;\big|\; (\forall k \in \{1,2,\ldots,n-1\} \mid P(k)) \Rightarrow P(n)\big)$.

Soit $n \in \mathbb{N}^*\setminus\{1\}$ et supposons $(\forall k \in \{1,2,\ldots,n-1\} \mid P(k))$.
Ainsi, pour tout entier k situé entre 1 et n exclusivement, nous avons $D(k) = 2k-1$.
$\langle$ *Il s'agit de notre hypothèse d'induction.* $\rangle$

On remarque que : $(*)\; 1 \le \lfloor \frac{n}{2} \rfloor < n$ et $(**)\; 1 \le \lceil \frac{n}{2} \rceil < n$. $\langle$ *Car* $n \ge 2$ $\rangle$

Démontrons maintenant $P(n)$, c'est à dire $D(n) = 2n-1$:

$$\begin{array}{ll} & D(n) \\ = & \quad \langle\ \textit{Définition de la suite } \langle\, D(n)\,\rangle_{n\in\mathbb{N}^*}\ \rangle \\ & D(\lfloor \frac{n}{2} \rfloor) + D(\lceil \frac{n}{2} \rceil) + 1 \\ = & \quad \langle\ \textit{Hypothèse d'induction, avec } [k := \lfloor \tfrac{n}{2} \rfloor],\ \textit{et remarque } (*).\ \rangle \\ & 2\cdot \lfloor \frac{n}{2} \rfloor - 1 + D(\lceil \frac{n}{2} \rceil) + 1 \\ = & \quad \langle\ \textit{Hypothèse d'induction, avec } [k := \lceil \tfrac{n}{2} \rceil],\ \textit{et remarque } (**).\ \rangle \\ & 2\cdot \lfloor \frac{n}{2} \rfloor - 1 + 2\cdot \lceil \frac{n}{2} \rceil - 1 + 1 \\ = & \quad \langle\ \textit{Arithmétique}\ \rangle \\ & 2\big(\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil\big) - 1 \end{array}$$

Distinguons deux cas :

Cas 1 : n est un nombre pair. Alors,

$$D(n) \;=\; 2\big(\lfloor \tfrac{n}{2} \rfloor + \lceil \tfrac{n}{2} \rceil\big) - 1 \;=\; 2\big(\tfrac{n}{2} + \tfrac{n}{2}\big) - 1 \;=\; 2n-1\,.$$

Cas 2 : n est un nombre impair. Alors,

$$D(n) \;=\; 2\big(\lfloor \tfrac{n}{2} \rfloor + \lceil \tfrac{n}{2} \rceil\big) - 1 \;=\; 2\big(\tfrac{n-1}{2} + \tfrac{n+1}{2}\big) - 1 \;=\; 2n-1\,.$$

Dans les deux cas, on a démontré que $D(n) = 2n - 1$.

Conclusion : On a bien $\big(\forall n \in \mathbb{N}^* \mid P(n)\big)$, c'est-à-dire : $D_n = 2n - 1 \quad \forall n \in \mathbb{N}^*$.

C.Q.F.D.

Insistons sur le fait que la dernière démonstration ne se serait pas faite aussi facilement en ayant recours au principe d'induction faible, puisque la définition par récurrence d'un terme $D(n)$ de la suite ne dépend pas du terme précédent $D(n-1)$, mais des deux termes situés "au milieu" de la suite $\langle\, D(1), D(2), \ldots, D(n)\,\rangle$.

2.3.4 Induction structurelle

Il existe d'autres types d'induction, mais celle qui est la plus utilisée en informatique est l'induction structurelle. Nous ne la verrons pas en profondeur ici, nous montrerons simplement un exemple pour illustrer son utilité. Nous ne verrons pas non plus sa définition formelle car cela demande un peu trop de notion à introduire.

Dès qu'on dispose d'un ordre partiel qui est *bien fondé*[8] sur un ensemble, on peut faire un raisonnement par induction. En fait, une définition récursive donne un tel ordre directement (on ne le démontrera pas). En informatique, on définit souvent des structures de façon récursive, en particulier les langages (de programmation, de spécification). Voici une définition récursive de ce qu'est une liste d'éléments de l'ensemble E :

— $[\,]$ est une liste

— si l est une liste et $e \in E$ alors $e :: l$ est une liste.

Notons L l'ensemble de toutes les listes. On est devant une définition récursive, comme pour les séries. Une liste est donc, soit vide, soit elle commence par un élément e suivi d'une autre liste (déjà construite). On peut définir récursivement des opérateurs sur les listes ainsi définies, par exemple, la longueur de $l \in L$ est définie par

— $long([\,]) = 0$

— $long(e :: l) = 1 + long(l)$

alors que la concaténation de 2 listes $l, t \in L$ est définie par

— $[\,]^\frown t = t$

— $(e :: l)^\frown t \;=\; e :: (l^\frown t)$

8. Disons seulement qu'un ordre sur un ensemble est bien fondé s'il n'y a pas de chaîne infinie strictement décroissante. Exemple : "$\leq$" sur $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ n'est pas bien fondé, mais l'ordre "a divise b" l'est sur $\mathbb{N}$ ou $\mathbb{Z}$, tout comme l'inclusion d'ensembles sur $P(A)$. C'est logique, l'induction commence au plus petit élément... s'il n'y en a pas, on ne peut rien faire.

Ces définitions sont basées sur la structure de la "première liste" qui est soit vide, soit un élément $e \in E$ suivi d'une liste (il est d'usage dans ce genre de définition d'omettre le quantificateur sur e : en effet, il y a un *il existe* caché car si une liste n'est pas vide, c'est qu'*il existe* $e \in E$ et $l \in L$ qui forment la liste en $e :: l$). Si on veut faire une démonstration par induction pour une propriété des listes, par exemple que la longueur de la concaténation de 2 listes est la somme des longueurs des listes, alors on voudrait faire une induction sur la structure de notre construction (ici une liste) plutôt qu'une induction sur $\mathbb{N}$.

Démonstration de *pour toutes listes l et t, on a $long(l^\frown t) = long(l) + long(t)$*
Soit $P(l)$ la proposition : $(\forall t \in L \mid long(l^\frown t) = long(l) + long(t))$. On veut $(\forall l \in L \mid P(l))$. Notons que ça fait intervenir deux "pour tout" (un $\forall l$ extérieur, en plus de celui à l'intérieur du P, le $\forall t$), mais notre induction est sur l, la première liste : soyons méthodique, et nous y arriverons.
Cas de base : démontrons $P([\,])$, i.e. : $(\forall t \in L \mid long([\,]^\frown t) = long([\,]) + long(t))$
Soit $t \in L$. Alors, comme voulu :

$$\begin{aligned} long([\,]^\frown t) &= long(t) && \langle \textit{ par définition de la concaténation } \rangle \\ &= 0 + long(t) && \langle \textit{ arithmétique } \rangle \\ &= long([\,]) + long(t) && \langle \textit{ arithmétique } \rangle \end{aligned}$$

Pas d'induction : démontrons $(\forall l \in L, \forall e \in E \mid P(l) \Rightarrow P(e :: l))$.
Soit $l \in L$, $e \in E$ et supposons $P(l)$, i.e.,

$$(\forall t \in L \mid long(l^\frown t) = long(l) + long(t)) \qquad (HI).$$

On veut démontrer $P(e :: l)$, i.e.[9],

$$\text{On veut } (\forall u \in L \mid long((e :: l)^\frown u) = long(e :: l) + long(u)).$$

Ainsi, soit $u \in L$, trouvons $long(e :: l^\frown u)$.

$$\begin{aligned} long((e :: l)^\frown u) &= long(e :: (l^\frown u)) && \langle \textit{ par définition de la concaténation } \rangle \\ &= 1 + long((l^\frown u)) && \langle \textit{ par définition de la longueur } \rangle \\ &= 1 + long(l) + long(u) && \langle \textit{ HI, avec } t := u \rangle \\ &= long(e :: l) + long(u) && \langle \textit{ par définition de la longueur } \rangle \end{aligned}$$

on a donc bien $P(e :: l)$, comme voulu, conséquemment $P(l)$ pour tout l, par induction

9. On utilise u plutôt que t pour éviter la confusion avec le t de (HI).

structurelle sur les listes.

C.Q.F.D.

Cette preuve par induction se base sur la *structure* de la liste et non sur $\mathbb{N}$. Ici nous avons omis de dire notre ordre sur les listes et nous n'avons pas démontré qu'il est bien fondé, mais cela est faisable, comme déjà mentionné. L'essentiel qu'on voulait montrer est que la preuve se base vraiment sur la structure de la liste : le cas de base est sur la liste vide (la plus petite liste) et on démontre que si une liste satisfait la propriété, alors le constructeur qui permet de construire une liste plus "grande" conserve la propriété dans cette nouvelle liste construite. Cela démontre que toute liste qui peut être construite satisfera l'énoncé.

Un autre exemple : si on veut démontrer une propriété d'invariance[10] P sur un programme, l'induction structurelle nous dit que les étapes suivantes suffiront pour y arriver :

— démontrer que P est vrai à l'état initial du programme
— un état qui satisfait P est transformé par chaque fonction et méthode du programme en un état qui satisfait aussi P.

Dans cet exemple, il y a un seul état initial, donc un seul cas de base. On peut faire de l'induction structurelle avec plusieurs cas de base. De même on peut avoir plusieurs "pas d'induction", comme dans cet exemple où on mentionne plusieurs fonctions et méthodes, qui sont des "transformateurs d'états". Ce sont ces transformateurs qui mènent d'un état à un autre, tout comme, dans l'induction sur $\mathbb{N}$, on passe d'un n au suivant. C'est beaucoup plus simple sur $\mathbb{N}$: un seul cas de base, un constructeur, "+1" ce qui fait qu'on n'a qu'un "pas d'induction" à vérifier.

Encore une fois, l'induction structurelle repose sur des bases mathématiques solides que nous avons éludées ici. Pour en savoir plus, nous vous suggérons le livre de Winskel (1993).

10. Une propriété d'invariance est une propriété qui doit être vraie à tout moment. Pensons à un système de bibliothèque avec des contraintes de cohérence, comme le nombre de livres qu'un utilisateur peut avoir en sa possession, etc.

2.3.5 Exercices sur l'induction mathématique

Exercice 1 : Étant donnée la formule :

$$\sum_{i=0}^{n} 2i \;=\; n(n+1)\,.$$

a) Vérifiez cette formule pour $n = 1$, 2, 5 et 10.
b) Démontrez par induction que cette formule est vraie pour tout $n \in \mathbb{N}$.

Exercice 2 : Soit $f : \mathbb{N} \longrightarrow \mathbb{R},$ une fonction qui satisfait la règle de récurrence suivante :

$$\begin{cases} f(0) & = & 3 \\ f(k+1) & = & 2 \cdot f(k) + 2k - 4 \quad \forall k \in \mathbb{N}\,. \end{cases}$$

a) Évaluez $f(0)$, $f(1)$, $f(2)$, $f(5)$ et $f(10)$.
b) Démontrez par induction que $f(n) = 2^n - 2n + 2 \quad \forall n \in \mathbb{N}$.

Exercice 3 : Soit la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par :

$$\begin{cases} a_0 & = & 2 \\ a_n & = & 3a_{n-1} + 2 \quad \forall n \in \mathbb{N}^*\,. \end{cases}$$

Montrez par induction que le terme général de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ est :

$$a_n \;=\; 3^{n+1} - 1 \quad \forall n \in \mathbb{N}\,.$$

Exercice 4 : Soit la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par :

$$\begin{cases} b_0 & = & -4 \\ b_n & = & 3\,b_{n-1} \,+\, 4n \,+\, 4 \quad \forall n \in \mathbb{N}^*\,. \end{cases}$$

Montrez par induction que le terme général de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ est :

$$b_n = 3^n - 2n - 5 \quad \forall n \in \mathbb{N}\,.$$

Exercice 5 : Soit la suite $\langle c_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par :

$$\begin{cases} c_0 &= 1 \\ c_1 &= 1 \\ c_n &= 4 \cdot c_{n-1} - 4 \cdot c_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\}\,. \end{cases}$$

Montrez par induction que le terme général de la suite $\langle c_n \rangle_{n\in\mathbb{N}}$ est :

$$c_n \;=\; 2^{n-1} \cdot (2-n) \quad \forall n \in \mathbb{N}\,.$$

Exercice 6 : Démontrez par induction que les deux fonctions suivantes sont équivalentes à la fonction exponentielle, c.-à-d. qu'elles sont égales à e^n pour tout $n \in \mathbb{N}$:

a) — $\texttt{exp}(0) = 1$
   — $\texttt{exp}(n) = e \cdot \exp(n-1)$ pour $n > 0$

b) — $\texttt{expBin}(0) = 1$
   — $\texttt{expBin}(n) = \texttt{expBin}(\frac{n}{2})^2$ si $n > 0$ est pair,
   — $\texttt{expBin}(n) = e \cdot (\texttt{expBin}(\frac{n-1}{2}))^2$ si n est impair.

c) Sans lien avec l'induction : laquelle des deux façons de calculer e^n est la plus "efficace" ?

Exercice 7 : Démontrez par induction sur n que la méthode suivante est équivalente à l'exponentiation de b par n modulo m, c.-à-d. qu'elle est égale à $b^n \bmod m$ pour tout $b, n, m \in \mathbb{N}$ (Quand on dit "par induction sur n", on dit qu'on va démontrer une proposition de la forme $(\forall n \mid P(n))$, donc que b et m seront fixés ; pour un indice sur quel P choisir, voir note [11]. Ensuite suivre les étapes) :

$\texttt{expmod}(b, n, m)$ On suppose $b, n, m \in \mathbb{N},\ m \geq 2; n \geq 0$

Si $n = 0$ **alors**
    retourner 1
Sinon
    Si n est pair **alors**
        Retourner $\texttt{expmod}(b, n/2, m)^2 \bmod m$
    Sinon
        Retourner $((\texttt{expmod}(b, \frac{n-1}{2}, m)^2 \bmod m) \cdot (b \bmod m)) \bmod m$
    Fin Si
Fin Si

11. Prenons $P(n) := (\forall b, m \in \mathbb{N} \mid b^n \bmod m = \mathit{expmod}(b, n, m))$

2.4 Cas particuliers de récurrences

L'essentiel de cette section consiste à se donner des outils nous permettant, étant donné une suite définie par récurrence, de trouver sa définition par terme général. Résoudre ce type de problème est faire de la **résolution de récurrences**.

Nous nous intéressons dans cette section à trois familles particulières de suites. Pour chacune des suites appartenant à une de ces familles, le terme général est facile à trouver.

2.4.1 Les suites arithmétiques

Définition 2.4.1. *Suite arithmétique.*
On dit qu'une suite $\langle a_n \rangle_{n\in\mathbb{N}}$ *est* arithmétique *de* premier terme t *et de* différence d *si :*

- $a_0 = t$;
- *la différence entre la valeur du terme* a_n *et celle du terme* a_{n-1} *est égale à* d $\forall n \in \mathbb{N}^*$.

Théorème 2.4.2. *Terme général d'une suite arithmétique*
Soit $\langle a_n \rangle_{n\in\mathbb{N}}$ *une suite. Alors les énoncés suivants sont équivalents :*

1. $\langle a_n \rangle_{n\in\mathbb{N}}$ *est une suite arithmétique de premier terme* t *et de différence* d.
2. $\langle a_n \rangle_{n\in\mathbb{N}}$ *est définie par récurrence par :*

$$\begin{cases} a_0 &= t \\ a_n &= a_{n-1} + d \quad \forall n \in \mathbb{N}^* . \end{cases}$$

3. $\langle a_n \rangle_{n\in\mathbb{N}}$ *est définie par terme général par :*

$$a_n = t + nd \quad \forall n \in \mathbb{N} .$$

Exemple : La suite des nombres pairs

La suite des nombres pairs que nous avons vue en introduction (équation (2.2), page 151) est une suite arithmétique de premier terme $a = 0$ et de différence $d = 2$, et on a bien que :

$$\begin{cases} b_0 &= 0 \\ b_n &= b_{n-1} + 2 \quad \forall n \in \mathbb{N}^* , \end{cases}$$

et que

$$b_n = n \cdot 2 \quad \forall n \in \mathbb{N} .$$

2.4.2 Les suites géométriques

Définition 2.4.3. *Suite géométrique.*
On dit qu'une suite $\langle a_n \rangle_{n\in\mathbb{N}}$ *est* géométrique *de* premier terme t *et de* raison r *si :*

- $a_0 = t$;
- *le rapport entre la valeur du terme* a_n *et celle du terme* a_{n-1} *est égal à* $r \quad \forall n \in \mathbb{N}^*$.

Notez que le **rapport** de a_n sur a_{n-1} est le résultat de la division de a_n par a_{n-1}, c'est-à-dire :

$$r \;=\; \frac{a_n}{a_{n-1}}\,.$$

Théorème 2.4.4. *Terme général d'une suite géométrique*
Soit $\langle a_n \rangle_{n\in\mathbb{N}}$ *une suite. Alors les énoncés suivants sont équivalents :*

1. $\langle a_n \rangle_{n\in\mathbb{N}}$ *est une suite géométrique de premier terme* t *et de raison* r.
2. $\langle a_n \rangle_{n\in\mathbb{N}}$ *est définie par récurrence par*

$$\left\{ \begin{array}{lcl} a_0 &=& t \\ a_n &=& a_{n-1} \cdot r \quad \forall n \in \mathbb{N}^*\,. \end{array} \right.$$

3. $\langle a_n \rangle_{n\in\mathbb{N}}$ *est définie par terme général par :*

$$a_n \;=\; t \cdot r^n \quad \forall n \in \mathbb{N}\,.$$

Exemple : La suite des puissances de 2

La suite des puissances de 2, c'est-à-dire la suite $\langle 1, 2, 4, 8, 16, 32, 64, \ldots \rangle$, est une suite géométrique de premier terme $a = 1$ et de raison $r = 2$, et on a bien que

$$\left\{ \begin{array}{lcl} b_0 &=& 1 \\ b_n &=& b_{n-1} \cdot 2 \quad \forall n \in \mathbb{N}^*\,, \end{array} \right.$$

et que

$$b_n \;=\; 1 \cdot 2^n \quad \forall n \in \mathbb{N}\,.$$

Notez que nous avons déjà étudié cette suite en introduction lors de l'analyse de l'algorithme "`Algo_Jouet_Deux`" (voir l'équation (2.7), page 155).

2.4.3 La suite des sommes de premiers termes d'une suite

Définition 2.4.5. *Suite des sommes de premiers termes d'une suite.*
Soit $\langle a_n \rangle_{n\in\mathbb{N}}$ *une suite. La* **suite des sommes de premiers termes** *de la suite* $\langle a_n \rangle_{n\in\mathbb{N}}$ *correspond à la suite* $\langle S_n \rangle_{n\in\mathbb{N}}$ *dont le nième terme est :*

$$S_n \;=\; \sum_{i=0}^{n} a_i \qquad \forall n \in \mathbb{N}\,.$$

Autrement dit, la suite $\langle S_n \rangle_{n\in\mathbb{N}}$ s'écrit en extension par :

$$\langle S_n \rangle_{n\in\mathbb{N}} \;=\; \langle\, a_0,\, (a_0 + a_1),\, (a_0 + a_1 + a_2),\; \ldots,\; (a_0 + a_1 + \cdots + a_n),\; \ldots \rangle\ .$$

De même, $\langle S_n \rangle_{n\in\mathbb{N}}$ est définie par récurrence par

$$\begin{cases} S_0 &= a_0 \\ S_n &= S_{n-1} + a_n \qquad \forall n \in \mathbb{N}^*\,. \end{cases}$$

Les deux prochains théorèmes permettent de trouver directement le terme général de la somme des premiers termes d'une suite arithmétique (définition 2.4.1) et de la somme des premiers termes d'une suite géométrique (définition 2.4.3).

Théorème 2.4.6. *Terme général des sommes de premiers termes d'une suite arithmétique*
Soit $\langle a_n \rangle_{n\in\mathbb{N}}$*, une suite arithmétique de premier terme* a *et de différence* d *et soit* $\langle S_n \rangle_{n\in\mathbb{N}}$ *la suite des sommes de premiers termes de la suite* $\langle a_n \rangle_{n\in\mathbb{N}}$*.*
Alors, $\langle S_n \rangle_{n\in\mathbb{N}}$ *est définie par terme général par :*

$$S_n \;=\; \frac{(a_0 + a_n)(n+1)}{2} \qquad \forall n \in \mathbb{N}\,.$$

Fréquemment, on s'intéresse à la suite des sommes des premiers termes de la suite arithmétique $\langle a_n \rangle_{n\in\mathbb{N}}$ *excluant* le premier terme a_0. En désignant cette suite $\langle S^*_n \rangle_{n\in\mathbb{N}^*}$, on obtient :

$$S^*_n \;=\; \sum_{i=1}^{n} a_i \;=\; \frac{(a_1 + a_n)\cdot n}{2} \qquad \forall n \in \mathbb{N}^*\,. \tag{2.9}$$

Théorème 2.4.7. *Terme général des sommes de premiers termes d'une suite géométrique*
Soit $\langle a_n \rangle_{n\in\mathbb{N}}$ une suite géométrique de premier terme a_0 et de raison $r \neq 1$ et soit $\langle S_n \rangle_{n\in\mathbb{N}}$ la suite des sommes de premiers termes de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$.

Alors, $\langle S_n \rangle_{n\in\mathbb{N}}$ est définie par terme général par :

$$S_n \;=\; \frac{a_0 \cdot (1 - r^{n+1})}{1 - r} \qquad \forall n \in \mathbb{N}\,.$$

Lorsqu'on s'intéresse à la suite des sommes des premiers termes de la suite géométrique $\langle a_n \rangle_{n\in\mathbb{N}}$ *excluant* le premier terme a_0, notée, $\langle S^*_n \rangle_{n\in\mathbb{N}^*}$, on obtient :

$$S^*_n \;=\; \sum_{i=1}^{n} a_i \;=\; \frac{a_1 \cdot (1 - r^n)}{1 - r} \qquad \forall n \in \mathbb{N}^*\,. \tag{2.10}$$

Remarquons que les deux théorèmes 2.4.6 et 2.4.7 contiennent l'expression "$(n+1)$", soit le nombre de termes de la somme qui donne S_n. Le terme "$(n+1)$" est remplacé par "n" dans les équations (2.9) et (2.10) respectivement, car la somme qui donne S^*_n contient n termes.

PENSEZ-Y!

Les trois remarques suivantes s'avèrent de bons exercices pour vérifier votre compréhension de l'arithmétique des sommes en notation sigma.

Remarque 1 : Il n'est pas nécessaire de retenir l'équation (2.9), puisqu'il est possible de l'obtenir aisément du théorème 2.4.6. En effet, si $\langle a_n \rangle_{n\in\mathbb{N}}$ est une suite arithmétique de premier terme a et de différence d, on a :

$$\begin{aligned}
S^*_n = \sum_{i=1}^{n} a_i &= \sum_{i=1}^{n} (a + id) && \langle\ \textit{Théorème 2.4.2 (3)}\ \rangle \\
&= (a + 1d) + (a + 2d) + (a + 3d) + \ldots + (a + nd) && \langle\ \textit{Écriture en extension}\ \rangle \\
&= (a + d + 0d) + (a + d + 1d) + (a + d + 2d) + \ldots + (a + d + (n-1)d) \\
& && \langle\ \textit{Arithmétique}\ \rangle \\
&= \sum_{i=0}^{n-1} (a + d + id) && \langle\ \textit{Écriture en notation sigma}\ \rangle \\
&= \frac{(a_1 + a_n)(\,(n-1) + 1\,)}{2} && \left\langle \begin{array}{l} \textit{Théorème 2.4.6, somme des } n-1 \textit{ premiers} \\ \textit{termes d'une suite arithmétique de premier} \\ \textit{terme } a_1 = a + d \textit{ et de différence } d. \end{array} \right\rangle \\
&= \frac{(a_1 + a_n) \cdot n}{2}\,.
\end{aligned}$$

Remarque 2 : De manière similaire à la remarque 1, l'équation (2.10) découle du théorème 2.4.7. Considérons une suite géométrique $\langle a_n \rangle_{n\in\mathbb{N}}$ de premier terme a_0 et de raison r. Alors :

$$\begin{aligned}
S_n^* = \sum_{i=1}^{n} a_i &= \sum_{i=1}^{n} a \cdot r^i && \langle \textit{ Théorème 2.4.4 (3) } \rangle \\
&= a \cdot r^1 + a \cdot r^2 + a \cdot r^3 + \ldots + a \cdot r^n && \langle \textit{ Écriture en extension } \rangle \\
&= a\,r \cdot r^0 + a\,r \cdot r^1 + a\,r \cdot r^2 + \ldots + a\,r \cdot r^{n-1} && \langle \textit{ Arithmétique } \rangle \\
&= \sum_{i=1}^{n} a\,r \cdot r^{i-1} && \langle \textit{ Écriture en notation sigma } \rangle \\
&= \frac{a_1 \cdot (\,1 - r^{(n-1)+1}\,)}{1-r} && \left\langle \begin{array}{l} \textit{Théorème 2.4.7, somme des } n-1 \textit{ premiers} \\ \textit{termes d'une suite géométrique de premier} \\ \textit{terme } a_1 = a\,r \textit{ et de raison } r. \end{array} \right\rangle \\
&= \frac{a_1 \cdot (\,1 - r^{n}\,)}{1-r}\,.
\end{aligned}$$

Remarque 3 : La somme (infinie) de tous les termes d'une suite géométrique de premier terme a et de raison r s'écrit de manière équivalente des deux manières suivantes :

$$\sum_{i=0}^{\infty} a \cdot r^i \quad \text{et} \quad \sum_{i=1}^{\infty} a \cdot r^{i-1}\,.$$

En effet, on voit facilement l'égalité des deux expressions en écrivant les sommes en extension :

$$\begin{aligned}
\sum_{i=0}^{\infty} a \cdot r^i &= a \cdot r^0 + a \cdot r^1 + a \cdot r^2 + a \cdot r^3 + \ldots \\
\sum_{i=i}^{\infty} a \cdot r^{i-1} &= a \cdot r^{1-1} + a \cdot r^{2-1} + a \cdot r^{3-1} + a \cdot r^{4-1} + \ldots
\end{aligned}$$

Exemple 1 : La somme des 100 premiers entiers positifs

Supposons que l'on désire calculer la somme des nombres naturels de 1 à 100 inclusivement, c'est-à-dire qu'on veut connaître le résultat de la somme suivante :

$$\sum_{i=1}^{100} i \;=\; 1 + 2 + 3 + 4 + \cdots + 100\,.$$

Remarquons que $1+2+3+4+\cdots+100$ est la somme des 100 premiers termes de la suite $\langle s_n\rangle_{n\in\mathbb{N}} = \langle 1,2,3,4,\cdots\rangle$; cette suite est arithmétique, de premier terme 1 et de différence 1. Par le théorème 2.4.2, on a :

$$s_n = 1 + n\cdot 1 \quad \forall n\in\mathbb{N}\,.$$

Ainsi,

$$\begin{aligned}
\sum_{i=1}^{100} i &= 1+2+3+4+\cdots+100 \\
&= s_0+s_1+s_2+s_3+\cdots+s_{99} && \langle\ \textit{Car } s_n = 100 \ \textit{ si } \ n+1=100, \textit{ et donc si } n=99\ \rangle \\
&= \frac{(s_0+s_{99})(99+1)}{2} && \langle\ \textit{Théorème 2.4.6}\ \rangle \\
&= \frac{(1+100)(99+1)}{2} \\
&= 5050\,.
\end{aligned}$$

Exemple 2 : Une somme de puissances de 2

On désire calculer la valeur de la somme suivante :

$$8+16+32+64+128+\cdots+1\,048\,576\,.$$

Remarquons qu'il s'agit d'une somme de premiers termes de la suite géométrique de premier terme 8 et de raison 2. Notons cette suite géométrique $\langle t_n\rangle_{n\in\mathbb{N}}$. Par le théorème 2.4.4, on a :

$$t_n = 8\cdot 2^n \quad \forall n\in\mathbb{N}\,.$$

Pour calculer le nombre de termes que l'on considère dans la somme, on cherche d'abord le $i\in\mathbb{N}$ tel que $t_i = 1\,048\,576$. On le trouve par des calculs arithmétiques simples [12] :

$$\begin{aligned}
& t_i = 8\cdot 2^i = 1\,048\,576 \\
\Leftrightarrow\ & 2^i = 131\,072 \\
\Leftrightarrow\ & \log_2(2^i) = \log_2(131\,072) \\
\Leftrightarrow\ & i = 17\,.
\end{aligned}$$

12. Rappelons que $\log_2(x) = \frac{\log_{10}(x)}{\log_{10}(2)}$

Ainsi, le résultat désiré est obtenu en calculant la somme des 18 premiers termes de la suite géométrique $\langle t_n \rangle_{n\in\mathbb{N}}$:

$$\begin{aligned}\sum_{i=0}^{17} t_i &= \frac{8\cdot(1-2^{17+1})}{1-2} \qquad \langle\ \textit{Théorème 2.4.7}\ \rangle \\ &= 2\,097\,144\,.\end{aligned}$$

Exemple 3 : Terme général du problème des tours de Hanoï

À la section 2.2, nous avons présenté un algorithme qui permet de résoudre le problème des tours de Hanoï en un nombre minimal de déplacements de disques (voir la page 163). Nous avons établi que ce nombre optimal de déplacements est donné par une suite $\langle h_n \rangle_{n\in\mathbb{N}}$, dont la définition par récurrence est la suivante (voir l'équation (2.8), page 165) :

$$\begin{cases} h_0 = 0 \\ h_n = 2\cdot h_{n-1}+1 \qquad \forall n\in\mathbb{N}^*. \end{cases}$$

En appliquant la méthode des substitutions à rebours, nous avons transformé la définition par récurrence de la suite $\langle h_n \rangle_{n\in\mathbb{N}}$ en une somme :

$$h_n = \sum_{j=0}^{n-1} 2^j \qquad \forall n\in\mathbb{N}\,. \tag{2.11}$$

Les notions introduites jusqu'alors ne nous permettaient pas de transformer cette somme pour obtenir le terme général de la suite $\langle h_n \rangle_{n\in\mathbb{N}}$. Désormais, le théorème 2.4.4 permet de constater que l'équation (2.11) correspond à une somme des n premiers termes de la suite géométrique de premier terme 1 et de raison 2. Ainsi, par le théorème 2.4.7, on obtient que le terme général de la suite $\langle h_n \rangle_{n\in\mathbb{N}}$ est :

$$h_n = \frac{1\cdot(1-2^{(n-1)+1})}{1-2} = \frac{1-2^n}{-1} = 2^n-1 \qquad \forall n\in\mathbb{N}\,. \tag{2.12}$$

Nous sommes donc parvenus à exprimer le nombre de déplacements minimaux nécessaires pour résoudre le problème des tours de Hanoï par un simple terme général.

Une méthode (pour reconnaître une suite)

Une suite $\langle s_n\rangle_{n\in\mathbb{N}}$ est-elle arithmétique ? géométrique ? somme d'arithmétique ? somme de géométrique ? Voici une méthode informelle. Prenons les suites suivantes en exemple.

$$\begin{cases} d_0 &= 0 \\ d_n &= d_{n-1}+2 \quad \forall n\in\mathbb{N}^*, \end{cases} \qquad \begin{cases} b_0 &= 1 \\ b_n &= b_{n-1}\cdot 2 \quad \forall n\in\mathbb{N}^*, \end{cases}$$

$$\begin{cases} S_0 &= 4 \\ S_n &= S_{n-1}+4\cdot 7^n \qquad \forall n\in\mathbb{N}^*. \end{cases} \qquad \begin{cases} T_0 &= 2 \\ T_n &= 3T_{n-1}+2^n \quad \forall n\in\mathbb{N}^* \end{cases}$$

Arithmétique ? on calcule $s_n - s_{n-1}$. Si le résultat est une constante, alors oui.
- $d_n - d_{n-1} = (d_{n-1}+2) - d_{n-1} = 2$, comme 2 est une constante : arithmétique.
- $b_n - b_{n-1} = (b_{n-1}\cdot 2) - b_{n-1} = b_{n-1}$, ce n'est pas une constante : non.
- $S_n - S_{n-1} = S_{n-1} + 4\cdot 7^n - S_{n-1} = 4\cdot 7^n$ ce n'est pas une constante : non.

Géométrique ? on calcule $\frac{s_n}{s_{n-1}}$. Si le résultat est une constante, alors oui.
- $\frac{b_n}{b_{n-1}} = \frac{b_{n-1}\cdot 2}{b_{n-1}} = 2$, c'est une constante : géométrique.
- $S_n/S_{n-1} = S_{n-1} + 4\cdot 7^n/S_{n-1}$ n'est pas une constante : non.

Somme de ? Aussitôt que s_n est de la forme $s_{n-1}+f(n)$, avec $f(0)=s_0$ ($n\in\mathbb{N}^*$), on est devant une somme de premiers termes de la suite $a_n := f(n)$. On regarde ensuite si la suite $\langle a_n\rangle_{n\in\mathbb{N}}$ est géométrique ou arithmétique.
Notons que ce critère implique que f ne peut pas être récursive (définie avec un "s_i").
(Notons aussi qu'il est équivalent de voir si $g(n) := s_n - s_{n-1}$ satisfait $g(0) = s_0$.)
- $\langle d_n\rangle_{n\in\mathbb{N}}$ ne satisfait pas le critère car $f(n)=2$ nous donne $f(0)=2\neq 0=d_0$. De toute façon, on avait déjà une arithmétique
- $\langle S_n\rangle_{n\in\mathbb{N}}$ satisfait le critère avec $f(n)=4\cdot 7^n$, pour lequel on a bien $f(0)=4\cdot 7^0=4=S_0$. On remarque que $a_n := f(n) = 4\cdot 7^n$ est une géométrique de premier terme 4 et de raison 7, on peut appliquer le théorème 2.4.7.
- $\langle b_n\rangle_{n\in\mathbb{N}}$ ne satisfait pas le critère parce que 2 multiplie b_{n-1}.
- $\langle T_n\rangle_{n\in\mathbb{N}}$ ne satisfait pas le critère parce qu'on trouve un facteur 3 devant T_{n-1}.

De façon équivalente : on obtient une fonction récursive $g(n) = T_n - T_{n-1} = 2T_{n-1} + 2^n$, ce qui nous donne $g(0) = 2T_{-1} + 2^0 \neq 2 = T_0$, le critère n'est pas satisfait. C'est pour cette raison qu'on dit plus haut que"f ne peut pas être récursive".

2.4.4 Exercices sur les cas particuliers de récurrences

Exercice 1 :

a) Est-ce que la suite $\langle c_n \rangle_{n\in\mathbb{N}}$, définie par le terme général $c_n = 5n-6 \quad \forall n \in \mathbb{N}$, est une suite arithmétique ?

b) Donnez c_0, c_1 et c_{200}.

c) Soit la suite $\langle S_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par : $\begin{cases} S_0 &= -6 \\ S_n &= S_{n-1} + 5n - 6 \quad \forall n \in \mathbb{N}^* . \end{cases}$

Montrez (sans utiliser l'induction) que le terme général de la suite $\langle S_n \rangle_{n\in\mathbb{N}}$ est

$$S_n = \frac{(n+1)(5n-12)}{2} \quad \forall n \in \mathbb{N} .$$

Exercice 2 : Trouvez le terme général des suites suivantes :

a) $\begin{cases} b_0 &= 0 \\ b_n &= b_{n-1} + n \quad \forall n \in \mathbb{N}^* . \end{cases}$

b) $w_n = 1 + 3 + 5 + 7 + 9 + \cdots + (2n+1) \quad \forall n \in \mathbb{N} .$

c) $\begin{cases} p_0 &= -2 \\ p_n &= p_{n-1} + 5n - 2 \quad \forall n \in \mathbb{N}^* . \end{cases}$

Exercice 3 : Soit la suite $\langle d_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par :

$$\begin{cases} d_0 &= 5 \cdot 2^3 \\ d_n &= d_{n-1} + 5 \cdot 2^{n+3} \quad \forall n \in \mathbb{N}^* . \end{cases}$$

Montrez (sans utiliser l'induction) que le terme général de la suite $\langle d_n \rangle_{n\in\mathbb{N}}$ est

$$d_n = \frac{5 \cdot 2^3 \, (1 - 2^{n+1})}{-1} \quad \forall n \in \mathbb{N} .$$

Exercice 4 : Vous placez $\$1000.^{00}$ dans un compte à intérêt composé de 5% par année.

Ainsi, après un an il y aura dans votre compte, $\$1000.^{00}$ + (5% *de* $\$1000.^{00}$*), c'est-à-dire, en tout* $\$1050.^{00}$. *Après deux ans, il y aura dans votre compte,* $\$1050.^{00}$ + (5% *de* $\$1050.^{00}$*), etc...*

Soit $\langle \$_n \rangle_{n\in\mathbb{N}}$, la suite qui donne le montant d'argent qu'il y a dans votre compte après n années.

a) Définissez $\langle \$_n \rangle_{n\in\mathbb{N}}$ par récurrence.

b) Trouvez le terme général de $\langle \$_n \rangle_{n\in\mathbb{N}}$.

c) Après 10 ans, combien d'argent y aura-t-il dans le compte ?

Exercice 5 : Évaluez la somme suivante :

$$32 + 8 + 2 + \frac{1}{2} + \ldots + \frac{1}{524288}\,.$$

2.5 Méthode des séries génératrices

Dans cette section nous allons développer une méthode plus générale de résolution de récurrences, la **méthode des séries génératrices**.

La **série génératrice** associée à la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ est une fonction $G : \mathbb{R} \longrightarrow \mathbb{R}$ qui est exprimée comme un polynôme contenant un nombre infini de termes :

$$G(x) \;=\; a_0 \,+\, a_1\, x \,+\, a_2\, x^2 \,+\, a_3\, x^3 \,+\, \ldots \,+\, a_n\, x^n \,+\, \ldots$$

Par exemple, la série génératrice associée à la suite des carrés parfaits correspond à la fonction $C : \mathbb{R} \longrightarrow \mathbb{R}$ suivante :

$$C(x) \;=\; 0 \,+\, 1\, x \,+\, 4\, x^2 \,+\, 9\, x^3 \,+\, \ldots \,+\, (n^2)\, x^n \,+\, \ldots$$

En fait, G n'est pas une fonction car il y a certains x pour lesquels la série ne converge pas. Cela sort du cadre du cours, mais G est défini seulement sur un certain *rayon de convergence*, qui contient toujours 0 et les réels dans un certain intervalle autour de zéro. Ceci ne nous dérange pas, nous utilisons G *en passant*, alors on le fait sur son rayon de convergence.

2.5.1 L'idée de la méthode

Examinons la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par

$$\begin{cases} b_0 &= 1 \\ b_n &= b_{n-1} \cdot 2 \quad \forall n \in \mathbb{N}^* \,. \end{cases}$$

Notez que cette récurrence est très simple à résoudre. En effet, nous avons déjà déterminé à la section 2.4.2 qu'il s'agit d'une suite géométrique de premier terme 1 et de raison 2. Le théorème 2.4.4 nous a permis d'énoncer directement que le terme général de la suite est :

$$b_n = 1 \cdot 2^n \quad \forall n \in \mathbb{N} \,.$$

Dans le texte qui suit, nous nous servons de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ comme premier exemple pour illustrer le fonctionnement de la méthode des séries génératrices. Nous développerons les outils nécessaires à l'utilisation de cette méthode par la suite, mais avons dès maintenant besoin du résultat suivant pour résoudre cette suite.

Une première série de puissance
Considérons la somme suivante, où x est un élément quelconque de $\mathbb{R} \setminus \{\frac{1}{2}\}$:

$$1 + 2 \cdot x + 2^2 \cdot x^2 + 2^3 \cdot x^3 + \ldots + 2^n \cdot x^n .$$

Il s'agit de la somme des $n+1$ premiers termes de la suite géométrique $\langle 1 \cdot (2x)^n \rangle_{n\in\mathbb{N}}$, dont le premier terme est 1 et et la raison est $2x$. Par le théorème 2.4.7, on a donc :

$$1 + 2 \cdot x + 2^2 \cdot x^2 + 2^3 \cdot x^3 + \ldots + 2^n \cdot x^n \;=\; \frac{1 \cdot (1 - (2x)^{n+1})}{1 - 2x} .$$

Supposons maintenant que $2x \in \,]-1, 1[$, c'est-à-dire que $x \in \left]\frac{-1}{2}, \frac{1}{2}\right[$. Alors on remarque facilement que dans ce cas, plus n devient grand, plus $(2x)^{n+1}$ se rapproche de 0. Donc, si on fait tendre n vers l'infini, la partie droite de l'équation ci-dessus va tendre vers $\frac{1\cdot(1-0)}{1-2x}$, c'est-à-dire vers $\frac{1}{1-2x}$. De plus, la partie de gauche de l'équation ci-dessus deviendra une somme contenant un nombre de plus en plus grand de termes, à la limite une somme contenant une infinité de termes.
Autrement dit, à la limite, lorsque $n \to \infty$, et si $x \in \left]\frac{-1}{2}, \frac{1}{2}\right[$, l'équation ci-dessus devient :

$$1 + 2 \cdot x + 2^2 \cdot x^2 + 2^3 \cdot x^3 + \ldots \;=\; \frac{1}{1 - 2x} . \tag{2.13}$$

On constate que la somme infinie "$1 + 2\cdot x + 2^2\cdot x^2 + 2^3\cdot x^3 + \ldots$" est en fait une fonction de x. En effet, pour tout $x \in \left]\frac{-1}{2}, \frac{1}{2}\right[$, cette somme infinie coïncide avec la fonction d'équation $f(x) = \frac{1}{1-2x}$.

Précisons que la fonction $f(x) = \frac{1}{1-2x}$ est une **fonction rationnelle**, c'est-à-dire une fonction qui peut s'exprimer comme le quotient de deux polynômes, les constantes étant ici vues comme des polynômes de degré 0. On dit que la somme infinie "$1 + 2\cdot x + 2^2\cdot x^2 + 2^3\cdot x^3 + \ldots$" est la **série de puissances** associée à la fonction rationnelle f.

Nous utilisons ce résultat dans la démonstration qui suit. Celle-ci illustre la méthode que nous allons utiliser afin de trouver le terme général de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$.

Démonstration Terme général de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ par la méthode des séries génératrices

1. Fabriquons d'abord la fonction G, correspondant à la série génératrice associée à partir de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$, de la manière suivante (et écrite de 2 façons) :

$$G(x) \;=\; b_0 + b_1\, x + b_2\, x^2 + b_3\, x^3 + \cdots + b_n\, x^n + \cdots \;=\; \sum_{i=0}^{\infty} b_i x^i$$

Remarquons que cette somme infinie est une fonction de x. Cette fonction encode en quelque sorte la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ puisque c'est la suite des coefficients de G.

Selon la définition de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$, $\quad b_n = b_{n-1} \cdot 2 \quad \forall n \in \mathbb{N}^*$,
ce qui implique que $\quad b_n - 2 \cdot b_{n-1} = 0 \quad \forall n \in \mathbb{N}^*$,
ce qui en extension donne : $\quad b_1 - 2 \cdot b_0 = 0$

$$b_2 - 2 \cdot b_1 = 0$$
$$b_3 - 2 \cdot b_2 = 0$$
$$\text{etc...}$$

Maintenant, nous allons essayer d'utiliser cette relation de récurrence et nos connaissances en algèbre pour arriver à écrire la fonction G sous une forme plus simple.

$$\begin{array}{rrcrcrcrcccrcc}
(\bigstar) & G(x) = & b_0 & + & b_1\,x & + & b_2\,x^2 & + & b_3\,x^3 & + & \cdots & + & b_n\,x^n & + & \cdots \\
& -2x \cdot G(x) = & & + & -2b_0\,x & + & -2b_1\,x^2 & + & -2b_2\,x^3 & + & \cdots & + & -2b_{n-1}\,x^n & + & \cdots \\
\hline
& G(x) - 2xG(x) = & b_0 & + & 0\,x & + & 0\,x^2 & + & 0\,x^3 & + & \cdots & + & 0\,x^n & + & \cdots
\end{array}$$

Le truc (première parenthèse)

Il y a 4 idées cruciales à comprendre ici (les 3 premières par vous-même) :

- pourquoi les colonnes des coefficients de $x, x^2, x^3, \ldots$ donnent 0 ✓
- pourquoi, $-2xG(x)$ donne $-2b_0\,x + -2b_1\,x^2 \ldots$ ✓
- comment choisit-on l'alignement des termes ✓
- pourquoi a-t-on choisi $-2x$ comme multiple de G dans la 2e ligne ?
  C'est en observant la récurrence en rouge ci-haut, après avoir écrit la ligne ($\bigstar$). On voit $b_1 - 2 \cdot b_0 = 0$; en y pensant un peu (eh oui), on remarque que si on réussissait à mettre $-2b_0$ dans la colonne du b_1 de la ligne ($\bigstar$), on obtiendrait 0 quand on fait la somme de la colonne. Pour que ce terme se trouve dans la bonne colonne, celle "de x^1" il faut que le terme soit $-2b_0x$, c'est-à-dire il faut que b_0 soit multiplié par $-2x$. On choisit donc de multiplier $G(x)$ par $-2x$, et on écrit les termes dans les bonnes colonnes. Par récurrence (presque par magie), cette simple observation nous assurera que toutes les colonnes subséquentes (i.e., les coefficients de tous les x^i qui suivent) s'annuleront.
- d'autres idées n'apparaissent pas dans cet exemple simple, nous y reviendrons.

Ce qui donne $G(x) - 2x \cdot G(x) \;=\; 1$ $\qquad \langle\ \textit{Car } b_0 = 1.\ \rangle$
Donc, on a $G(x)(1 - 2x) \;=\; 1$
Donc, on a $G(x) \;=\; \frac{1}{(1-2x)}$, ce qui est une forme beaucoup plus simple pour exprimer la fonction G.

2. Remarquons que nous connaissons déjà la série de puissances associée à $\frac{1}{(1-2x)}$, c'est

$$1 + 2 \cdot x + 2^2 \cdot x^2 + 2^3 \cdot x^3 + \cdots + 2^n \cdot x^n + \cdots . \qquad \langle \textit{ Voir équation (2.13) } \rangle$$

3. Cette constatation nous permet de déduire le terme général de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$, puisque :
   On a d'une part que
   $$\begin{array}{rcccccccccccc} G(x) & = & b_0 & + & b_1\,x & + & b_2\,x^2 & + & b_3\,x^3 & + & \cdots & + & b_n\,x^n & + & \cdots \\ \text{et d'autre part que} & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & & & \updownarrow & & \\ G(x) & = & 1 & + & 2\,x & + & 2^2\,x^2 & + & 2^3\,x^3 & + & \cdots & + & 2^n\,x^n & + & \cdots \end{array}$$
   Avec la notation Σ, cela s'écrit
   $$\sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} 2^i x^i,$$
   et cela implique indirectement le résultat cherché :
   $$b_n \;=\; 2^n \quad \forall n \in \mathbb{N}.$$
   C.Q.F.D.

Pour trouver le terme général de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$, la solution par la méthode des séries génératrices que nous venons de présenter est bien sûr nettement plus compliquée que la solution présentée à la section 2.4.2 sur les suites géométriques. Notre nouvelle solution a cependant l'avantage d'être généralisable à des récurrences que nous ne pouvions résoudre jusqu'à maintenant.

2.5.2 Méthode de résolution et modèles de séries de puissances

On peut résumer ainsi la **méthode des séries génératrices** pour la résolution de récurrences :

Étape 1 : À partir de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$, on construit [13] la **série génératrice**

$$G(x) \;=\; \sum_{i=0}^{\infty} a_i\,x^i \;=\; a_0 + a_1\,x + a_2\,x^2 + a_3\,x^3 + \cdots + a_n\,x^n + \cdots \qquad (2.14)$$

Puis en se servant astucieusement de la relation de récurrence définissant $\langle a_n \rangle_{n\in\mathbb{N}}$, on exprime G sous la forme d'une **fonction rationnelle**.

13. Notez que dans l'équation (2.14), le théorème 2.5.1 et le corolaire 2.5.2, nous exprimons les sommes à la fois en notation sigma et en extension. Les deux notations sont équivalentes et il appartient à vous d'adopter celle que vous préférez lorsque vous appliquez la méthode des séries génératrices.

Étape 2 : On décompose la fonction rationnelle trouvée à l'étape 1 en **fractions partielles**, de façon que pour chacune de ces fractions, on connaisse sa **série de puissances** associée. Ensuite, on recompose les différentes séries de puissances associées aux fractions partielles de façon à obtenir la série de puissances associée à G.

Étape 3 : À partir de la série de puissance trouvée à l'étape 2, on déduit le **terme général** de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$. À cette étape, on doit souvent trouver la valeur de constantes inconnues. Pour ce faire, on substitue les valeurs des cas de base de la définition par récurrence de $\langle a_n \rangle_{n\in\mathbb{N}}$ et en résolvant le système d'équations linéaire ainsi obtenu.

Mais avant de pouvoir efficacement résoudre des récurrences par cette méthode, il nous faut connaître plusieurs modèles de séries de puissances et savoir comment on décompose en fractions partielles.

Théorème 2.5.1. *Modèles de séries de puissances*
Soit $a,\ b \in \mathbb{R} \setminus \{0\}$, *alors* $\forall x \in \left]\frac{-1}{|b|}, \frac{1}{|b|}\right[$, *on a que*

$$\texttt{a}: \quad \frac{a}{1-bx} = \sum_{i=0}^{\infty} a\,b^i\,x^i = a + a\,b\,x + a\,b^2\,x^2 + a\,b^3\,x^3 + \cdots + a\,b^n\,x^n + \cdots$$

$$\texttt{b}: \quad \frac{a}{(1-bx)^2} = \sum_{i=0}^{\infty} (i+1)a\,b^i\,x^i = a + 2a\,b\,x + 3a\,b^2\cdot x^2 + \cdots + (n+1)a\,b^n\,x^n + \cdots$$

$$\texttt{c}: \quad \frac{ax}{(1-bx)^2} = \sum_{i=0}^{\infty} i\,a\,b^{i-1}\,x^i = 0 + a\,x + 2a\,b\,x^2 + 3a\,b^2\,x^3 + \cdots + n\,a\,b^{n-1}\,x^n + \cdots$$

$$\texttt{d}: \quad \frac{a}{(1-bx)^3} = \sum_{i=0}^{\infty} \frac{(i+2)(i+1)\,a\,b^i}{2}\,x^i = \frac{2\cdot 1\,a}{2} + \frac{3\cdot 2\,a\,b}{2}x + \frac{4\cdot 3\,a\,b^2}{2}x^2 + \frac{5\cdot 4\,a\,b^3}{2}x^3 + \cdots + \frac{(n+2)(n+1)\,a\,b^n}{2}\,x^n + \cdots$$

En particulier, nous avons donc les séries de puissances suivantes.

Corollaire 2.5.2. *Cas particuliers des modèles de séries de puissances*

$$\texttt{a}: \quad \frac{1}{1-x} = \sum_{i=0}^{\infty} x^i = 1 + x + x^2 + x^3 + x^4 + \cdots + x^n + \cdots$$

$$\texttt{b}: \quad \frac{1}{1+x} = \sum_{i=0}^{\infty} (-1)^i\, x^i = 1 + (-1)x + (-1)^2x^2 + (-1)^3x^3 + \cdots$$

$$\texttt{c}: \quad \frac{1}{(1-x)^2} = \sum_{i=0}^{\infty} (i+1)\, x^i = 1 + 2x + 3x^2 + 4x^3 + \cdots + (n+1)\, x^n + \cdots$$

$$\texttt{d}: \quad \frac{x}{(1-x)^2} = \sum_{i=0}^{\infty} i\, x^i = 0 + x + 2x^2 + 3x^3 + 4x^4 + \cdots + n\, x^n + \cdots$$

$$\texttt{e}: \quad \frac{1}{(1-x)^3} = \sum_{i=0}^{\infty} \frac{(i+2)(i+1)}{2}\, x^i = \frac{2\cdot1}{2} + \frac{3\cdot2}{2}\, x + \frac{4\cdot3}{2}\, x^2 + \cdots + \frac{(n+2)(n+1)}{2}\, x^n + \cdots$$

Voici enfin la forme de décomposition en fractions partielles de certaines des familles de fonctions rationnelles. Remarquons que le numérateur de chacune des fractions partielles est toujours une constante.

Théorème 2.5.3. *Décomposition en fractions partielles*

$$\texttt{a}: \quad \frac{ax+b}{(cx+d)(ex+f)} = \frac{A}{cx+d} + \frac{B}{ex+f}$$

⟨ *Pourvu que* $y = cx + d$ *et* $y = ex + f$ *aient des zéros différents.* ⟩

$$\texttt{b}: \quad \frac{ax+b}{(cx+d)^2} = \frac{A}{cx+d} + \frac{B}{(cx+d)^2}$$

$$\texttt{c}: \quad \frac{ax^2+bx+c}{(dx+e)(fx+g)(hx+i)} = \frac{A}{dx+e} + \frac{B}{fx+g} + \frac{C}{hx+i}$$

⟨ *Pourvu que* $y = dx + e$, $y = fx + g$ *et* $y = hx + i$ *aient des zéros tous différents.* ⟩

$$\texttt{d}: \quad \frac{ax^2+bx+c}{(dx+e)^2(fx+g)} = \frac{A}{dx+e} + \frac{B}{(dx+e)^2} + \frac{C}{fx+g}$$

⟨ *Pourvu que* $y = dx + e$ *et* $y = fx + g$ *aient des zéros différents.* ⟩

$$\texttt{e}: \quad \frac{ax^2+bx+c}{(dx+e)^3} = \frac{A}{dx+e} + \frac{B}{(dx+e)^2} + \frac{C}{(dx+e)^3}$$

Le résultat énoncé au théorème 2.5.3 se généralise à toutes les fonctions rationnelles ; cependant, dans le cas où il y a au dénominateur des zéros qui soient des nombres complexes, le problème devient plus difficile. Notez que nous ne démontrons pas ici pourquoi chacune des fonctions rationnelles appartenant à une de ces familles se décompose effectivement comme le dit le théorème 2.5.3.

2.5.3 Quelques exemples de résolution de récurrences

Exemple 1-a (en représentant les sommes en extension)

Trouvons le terme général d'une suite $\langle a_n \rangle_{n\in\mathbb{N}}$ dont la définition par récurrence est la suivante :

$$\begin{cases} a_0 &= 1 \\ a_n &= 3 \cdot a_{n-1} + 4^n \quad \forall n \in \mathbb{N}^* \,. \end{cases}$$

Prenez note que, au cours de la démarche suivante, nous représentons toutes les sommes par la notation en extension.

Étape 1 : (on exprime la série génératrice sous la forme d'une fonction rationnelle)

- On remarque que : $a_n \; - \; 3 \cdot a_{n-1} - (4^n) \; = \; 0 \quad \forall n \in \mathbb{N}^*$;
- ce qui en extension donne : $\quad a_1 - 3 \cdot a_0 - 4 \; = 0$
  $a_2 - 3 \cdot a_1 - 4^2 = 0$
  $a_3 - 3 \cdot a_2 - 4^3 = 0$
  $a_4 - 3 \cdot a_3 - 4^4 = 0$
  etc...
- Posons $G(x) \; = \sum_{i=0}^{\infty} a_i x^i \; = \; a_0 \, + \, a_1 \, x \, + \, a_2 \, x^2 \, + \, a_3 \, x^3 \, + \, \cdots \, + \, a_n \, x^n \, + \, \cdots .$

Alors,

$$\begin{array}{rcccccccccc}
G(x) & = & a_0 & + & a_1x + & a_2x^2 + & a_3x^3 + \cdots + & a_nx^n + \cdots & & \\
-3x \cdot G(x) & = & & + & -3 \cdot a_0x + & -3 \cdot a_1x^2 + & -3 \cdot a_2x^3 + \cdots + & -3 \cdot a_{n-1}x^n + \cdots & & \\
-\frac{1}{1-4x} & = & -1 & + & -4x + & -(4^2)x^2 + & -(4^3)x^3 + \cdots + & -(4^n)x^n + \cdots & (\bigstar) & \\
\hline
G(x) - 3xG(x) - \frac{1}{1-4x} & = & a_0 - 1 + & & 0x + & 0x^2 + & 0x^3 + \cdots + & 0x^n + \cdots & &
\end{array}$$

⟨ *La ligne* (★) *est obtenue par le théorème 2.5.1-a, avec* $[a := -1]$ *et* $[b := 4]$ ⟩

> LE TRUC (DEUXIÈME PARENTHÈSE)
>
> Voici d'où vient la ligne (★). Une fois qu'on a choisi $-3x$ comme coefficient de $G(x)$, notre colonne $a_1x - 3a_0x$ ne s'annule pas tout de suite, il faut ajouter $-4x$ (notez que ce terme ne contient pas de a_i). On continue d'écrire les termes manquants de x^2, x^3 et, plus important, x^n. On obtient le terme $-(4^n)x^n$ en position n. C'est là qu'on va voir le théorème 2.5.1 ou le corollaire 2.5.2. On y trouve que $\sum_{i=0}^{\infty} -(4^n)x^n = -\frac{1}{1-4x}$. C'est ce qu'on écrit à gauche du "=". Finalement on complète la ligne avec le ou les termes manquants : ici, il fallait ajouter "-1" dans la même colonne que a_0.

Ce qui donne $G(x) - 3x\,G(x) - \frac{1}{1-4x} \;=\; 0$ $\quad\langle\; \textit{Car} \quad a_0 - 1 \;=\; 1 - 1 \;=\; 0. \;\rangle$
Donc, on a $\quad G(x)(1-3x) \;=\; \frac{1}{1-4x}$
Donc, on a $\quad G(x) \;=\; \frac{1}{(1-3x)(1-4x)}$, notre forme plus simple pour exprimer la fonction G.

Étape 2 : (on trouve la série de puissances associée à G)

Par le théorème 2.5.3-a, on obtient :

$$G(x) \;=\; \frac{1}{(1-3x)(1-4x)} \;=\; \frac{A}{1-3x} + \frac{B}{1-4x}\,.$$

On applique ensuite le théorème 2.5.1-a sur chacune des deux fractions partielles :

$$\begin{aligned}
G(x) \;&=\; \sum_{i=0}^{\infty} A\,3^i\,x^i + \sum_{i=0}^{\infty} B\,4^i\,x^i \\
&=\; A \;+\; A\cdot 3\,x \;+\; A\cdot 3^2\,x^2 \;+\; A\cdot 3^3\,x^3 + \cdots + A\cdot 3^n\,x^n \;+\; \cdots \\
&\qquad + B \;+\; B\cdot 4\,x \;+\; B\cdot 4^2\,x^2 \;+\; B\cdot 4^3\,x^3 + \cdots + B\cdot 4^n\,x^n \;+\; \cdots \\
&=\; (A+B) \;+\; (3\,A + 4\,B)\cdot x \;+\; (3^2\,A + 4^2\,B)\cdot x^2 \;+\; (3^3\,A + 4^3\,B)\cdot x^3 \\
&\qquad + \cdots + (3^n\,A + 4^n\,B)\cdot x^n \;+\; \cdots \\
&=\; \sum_{i=0}^{\infty} (A\,3^i + B\,4^i)\,x^i
\end{aligned}$$

(Nous pourrons éviter d'écrire la somme en extension par la suite.)

Étape 3 : (on trouve le terme général de la suite)

Le terme général de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ est donné par :

$$a_n \;=\; 3^n\,A + 4^n\,B\,.$$

Il ne nous reste plus qu'à calculer les valeurs des constantes A et B. Par la définition de la récurrence, nous savons que $a_0 = 1$ et $a_1 = 3\cdot a_0 + 4^1 = 7$. Donc :

$$\begin{aligned}
& a_0 \;=\; 3^0\,A + 4^0\,B \;=\; A + B \;=\; 1 \\
\Leftrightarrow\; & B \;=\; 1 - A\,, && (*) \\
& a_1 \;=\; 3^1\,A + 4^1\,B \;=\; 3\,A + 4\,B \;=\; 7 \\
\Leftrightarrow\; & 3\,A \;=\; 7 - 4\,B\,, && (**) \\
& 3\,A \;=\; 7 - 4\,(1-A) \;=\; 3 + 4\,A && \langle\; \textit{Substitutions de (*) dans (**)} \;\rangle \\
\Leftrightarrow\; & A \;=\; -3\,, && (***) \\
& B \;=\; 1 - (-3) \;=\; 4\,. && \langle\; \textit{Substitutions de (***) dans (*)} \;\rangle
\end{aligned}$$

Avec ces valeurs de A et B, on obtient le terme général suivant :

$$\begin{aligned} a_n &= 3^n \cdot (-3) + 4^n \cdot 4 \\ &= -(3^{n+1}) + 4^{n+1}. \end{aligned}$$

Conclusion : La définition par terme général est $a_n = -(3^{n+1}) + 4^{n+1} \quad \forall n \in \mathbb{N}$.

Exemple 1-b (en représentant les sommes par la notation sigma)

Dans l'exemple précédent, nous avons fait le choix d'écrire toutes les sommes en extension. Nous reprenons maintenant le même exemple en utilisant cette fois-ci la notation sigma pour représenter les sommes. Notons immédiatement que, bien que les deux méthodes sont équivalentes, nous jugeons qu'il est plus naturel d'utiliser la notation en extension pour l'étape 1 (la démarche qui suit est d'ailleurs la seule du document qui utilise la notation sigma pour cette étape). Par contre, la notation sigma se prête habituellement bien à l'étape 2.

Rappelons que notre objectif est de trouver le terme général de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ dont la définition par récurrence est :

$$\left\{ \begin{array}{lcl} a_0 &=& 1 \\ a_n &=& 3 \cdot a_{n-1} + 4^n \quad \forall n \in \mathbb{N}^* \,. \end{array} \right.$$

Étape 1 : (on exprime la série génératrice sous la forme d'une fonction rationnelle)

- On remarque que : $a_n - 3 \cdot a_{n-1} - (4^n) = 0 \quad \forall n \in \mathbb{N}^*$;
- Posons $G(x) = \sum_{i=0}^{\infty} a_i \, x^i$.

Alors [14],

$$\begin{aligned} & G(x) - 3x \cdot G(x) - \frac{1}{1-4x} \\ &= \sum_{i=0}^{\infty} a_i \, x^i - 3x \sum_{i=0}^{\infty} a_i \, x^i - \sum_{i=0}^{\infty} 4^i \, x^i \end{aligned}$$

⟨ *Définition de G et théorème 2.5.1-a* ⟩

14. C'est le même truc que précédemment pour trouver "$-3x$", mais c'est plus difficile à voir.

$$= \left[a_0 + \sum_{i=1}^{\infty} a_i\, x^i\right] - \left[\sum_{i=0}^{\infty} 3a_i\, x^{i+1}\right] - \left[1 + \sum_{i=1}^{\infty} 4^i\, x^i\right] \qquad \langle\ \textit{Arithmétique}\ \rangle$$

$$= \left[a_0 + \sum_{i=1}^{\infty} a_i\, x^i\right] - \left[\sum_{i=1}^{\infty} 3a_{i-1}\, x^i\right] - \left[1 + \sum_{i=1}^{\infty} 4^i\, x^i\right] \qquad \left\langle\ \textit{Car} \sum_{i=0}^{\infty} f(x) \;=\; \sum_{i=1}^{\infty} f(x-1)\ \forall f : \mathbb{N} \to \mathbb{R}\ \right\rangle$$

$$= a_0 - 1 + \sum_{i=1}^{\infty} \Big[\, a_i - 3a_{i-1} - 4^i \,\Big] \cdot x^i \qquad \langle\ \textit{Arithmétique}\ \rangle$$

$$= a_0 - 1 + 0 \qquad \langle\ \textit{Car}\ a_n - 3 \cdot a_{n-1} - (4^n) \;=\; 0\ \forall n \in \mathbb{N}^*\ \rangle$$

$$= 1 - 1 + 0 \qquad \langle\ \textit{Car}\ a_0 \;=\; 1\ \rangle$$

$$= 0$$

Ce qui donne $G(x) - 3x\,G(x) - \frac{1}{1-4x} \;=\; 0$
Donc, on a $\quad G(x)(1-3x) \;=\; \frac{1}{1-4x}$ et $G(x) \;=\; \frac{1}{(1-3x)(1-4x)}$.

Étape 2 : (on trouve la série de puissances associée à G)

$$\begin{aligned}
G(x) &= \frac{1}{(1-3x)(1-4x)} \\
&= \frac{A}{1-3x} + \frac{B}{1-4x} && \langle\ \textit{Théorème 2.5.3-a}\ \rangle \\
&= \sum_{i=0}^{\infty} A \cdot 3^i\, x^i \;+\; \sum_{i=0}^{\infty} B \cdot 4^i\, x^i && \langle\ \textit{Théorème 2.5.1-a (2 fois)}\ \rangle \\
&= \sum_{i=0}^{\infty} \Big[A \cdot 3^i + B \cdot 4^i\Big]\, x^i\,. && \langle\ \textit{Arithmétique}\ \rangle
\end{aligned}$$

Étape 3 : (on trouve le terme général de la suite)

L'étape 3 est identique à celle présentée par l'exemple 1-a.

Conclusion : La définition par terme général est $\quad a_n \;=\; -(3^{n+1}) + 4^{n+1} \quad \forall n \in \mathbb{N}\,.$

On constate que la démarche demeure essentiellement la même en utilisant la notation en extension (exemple 1-a) ou la notation sigma (exemple 1-b). Il appartient donc à vous d'adopter l'une ou l'autre de ces notations.

Pour les exemples présentés dans le reste de ce document, nous allons préférer la notation en extension pour effectuer l'étape 1 de la méthode des séries génératrices, car elle permet d'illustrer clairement l'astuce qui permet aux termes de s'annuler entre eux. Cependant, nous allons adopter l'écriture en notation sigma pour effectuer la deuxième étape de la méthode des séries génératrices, car elle est plus concise et tout aussi compréhensible que la notation en extension.

Propriétés des polynômes de degré 2

Avant de faire l'exemple qui suit, nous avons besoin de faire un rappel de certaines propriétés des polynômes de degré 2. Les propriétés qui suivent sont valides même si les zéros du polynôme ne sont pas des nombres réels, c'est-à-dire même si $b^2 - 4ac < 0$. Dans ce cas cependant, les calculs se font dans les nombres complexes.

Proposition 2.5.4. *Propriétés des zéros d'un polynôme de degré 2*

Soit $p(x) = ax^2 + bx + c$, *un polynôme de degré deux.*

Soit $\rho_1 \stackrel{\text{def}}{=} \dfrac{-b + \sqrt{b^2 - 4ac}}{2a}$ *et* $\rho_2 \stackrel{\text{def}}{=} \dfrac{-b - \sqrt{b^2 - 4ac}}{2a}$.

Alors,

- ρ_1 *et* ρ_2 *sont appelés les* **zéros du polynôme** p *parce que*

$$p(\rho_1) = 0, \quad p(\rho_2) = 0 \quad et \quad p(x) \neq 0 \quad \forall x \neq \rho_1, \rho_2 \,.$$

- *Le polynôme* p *se factorise toujours ainsi :*

$$p(x) = a(x - \rho_1)(x - \rho_2)$$

- *De plus, si le polynôme est unitaire (c'est-à-dire si* $a = 1$*), on a toujours que*

$$\begin{cases} (*) & \rho_1 + \rho_2 = -b \\ (**) & \rho_1 \cdot \rho_2 = c. \end{cases}$$

Pour les calculs que nous aurons à faire dans ce chapitre, la proposition suivante, qui découle presque directement de la précédente, nous sera très utile. Elle sera utile dans certains cas, à la toute fin de l'étape 1 (comme nous verrons dans l'exemple suivant).

Proposition 2.5.5. *Factorisation d'un polynôme de degré 2*
Soit $q(x) = 1 - rx - sx^2$, *un polynôme de degré deux dont le coefficient de* x^0 *est 1. Considérons le polynome* $p(x) = x^2 - rx - s$ *; soit* ρ_1 *et* ρ_2 *les deux zéros (non nécessairement distincts) du polynôme p. Alors le polynôme* $q(x)$ *se factorise ainsi :*

$$1 - rx - sx^2 = (1 - \rho_1 x)\,(1 - \rho_2 x)\,.$$

Exemple 2 : La suite de Fibonacci

À l'aide de la méthode des séries génératrices, résolvons la récurrence de Fibonacci :

$$\begin{cases} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\}\,. \end{cases}$$

Étape 1 : (on exprime la série génératrice sous la forme d'une fonction rationnelle)

- On remarque que : $f_n - f_{n-1} - f_{n-2} = 0 \qquad \forall n \in \mathbb{N} \setminus \{0,1\}$;
- ce qui en extension donne : $f_2 - f_1 - f_0 = 0$
  $f_3 - f_2 - f_1 = 0$
  $f_4 - f_3 - f_2 = 0$
  etc...
- Posons $G(x) = \sum_{i=0}^{\infty} f_i\, x^i$

Alors,

$$\begin{array}{rcccccccccccc} G(x) &=& f_0 &+& f_1x &+& f_2x^2 &+& f_3x^3 &+\cdots+& f_nx^n &+\cdots \\ -x\cdot G(x) &=& &+& -f_0x &+& -f_1x^2 &+& -f_2x^3 &+\cdots+& -f_{n-1}x^n &+\cdots \\ -x^2\cdot G(x) &=& &&&+& -f_0x^2 &+& -f_1x^3 &+\cdots+& -f_{n-2}x^n &+\cdots \\ \hline G(x) - xG(x) - x^2G(x) &=& f_0 &+& (f_1-f_0)x &+& 0x^2 &+& 0x^3 &+\cdots+& 0x^n &+\cdots \end{array}$$

Ce qui donne $G(x) - x\,G(x) - x^2\,G(x) = x$ $\quad \langle$ *Car* $f_0 = 0$ *et* $f_1 - f_0 = 1 - 0 = 1.$ $\rangle$
Donc, on a $G(x)(1 - x - x^2) = x$

Donc, on a $G(x) = \dfrac{x}{1 - x - x^2}$.

Donc on a $G(x) = \dfrac{x}{\left(1 - (\frac{1+\sqrt{5}}{2})x\right)\left(1 - (\frac{1-\sqrt{5}}{2})x\right)}$. $\quad \left\langle \begin{array}{l} \textit{Voir Proposition 2.5.5, avec } q(x) := 1 - x - x^2. \\ \textit{Les deux zéros de } p(x) = x^2 + -1\cdot x - 1 \\ \textit{étant } \left(\frac{1+\sqrt{5}}{2}\right) \textit{ et } \left(\frac{1-\sqrt{5}}{2}\right). \end{array} \right\rangle$

Pour simplifier l'écriture, posons $\rho_1 := \left(\frac{1+\sqrt{5}}{2}\right)$ et $\rho_2 := \left(\frac{1-\sqrt{5}}{2}\right)$.

Donc on a $G(x) = \dfrac{x}{(1-\rho_1 x)\,(1-\rho_2 x)}$.

Étape 2 : (on trouve la série de puissances associée à G)

$$\begin{aligned}
G(x) &= \frac{x}{(1-\rho_1 x)(1-\rho_2 x)} \\
&= \frac{A}{1-\rho_1 x} + \frac{B}{1-\rho_2 x} && \langle \textit{ Théorème 2.5.3-a } \rangle \\
&= \sum_{i=0}^{\infty} A\cdot\rho_1^i\, x^i \;+\; \sum_{i=0}^{\infty} B\cdot\rho_2^i\, x^i && \langle \textit{ Théorème 2.5.1-a (2 fois) } \rangle \\
&= \sum_{i=0}^{\infty} \left[A\cdot\rho_1^i + B\cdot\rho_2^i\right] x^i\,. && \langle \textit{ Arithmétique } \rangle
\end{aligned}$$

Étape 3 : (on trouve le terme général de la suite)

Le terme général de la suite est donné par : $f_n = A\cdot\rho_1^n + B\cdot\rho_2^n$.
Calculons les valeurs des constantes A et B. Par la définition de la récurrence de la suite de Fibonacci, nous savons que $f_0 = 0$ et $f_1 = 1$. Donc :

$$\begin{aligned}
f_0 = 0 &= A\cdot\rho_1^0 + B\cdot\rho_2^0 = A + B \\
\Leftrightarrow\; B &= -A\,, && (\clubsuit)
\end{aligned}$$

$$\begin{aligned}
f_1 = 1 &= A\cdot\rho_1^1 + B\cdot\rho_2^1 \\
&= A\cdot\rho_1 + (-A)\cdot\rho_2 && \langle \textit{ Par l'équation } (\clubsuit) \rangle \\
&= A\cdot(\rho_1 - \rho_2) \\
\Leftrightarrow\; A &= \frac{1}{\rho_1 - \rho_2} \\
&= \frac{1}{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}} && \langle \textit{ Définitions de } \rho_1 \textit{ et } \rho_2 \rangle \\
&= \frac{1}{\sqrt{5}}\,, && \langle \textit{ Simplifications arithmétiques } \rangle \\
B &= -\frac{1}{\sqrt{5}}\,. && \langle \textit{ Substitution de la valeur de } A \textit{ dans } (\clubsuit) \rangle
\end{aligned}$$

Conclusion :

$$\text{Le terme général est} \quad f_n = \frac{1}{\sqrt{5}}\,\rho_1^n + \frac{-1}{\sqrt{5}}\,\rho_2^n \quad \forall n \in \mathbb{N}\,.$$

$$\text{Autrement dit :} \quad f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{-1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}\,.$$

2.5.4 Application aux relations de récurrence linéaires et homogènes

Une relation de récurrence est dite linéaire et homogène lorqu'elle répond à la définition suivante :

Définition 2.5.6. *Récurrence linéaire et homogène.*
Une relation de récurrence est dite linéaire, homogène d'ordre k *si la formule permettant de calculer* $n^{\text{ème}}$ *terme de la suite est une combinaison linéaire des* k *termes précédents.*

Voici quelques exemples de telles relations de récurrences :

— La relation de récurrence de la suite de Fibonacci (équation (2.3), page 151) est une relation linéaire, homogène d'ordre 2. En effet, la formule permettant de calculer le $n^{\text{ème}}$ terme de la suite est une combinaison linéaire des deux termes précédents :

$$f_n = 1 \cdot f_{n-1} + 1 \cdot f_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\}\,.$$

— La relation de récurrence suivante est une relation linéaire, homogène d'ordre 4 :

$$\begin{cases} a_0 = 9 \\ a_1 = \pi \\ a_2 = 3 \\ a_3 = 54 \\ a_n = 8 \cdot a_{n-2} + 7 \cdot a_{n-4} \qquad \forall n \in \mathbb{N} \setminus \{0,1,2,3\}\,. \end{cases}$$

Notons que la formule permettant de calculer a_n, le $n^{\text{ème}}$ terme de la suite, est bien une combinaison linéaire des 4 termes précédents puisque

$$a_n = 0 \cdot a_{n-1} + 8 \cdot a_{n-2} + 0 \cdot a_{n-3} + 7 \cdot a_{n-4}\,.$$

— La relation de récurrence d'une suite géométrique (définition 2.4.3, page 185) est une relation linéaire, homogène d'ordre 1.

On peut conclure du dernier exemple qu'il existe une formule permettant de résoudre très rapidement les relations de récurrence linéaire et homogènes d'ordre 1 (voir le théorème 2.4.4, page 185). Le prochain résultat (théorème 2.5.7) nous donne une formule permettant de résoudre très rapidement les relations de récurrences linéaires, homogènes d'ordre 2. Nous démonstrons ensuite ce théorème à l'aide de la méthode des séries génératrices.

Théorème 2.5.7. *Récurrences linéaires, homogènes d'ordre 2*
Soit $\langle a_n \rangle_{n\in\mathbb{N}}$ *une suite définie récursivement par :*

$$\begin{cases} a_0 &= a \\ a_1 &= b \\ a_n &= r \cdot a_{n-1} + s \cdot a_{n-2} \qquad \forall n \in \mathbb{N} \setminus \{0,1\}\,, \end{cases}$$

où a, b, r *et* s *sont des constantes réelles.*

Soit p, *le polynôme caractéristique de la suite* $\langle a_n \rangle_{n\in\mathbb{N}}$, *(c.-à-d. :* $p(x) = x^2 - rx - s$*).*
Et soit ρ_1 *et* ρ_2 *les zéros de ce polynôme.*

Alors, le terme général de la suite est :

$$\begin{array}{lrcll} \texttt{a}: & a_n & = & A \cdot (\rho_1)^n + B \cdot (\rho_2)^n & \forall n \in \mathbb{N} \qquad \textit{si } \rho_1 \neq \rho_2\,, \\ \texttt{b}: & a_n & = & A \cdot (\rho_1)^n + B \cdot n \cdot (\rho_1)^n & \forall n \in \mathbb{N} \qquad \textit{si } \rho_1 = \rho_2\,, \end{array}$$

où A *et* B *sont deux constantes déterminées par les conditions initiales de la récurrence (c.-à-d. : par* $a_0 = a$ *et* $a_1 = b$*).*

Démonstration du théorème 2.5.7 (Récurrences linéaires, homogènes d'ordre 2)
Soit $\langle a_n \rangle_{n\in\mathbb{N}}$ une suite telle que définie dans l'énoncé du théorème, p le polynôme caractéristique de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ et ρ_1, ρ_2 les zéros du polynôme p.

On désire démontrer que le terme général de la suite est :

$$\begin{array}{lrcll} \texttt{a}: & a_n & = & A \cdot (\rho_1)^n + B \cdot (\rho_2)^n & \forall n \in \mathbb{N} \qquad \text{si } \rho_1 \neq \rho_2\,, \\ \texttt{b}: & a_n & = & A \cdot (\rho_1)^n + B \cdot n \cdot (\rho_1)^n & \forall n \in \mathbb{N} \qquad \text{si } \rho_1 = \rho_2\,, \end{array}$$

On démontre séparément le cas où $\rho_1 \neq \rho_2$ et le cas où $\rho_1 = \rho_2$. Précisons que les deux cas sont des applications de la méthode des séries génératrices.

Cas 1 : $\rho_1 \neq \rho_2$.

La démonstration pour ce cas est très semblable à la solution de l'exemple de la suite de Fibonacci (voir page 205).

Étape 1 :

(on exprime la série génératrice sous la forme d'une fonction rationnelle)

- On remarque que : $a_n - r \cdot a_{n-1} - s \cdot a_{n-2} = 0 \qquad \forall n \in \mathbb{N} \setminus \{0,1\}\,;$
- ce qui en extension donne :
$$\begin{aligned} a_2 - ra_1 - sa_0 &= 0 \\ a_3 - ra_2 - sa_1 &= 0 \\ a_4 - ra_3 - sa_2 &= 0 \\ &\text{etc...} \end{aligned}$$
- Posons $G(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1\,x + a_2\,x^2 + a_3\,x^3 + \cdots + a_n\,x^n + \cdots.$

Alors,

$$\begin{array}{rcccccccc}
G(x) & = & a_0 + & a_1x + & a_2x^2 + & a_3x^3 + \cdots + & a_nx^n + \cdots \\
-rx \cdot G(x) & = & + & -ra_0x + & -ra_1x^2 + & -ra_2x^3 + \cdots + & -ra_{n-1}x^n + \cdots \\
-sx^2 \cdot G(x) & = & & & + -sa_0x^2 + & -sa_1x^3 + \cdots + & -sa_{n-2}x^n + \cdots \\
\hline
G(x) - rxG(x) - sx^2G(x) & = & a_0 + (a_1 - ra_0)x + & & 0x^2 + & 0x^3 + \cdots + & 0x^n + \cdots
\end{array}$$

Ce qui donne $G(x) - rx\,G(x) - sx^2\,G(x) \;=\; a_0 + (a_1 - ra_0)x$

Donc, on a :

$$\begin{aligned}
& G(x)(1 - rx - sx^2) \;=\; a_0 + (a_1 - ra_0)x \\
\Leftrightarrow\quad & G(x) \;=\; \frac{a_0 + (a_1 - ra_0)x}{1 - rx - sx^2} \\
& \;=\; \frac{a_0 + (a_1 - ra_0)x}{(1 - \rho_1\,x)\;(1 - \rho_2\,x)}\,. \qquad \left\langle \begin{array}{l} \textit{Proposition 2.5.5, avec } q(x) := 1 - rx - sx^2. \\ \textit{Les deux zéros de } p(x) \;=\; x^2 - rx - s \textit{ étant} \\ \textit{par hypothèse } \rho_1 \textit{ et } \rho_2. \end{array} \right\rangle
\end{aligned}$$

Étape 2 : (on trouve la série de puissances associée à G)

$$\begin{aligned}
G(x) \;&=\; \frac{a_0 + (a_1 - ra_0)x}{(1 - \rho_1 x)(1 - \rho_2 x)} \\
&=\; \frac{A}{1 - \rho_1 x} + \frac{B}{1 - \rho_2 x} && \langle\ \textit{Théorème 2.5.3-a}\ \rangle \\
&=\; \sum_{i=0}^{\infty} A \cdot (\rho_1)^i\, x^i \;+\; \sum_{i=0}^{\infty} B \cdot (\rho_2)^i\, x^i && \langle\ \textit{Théorème 2.5.1-a (2 fois)}\ \rangle \\
&=\; \sum_{i=0}^{\infty} \Big[A \cdot (\rho_1)^i + B \cdot (\rho_2)^i\Big]\, x^i\,. && \langle\ \textit{Arithmétique}\ \rangle
\end{aligned}$$

Étape 3 : (on trouve le terme général de la suite)

La définition par terme général est bien : $\quad a_n \;=\; A\,(\rho_1)^n + B\,(\rho_2)^n \quad \forall n \in \mathbb{N}\,.$

$\langle$ **Cas 1 démontré** $\rangle$

Cas 2 : $\rho_1 = \rho_2$.

Étape 1 :

(on exprime la série génératrice sous la forme d'une fonction rationnelle)

L'étape 1 est presque identique à celle que nous avons faite pour le cas 1.

On pose d'abord

$$G(x) \;=\; \sum_{i=0}^{\infty} a_i x^i \;=\; a_0 \,+\, a_1\,x \,+\, a_2\,x^2 \,+\, a_3\,x^3 \,+\, \cdots \,+\, a_n\,x^n \,+\, \cdots\,.$$

En reproduisant la démarche de l'étape 1 du cas 1, on obtient :

$$G(x) \;=\; \frac{a_0 + (a_1 - r a_0)x}{(1-\rho_1\,x)\;(1-\rho_2\,x)}\,,$$

où ρ_1 et ρ_2 sont les zéros du polynôme $p(x) \;=\; x^2 - rx - s$.

Comme nous sommes dans le cas où $\rho_1 = \rho_2$, on a :

$$G(x) \;=\; \frac{a_0 + (a_1 - r a_0)x}{(1-\rho_1\,x)^2}\,.$$

Étape 2 : (on trouve la série de puissances associée à G)

$$\begin{aligned}
G(x) &= \frac{a_0 + (a_1 - r a_0)x}{(1-\rho_1\,x)^2} \\
&= \frac{C}{(1-\rho_1\,x)} + \frac{D}{(1-\rho_1\,x)^2} && \langle\ \textit{Théorème 2.5.3-b}\ \rangle \\
&= \sum_{i=0}^{\infty} C\cdot(\rho_1)^i\,x^i \;+\; \sum_{i=0}^{\infty}(i+1)\,D\cdot(\rho_1)^i\,x^i && \left\langle \begin{array}{l}\textit{Théorème 2.5.1-a et}\\ \textit{théorème 2.5.1-b}\end{array}\right\rangle \\
&= \sum_{i=0}^{\infty}\Big[C\cdot(\rho_1)^i + (i+1)\,D\cdot(\rho_1)^i\Big]\,x^i\,. && \langle\ \textit{Arithmétique}\ \rangle
\end{aligned}$$

Étape 3 : (on trouve le terme général de la suite)

$$\begin{array}{lll}
\text{Le terme général est} & a_n = C\,(\rho_1)^n + (n+1)\cdot D\,(\rho_1)^n & \forall n\in\mathbb{N}. \\
\text{Ce qui est équivalent à} & a_n = C\,(\rho_1)^n + n\cdot D\,(\rho_1)^n + D\,(\rho_1)^n & \forall n\in\mathbb{N}. \\
\text{Ce qui est équivalent à} & a_n = (C+D)\,(\rho_1)^n + n\cdot D\,(\rho_1)^n & \forall n\in\mathbb{N}.
\end{array}$$

Ce qui, si on pose $[A := C + D]$ et $[B := D]$, est équivalent à :

$$a_n = A\,(\rho_1)^n + n\cdot B\,(\rho_1)^n \quad \forall n\in\mathbb{N}\,.$$

$\langle$ **Cas 2 démontré** $\rangle$

C.Q.F.D.

Exemple de la suite de Fibonacci

Utilisons le théorème 2.5.7 pour trouver le terme général de la suite de Fibonacci :

$$\begin{cases} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\}\,. \end{cases}$$

(1) Trouvons la "forme" du terme général de la suite.

Le polynôme caractéristique de la suite $\langle f_n \rangle_{n\in\mathbb{N}}$ est $p(x) = x^2 - (1)\cdot x - (1)$.

Et les deux zéros de ce polynôme sont

$$\rho_1 = \frac{-(-1) + \sqrt{(-1)^2 - 4\cdot 1\cdot(-1)}}{2\cdot 1} = \frac{1+\sqrt{5}}{2}\,,$$
$$\rho_2 = \frac{-(-1) - \sqrt{(-1)^2 - 4\cdot 1\cdot(-1)}}{2\cdot 1} = \frac{1-\sqrt{5}}{2}\,.$$

Donc, par le théorème 2.5.7, la forme du terme général de la suite est

$$f_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}\,,$$

où A et B sont deux constantes.

(2) Trouvons les valeurs des constantes A et B.

On sait que $\begin{cases} A\left(\frac{1+\sqrt{5}}{2}\right)^0 + B\left(\frac{1-\sqrt{5}}{2}\right)^0 = f_0 = 0 \\ A\left(\frac{1+\sqrt{5}}{2}\right)^1 + B\left(\frac{1-\sqrt{5}}{2}\right)^1 = f_1 = 1 \end{cases}$

Ce qui donne $\begin{cases} A + B = 0 \\ A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = 1 \end{cases}$

En résolvant, on trouve facilement que $A = \dfrac{1}{\sqrt{5}}$ et $B = \dfrac{-1}{\sqrt{5}}$.

(3) Le terme général cherché est :

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{-1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}\,.$$

2.5.5 Exercices sur la méthode des séries génératrices

Exercice 1 : Exprimez les séries génératrices des suites suivantes sous forme de fonctions rationnelles :

a) $\begin{cases} a_0 &= 1 \\ a_n &= 2 \cdot a_{n-1} + 3^n \quad \forall n \in \mathbb{N}^* \end{cases}$ *b)* $\begin{cases} b_0 &= 1 \\ b_n &= b_{n-1} + n \quad \forall n \in \mathbb{N}^* \end{cases}$

c) $\begin{cases} c_0 &= 1 \\ c_1 &= 1 \\ c_n &= c_{n-1} + c_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$ *d)* $\begin{cases} d_0 &= 1 \\ d_1 &= 1 \\ d_n &= 4 \cdot d_{n-1} - 4 \cdot d_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

Exercice 2 : Décomposez en fractions partielles les fonctions rationnelles suivantes :

a) $a(x) = \dfrac{1}{(x+4)(x+3)}$ *b)* $b(x) = \dfrac{x}{(1-x)^2(1+x)}$ *c)* $c(x) = \dfrac{x}{(x-1)(x-2)(x-3)}$

d) $d(x) = \dfrac{1-3x}{1-4x+4x^2}$ *e)* $e(x) = \dfrac{1-3x}{(1-2x)^2}$ *f)* $f(x) = \dfrac{x^2+2x+3}{(x-1)^2\,(x-2)}$

Exercice 3 : Trouvez la série de puissances associée à chacune des fonctions suivantes.

a) $a(x) = \dfrac{1}{(1-5x)}$ *b)* $b(x) = \dfrac{3}{x-5}$ *c)* $c(x) = \dfrac{\frac{3}{2}}{1-2x} + \dfrac{\frac{-1}{2}}{(1-2x)^2}$

Exercice 4 : Pour chacune des suites définies par récurrence suivantes, résolvez la récurrence par la méthode des séries génératrices.

a) $\begin{cases} a_0 &= 2 \\ a_n &= 3a_{n-1} + 2^n \quad \forall n \in \mathbb{N}^* \end{cases}$

b) $\begin{cases} b_0 &= 0 \\ b_n &= b_{n-1} + n \quad \forall n \in \mathbb{N}^* \end{cases}$

c) $\begin{cases} c_0 &= 1 \\ c_1 &= 8 \\ c_n &= 6 \cdot c_{n-1} - 9 \cdot c_{n-2} + 2^n \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

Exercice 5 : Trouvez le terme général de la suite suivante :

$$\begin{cases} d_0 &= 1 \\ d_1 &= 8 \\ d_n &= 6 \cdot d_{n-1} - 9 \cdot d_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\}\,. \end{cases}$$

Exercice 6 : En utilisant le théorème sur les récurrences linéaires homogènes d'ordre 2, exprimez les suites suivantes sous forme de fonctions rationnelles :

a) $\begin{cases} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

b) $\begin{cases} b_0 &= 2 \\ b_1 &= 6 \\ b_n &= b_{n-1} + b_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

c) $\begin{cases} c_0 &= 1 \\ c_1 &= 4 \\ c_n &= 4 \cdot c_{n-1} - 4 \cdot c_{n-2} \ \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

d) $\begin{cases} d_0 &= 1 \\ d_1 &= 1 \\ d_n &= 4 \cdot d_{n-1} - 4 \cdot d_{n-2} \ \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

2.6 Approximation par une intégrale

Jusqu'à maintenant, ce chapitre a présenté des méthodes permettant de calculer le terme général *exact* d'une suite. Ces méthodes ne s'appliquent malheureusement pas dans tous les cas, et on se contente parfois d'approximer le terme général d'une suite.

La méthode d'**approximation par une intégrale** présentée dans cette section permet *dans certains cas* de calculer une borne inférieure et une borne supérieure d'une suite que exprimée sous la forme d'une somme. Typiquement, on a recours à cette méthode lorsque la méthode des substitutions à rebours (section 2.2) nous a permis de transformer une définition par récurrence d'une suite en une somme en notation sigma, mais que nous ne connaissons aucune propriété qui permet de transformer cette somme en un terme général.

2.6.1 Description de la méthode

Supposons que le terme général d'une suite $\langle a_n \rangle_{n\in\mathbb{N}}$ est exprimé par une somme des valeurs d'une fonction f évaluée de 0 à n. Autrement dit, $a_n = f(0) + f(1) + f(2) + \ldots + f(n)$ ou, de manière équivalente :

$$a_n \;=\; \sum_{i=0}^{n} f(i) \qquad \forall n \in \mathbb{N}\,.$$

Nous pouvons représenter géométriquement le terme a_n comme l'aire cumulative de $n+1$ rectangles de largeur 1 et de hauteurs $f(0), f(1), f(2), \ldots, f(n)$. Il parait donc naturel d'approximer le terme général de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ en calculant l'aire sous la courbe de la fonction f pour un intervalle de valeurs judicieusement choisies. Il s'agit de l'idée sur laquelle est basée la méthode d'approximation par une intégrale.

Afin d'appliquer cette méthode, on doit d'abord s'assurer que f est une fonction non décroissante ou encore une fonction non croissante sur l'intervalle de valeurs qui nous intéresse. Une **fonction non décroissante** sur l'intervalle $[a, b]$ est une fonction qui est croissante ou constante pour tout $x \in [a, b]$. De même, une **fonction non croissante** sur l'intervalle $[a, b]$ est une fonction qui est décroissante ou constante pour tout $x \in [a, b]$.

Définition 2.6.1. *Fonctions non décroissantes et fonctions non croissantes.*
Soit une fonction $f \subset \mathbb{R}^2$ *et un intervalle* $[a,b] \subseteq \mathrm{Dom}(f)$. *On dit que :*

a : f *est non décroissant sur* $[a,b] \quad \Leftrightarrow \quad (\forall x,y \in [a,b] \mid x<y \Rightarrow f(x) \leq f(y))$

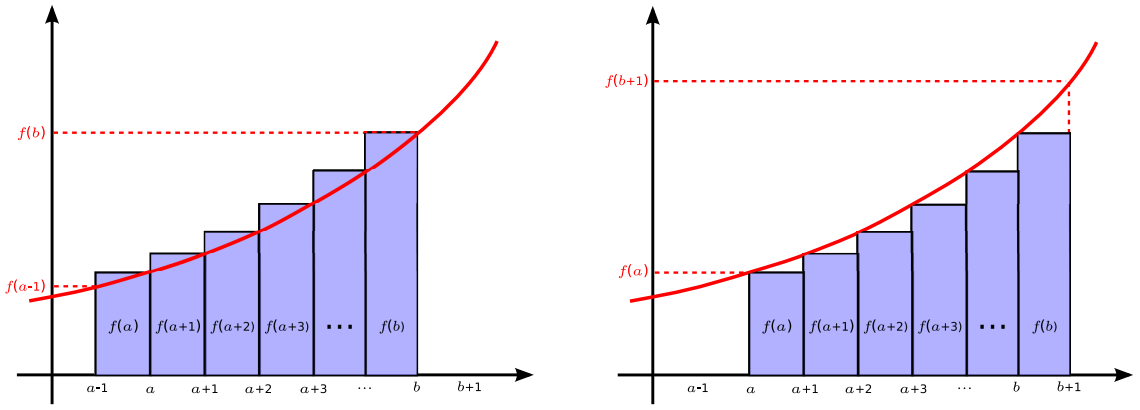
b : f *est non croissant sur* $[a,b] \quad \Leftrightarrow \quad (\forall x,y \in [a,b] \mid x<y \Rightarrow f(x) \geq f(y))$

Le théorème 2.6.2 suivant permet de calculer une borne inférieure et une borne supérieure d'une somme. Bien que nous ne démontrons pas ce théorème, la figure 2.3 en donne une interprétation géométrique qui permet de bien comprendre l'astuce derrière cette méthode.

Théorème 2.6.2. *Bornes d'une somme.*
Soit une fonction $f \subset \mathbb{R}^2$. *Alors :*

a : $\displaystyle\int_{a-1}^{b} f(x)dx \leq \sum_{i=a}^{b} f(i) \leq \int_{a}^{b+1} f(x)dx$ *si* f *est non décroissant sur* $[a-1,b+1]$

b : $\displaystyle\int_{a}^{b+1} f(x)dx \leq \sum_{i=a}^{b} f(i) \leq \int_{a-1}^{b} f(x)dx$ *si* f *est non croissant sur* $[a-1,b+1]$



(a) Borne inférieure d'une somme. (b) Borne supérieure d'une somme.

FIGURE 2.3 – Illustration du théorème 2.6.2-a : Bornes de la somme des valeurs d'une fonction f non décroissante évaluée entre a et b.

2.6.2 Bref rappel sur le calcul intégral

Voici quelques formules d'intégration couramment utilisées :

$$\texttt{a}: \int k \cdot dx = k \cdot x + C \qquad \texttt{b}: \int x^a \cdot dx = \frac{x^{a+1}}{a+1} + C \text{ pour } a \neq -1$$

$$\texttt{c}: \int \frac{1}{x} \cdot dx = \ln|x| + C \qquad \texttt{d}: \int \frac{c}{a\,x+b} \cdot dx = \frac{c}{a} \ln|a\,x+b| + C$$

$$\texttt{e}: \int e^x \cdot dx = e^x + C \qquad \texttt{f}: \int a^x \cdot dx = \frac{a^x}{\ln a} + C$$

$$\texttt{g}: \int \ln x \cdot dx = x \ln x - x + C \qquad \texttt{h}: \int \log_a x \cdot dx = x \log_a x - \frac{x}{\ln a} + C$$

$$\texttt{i}: \int \Big(f(x) + g(x) \Big) \cdot dx = \int f(x) \cdot dx + \int g(x) \cdot dx$$

En notant $F = \int f(x) \cdot dx$, l'intégrale selon x de la fonction $f(x)$ sur l'intervalle $[a, b]$ est donnée par :

$$\int_a^b f(x) \cdot dx = \Big[F(x) \Big]_a^b = F(b) - F(a)\,.$$

Par exemple : $\displaystyle\int_{-2}^{4} x^2 \cdot dx = \left[\frac{x^3}{3} \right]_{-2}^{4} = \frac{4^3}{3} - \frac{(-2)^3}{3} = \frac{64-(-8)}{3} = \frac{72}{3} = 24\,.$

2.6.3 Quelques exemples

Exemple 1 : Somme des nombres cubiques

On s'intéresse à la suite $\langle C_n \rangle_{n \in \mathbb{N}^*}$ correspondant à la somme nombres cubiques que l'on définit ainsi :

$$C_n = \sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \ldots + n^3 \quad \forall n \in \mathbb{N}^*\,.$$

En supposant que nous ne connaissons pas la règle qui permet de calculer directement le terme général de cette suite, nous allons utiliser l'approximation par une intégrale pour obtenir une borne inférieure et une borne supérieure de C_n.

Remarquons d'abord que $f(x) = x^3$ est une fonction non décroissante sur l'intervalle

$[0, n+1]$ pour tout $n \geq 1$. Calculons l'intégrale selon la variable x de la fonction $f(x)$:

$$\int x^3 \cdot dx \;=\; \frac{x^4}{4} + C\,.$$

En appliquant le théorème 2.6.2-a, nous obtenons :

$$\begin{array}{rrcccl} & \left[\frac{x^4}{4}\right]_0^n & \leq & \sum_{i=1}^{n} i^3 & \leq & \left[\frac{x^4}{4}\right]_1^{n+1} \\ \Leftrightarrow & \frac{n^4}{4} - \frac{0^4}{4} & \leq & \sum_{i=1}^{n} i^3 & \leq & \frac{(n+1)^4}{4} - \frac{1^4}{4} \\ \Leftrightarrow & \frac{n^4}{4} & \leq & \sum_{i=1}^{n} i^3 & \leq & \frac{(n+1)^4 - 1}{4}\,. \end{array}$$

Ainsi, $\quad \frac{n^4}{4} \;\leq\; C_n \;\leq\; \frac{(n+1)^4 - 1}{4} \quad \forall n \in \mathbb{N}^*\,.$

Exemple 2 : La récurrence des tours de Hanoï

À la section 2.2-a, nous avons formulé la définition par récurrence de la suite $\langle h_n \rangle_{n\in\mathbb{N}}$, qui donne le nombre optimal de déplacements nécessaires pour résoudre le problème des tours de Hanoï (équation (2.8), page 165). Lorsque nous avons appliqué la méthode des substitutions à rebours à la définition par récurrence de la suite donnant le nombre optimal de déplacements nécessaires pour résoudre le problème des tours de Hanoï (page 166), nous avons exprimé le terme h_n par une somme :

$$h_n \;=\; \sum_{j=0}^{n-1} 2^j \qquad \forall n \in \mathbb{N}\,.$$

À la section 2.4.3, nous avons constaté que cette somme correspond à un cas particulier de récurrence, c'est-à-dire que la suite $\langle h_n \rangle_{n\in\mathbb{N}}$ est la somme des premiers termes d'une suite géométrique (équation (2.12), page 190).

Pour les besoins de cet exemple, nous supposons ici que nous n'avons pas connaissance du cas particulier des sommes de premiers termes de suite géométrique. Dans cette situation, nous pouvons utiliser la méthode d'approximation par une intégrale pour borner la valeur des termes de la suite $\langle h_n \rangle_{n\in\mathbb{N}}$.

Remarquons d'abord que $f(x) = 2^x$ est une fonction non décroissante sur l'intervalle

$[-1, n]$ pour tout $n \geq 0$. Calculons l'intégrale selon la variable x de la fonction $f(x)$:

$$\int 2^x \cdot dx \;=\; \frac{2^x}{\ln 2} + C\,.$$

En appliquant le théorème 2.6.2, nous obtenons :

$$\begin{array}{rcccl} & \left[\dfrac{2^x}{\ln 2}\right]_{-1}^{n-1} & \leq & \displaystyle\sum_{j=0}^{n-1} 2^j & \leq & \left[\dfrac{2^x}{\ln 2}\right]_{0}^{n} \\ \Leftrightarrow & \dfrac{2^{n-1}}{\ln 2} - \dfrac{2^{-1}}{\ln 2} & \leq & \displaystyle\sum_{j=0}^{n-1} 2^j & \leq & \dfrac{2^n}{\ln 2} - \dfrac{2^0}{\ln 2} \\ \Leftrightarrow & \dfrac{2^{n-1} - \frac{1}{2}}{\ln 2} & \leq & \displaystyle\sum_{j=0}^{n-1} 2^j & \leq & \dfrac{2^n - 1}{\ln 2}\,. \end{array}$$

Ainsi, $\dfrac{2^{n-1} - \frac{1}{2}}{\ln 2} \;\leq\; h_n \;\leq\; \dfrac{2^n - 1}{\ln 2} \quad \forall n \in \mathbb{N}\,.$

Exemple 3 : Somme des inverses des premiers nombres naturels

Approximons par une intégrale la suite $\langle I_n \rangle_{n \in \mathbb{N}^*}$ suivante :

$$I_n \;=\; \sum_{i=1}^{n} \frac{1}{i} \;=\; \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n} \quad \forall n \in \mathbb{N}^*\,.$$

Nous considérons la fonction $f(x) = \frac{1}{x}$. Calculons l'intégrale de $f(x)$ selon x :

$$\int \frac{1}{x} \cdot dx \;=\; \ln x + C\,.$$

Remarquons que $f(0)$ n'est pas défini (car $\frac{1}{0}$ est indéfini). Pour pouvoir appliquer le théorème 2.2, réécrivons la définition de $\langle I_n \rangle_{n \in \mathbb{N}^*}$:

$$I_n \;=\; \sum_{i=1}^{n} \frac{1}{i} \;=\; 1 + \sum_{i=2}^{n} \frac{1}{i} \quad \forall n \in \mathbb{N}^*\,.$$

Nous appliquons maintenant le 2.2-b. Comme la fonction $f(x) = \frac{1}{x}$ est non croissante sur

l'intervalle $[1, n+1]$ pour tout $n \geq 1$, nous avons :

$$\begin{array}{rrcccl} & \Big[\ln x\Big]_2^{n+1} & \leq & \displaystyle\sum_{i=2}^{n} \frac{1}{i} & \leq & \Big[\ln x\Big]_1^{n} \\ \Leftrightarrow & \ln(n+1) - \ln(2) & \leq & \displaystyle\sum_{i=2}^{n} \frac{1}{i} & \leq & \ln(n) - \ln(1) \\ \Leftrightarrow & \ln\left(\frac{n+1}{2}\right) & \leq & \displaystyle\sum_{i=2}^{n} \frac{1}{i} & \leq & \ln(n) \\ \Leftrightarrow & 1 + \ln\left(\frac{n+1}{2}\right) & \leq & 1 + \displaystyle\sum_{i=2}^{n} \frac{1}{i} & \leq & 1 + \ln(n)\,. \end{array}$$

Ainsi, $\quad 1 + \ln\left(\dfrac{n+1}{2}\right) \;\leq\; I_n \;\leq\; 1 + \ln(n) \quad \forall n \in \mathbb{N}^*\,.$

2.6.4 Exercices sur l'approximation par une intégrale

Exercice 1 : En vous inspirant de la figure 2.3 (page 215), illustrez le théorème 2.6.2-b qui permet de borner une somme possédant la forme suivante :

$$\sum_{i=a}^{b} f(i), \quad \text{où } f \text{ est une fonction } \textit{non croissante} \text{ sur l'intervalle } [a-1, b+1]\,.$$

Exercice 2 : En appliquant la méthode d'approximation par une intégrale, trouvez une borne inférieure et une borne supérieure des suites suivantes.

a) $a_n = 5 \cdot \sum_{i=1}^{n} i^4 \quad \forall n \in \mathbb{N}^*\,.$

b) $b_n = 5 \cdot \sum_{i=-2}^{n} i^4 \quad \forall n \in \mathbb{N}^*\,.$

c) $c_n = \sum_{i=1}^{n} i^k \quad \forall n \in \mathbb{N}^* \quad$ (où $k \in \mathbb{N}^*$ est une constante).

d) $d_n = \sum_{i=1}^{n} \frac{1}{i^2} \quad \forall n \in \mathbb{N}^*$..

e) $e_n = \sum_{i=1}^{n} (i + \ln i - 1) \quad \forall n \in \mathbb{N}^*\,.$

f) $f_n = \log(n!) \quad \forall n \in \mathbb{N}^*\,.$
Rappels : $n! \stackrel{\text{def}}{=} 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ et $\log(a \cdot b) = \log a + \log b \;\; \forall a, b > 0$

Exercice 3 : Décrivez une circonstance où la méthode d'approximation par une intégrale donne la valeur exacte de la somme. Autrement dit, exprimez une fonction f pour laquelle les bornes inférieure et supérieure obtenues par le théorème 2.6.2 sont égales à la valeur de la somme.

Chapitre 3

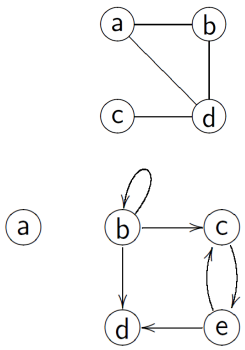
Théorie des graphes

Un graphe est une structure mathématique qui contient des **sommets**, dont certains sont reliés entre eux par des **arêtes**. Selon le contexte, les arêtes d'un graphe peuvent posséder ou non une orientation. Dans ce document, le terme **graphe** employé seul désigne un graphe dont les arêtes ne sont pas orientées et le terme **digraphe** désigne un graphe dont les arêtes sont orientées. Le terme **arc** désigne plus spécifiquement une arête orientée d'un digraphe.

On utilise la notation suivante :

— Étant donné un graphe G_1, on note l'ensemble de ses sommets "$V(G_1)$" et l'ensemble de ses arêtes "$E(G_1)$". Ainsi, si les sommets a et b de G_1 sont reliées par une arête, on a $a \in V(G_1)$, $b \in V(G_1)$ et $[a, b] \in E(G_1)$. Le choix des lettres V et E provient des termes anglais "Vertices" et "Edges".

— Étant donné un digraphe G_2, on note l'ensemble de ses sommets "$V(G_2)$" et l'ensemble de ses arcs "$A(G_2)$". Ainsi, si G_2 possède un arc du sommet e et vers le sommet d, on a $e \in V(G_2)$, $d \in V(G_2)$ et $\langle e, d\rangle \in A(G_2)$.



$$\begin{aligned} E(G_1) &= \{\, [a,b], [a,d], [b,d], [c,d] \,\} \\ V(G_1) &= \{\, a, b, c, d \,\} \end{aligned}$$

$$\begin{aligned} A(G_2) &= \{\, \langle b,b\rangle, \langle b,c\rangle, \langle b,d\rangle, \langle c,e\rangle, \langle e,c\rangle, \langle e,d\rangle \,\} \\ V(G_2) &= \{\, a, b, c, d, e \,\} \end{aligned}$$

FIGURE 3.1 – Exemples d'un graphe G_1 et d'un digraphe G_2.

Plusieurs problèmes se représentent naturellement par un graphe. Nous n'avons qu'à penser à une carte géographique (où les villes sont des sommets et les routes sont des arêtes), un réseau informatique (constitué d'ordinateurs reliés par des câbles optiques), un circuit électronique (constitué de puces reliées par des circuits imprimés), etc.

La théorie des graphes est aussi utilisée pour représenter beaucoup d'autres problèmes qui ne s'apparentent pas à un graphe au premier coup d'oeil. Quelques-uns de ces problèmes sont la création d'horaires, l'assemblage d'un génome humain et la gestion de l'espacement entre les mots par un traitement de texte afin que toutes les lignes d'un paragraphe soient justifiées (de longueur pleine).

3.1 Éléments de base

Cette section présente une série de définitions souvent utilisées en théorie des graphes. Nous faisons par la suite référence à ces définitions au besoin dans les sections subséquentes.

3.1.1 Graphes et digraphes

Les définitions 3.1.1 et 3.1.2 présentent les graphes et les digraphes comme des cas particuliers de relations. Cependant, une relation est, dans la plupart des cas, présentée par une règle d'association, liant certains éléments de l'ensemble de départ et de l'ensemble d'arrivé. Généralement, on considère un graphe (ou un digraphe) comme un objet en soi, et on en étudie la structure. Ainsi, on réfère habituellement explicitement aux sommets et aux arêtes pour définir un graphe, que ce soit par des ensembles définis en extension ou par un dessin, tel qu'illustré par la figure 3.1. Les problèmes étudiés par la théorie des graphes ne sont donc pas les mêmes que ceux étudiés à l'aide des relations. C'est pourquoi la théorie des graphes est une branche distincte des mathématiques.

Définition 3.1.1. *Graphes, sommets et arêtes*

a : *Un* **graphe** *(ou* **graphe non orienté***) est une relation binaire symétrique et irreflexive.*

b : *Si G est un graphe, les éléments sur lesquels la relation G est définie sont appelés les* **sommets** *du graphe G. L'ensemble de tous les sommets de G est noté $V(G)$.*

c : *Si deux sommets x et y sont en relation dans un graphe G (autrement dit, $\langle x, y\rangle \in G$ et $\langle y, x\rangle \in G$), on dit qu'il y a une* **arête** *entre x et y et cette arête est notée $[x, y]_G$ ou*

$[y,x]_G$ *(ou simplement* $[x,y]$ *ou* $[y,x]$ *s'il n'y a aucune confusion possible). L'ensemble de toutes les arêtes de* G *est noté* $E(G)$.

Les sommets x et y sont appelés les **extrémités** de l'arête $[x,y]_G$ et cette arête est dite une **arête incidente** au sommet x et au sommet y. De plus les sommets x et y seront dit **adjacents** (ou *voisins*) dans G. Insistons sur le fait que $[x,y]_G = [y,x]_G$.

Définition 3.1.2. *Digraphes, sommets et arcs.*

a : *Un* **digraphe** *(ou* **graphe orienté***) est une relation binaire.*

b : *Si* G *est un digraphe, les éléments sur lesquels la relation* G *est définie sont appelés les* **sommets** *du digraphe* G*. L'ensemble de tous les sommets de* G *est noté* $V(G)$.

c : *Si deux sommets* x *et* y *sont en relation dans un digraphe* G *tel que* $x\,G\,y$ *(autrement dit,* $\langle x,y\rangle \in G$*), on dit qu'il* y *a un* **arc** *de* x *vers* y *et cet arc est noté* $\langle x,y\rangle_G$ *(ou simplement* $\langle x,y\rangle$ *s'il n'y a aucune confusion possible). L'ensemble de tous les arcs de* G *est noté* $A(G)$.

Les sommets x et y sont respectivement appelés l'**origine** et la **destination** de l'arc $\langle x,y\rangle_G$, et cet arc est dit un **arc sortant** du sommet x et un **arc entrant** du sommet y. Un arc $\langle x,x\rangle_G$ ayant le même sommet d'origine et de destination est dit une **boucle**.

Définition 3.1.3. *Cas particuliers de graphes.*

a : *Un* **graphe régulier** *d'ordre* k *est un graphe dont tous ses sommets sont de degré* k.

b : *Un* **graphe complet** *d'ordre* n *(noté* K_n*) est un graphe qui a exactement* n *sommets et où pour tout* $x,y \in V(K_n)$ *tels que* $x \neq y$*, on a* $[x,y] \in E(K_n)$.

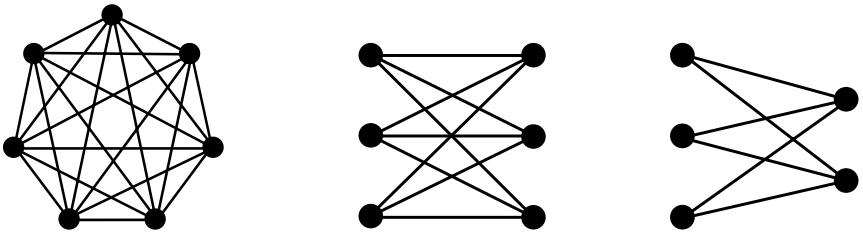
c : *Un graphe* G *est un* **graphe biparti** *de bipartition* A *et* B *si*
- *—* A *et* B *forment une bipartition de* $V(G)$ *(c.-à-d. :* $A \cap B = \emptyset$ *et* $V(G) = A \cup B$*), et*
- *— pour toute arête de* G*, une extrémité appartient à* A *et l'autre à* B.

d : *Un* **graphe biparti complet** *d'ordres* n *et* m *(noté* $K_{n,m}$*) est un graphe biparti de bipartition* A *et* B *tel que* $|A| = n$ *et* $|B| = m$*, et pour tout* $\langle x,y\rangle \in A \times B$*, on a* $[x,y] \in E(K_{n,m})$.

3.1.2 Voisins et degré d'un sommet

Définition 3.1.4. *Voisins et degré d'un sommet*

Étant donné un sommet x *d'un graphe* G*,*



(a) Graphe K_7 (b) Graphe $K_{3,3}$ (c) Graphe $K_{3,2}$

FIGURE 3.2 – Exemples d'un graphe complet (définition 3.1.3-b) et de deux graphes bipartis complets (définition 3.1.3-d).

a : *Un sommet $y \in V(G)$ est un* **voisin** *du sommet $x \in V(G)$ lorsque G possède une arête $[x, y]_G$. L'ensemble de tous les voisins de x dans G est noté $\mathcal{N}_G(x)$.*

b : *Le* **degré** *de x dans G est égal au nombre de voisins x dans G, et est noté* $\deg_G(x)$. *Autrement dit* $\deg_G(x) = \left|\mathcal{N}_G(x)\right|$.

À titre d'exemple, le graphe G_1 présenté à la figure 3.1 est tel que :

$$\mathcal{N}_{G_1}(a) \;=\; \{b, d\} \quad \text{et} \quad \mathcal{N}_{G_1}(c) \;=\; \{d\}\,.$$

3.1.3 Sous-graphes et décompositions

Définition 3.1.5. *Sous-graphes.*

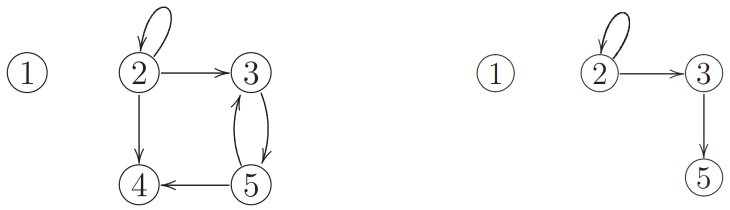
a : *Un graphe H est dit* **sous-graphe** *d'un graphe G (noté : $H \lhd G$) si :*
$V(H) \subseteq V(G) \quad$ *et* $\quad E(H) \subseteq E(G)\,.$

b : *Un graphe H est un* **sous-graphe couvrant** *d'un graphe G (ou* sous-graphe partiel*) si :*
$H \lhd G \quad$ *et* $\quad V(H) = V(G)\,.$

c : *Un graphe H est un* **sous-graphe induit** *d'un graphe G si :*
$H \lhd G \quad$ *et* $\quad \big(\ \forall x, y \in V(H) \mid [x, y] \in E(G) \Rightarrow [x, y] \in E(H)\ \big)\,.$

La définition 3.1.5 ci-haut se généralise directement au cas des digraphes en remplaçant simplement les ensembles d'arêtes $E(G)$ et $E(H)$ par les ensembles d'arcs $A(G)$ et $A(H)$. Comme le montre l'exemple de la figure 3.3, un digraphe H est un **sous-digraphe** d'un digraphe G (noté : $H \lhd G$) si $V(H) \subseteq V(G)$ et $A(H) \subseteq A(G)$.

Définition 3.1.6. *Décomposition d'un graphe.*
Une **décomposition** *d'un graphe G est un ensemble de sous-graphes $\{H_1, H_2, \ldots, H_l\}$ tel que chaque arête de G appartient à un et un seul membre de la décomposition.*



(a) Digraphe G (b) Digraphe H

FIGURE 3.3 – Exemples de deux digraphes G et H qui ont la propriété $H \lhd G$, c'est-à-dire que H est un sous-graphe de G (mais il n'est pas induit).

Similairement, une *décomposition* d'un digraphe G est un ensemble de sous-graphes tel que chaque arc de G appartient à un et un seul membre de la décomposition.

3.1.4 Chaînes, chemins et cycles

Définition 3.1.7. *Chaînes.*
Soit G un graphe.

a : *Une* **chaîne** *de G est une séquence de la forme*

$$\langle\, x_1,\, [x_1, x_2],\, x_2,\, [x_2, x_3],\, x_3,\, \ldots\,,\, x_{n-1},\, [x_{n-1}, x_n],\, x_n \,\rangle\,.$$

Les sommets x_1 et x_n sont appelés les extrémités *de la chaîne.*

b : *Une* **chaîne simple** *de G est une chaîne où chaque arête apparaît au plus une fois.*

c : *Une* **chaîne élémentaire** *de G est une chaîne simple où chaque sommet de G apparaît au plus une fois, à l'exception des deux extrémités qui peuvent être égales.*

d : *Étant donnés $A, B \subseteq V(G)$, une AB-***chaîne** *de G est une chaîne dont une extrémité appartient à A et l'autre à B.*

e : *Étant donnés $x, y \in V(G)$, une xy-***chaîne** *de G est une $\{x\}\{y\}$-chaîne.*

Pour simplifier la notation, une chaîne $\langle\, x_1,\, [x_1, x_2],\, x_2,\, \ldots\,,\, x_{n-1},\, [x_{n-1}, x_n],\, x_n \,\rangle$ qui est simple ou élémentaire pourra être simplement notée $\langle\, x_1,\, x_2,\, x_3,\, \ldots\,,\, x_{n-1},\, x_n \,\rangle$.

Dans un digraphe, on désigne par le terme **chemin** une séquence de la forme :

$$\langle\, x_1,\, \langle x_1, x_2\rangle\,,\, x_2,\, \langle x_2, x_3\rangle\,,\, x_3,\, \ldots\,,\, x_{n-1},\, \langle x_{n-1}, x_n\rangle\,,\, x_n \,\rangle\,.$$

Un **chemin simple** est un chemin où chaque arc apparaît au plus une fois et un **chemin élémentaire** est un chemin simple où chaque sommet de G apparaît au plus une fois.

Définition 3.1.8. *Cycles*

a : *Un* **cycle** *(ou cycle simple) est une chaîne simple dont les deux sommets extrémités sont identiques.*

b : *Un* **cycle élémentaire** *est une chaîne élémentaire dont les deux sommets extrémités sont identiques.*

3.1.5 Connexité d'un graphe

Définition 3.1.9. *Graphes connexes.*
Un graphe G est **connexe** *si pour toute paire x, y de sommets de G, il existe une chaîne dont les extrémités sont x et y.*

Définition 3.1.10. *Digraphes fortement et faiblement connexes.*

a : *Un digraphe G est* **fortement connexe** *si pour toute paire x, y de sommets de G, il existe un chemin du sommet x au sommet y et un chemin du sommet y au sommet x.*

b : *Un digraphe G est* **faiblement connexe** *si le graphe sous-jacent est connexe,*

Dans la dernière définition, on considère qu'un **graphe sous-jacent** au digraphe G est un graphe G' tel que $V(G') = V(G)$ et $E(G') = \{[x, y] \mid \langle x, y\rangle \in A(G)\}$. Autrement dit, le graphe G' est obtenu en transformant tous les arcs du digraphe G en arêtes.

Définition 3.1.11. *Composante connexe*
Une **composante connexe** *(ou* composante*) d'un graphe G est un sous graphe connexe H de G qui est maximal (c.-à-d. : que H est connexe et pour tout H' tel que $H \lhd H' \lhd G$, H' n'est pas connexe).*

La dernière définition s'adapte directement aux digraphes. Ainsi, une **composante fortement connexe** d'un digraphe G est un sous-graphe fortement connexe H de G (voir la définition 3.1.10-a) qui est maximal. De même, une **composante faiblement connexe** d'un digraphe G est un sous-graphe faiblement connexe H de G (voir la définition 3.1.10-b) qui est maximal.

Définition 3.1.12. *Graphes k-connexes et k-arêtes-connexes.*
Soit $k \in \mathbb{N}^*$ et G un graphe

a : *Le graphe G est k-***connexe** *si pour tout ensemble $S \subseteq V(G)$ de cardinalité $< k$, le graphe formé par les sommets $V(G) \setminus S$ et les arêtes $\{[x, y]_G \mid x, y \notin S\}$ est connexe ;*

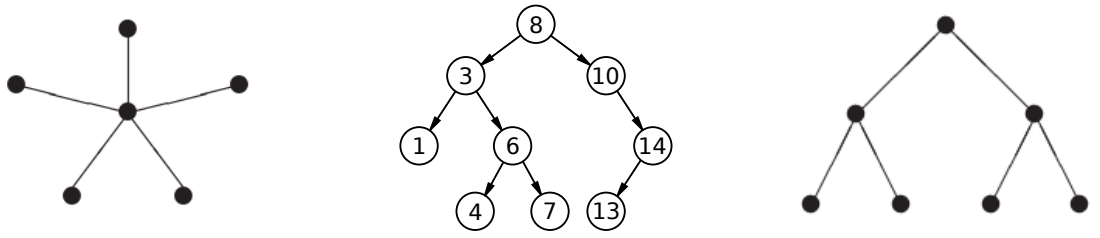
b : *Le graphe G est k-***arêtes-connexe** *si pour tout ensemble $S' \subseteq E(G)$ de cardinalité $< k$, le graphe formé par les sommets $V(G)$ et les arêtes $E(G) \setminus S'$ est connexe ;*

Clairement, un graphe 1-connexe est connexe et un graphe 1-arête-connexe est connexe. De plus tout graphe k-connexe est aussi k-arête-connexe, mais le contraire n'est pas nécessairement vrai.

3.1.6 Arbres

Définition 3.1.13. *Arbres.*
Un graphe T est un **arbre** *s'il est connexe et ne contient aucun cycle.*

On utilise souvent le mot **noeud** pour référer aux sommets d'un arbre. De même, il est parfois naturel de remplacer les arêtes d'un arbre par des arcs (orientés), obtenant ainsi un digraphe que l'on nomme une **arborescence** (que l'on peut aussi nommer un *arbre enraciné*). Tous les sommets d'une arborescence doivent posséder un seul arc entrant, à l'exception d'un seul sommet qui ne possède aucun arc entrant. Ce dernier sommet est appelé la **racine**. Les sommets de l'arborescence ne possédant aucun arc sortant sont appelés les **feuilles**. Tous les sommets possédant au moins un arc sortant (incluant la racine) sont appelés les **noeuds internes**.



(a) Arbre (b) Arborescence (c) Arbre binaire complet

FIGURE 3.4 – Les graphes (a) et (c) sont des arbres et le digraphe (b) est une arborescence. (L'image (b) provient de Wikipédia.)

Définition 3.1.14. *Arbres binaires*
Un **arbre binaire** *T est un arbre qui contient un sommet de degré 2 et dont tous les autres sommets sont de degrés 1 ou 3.*

On utilise le vocabulaire suivant :

— La **racine** de T est l'unique sommet de degré 2 ;
— Les sommets de degrés 1 sont les **feuilles** de T ;
— Les sommets qui ne sont pas des feuilles (incluant la racine) sont appelés les **noeuds internes** de T ;
— Soit une chaîne élémentaire $\langle x_1, x_2, \ldots, x_n \rangle$, où x_1 est la racine et x_n une feuille de l'arbre T. Pour tout $i \in \{1, \ldots, n-1\}$, on dit que x_i est le **père** de x_{i+1} et que x_{i+1} est le **fils** de x_i ;

— Le **niveau** d'un sommet x dans l'arbre T équivaut à la longueur de l'unique chaîne élémentaire allant de la racine de T au sommet x ;
— La **hauteur** (ou la *profondeur*) de l'arbre T est égale au niveau maximal de ses sommets.

Définition 3.1.15. *Arbres binaires complets.*
Un **arbre binaire complet** *(ou* arbre binaire parfait*) est un arbre binaire dont toutes les feuilles sont au même niveau (ce niveau étant égal à la hauteur de l'arbre).*

3.1.7 Représentation matricielle

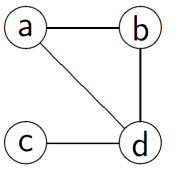
Définition 3.1.16. *Matrice d'ajacence d'un digraphe*
Soit un digraphe G dont on numérote les sommets $V(S) = \{s_1, s_2, \ldots, s_n\}$ (où $n = |V(G|$).
La **matrice d'ajacence** *M du digraphe G est une matrice booléenne de taille $n \times n$ telle que :*

$$M_{i,j} \stackrel{\text{def}}{=} \langle s_i, s_j \rangle \in A(G) \quad \forall i, j \in \{1, 2, \ldots, n\}\,.$$

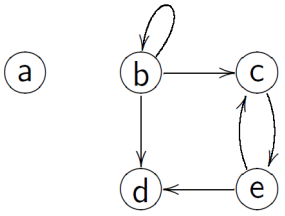
La matrice d'adjacence M d'un graphe G est obtenue de façon similaire, en remplaçant la notion d'arc par celle d'arête :

$$M_{i,j} \stackrel{\text{def}}{=} [s_i, s_j] \in E(G) \quad \forall i, j \in \{1, 2, \ldots, n\}\,.$$

Les matrices sont l'une des structures de données utilisées en informatique pour représenter des graphes. Typiquement, on utilise des 1 et des 0 pour représenter les valeurs de vérité `vrai` et `faux` à l'intérieur d'une matrice d'adjacence. À titre d'exemple, voici la matrice d'ajacence M_1 du graphe G_1 et la matrice d'adjacence M_2 du digraphe G_2 :



$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$



$$M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

La matrice d'adjacence d'un graphe (telle la matrice M_1 ci-haut) est toujours :

— Une matrice symétrique (c'est-à-dire $M_{i,j} = M_{j,i} \ \ \forall i, j \in \{1, 2, \ldots, n\}$) ;

— Une matrice de diagonale nulle (c'est-à-dire $M_{i,i} = 0 \ \ \forall i \in \{1, 2, \ldots, n\}$).

3.1.8 Exercices sur les éléments de base

Exercice 1 : Six équipes sont inscrites à un tournoi de Hockey de garage. Dans la première phase du tournoi, chaque équipe doit affronter toutes les autres une et une seule fois.

a) Construisez un graphe représentant toutes les parties possibles.

b) Quel type de graphe obtenez-vous ?

c) Combien de parties comporte la première phase du tournoi ?

Exercice 2 : Le représentant d'une compagnie de balayeuses centrales doit visiter quatre résidants d'un même immeuble en une même soirée. Chaque visite dure une heure et le représentant a suggéré aux résidents quatre plages horaires : 18h00, 19h00, 20h00 et 21h00. Voici les disponibilités des résidents :

Résident	18h00	19h00	20h00	21h00
Sébastien	✓	✓	✓	
Jean-Francis	✓	✓		
Brice			✓	✓
Alexandre		✓	✓	

a) Représentez cette situation par un graphe.

b) Quel type de graphe obtenez-vous ?

c) Expliquez comment déduire du graphe un horaire possible pour le représentant (notez qu'on peut voir un horaire comme une fonction bijective entre l'ensemble des résidents et l'ensemble des plages horaires).

d) Donnez tous les horaires possibles pour ce problème.

Exercice 3 :

a) Sept étudiants vont en vacances. Chacun va envoyer une carte postale à exactement trois des autres étudiants. Est-ce possible que pour chaque étudiant x, les étudiants qui écrivent à x soient exactement ceux à qui x a écrit ?

b) Qu'arrive-t-il si on remplace "trois" par un autre nombre entre 0 et 6 (inclusivement) à l'exercice précédent ?

Exercice 4 : Considérons la matrice d'adjacence M_1 d'un digraphe G_1 et la matrice d'adjacence M_2 d'un digraphe G_2 :

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

a) Donnez une représentation graphique des digraphes G_1 et G_2.

b) Calculez le produit matriciel suivant [1] : $M_3 = M_1 \times M_2$.

c) En examinant la matrice M_3 calculée précédemment, dites comment on peut interpréter le produit matriciel de deux matrices d'adjacence.

1. Pour un rappel sur le produit matriciel, voir : http://fr.wikipedia.org/wiki/Produit_matriciel

3.2 Les graphes en tant que relations

Puisque les graphes et les digraphes sont définis comme des relations (voir les définitions 3.1.1 et 3.1.2 à la page 222), nous pouvons étudier les graphes à la lumière des propriétés des relations définies au chapitre 1 et des résultats mathématiques associés. Considérant cela, on constate que l'on possède déjà plusieurs outils pour guider notre analyse des graphes. Cette section présente quelques exemples qui mettent à profit ce lien entre le graphe (ou le digraphe) G et la relation dont l'ensemble de départ est $V(G)$ et l'ensemble d'arrivée est $V(G)$.

3.2.1 Opérateurs sur les graphes

Les opérateurs sur les relations définis à la section 1.4.3 (page 83) sont aussi applicables sur des graphes. En fait, les différentes illustrations de cette section présentent toutes des graphes transformés par l'application de certains opérateurs (voir les figures 1.7, 1.8 et 1.9).

Composition d'un graphe

Attardons-nous d'abord à l'opérateur de composition des relations (voir définition 1.4.7, page 84). La **composition** d'un graphe G avec lui-même est notée $G \circ G$ (ou G^2, en adoptant la définition 1.4.9 de l'opérateur puissance). On voit facilement que la présence d'une arête reliant le sommet a et b dans le graphe $G \circ G$ signifie qu'il existe une chaîne de longueur 2 reliant les sommets a et b dans le graphe G. Autrement dit :

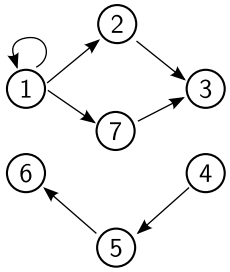
$$[a, b] \in E(G \circ G) \;\Leftrightarrow\; (\,\exists x \in V(G) \mid [a, x] \in E(G) \wedge [x, c] \in E(G)\,)\ .$$

Similairement, si G est un digraphe, on a :

$$\langle a, b\rangle \in A(G \circ G) \;\Leftrightarrow\; (\,\exists x \in V(G) \mid \langle a, x\rangle \in A(G) \wedge \langle x, c\rangle \in A(G)\,)\,.$$

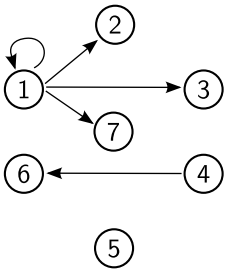
La figure 3.5 illustre le lien entre la composition d'un graphe et le produit matriciel de la matrice d'adjacence (voir définition 3.1.16, page 228). Rappelons que $M \times M$ représente le produit matriciel entre la matrice M et elle-même.

On a que pour tout graphe (ou digraphe) G de matrice d'adjacence M, il y a une arête (ou un arc) reliant les sommets s_i et s_j dans $G \circ G$ si et seulement si l'élément (i, j) de la matrice $M \times M$ est différent de 0. Notons de plus que la valeur de l'élément (i, j) de $M \times M$



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

(a) Graphe G et matrice d'adjacence M correspondante



$$M \times M = \begin{pmatrix} 1 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(b) Graphe $G \circ G$ et matrice d'adjacence $M \times M$ correspondante

FIGURE 3.5 – Exemple illustrant le lien entre la composition d'un graphe et le produit matriciel de la matrice d'adjacence.

est toujours un nombre entier et indique le nombre de façons qu'on peut joindre le sommet s_j à partir du sommet s_i en exactement deux étapes.

Clôture transitive d'un digraphe

Examinons maintenant l'opérateur de clôture (voir définition 1.4.11, page 87). Appliqué sur un digraphe G, l'opérateur de **clôture transitive** G^+ et l'opérateur de **clôture transitive et réflexive** G^* permettent d'obtenir des digraphes dont les sommets sont inchangés (c'est-à-dire $V(G^+) = V(G^*) = V(G)$) et les arcs sont donnés par :

$$\begin{aligned} A(G^+) &= A(G) \cup A(G \circ G) \cup A(G \circ G \circ G) \cup A(G \circ G \circ G \circ G) \cup \dots \\ A(G^*) &= \mathbf{I}_{V(G)} \cup A(G^+), \end{aligned}$$

où $\mathbf{I}_{V(G)}$ est la relation identité (définition 1.4.6), c'est-à-dire le digraphe qui est exactement composé de tous les arcs $\langle x, x \rangle$, pour $x \in V(G)$.

3.2.2 Isomorphisme de graphes

Intuitivement, deux graphes sont isomorphes lorsqu'ils possèdent la même *forme*, même si leurs sommets possèdent des noms différents ou qu'on les représente de manières distinctes.

Définition 3.2.1. *Isomorphisme.*

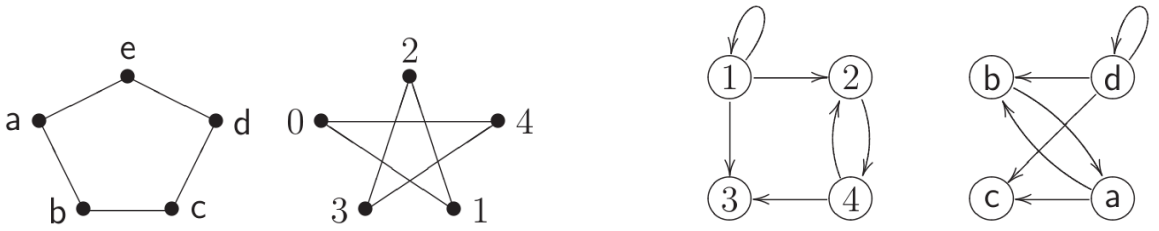
a : *Un* **isomorphisme** *entre le graphe G_1 et le graphe G_2 est une fonction bijective $f : V(G_1) \longrightarrow V(G_2)$ telle que*

$$\big(\forall x, y \mid [x, y] \in E(G_1) \;\Leftrightarrow\; [f(x), f(y)] \in E(G_2)\big)\,.$$

b : *Un* **isomorphisme** *entre le digraphe G_1 et le digraphe G_2 est une fonction bijective $f : V(G_1) \longrightarrow V(G_2)$ telle que*

$$\big(\forall x, y \mid \langle x, y\rangle \in A(G_1) \;\Leftrightarrow\; \langle f(x), f(y)\rangle \in A(G_2)\big)\,.$$

Deux graphes (ou digraphes) sont **isomorphes** si et seulement si *il existe* un isomorphisme entre ces deux graphes (ou ces deux digraphes).



(a) Graphes isomorphes (b) Digraphes isomorphes

FIGURE 3.6 – Exemples de deux graphes isomorphes (définition 3.2.1-a) et de deux digraphes isomorphes (définition 3.2.1-b).

Pour démontrer que deux graphes (ou digraphes) G_1 et G_2 sont isomorphes, il suffit de donner un isomorphisme entre G_1 et G_2. Autrement dit, il s'agit de trouver une fonction bijective f associant chacun des sommets de G_1 à *un et un seul* des sommets de G_2 et qui préserve les arêtes.

La figure 3.6a présente un exemple de deux graphes isomorphes. Un isomorphisme entre ces deux graphes est la fonction $\{\langle a, 0\rangle, \langle b, 1\rangle, \langle c, 2\rangle, \langle d, 3\rangle, \langle e, 4\rangle\}$. De même, la figure 3.6b présente un exemple de deux digraphes isomorphes. Un isomorphisme entre ces deux digraphes est la fonction $\{\langle 1, d\rangle, \langle 2, b\rangle, \langle 3, c\rangle, \langle 4, a\rangle\}$.

3.2.3 Exercices sur les graphes en tant que relations

Exercice 1 : Considérez l'ensemble de sommets $S = \{1, 2, 3, 4\}$ et les deux digraphes suivants :

$$\begin{aligned} G &= \{\langle 2,3\rangle, \langle 3,3\rangle, \langle 4,3\rangle\} \subset S^2, \\ H &= \{\langle 1,2\rangle, \langle 2,4\rangle, \langle 3,1\rangle, \langle 4,3\rangle\} \subset S^2. \end{aligned}$$

a) Calculez $G \cup H$, $G \cap H$, G^c, H^{-1}, $G \circ H$, G^2 et H^2.

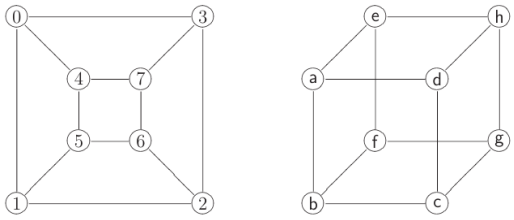
b) Donnez la représentation graphique des digraphes G, H et H^2.

c) Donnez la matrice d'adjacence des digraphes G, H et H^2.

d) Dites lesquelles des propriétés suivantes les relations G et H possèdent :

réflexivité, irréflexivité, symétrie, antisymétrie, asymétrie, transitivité, équivalence, totalité, surjectivité, déterminisme, injectivité, fonction partielle, fonction, fonction bijective, ordre partiel, ordre partiel strict, ordre total.

Exercice 2 : Montrez que les deux graphes suivants sont isomorphes.



3.3 Degrés des sommets et nombre d'arêtes

Théorème 3.3.1. *Nombre d'arêtes d'un graphe complet.*
Soit K_n le graphe complet à n sommets. Alors

$$\Big|E(K_n)\Big| \;=\; \frac{n\cdot(n-1)}{2}\,.$$

Notez que la notion de graphe complet a été introduite par la définition 3.1.3-b (page 223).

Démonstration du théorème 3.3.1
Considérons le prédicat $P(n)$: Le graphe complet K_n possède $\dfrac{n\cdot(n-1)}{2}$ arêtes.

Démontrons que $P(n)$ est vrai pour tout $n \in \mathbb{N}^*$. Par le principe d'induction mathématique (théorème 2.3.2), il suffit de démontrer :

$$P(1) \;\wedge\; (\forall n \in \mathbb{N}\setminus\{0,1\} \mid P(n-1) \Rightarrow P(n))\,.$$

Montrons $P(1)$. (*C'est-à-dire, montrons que le graphe K_1 possède $\dfrac{1\cdot(1-1)}{2} = 0$ arête*).

Par définition, le graphe K_1 possède un seul sommet, donc il est clair que K_1 ne possède aucune arête.

Montrons $(\forall n \in \mathbb{N}\setminus\{0,1\} \mid P(n-1) \Rightarrow P(n))$.

Soit $n \in \mathbb{N}\setminus\{0,1\}$, choisi tel que $P(n-1)$ est vrai.

$$\Big\langle \textit{ C'est-à-dire, tel que le graphe } K_{n-1} \textit{ possède } \frac{(n-1)\cdot(n-2)}{2} \textit{ arêtes } \Big\rangle$$

Montrons $P(n)$. $\Big\langle$ *C'est-à-dire que le graphe K_n possède* $\dfrac{n\cdot(n-1)}{2}$ *arêtes* $\Big\rangle$

Pour créer le graphe complet K_n, on ajoute un nouveau sommet au graphe K_{n-1}. On relie ensuite le nouveau sommet à chacun des sommets de l'ensemble $V(K_{n-1})$. C'est donc dire que le graphe K_n possède $n-1$ arêtes de plus que le graphe K_{n-1}.
Par hypothèse d'induction, on a que K_{n-1} possède $\frac{(n-1)\cdot(n-2)}{2}$ arêtes. Donc :

$$\begin{aligned}
|E(K_n)| &= |E(K_{n-1})| + (n-1) \\
&= \frac{(n-1)\cdot(n-2)}{2} + (n-1) && \langle\ \textit{Hypothèse d'induction}\ \rangle \\
&= \frac{(n-1)\cdot(n-2) + (n-1)\cdot 2}{2} \\
&= \frac{n\cdot(n-1)}{2}\,. && \langle\ \textit{Arithmétique (simplifications)}\ \rangle
\end{aligned}$$

Conclusion : On a démontré que graphe complet K_n possède $\dfrac{n\cdot(n-1)}{2}$ arêtes, $\forall n \in \mathbb{N}^*$.

C.Q.F.D.

Corollaire 3.3.2. *Nombre maximal d'arêtes.*
Soit G un graphe. Alors

$$\Big|E(G)\Big| \;\leq\; \frac{\Big|V(G)\Big| \cdot \Big(\Big|V(G)\Big| - 1\Big)}{2},$$

et il y a égalité si et seulement si G est un graphe complet.

Proposition 3.3.3. *Somme des degrés d'un graphe.*
Soit G un graphe et $V(G) = \{x_1, x_2, \ldots, x_{|V(G)|}\}$ l'ensemble des sommets de G. Alors :

$$\sum_{i=1}^{|V(G)|} \deg_G(x_i) \;=\; 2 \cdot \Big|E(G)\Big|.$$

Démonstration de la proposition 3.3.3

Une idée de cette démonstration sera faite en classe.

Corollaire 3.3.4. *Nombre de sommets de degré impair*
Si G a un nombre fini de sommets alors G contient un nombre pair de sommets de degré impair.

Démonstration du corollaire 3.3.4

Une idée de cette démonstration sera faite en classe.

Clairement, si G est connexe alors son degré minimum est ≥ 1 (sauf si G est le graphe à un seul sommet). Le lemme suivant établit que réciproquement, si le degré minimum est suffisamment grand, alors G est connexe.

Lemme 3.3.5. *Degré minimum d'un graphe et connexité.*
Soit G un graphe de degré minimum k.

$$\textit{Si}\;\; k \;\geq\; \frac{|V(G)| - 1}{2} \quad \textit{alors}\;\; G \;\textit{est connexe.}$$

Démonstration du lemme 3.3.5

Supposons le contraire et cherchons une contradiction.

Soit un graphe G de degré minimum k tel que G n'est pas connexe et $k \geq \dfrac{|V(G)|-1}{2}$.

Soit H la composante connexe de G contenant le moins de sommets.

Considérons les deux arguments suivants :

(A) Comme le graphe G n'est pas connexe, il contient au moins 2 composantes connexes. Comme H est la plus petite, elle contient au plus la moitié des sommets de G. Donc :

$$|V(H)| \;\leq\; \frac{|V(G)|}{2}\,. \tag{3.1}$$

(B) Soit un sommet $x \in V(H)$ ⟨ *Un tel x existe, car H est non-vide* ⟩

Comme $\deg_G(x) \geq k$, on a que H contient au moins $k+1$ sommets

⟨ *C'est-à-dire le sommet x et ses k voisins* ⟩

Donc :

$$\begin{aligned} |V(H)| &\geq k+1 \\ &\geq \frac{|V(G)|-1}{2}+1 \qquad \Big\langle \textit{ Car par choix de } G, \textit{ on a } k \geq \tfrac{|V(G)|-1}{2} \Big\rangle \\ &= \frac{|V(G)|+1}{2} \\ &> \frac{|V(G)|}{2}\,. \end{aligned}$$

Nous avons montré en **(A)** que $|V(H)| \leq \dfrac{|V(G)|}{2}$ et en **(B)** que $|V(H)| > \dfrac{|V(G)|}{2}$, ce qui est une contradiction.

C.Q.F.D.

3.4 Arbres

Les arbres sont une structure de données souvent utilisée en informatique pour emmagasiner de l'information. Cette section présente et démontre quelques propriétés intéressantes des arbres. Pour bien les comprendre, il est conseillé de reviser la nomenclature propre aux arbres à la section 3.1.6 (page 227).

3.4.1 Sommets et arêtes d'un arbre

Le premier lemme démontré n'a que peu d'intérêt en soi, mais il sera utile lors de la démonstration du théorème suivant.

Lemme 3.4.1.
Un arbre qui contient au moins une arête a au moins deux sommets de degré 1.

Démonstration du lemme 3.4.1
Soit un arbre T et C une chaîne élémentaire de longueur maximale du graphe T telle que :

$$C \;=\; \langle x_1,\; x_2,\; x_3,\; \ldots\;, x_n \rangle\;.$$

Démontrons que les sommets x_1 et x_n sont des feuilles (autrement dit, des sommets de degré 1). Pour ce faire, supposons le contraire et cherchons une contradiction.

Supposons que x_1 n'est pas une feuille ou x_n n'est pas une feuille.
Sans perte de généralité, traitons le cas où x_1 n'est pas une feuille
⟨ *Le cas où x_n n'est pas une feuille correspond à traiter la chaîne inverse $\langle x_n, x_{n-1}, \ldots, x_1 \rangle$* ⟩

Puisque x_1 n'est pas une feuille, x_1 possède au moins un voisin différent de x_2.
Notons ce voisin y.

Le sommet y doit appartenir à la chaîne C, car sinon la chaîne C ne serait pas de longueur maximale. ⟨ *Puisqu'on obtiendrait une chaîne plus longue en y ajoutant le sommet y.* ⟩

Donc $y = x_i$ pour un entier $i \in \{3, 4, \ldots, n\}$
Ce qui implique que $\langle y, x_1, x_2, \ldots, x_i \rangle$ est un cycle.
Mais, par définition, T est un arbre et ne contient pas de cycles.

C.Q.F.D.

Théorème 3.4.2. *Nombre de sommets d'un arbre.*
Soit G un graphe connexe, alors

$$G \text{ est un arbre} \quad \Leftrightarrow \quad \Big|V(G)\Big| = \Big|E(G)\Big| + 1\,.$$

Démonstration partielle du théorème 3.4.2 G est un arbre $\Rightarrow |V(G)| = |E(G)| + 1$.

$\boxed{\Rightarrow :}$ Pour effectuer cette démonstration, nous démontrons par induction la véracité du prédicat suivant pour tout $n \in \mathbb{N}^*$:

$$P(n) : \quad \text{Tout arbre de } n \text{ sommets possède } n-1 \text{ arêtes}$$

Par le principe d'induction (théorème 2.3.2, avec $[n_0 := 1]$), il suffit de démontrer :

$$P(1) \ \wedge \ (\forall n \in \mathbb{N}^* \backslash \{1\} \mid P(n-1) \Rightarrow P(n))\,.$$

Montrons $P(1)$. ⟨ *C'est-à-dire, montrons qu'un arbre à 1 sommet possède $1-1$ arête* ⟩

Il n'existe qu'un seul arbre à un sommet (c'est l'arbre •), et il a zéro arête.
On a bien q'un arbre à 1 sommet possède $1 - 1 = 0$ arête

Montrons $(\forall n \in \mathbb{N}^* \backslash \{1\} \mid P(n-1) \Rightarrow P(n))$.

Supposons que $P(n-1)$ est vrai, c'est-à-dire que tous les arbres de $n-1$ sommets possèdent $n-2$ arêtes. ⟨ *C'est notre hypothèse d'induction* ⟩

Montrons maintenant $P(n)$.
Soit T un arbre de n sommets. ⟨ *Montrons que T possède $n-1$ arête* ⟩
On choisit x, une feuille de T.
⟨ *x existe car, par le lemme 3.4.1, on sait que T a au moins une feuille* ⟩

Construisons le graphe T^* en retirant de T le sommet x et l'unique arête incidente à x.
Notons que T^* est toujours un graphe connexe et sans cycle.
Donc T^* est un arbre de $n-1$ sommets.
Ce qui implique que T^* possède $n-2$ arêtes. ⟨ *Par l'hypothèse d'induction* ⟩
Donc T possède $n-1$ arêtes. ⟨ *Car T^* a été obtenu en enlevant une arête à T* ⟩

Conclusion : On a bien $\big(\forall n \in \mathbb{N}^* \mid P(n)\big)$,
Autrement dit : Tout arbre de n sommets possède $n-1$ arêtes.

C.Q.F.D.

Le théorème 3.4.2, nous donne immédiatement le corollaire suivant.

Corollaire 3.4.3. *Nombre de sommets maximal d'un graphe connexe.*
Si G est un graphe connexe, alors

$$\Big|V(G)\Big| \;\leq\; \Big|E(G)\Big| + 1\,.$$

Théorème 3.4.4. *Définitions équivalentes d'un arbre.*
Soit T un graphe, les énoncés suivants sont équivalents :

1 – *T est un arbre ;*

2 – $\Big|V(T)\Big| = \Big|E(T)\Big| + 1$ *et T est connexe ;*

3 – *pour tout x, $y \in V(T)$, il existe (dans T) une et une seule chaîne élémentaire dont les extrémités sont x et y ;*

4 – *T est connexe, mais pour toute arête $e \in E(T)$, le graphe formé des sommets $V(T)$ et des arêtes $E(T) \setminus \{e\}$ ne l'est pas ;*

5 – *T est acyclique, mais pour toute paire de sommets x, $y \in V(T)$ tel que $[x, y] \notin E(G)$, le graphe formé des sommets $V(T)$ et des arêtes $E(T) \cup [x, y]$ ne l'est pas.*

Démonstration du théorème 3.4.4

Une idée de cette démonstration sera faite en classe.

3.4.2 Propriétés des arbres binaires

Les arbres binaires sont une structure de données souvent utilisée en informatique pour emmagasiner de l'information.

Proposition 3.4.5. *Propriétés des arbres binaires complets.*
Soit T un arbre binaire complet comportant n noeuds. Alors :

a : *T contient* $\dfrac{n+1}{2}$ *feuilles.*

b : *T contient* $\dfrac{n-1}{2}$ *sommets internes.*

c : *La hauteur de T est :* $\log_2(n+1) - 1\,.$

Pour démontrer la proposition 3.4.5, nous allons supposer que nous connaissons la hauteur de l'arbre T et nous en déduirons les autres quantités. Il sera plus simple de procéder ainsi que de supposer que nous connaissons le nombre noeuds n. Il suffira d'effectuer de simples calculs arithmétiques pour retrouver l'énoncé de la proposition.

Démonstration de la proposition 3.4.5

Soit un arbre binaire complet T de hauteur $h \in \mathbb{N}$.

(A) Calculons f, le nombre de feuilles de T.

Définissons récursivement la suite $\langle F(x) \rangle_{x\in\mathbb{N}}$, dont le $x$ième terme correspond au nombre de feuilles dans un arbre binaire complet de hauteur x. Remarquons que l'arbre de hauteur 0 possède une feuille (c'est le cas particulier où l'arbre consiste en un graphe d'un seul sommet) et que l'arbre de hauteur $x \geq 1$ possède le double de feuilles de l'arbre de hauteur $x-1$. Nous avons donc :

$$\begin{cases} F(0) &= 1 \\ F(x) &= 2 \cdot F(x-1) \quad \forall x \in \mathbb{N}^* \,. \end{cases}$$

La suite $\langle F(x) \rangle_{x\in\mathbb{N}}$ est une suite géométrique de premier terme 1 et de raison 2. Le théorème 2.4.4 nous permet d'énoncer le terme général de la suite : $F(x) = 2^x \; \forall x \in \mathbb{N}$. Ainsi, l'arbre T de hauteur h possède $f = 2^h$ feuilles.

(B) Calculons n, le nombre de noeuds de T.

Comme T est un arbre binaire complet, il contient un nombre de noeuds égal à la somme du nombre de feuilles des arbres binaires complets de hauteur 0 à h. Ainsi :

$$n = \sum_{x=0}^{h} F(x) \,.$$

La valeur n est donc donnée par la somme des h premiers termes de la suite géométrique $\langle F(x) \rangle_{x\in\mathbb{N}}$. Par le théorème 2.4.7, nous obtenons :

$$n = \frac{1 \cdot (1 - 2^{h+1})}{1-2} = 2^{h+1} - 1 \,.$$

(C) Calculons i, le nombre de noeuds internes de T.

Le nombre de noeuds internes i de T correspond simplement à la différence entre le nombre de noeuds total n et le nombre de feuilles. Ainsi, on a :

$$i = n - f = 2^{h+1} - 1 - 2^h = 2^h - 1 = f - 1 \,.$$

(D) Exprimons h, f et i en fonction du nombre de noeuds n.

$$\begin{aligned} & n = 2^{h+1} - 1 \\ \Leftrightarrow \; & 2^{h+1} = n + 1 \\ \Leftrightarrow \; & \log_2(2^{h+1}) = \log_2(n+1) \\ \Leftrightarrow \; & h = \log_2(n+1) - 1 \,, \end{aligned}$$

$$\begin{aligned} f &= 2^h \\ &= 2^{\log_2(n+1)-1} \\ &= 2^{\log_2(n+1)} \cdot 2^{-1} \\ &= \frac{n+1}{2} \,, \end{aligned}$$

$$\begin{aligned} i = f - 1 &= \frac{n+1}{2} - 1 \\ &= \frac{n+1-2}{2} \\ &= \frac{n-1}{2} \,. \end{aligned}$$

C.Q.F.D.

3.4.3 Exercices sur les arbres

Exercice 1 : (*Aucune justification n'est demandée pour ce numéro.*)

a) Énumérez (à isomorphisme près) tous les arbres binaires ayant exactement 6 feuilles.

b) Combien de sommets peut avoir un arbre binaire ayant exactement 6 feuilles.

c) Combien de sommets peut avoir un arbre binaire ayant exactement k feuilles (avec $k \geq 2$).

Exercice 2 : Définissons un *arbre trinaire* comme un arbre qui contient un sommet de degré 3 (la *racine*) et dont tous les autres sommets sont de degré 1 (les *feuilles*) ou de degré 4. Comme pour un arbre binaire, le *niveau* d'un sommet x d'un arbre trinaire équivaut à la longueur de l'unique chaîne allant de la racine au sommet x et la *hauteur* d'un arbre trinaire est égale au niveau maximal de ses feuilles. Finalement, un *arbre trinaire complet* est un arbre trinaire dont toutes les feuilles sont au même niveau.

a) Dessinez trois arbres : un arbre trinaire complet de hauteur 2, un arbre trinaire complet de hauteur 3 et un arbre trinaire complet de hauteur 4.

b) Donnez l'expression du nombre de feuilles d'un arbre trinaire complet en fonction de sa hauteur.

c) Donnez l'expression du nombre de noeuds d'un arbre trinaire complet en fonction de sa hauteur. (Indice : Vous pouvez vous servir du résultat obtenu en (b) et des résultats présentés à la section 2.4.3 sur les *suites des sommes de premiers termes d'une suite*.)

Exercice 3 : Un arbre est toujours un graphe biparti. Décrivez une méthode pour créer une bipartition à partir de n'importe quel arbre (Rappel : les concepts de *graphe biparti* et de *bipartition* ont été introduits par la définition 3.1.3-c).

3.5 Graphes planaires

Définition 3.5.1. *Graphes planaires et représentations planaires*

a : *Un* **graphe planaire** *est un graphe qui peut être tracé dans un plan sans qu'aucune de ses arêtes en croise une autre.*

b : *Une* **représentation planaire** *est une représentation dans le plan* $\mathbb{R}^2$ *d'un graphe planaire.*

On considère qu'une représentation planaire est un graphe G tel que :

1. $V(G) \subseteq \mathbb{R}^2$;
2. $\forall e \in E(G)$, e est une portion de courbe de $\mathbb{R}^2$ entre deux sommets $u, v \in V(G)$;
3. il existe au plus une arête entre deux sommets donnés ;
4. l'intérieur d'une arête ne contient pas de sommets et n'intersecte aucune autre arête.

FIGURE 3.7 – Deux représentations d'un même graphe planaire. Seul le graphe de droite est une représentation planaire. (Version modifiée d'une image provenant de Wikipédia.)

On désigne par le terme **région** (ou *face*) chacun des polygones bornés par les arêtes d'une représentation planaire. De plus, une représentation planaire (finie) possède une région qui est non bornée, que l'on nomme la **région extérieure** (ou *face extérieure*).

Étant donné une représentation planaire G, comme pour tout graphe :

- $V(G)$ représente l'ensemble des sommets de G ;
- $E(G)$ représente l'ensemble des arêtes de G.

De plus, dans le cas spécifique d'une représentation planaire :

- $F(G)$ représente l'ensemble des régions de G (incluant la région extérieure).

Lemme 3.5.2. *Représentations planaires et cycles.*
Soit une représentation planaire G et $e \in E(G)$.

- a : *Si e appartient à un cycle de G, alors e fait partie de la frontière d'exactement deux régions de G.*
- b : *Si e n'est dans aucun cycle de G, alors e fait partie de la frontière d'exactement une région de G.*

Théorème 3.5.3. *Formule d'Euler*
Soit G une représentation planaire connexe. Alors

$$\Big|V(G)\Big| + \Big|F(G)\Big| - \Big|E(G)\Big| \;=\; 2\,.$$

Démonstration du théorème 3.5.3
Supposons le contraire, c'est-à-dire qu'il existe un graphe qui est une représentation planaire et qui ne satisfait pas la formule d'Euler. Parmi toutes les représentations planaires qui ne satisfont pas la formule d'Euler, choisissons-en un qui contient le plus petit nombre possible d'arêtes. Notons ce graphe G_0.

Nous avons donc :

$$\Big|V(G_0)\Big| + \Big|F(G_0)\Big| - \Big|E(G_0)\Big| \;\neq\; 2\,. \tag{3.2}$$

Mais pour toute représentation planaire connexe H :

$$\text{si } \Big|E(H)\Big| < \Big|E(G_0)\Big| \quad \text{alors on a} \quad \Big|V(H)\Big| + \Big|F(H)\Big| - \Big|E(H)\Big| \;=\; 2\,. \tag{3.3}$$

Alors, il y a deux cas à considérer :

Cas 1 : G_0 contient un cycle C.
Soit $e \in E(C)$.
Alors par le lemme 3.5.2-a, l'arête e est la frontière d'exactement deux régions.
Soit le graphe H tel que $V(H) = V(G_0)$ et $E(H) = E(G_0) \setminus \{e\}$.

⟨ *C'est à dire, le sous-graphe obtenu de G_0 qui a exactement les mêmes sommets que G_0 et toutes les arêtes de G_0 sauf l'arête e.* ⟩

On a donc :

(i) $\Big|E(H)\Big| = \Big|E(G_0)\Big| - 1$

(ii) $\Big|V(H)\Big| = \Big|V(G_0)\Big|$

(iii) $\Big|F(H)\Big| = \Big|F(G_0)\Big| - 1$

⟨ *car les deux régions séparées par e dans G_0 n'en forment plus qu'une dans H.* ⟩

Notons que puisque G_0 est connexe, H est lui aussi connexe car s'il existe entre deux sommets un chemin de G_0 qui passe par l'arête e, alors (en faisant un détour par les arêtes $E(C) \setminus \{e\}$) il existe entre ces deux mêmes sommets, un chemin de G_0 qui ne passe pas par e et qui donc est également un chemin de H.

Donc le graphe H est une représentation planaire connexe ; il découle donc de l'item (i) et de l'équation (3.3) que H satisfait la formule d'Euler.

Donc,

$$\begin{aligned} 2 &= \Big|V(H)\Big| + \Big|F(H)\Big| - \Big|E(H)\Big| \\ &= \Big|V(G_0)\Big| + \Big(\Big|F(G_0)\Big| - 1\Big) - \Big(\Big|E(G_0)\Big| - 1\Big) && \langle \textit{ Voir (i), (ii) et (iii). } \rangle \\ &= \Big|V(G_0)\Big| + \Big|F(G_0)\Big| - \Big|E(G_0)\Big| && \langle \textit{ Propriétés de l'arithmétique. } \rangle \end{aligned}$$

On a donc à la fois que G_0 satisfait et ne satisfait pas la formule d'Euler. Ceci est une contradiction.

Cas 2 : G_0 ne contient pas de cycle.
Comme G_0 est connexe, G_0 est donc un arbre.

Donc $\Big|F(G_0)\Big| = 1$.
$\langle$ *Car une représentation planaire qui est un arbre n'a qu'une région, la région extérieure.* $\rangle$

De plus, par le théorème 3.4.2 , on sait que $\Big|V(G_0)\Big| = \Big|E(G_0)\Big| + 1$.
Ce qui implique que

$$\Big|V(G_0)\Big| - \Big|E(G_0)\Big| = 1$$

On a donc que

$$\Big|V(G_0)\Big| + \Big|F(G_0)\Big| - \Big|E(G_0)\Big| = 1 + 1 = 2$$

Ainsi, dans ce $2^{\text{ème}}$ cas, nous avons également que G_0 satisfait et ne satisfait pas la formule d'Euler.
Encore une fois, donc, nous obtenons une contradiction.

C.Q.F.D.

Proposition 3.5.4. *Nombre d'arêtes maximal d'un graphe planaire.*
Soit G un graphe planaire connexe tel que $\Big|V(G)\Big| \geq 4$, alors

$$\Big|E(G)\Big| \leq 3\Big|V(G)\Big| - 6\,.$$

Démonstration de la proposition 3.5.4
Soit G une représentation planaire d'un graphe planaire connexe, tel que $\Big|V(G)\Big| \geq 4$.
Voici deux observations :

1. Comme G est connexe et a au moins 4 sommets, chaque région de G a au moins 3 arêtes.
   ⟨ *Les seules exceptions étant les graphes* •, •—• *et* •—•—• *qui ont tous moins de 4 sommets.* ⟩
2. Chaque arête de G est contenue dans au plus 2 régions de G. ⟨ *Voir le lemme 3.5.2.* ⟩

Notons par $f_1, f_2, \ldots, f_{|F(G)|}$ les régions de G et par m_i le nombre d'arêtes contenues dans la région f_i pour $i \in \{1, 2, \ldots, |F(G)|\}$.

Alors, il découle des deux observations que

$$3\Big|F(G)\Big| \;\leq\; m_1 + m_2 + \cdots + m_{|F(G)|} \;\leq\; 2\Big|E(G)\Big|$$

Ce qui implique que

$$\Big|F(G)\Big| \;\leq\; \frac{2}{3}\Big|E(G)\Big| \tag{3.4}$$

Par la formule d'Euler, on sait que $2 = \Big|V(G)\Big| + \Big|F(G)\Big| - \Big|E(G)\Big|$.

En combinant avec l'équation (3.4), on obtient

$$2 \;\leq\; \Big|V(G)\Big| \;+\; \frac{2}{3}\Big|E(G)\Big| \;-\; \Big|E(G)\Big|$$

C'est-à-dire

$$2 \;\leq\; \Big|V(G)\Big| \;-\; \frac{1}{3}\Big|E(G)\Big|$$

C'est-à-dire

$$\frac{1}{3}\Big|E(G)\Big| \;\leq\; \Big|V(G)\Big| \;-\; 2$$

C'est-à-dire

$$\Big|E(G)\Big| \;\leq\; 3\Big|V(G)\Big| \;-\; 6\,.$$

C.Q.F.D.

Proposition 3.5.5. *Tout graphe planaire a un sommet de degré* ≤ 5.

Démonstration de la proposition 3.5.5

Supposons le contraire.

Soit G un graphe planaire de degré minimum ≥ 6.

Notons par d_{Max} le degré maximum de G

et par n_i le nombre de sommets de degré i pour $i = 6, 7, \ldots, d_{Max}$.

Alors on a

$$\left|E(G)\right| \;=\; \frac{1}{2}\left(6n_6 + 7n_7 + 8n_8 + \cdots + d_{Max}n_{d_{Max}}\right) \tag{3.5}$$

Par la proposition 3.5.4, on sait que $\left|E(G)\right| \;\leq\; 3\,\left|V(G)\right| - 6$.

En combinant avec l'équation (3.5), on obtient

$$\frac{1}{2}\left(6n_6 + 7n_7 + 8n_8 + \cdots + d_{Max}n_{d_{Max}}\right) \;\leq\; 3\left(n_6 + n_7 + n_8 + \cdots + n_{d_{Max}}\right) \;-\; 6$$

C'est-à-dire

$$\left(6n_6 + 7n_7 + 8n_8 + \cdots + d_{Max}n_{d_{Max}}\right) \;\leq\; 6\left(n_6 + n_7 + n_8 + \cdots + n_{d_{Max}}\right) \;-\; 12$$

C'est-à-dire

$$n_7 + 2n_8 + \cdots + (d_{Max} - 6)n_{d_{Max}} \;\leq\; -12 \tag{3.6}$$

Notons que $n_7 + 2n_8 + \cdots + (d_{Max} - 6)n_{d_{Max}} \geq 0$

⟨ *Car c'est le résultat de sommes et de produits de nombres positifs ou nuls.* ⟩

L'équation (3.6) nous donne donc qu'un nombre ≥ 0 est plus petit ou égal à -12,
ce qui est une contradiction.

C.Q.F.D.

3.6 Chaînes et chemins

3.6.1 Propriétés d'un graphe connexe

Proposition 3.6.1. *Connexité et chaîne élémentaires.*
Un graphe G est connexe si et seulement si pour toute paire x, y de sommets de G, il existe une chaîne élémentaire dont les extrémités sont x et y.

Démonstration de la proposition 3.6.1

Une idée de cette démonstration sera faite en classe.

3.6.2 Cycles d'un graphe

Proposition 3.6.2. *Connexité d'un cycle*

a : *Un cycle est toujours 2-arêtes-connexe ;*

b : *Un cycle élémentaire est toujours 2-connexe (et donc 2-arêtes-connexe).*

Démonstration de la proposition 3.6.2

Une idée de cette démonstration sera faite en classe.

Proposition 3.6.3. *Connexité d'un cycle*
Soit H un graphe (fini), alors les énoncés suivants sont équivalents :

- *H est un cycle élémentaire ;*
- *H est un graphe connexe et régulier d'ordre 2 ;*
- *H est un cycle qui ne contient pas d'autre cycle.*

Démonstration de la proposition 3.6.3

Une idée de cette démonstration sera faite en classe.

Définition 3.6.4. *Graphes eulériens et cycles eulériens.*
Un **cycle eulérien** *d'un graphe est un cycle passant par chacune des arêtes du graphe. Un graphe qui contient un tel cycle est un* **graphe eulérien**.

Autrement dit, un cycle eulérien d'un graphe G est une séquence de la forme

$$\langle\, x_1,\, [x_1, x_2],\, x_2,\, [x_2, x_3],\, x_3,\, \ldots\,,\; x_{n-1},\, [x_{n-1}, x_n],\, x_n,\, [x_n, x_1], x_1 \,\rangle,$$

où chaque arête de $E(G)$ apparaît une et une seule fois.

Théorème 3.6.5. (Euler, Hierholzer, Veblen)
Soit G un graphe fini et connexe. Alors les énoncés suivants sont équivalents :

(i) G est eulérien ;
(ii) G n'a pas de sommet de degré impair ;
(iii) G a une décomposition en cycles élémentaires ;

Démonstration du théorème 3.6.5

Une idée de cette démonstration sera faite en classe.

Un cycle eulérien est une promenade qui passe une et une seule fois par chaque arête du graphe, la définition suivante est l'analogue "sommet" du cycle eulérien en ce sens qu'il s'agit d'une promenade qui passe une et une seule fois par chaque sommet.

Définition 3.6.6. *Graphes hamiltoniens et cycles hamiltoniens*
Un **cycle hamiltonien** *d'un graphe est un cycle élémentaire passant par chacun des sommets du graphe. Un graphe qui contient un tel cycle est un* **graphe hamiltonien**.

Autrement dit, un cycle hamiltonien d'un graphe G est une séquence de la forme

$$\langle\, x_1,\, [x_1, x_2],\, x_2,\, [x_2, x_3],\, x_3,\, \ldots\,,\; x_{n-1},\, [x_{n-1}, x_n],\, x_n,\, [x_n, x_1], x_1 \,\rangle,$$

où chaque sommet de $V(G)$ apparaît une et une seule fois.

Théorème 3.6.7. *K_n est hamiltonien $\forall n \in \mathbb{N}^*$.*

Le théorème suivant présente un résultat intéressant concernant les graphes hamiltoniens. Ce théorème ne sera pas démontré dans le cadre de ce cours.

Théorème 3.6.8. ***(Dirac 1952)***
Tout graphe ayant $n \geq 3$ sommets et degré minimum $\geq \frac{n}{2}$ est hamiltonien.

Le Théorème 3.6.8 est une conséquence évidente du lemme 3.3.5 et du résultat suivant.

Théorème 3.6.9. ***(Ore 1960)***
Soit G un graphe connexe ayant $n \geq 3$ sommets tels que pour toute paire x, y de sommets distincts non adjacents de G, on a $\deg_G(x) + \deg_G(y) \geq n$. Alors G est hamiltonien.

3.6.3 Algorithmes de recherche du plus court chemin

Plusieurs problèmes en informatique peuvent s'exprimer comme un problème de recherche du chemin le plus court dans un digrahe (ou encore de la chaîne le plus courte dans un graphe). Par exemple, pour connaître le chemin le plus court entre deux villes, on peut représenter un réseau de transport par un digraphe, tel que les sommets correspondent à différentes villes et les arcs correspondent aux liens (terrestres ou aériens) entre les villes.

Graphes valués

Lorsqu'on s'intéresse à ce genre de problème, on a souvent recours à un **graphe valué** (ou digraphe valué) [2], pour lequel chaque arête du graphe (ou arc du digraphe) est associée à une valeur. Cette valeur est souvent un nombre réel. Dans le cadre de ce cours, on représente un graphe valué G en spécifiant une fonction $w : E(G) \longrightarrow \mathbb{R}$. (ou une fonction $w : A(G) \longrightarrow \mathbb{R}$) dans le cas d'un digrahe). La figure 3.8 donne un exemple de représentation graphique d'un graphe valué.

Dans le cas où un digraphe représente un réseau de transport, la valeur associée à chaque arc peut représenter le temps pour se déplacer d'une ville à l'autre, ou encore le coût engendré par le déplacement.

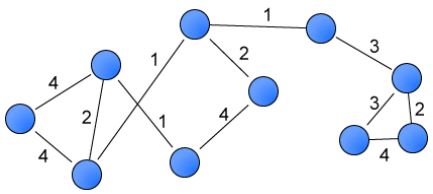


FIGURE 3.8 – Exemple d'un graphe valué. (Image provenant de Wikipédia)

2. On utilise parfois les termes *graphe pondéré* et *digraphe pondéré*.

Algorithme de Dijkstra

L'algorithme de Dijkstra permet de trouver le plus court chemin entre deux sommets d'un digraphe valué dont les valeurs des arcs sont non-négatives. La première version de cet algorithme a été publiée en 1959 par l'informaticien hollandais Edsger Dijkstra (1930 – 2002).

Le pseudo-code présenté ci-dessus prend en argument un digraphe G, les valeurs (non-négatives) des arêtes sous la forme d'une fonction $w : A(G) \longrightarrow \mathbb{R}^*$ et une paire de sommets $a, z \in V(G)$ spécifiant les deux sommets entre lesquels on désire trouver un chemin.

Notez que l'algorithme retourne la longueur totale du plus court chemin entre les sommets a et z. Si aucun chemin ne relie a et z, l'algorithme retourne une valeur infinie (∞).

`Algorithme_Dijkstra` (Digraphe G, valeurs w, origine a, destination z)

Initialiser :

- $Q \leftarrow V(G)$ ⟨ *Pendant l'exécution, Q contient les sommets non visités* ⟩
- $dist(v) \leftarrow \infty \quad \forall v \in Q \setminus \{a\}$ ⟨ *La distance de tous les sommets (sauf a) est inconnue* ⟩
- $dist(a) \leftarrow 0$ ⟨ *Le sommet source est à une distance nulle de lui-même* ⟩

Tant que $|Q| > 0$ **Faire** ⟨ *Tant qu'il reste des sommets à visiter...* ⟩

$u \leftarrow$ Un élément de Q dont la valeur $dist(u)$ est minimale
$Q \leftarrow Q \setminus \{u\}$ ⟨ *On sélectionne le sommet u à visiter* ⟩

Si $u = z$ **alors**
Retourner $dist(z)$ ⟨ *On a trouvé la distance minimale de a à z* ⟩
Fin Si

Pour tout $v \in \mathcal{N}(u) \cap Q$ **Faire** ⟨ *Mise à jour de la distance des voisins de u* ⟩
Si $dist(u) + w(\langle u, v\rangle) < dist(v)$ **alors**
$dist(v) \leftarrow dist(u) + w(\langle u, v\rangle)$
Fin Si
Fin Pour

Fin Tant que

Retourner ∞ ⟨ *Aucun chemin trouvé* ⟩

Algorithme de Floyd-Warshall

L'algorithme de Dijkstra s'avère une stratégie efficace pour trouver le plus court chemin entre deux sommets spécifiques dans un graphe. Dans certaines situations, on désire plutôt connaître les plus courts chemins entre toutes les paires de sommets dans un graphe. C'est ce que permet de faire l'algorithme de Floyd-Warshall. Cet algorithme fut présenté en 1962 de manière indépendante par les informaticiens états-uniens Robert W. Floyd (1936 – 2001) et Stephen Warshall (1935 – 2006). Le même algorithme avait été formulé en 1959 par le mathématicien français Bernard Roy (1934 – . . .).

`Algorithme_Floyd_Warshall` (Digraphe G, valeurs w)

Initialiser : $dist(v_i, v_j) \leftarrow \begin{cases} w(\langle v_i, v_j \rangle) & \text{si } \langle v_i, v_j \rangle \in A(G) \\ 0 & \text{si } v_i = v_j \\ \infty & \text{sinon.} \end{cases} \qquad \forall \langle v_i, v_j \rangle \in \big(V(G)\big)^2$

Pour tout $v_i \in V(G)$ **Faire**
  Pour tout $v_j \in V(G)$ **Faire**
    Pour tout $v_k \in V(G)$ **Faire**

$$dist(v_i, v_j) \leftarrow \min\{\, dist(v_i, v_j),\ dist(v_i, v_k) + dist(v_k, v_j) \,\}$$

    Fin Pour
  Fin Pour
Fin Pour

Retourner *dist* ⟨ *Retourne les distances entre toutes les paires de sommets* ⟩

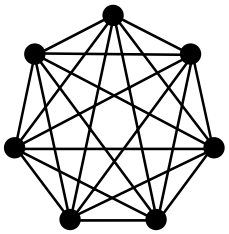
Notez que si le digraphe G comporte n sommets numérotés tels que $V(G) = \{v_1, v_2, \ldots, v_n\}$, l'étape d'initialisation est équivalente à créer une matrice de taille $n \times n$. Ainsi, l'algorithme Floyd-Warshall est souvent implanté à l'aide d'une matrice et les boucles de la forme "**Pour tout** $v_i \in V(G)$" sont remplacées par des boucles "**Pour tout** i **de** 1 **à** n".

3.6.4 Exercices sur les chaînes et chemins

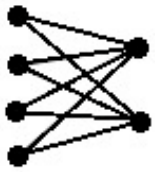
Exercice 1 : Pour chacun des graphes ci-dessous, dites s'il s'agit d'un graphe

a) eulérien. Si oui, exhibez un cycle eulérien.

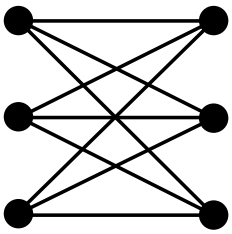
b) hamiltonien. Si oui, exhibez un cycle hamiltonien.



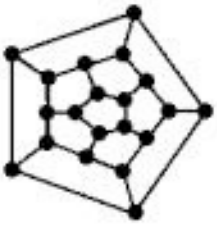
K_7



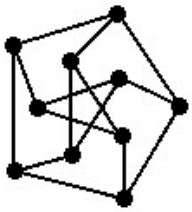
$K_{4,2}$



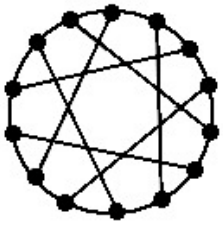
$K_{3,3}$



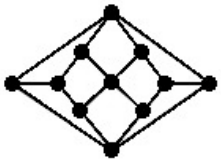
Le dodécaèdre



Le graphe de Petersen



Le graphe d'Heawood



Le graphe d'Herschel

Exercice 2 : On veut asseoir cinq couples autour d'une table ronde de telle sorte que pour chaque deux couples, au moins un des membres du premier couple soit assis à côté d'au moins un membre du deuxième couple. Est-ce possible ?

Exercice 3 : L'algorithme de Dijkstra présenté à la page 252 retourne la longueur du plus court chemin entre le sommet d'origine et le sommet de destination z, mais ne permet pas de connaître la nature de ce chemin. Suggérez une modification à l'algorithme afin qu'il retourne le chemin le plus court (sous la forme, par exemple, d'une liste de sommets). ÙÙÙÙÙ

Annexe A : Alphabet grec

Lettre minuscule	Lettre majuscule	Nom français
α	A	alpha
β	B	bêta
γ	Γ	gamma
δ	Δ	delta
ϵ	E	epsilon
ζ	Z	zêta
η	H	êta
θ	Θ	thêta
ι	I	iota
κ	K	kappa
λ	Λ	lambda
μ	M	mu
ν	N	nu
ξ	Ξ	xi
o	O	omicron
π	Π	pi
ρ	P	rhô
σ	Σ	sigma
τ	T	tau
υ	Y	upsilon
ϕ	Φ	phi
χ	X	ki
ψ	Ψ	psi
ω	Ω	omega

Annexe B : Documents LaTeX

LaTeX (prononcé “la-tek”, car le dernier ‘X” est plutôt un “ki” grec, majuscule) est un langage permettant de rédiger des documents de qualité professionnelle (dont le présent document !). Son utilisation est particulièrement répandue en informatique et en mathématiques, car il permet d'inclure facilement des expressions mathématiques au travers du texte, contrairement à plusieurs éditeurs de texte populaires, tel Microsoft Word. Mais la relative facilité avec laquelle il est possible de créer de très beaux documents à l'aide de LaTeX font que cet outil est aussi utilisé dans plusieurs autres domaines [3].

Ce langage peut sembler rébarbatif au premier abord, et son apprentissage demande une certaine persévérance. Cela dit, une fois qu'on y est habitué, il devient impensable de rédiger des documents à fort contenu mathématique autrement ! Dans le cadre de ce cours, l'utilisation de LaTeX n'est pas obligatoire. Nous pensons toutefois qu'il agit d'un bon apprentissage, particulièrement pour les étudiants qui envisagent de continuer leurs études aux cycles supérieurs, car ils utiliseront assurément LaTeX pour rédiger des articles destinés à des conférences et des journaux scientifiques.

Pour la petite histoire, LaTeX est basé sur le langage TeX, qui a été développé par l'informaticien célèbre Donald Knuth (récipiendaire d'un prix Turing en 1974), au début de la rédaction de son ouvrage mythique “The Art of Computer Programming”. Voici ce qu'on en dit sur Wikipédia [4] :

> Mécontent de la façon dont étaient imprimés ses livres, [Knuth] consacra plusieurs années de sa vie, à partir de 1977, pour écrire un logiciel lui permettant d'obtenir un rendu correct des formules mathématiques pour la typographie professionnelle. [...] Le but de Knuth quand il a créé TeX était d'avoir un langage de description de contenu permettant d'obtenir un rendu de grande qualité avec un minimum d'efforts et qui serait indépendant de l'architecture matérielle. Fourni avec ses sources, TeX est l'un des premiers logiciels libres, ou presque.

3. Certaines rumeurs veulent que des étudiants au baccalauréat en histoire et en philosophie aient vu leurs notes augmentées d'au moins 5% depuis qu'ils utilisent LaTeX pour rédiger leurs dissertations !

4. http://fr.wikipedia.org/wiki/Donald_Knuth, 10 septembre 2011

Avant goût de l'environnement mathématique de LaTeX

Un fichier source LaTeX n'est qu'un document texte dans lequel on insère différentes commandes qui seront ensuite traduites lors de la compilation. À l'intérieur d'un paragraphe, on peut à tout moment entourer une expression de signes de dollar pour invoquer l'"environnement mathématique". Par exemple, l'expression "`$x^2 + y^2 = z^2$`" sera traduite par le compilateur LaTeX en $x^2 + y^2 = z^2$. Voici quelques autres exemples d'expressions mathématiques (l'environnement "itemize" est utilisé pour produire une liste) :

```
\begin{itemize}
 \item $x_1^a \cdot x_2^a = (x_1 \cdot x_2)^a$;
 \item $\neg (p \wedge q) \Leftrightarrow \neg p \vee \neg q$;
 \item $(S \cup T)^c = S^c \cap T^c$;
 \item $A \subseteq B \Leftrightarrow \{ \forall e \ | \ e \in A \Rightarrow e \in B \}$;
 \item $\rho \subset \mathbb{N} \times \mathbb{N}^*$.
\end{itemize}
```

Voici le rendu du code précédent une fois compilé par LaTeX :

— $x_1^a \cdot x_2^a = (x_1 \cdot x_2)^a$;
— $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$;
— $(S \cup T)^c = S^c \cap T^c$;
— $A \subseteq B \Leftrightarrow \{\forall e \mid e \in A \Rightarrow e \in B\}$;
— $\rho \subset \mathbb{N} \times \mathbb{N}^*$.

Pour écrire des formules mathématiques sur plusieurs lignes, on peut utiliser un bloc "eqnarray" :

```
\begin{eqnarray*}
  \beta_0 + \sum_{\alpha=1}^n \alpha &=& \beta_0 + 1+2+3 + \ldots + n \\
  &=& \beta_0 + \frac{n \cdot (n+1)}{2} \\
  &=& \beta_0 + \frac{1}{2} \left( n^2 + n \right) \\
  &\leq& \beta_0 + n^2 \ .
\end{eqnarray*}
```

Ce qui, une fois compilé, produira le contenu suivant :

$$\begin{aligned} \beta + \sum_{\alpha=1}^{n} \alpha &= \beta + 1 + 2 + 3 + \ldots + n \\ &= \beta + \frac{n \cdot (n+1)}{2} \\ &= \beta + \frac{1}{2}\left(n^2 + n\right) \\ &\leq \beta + n^2 + n \ . \end{aligned}$$

La section suivante présente quelques références grâce auxquelles vous pourrez en apprendre davantage. On vous fournira aussi, sur le site web du cours, quelques documents sources en exemple.

Références LaTeX

Il existe *beaucoup* de sites web de références pour apprendre à utiliser LaTeX. En voici quelques-uns :

- Wikibooks (la version française ne semble pas être une traduction directe de la version anglaise. À vous de choisir la version qui vous convient le mieux !)
  - En français : http://fr.wikibooks.org/wiki/latex
  - En anglais : http://en.wikibooks.org/wiki/latex

- The Not So Short Introduction to LaTeX : considéré par plusieurs comme LA référence. Les explications sont très complètes, peut-être même un peu trop si vous voulez vous en tenir aux connaissances de base :
  - Version originale anglaise :
    http://mirror.ctan.org/info/lshort/english/lshort.pdf
  - Traduction française :
    http://mirror.ctan.org/info/lshort/french/lshort-fr.pdf

- Art of Problem Solving (en anglais seulement) : ce site web contient des explications claires et succinctes pour débuter avec LaTeX, bien qu'il prend parfois en considération que vous utilisez l'éditeur TeXnicCenter sous Windows.
  http://www.artofproblemsolving.com/Wiki/index.php/LaTeX:About

- MαthIM : Un système de clavardage en ligne (*chat*) qui accepte les formules LaTeX.
  http://mathim.com/
- Detexify[2] - LaTeX symbol classifier : il suffit de dessiner un symbole avec la souris et le système suggère le symbole LaTeX correspondant (utile et amusant !) :
  http://detexify.kirelabs.org/

Logiciels pour utiliser LaTeX

Pour pouvoir compiler un fichier LaTeX, il vous faut une distribution contenant les paquets définissant les commandes et le compilateur LaTeX. Une fois que vous possédez cela, il est

possible d'écrire votre document à l'aide d'un simple éditeur de texte (tel "notepad" sous Windows !), pour ensuite le compiler en ligne de commande à l'aide de l'exécutable `pdflatex`. Cette méthode de travail est peu conviviale, c'est pourquoi il existe des éditeurs de code LaTeX, qui offrent plusieurs raccourcis pour faciliter la rédaction du document source et pour exécuter les commandes de compilation. Il s'agit exactement de la même logique que lorsque vous utilisez un environnement de développement pour écrire le code source d'un programme informatique.

Éditeur multiplateforme L'éditeur "TeXstudio" fonctionne à la fois sur Linux, Windows et MacOS.

— http://texstudio.sourceforge.net/

Pour utiliser 'TeXstudio", vous devez d'abord installer une distribution LaTeX propre à votre système d'exploitation (voir les paragraphes suivants).

Linux La distribution LaTeX est "TeX Live". Nous vous suggérons aussi d'installer le paquet "texlive-lang-french" pour pouvoir écrire convenablement les accents et guillemets. Vous pouvez normalement installer ces programmes à partir de la plupart des gestionnaires de paquet. Sous Ubuntu, la ligne de commande suivante effectuera tout le travail nécessaire :

— `sudo apt-get install texlive texlive-lang-french`

Outre "TeXstudio", un autre un éditeur convivial pour Linux est "Kile'. Sous Ubuntu, vous pouvez l'installer en ligne de commande :

— `sudo apt-get install kile`

Windows La distribution LaTeX répandue est "MiKTeX" et un éditeur communément utilisé est "TeXnicCenter". Lors de la compilation de sources LaTeX nécessitant des paquets que vous ne possédez pas, MiKTeX vous suggérera de les installer automatiquement.

— http://miktex.org/

— http://www.texniccenter.org/

MacOS La distribution LaTeX répandue est "TeX Live" et un éditeur communément utilisé est "TeXShop". TeX Live et TeXShop sont regroupés dans la distribution "MacTeX" disponnible à l'adresse suivante :

— http://www.tug.org/mactex/

LaTeX et Subversion (SVN)

Étant donné que les fichiers sources d'un document LaTeX sont des fichiers textes, ils se prêtent bien à l'utilisation d'un système de versionnage de fichiers, tel SVN (ou encore Git). Cela peut être un bon moyen de travailler en équipe, ou simplement de s'assurer que vos documents sont conservés en sécurité sur un serveur distant.

Tous les étudiants qui suivent un cours au département d'informatique et de génie logiciel peuvent demander d'obtenir un dépôt SVN hébergé par les serveurs de la faculté. Il suffit de remplir un formulaire sur le site web PIXEL (une fois connecté à votre compte PIXEL, allez dans le menu "Aplications → Logiciels → Création d'un dépôt SVN").

Références et suggestions de lecture

Aigner, M. et G. M. Ziegler. 2010, *Proofs from THE BOOK*, 4e éd., Springer, ISBN 978-3642008559.

Cogis, O. et C. Robert. 2003, *Théorie des Graphes : Au-delà des ponts de Königsberg, Problèmes, théorèmes, algorithmes*, Vuibert, ISBN 2-7117-5321-2.

Doxiadis, A. et C. H. Papadimitriou. 2009, *Logicomix : an epic search for truth*, Bloomsbury, ISBN 9780747597209.

Doxiadis, A. et C. H. Papadimitriou. 2010, *Logicomix*, Vuibert, Paris, ISBN 978-2-7117-4351-3. Traduction française de : Logicomix : an epic search for truth.

Goodaire, E. G. et M. M. Parmenter. 2001, *Discrete Mathematics with Graph Theory*, 2e éd., Prentice Hall PTR, Upper Saddle River, NJ, USA, ISBN 0130920002.

Graham, R. L., D. E. Knuth et O. Patashnik. 1994, *Concrete Mathematics : A Foundation for Computer Science (2nd Edition)*, 2e éd., Addison-Wesley Professional, ISBN 0201558025.

Rosen, K. H. 1998, *Mathématiques discrètes*, Chenelière/McGraw-Hill, Montréal-Toronto, ISBN 2-83461-176-5. Traduction de la 3e édition : Discrete Mathematics and its applications.

Velleman, D. J. 2006, *How to prove it : a structured approach*, 2e éd., Cambridge University Press, ISBN 9780521861243.

Winskel, G. 1993, *The formal semantics of programming languages - an introduction*, Foundation of computing series, MIT Press, ISBN 978-0-262-23169-5.

Index

Section 1.1.6 – Exercices sur l'algèbre booléenne

Exercice 1

Donnez des valeurs de vérité à p et q telles que

1. $p \vee q$ est vrai et $p \wedge q$ est faux
2. $p \vee q$ est vrai et $p \Rightarrow q$ est faux
3. $p \Rightarrow q$ et $q \Rightarrow p$ sont vrais

Exercice 2

Existe-t-il des valeurs de vérité pour p et q telles que (justifiez)

1. $p \wedge q$ est vrai et $p \vee q$ est faux
2. $p \Rightarrow q$ est vrai et $p \vee q$ est faux
3. $p \Rightarrow q$ est vrai et $q \Rightarrow p$ est faux
4. $q \Rightarrow (p \vee \neg p)$ est vrai
5. $(p \vee \neg p) \Rightarrow (q \wedge \neg q)$ est vrai

Exercice 3

Démontrez les propriétés suivantes à l'aide d'une table de vérité :

a) Deuxième loi de De Morgan (Proposition 1.1.4-b) : $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$.

Réponse : Soit p et q deux expressions booléennes.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$(\neg p \wedge \neg q)$	Proposition 1.1.4-b)
v	v	v	f	f	f	f	v
v	f	v	f	f	v	f	v
f	v	v	f	v	f	f	v
f	f	f	v	v	v	v	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$" est vraie.

C.Q.F.D.

b) Distributivité de la disjonction (Proposition 1.1.7-f) : $(p \wedge q) \vee r \;\Leftrightarrow\; (p \vee r) \wedge (q \vee r)$.
Réponse : Soit p, q et r des expressions booléennes.

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$	$p \vee r$	$q \vee r$	$(p \vee r) \wedge (q \vee r)$	Proposition 1.1.7-f)
v	v	v	v	v	v	v	v	v
v	v	f	v	v	v	v	v	v
v	f	v	f	v	v	v	v	v
v	f	f	f	f	v	f	f	v
f	v	v	f	v	v	v	v	v
f	v	f	f	f	f	v	f	v
f	f	v	f	v	v	v	v	v
f	f	f	f	f	f	f	f	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p, q et r, l'expression "$(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$" est vraie.

C.Q.F.D.

Exercice 4

Quand on veut démontrer des énoncés complexes, il est essentiel de savoir, en quelque sorte, éliminer les signes de négation qui sont dans le chemin. Faites-le pour les expressions suivantes (c'est une démonstration par succession d'équivalence, mais on ne sait pas à quoi on va arriver) : une négation ne doit se retrouver que devant une variable simple et non devant une parenthèse. Il suffit d'utiliser les règles de De Morgan, la double négation et la définition de l'implication (voilà pourquoi il faut savoir ces règles par coeur !!!) On ne demande pas d'autre transformation ici.

1. $\neg(p \vee \neg q)$ **Réponse :** $\neg p \wedge q$
2. $\neg(\neg(p \wedge q))$ **Réponse :** $p \wedge q$
3. $\neg(p \Rightarrow q)$ **Réponse :** $p \wedge \neg q$
4. $\neg(\neg p \wedge (q \vee \neg p))$ **Réponse :** $p \vee (\neg q \wedge p)$
5. $\neg(\neg p \Rightarrow (q \vee \neg p))$ **Réponse :** $\neg p \wedge (\neg q \wedge p)$

Exercice 5

Démontrez les propriétés suivantes à l'aide de la technique de démonstration par succession d'équivalences :

a) Deuxième loi de De Morgan (Proposition 1.1.4-b) : $\neg(p \vee q) \;\Leftrightarrow\; \neg p \wedge \neg q$.
NB : Vous pouvez utiliser la Première loi de De Morgan (Proposition 1.1.4-a) et la

propriété de la double négation (Proposition 1.1.5-a).

Réponse : Soit p et q deux expressions booléennes. Démontrons "$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$" :

$$
\begin{array}{ll}
 & \neg(p \vee q) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.5-a – Double négation, 2 fois } \rangle \\
 & \neg(\,\neg(\neg p) \vee \neg(\neg q)\,) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.4-a – Première loi de De Morgan, avec } [p := (\neg p)] \textit{ et } [q := (\neg q)] \rangle \\
 & \neg(\,\neg(\neg p \wedge \neg q)\,) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.5-a – Double négation, avec } [p := (\neg p \wedge \neg q)] \rangle \\
 & \neg p \wedge \neg q
\end{array}
$$

C.Q.F.D.

b) Distributivité de la disjonction (Proposition 1.1.7-f) : $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$.
NB : Vous pouvez utiliser les lois de De Morgan (Proposition 1.1.4), la distributivité de la conjonction (Proposition 1.1.6-f) et la propriété de la double négation (Proposition 1.1.5-a).

Réponse : Soit p, q et r des expressions booléennes. Démontrons "$(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$" :

$(p \wedge q) \vee r$
$\Leftrightarrow$ $\langle$ *Prop 1.1.5-a – Double négation* $\rangle$
$\neg[\neg(\,(p \wedge q) \vee r)\,]$
$\Leftrightarrow$ $\langle$ *Prop 1.1.4-b – Deuxième loi de De Morgan, avec* $[p := (p \wedge q)]$ *et* $[q := r]$ $\rangle$
$\neg[\neg(p \wedge q) \wedge \neg r]$
$\Leftrightarrow$ $\langle$ *Prop 1.1.4-a – Première loi de De Morgan* $\rangle$
$\neg[(\neg p \vee \neg q) \wedge \neg r]$
$\Leftrightarrow$ $\langle$ *Prop 1.1.6-f – Distributivivité de la conjonction, avec* $[p := \neg p]$, $[q := \neg q]$ *et* $[r := \neg r]$ $\rangle$
$\neg[(\neg p \wedge \neg r) \vee (\neg q \wedge \neg r)]$
$\Leftrightarrow$ $\langle$ *Prop 1.1.4-b – Deuxième loi de De Morgan, deux fois* $\rangle$
$\neg[\neg(p \vee r) \vee \neg(q \vee r)]$
$\Leftrightarrow$ $\langle$ *Prop 1.1.4-a – Première loi de De Morgan, avec* $[p := (p \vee r)]$ *et* $[q := (q \vee r)]$ $\rangle$
$\neg[\neg(\,(p \vee r) \wedge (q \vee r)\,)]$
$\Leftrightarrow$ $\langle$ *Prop 1.1.5-a – Double négation* $\rangle$
$(p \vee r) \wedge (q \vee r)$ **C.Q.F.D.**

c) Contradiction (Proposition 1.1.5-c) : $p \wedge \neg p \Leftrightarrow$ `faux`. Vous pouvez utiliser les propositions qui viennent avant... ! et c'est plus facile de commencer par l'expression de droite.

Réponse : Soit p une expression booléenne. Démontrons "$p \wedge \neg p \Leftrightarrow$ `faux`" :

$p \wedge \neg p$
$\Leftrightarrow$ $\langle$ *Prop 1.1.5-a – Double négation* $\rangle$
$\neg(\neg p) \wedge \neg p$
$\Leftrightarrow$ $\langle$ *Prop 1.1.4-b – Deuxième loi de De Morgan* $\rangle$
$\neg(\neg p \vee p)$
$\Leftrightarrow$ $\langle$ *Prop 1.1.7-d – Commutativité de la disjonction* $\rangle$
$\neg(p \vee \neg p)$
$\Leftrightarrow$ $\langle$ *Prop 1.1.5-b – Tiers exclu* $\rangle$
$\neg(\texttt{vrai})$
$\Leftrightarrow$ $\langle$ *Def 1.1.1 – Définition de la négation* $\rangle$
`faux`

C.Q.F.D.

Exercice 6

Considérez l'opérateur **ou exclusif** "$\veebar$" possédant la table de vérité suivante :

p	q	$p \veebar q$
v	v	f
v	f	v
f	v	v
f	f	f

Écrivez une définition possible de l'opérateur "$\veebar$" en utilisant seulement (justifiez brièvement vos réponses) :

a) L'opérateur de négation "$\neg$", de disjonction "$\vee$" et de conjonction "$\wedge$" ;

Réponse : On se base sur l'observation suivante : "$p \veebar q$" est vraie lorsque p et q sont différents, c'est-à-dire que l'un est `vrai` et que l'autre est `faux`. On obtient :

$$p \veebar q \stackrel{\text{def}}{=} (p \wedge \neg q) \vee (\neg p \wedge q)\,.$$

b) L'opérateur de négation "$\neg$" et de disjonction "$\vee$" ;

Réponse : À partir de l'expression trouvée en (a), on applique la première loi de De Morgan sur les deux expressions entre parenthèses. On obtient :

$$p \veebar q \stackrel{\text{def}}{=} \neg(\neg p \vee q) \vee \neg(p \vee \neg q)\,.$$

c) L'opérateur de négation "$\neg$" et le si et seulement si "$\Leftrightarrow$" .

Réponse : À partir de la solution trouvée en (b), on transforme les deux expressions entre parenthèses en appliquant la définition de l'implication. On obtient :

$$\neg(p \Rightarrow q) \vee \neg(q \Rightarrow p)\,.$$

Par la suite, on applique la première loi de De Morgan pour transformer la disjonction en conjonction :

$$\neg\,[\,(p \Rightarrow q) \wedge (q \Rightarrow p)\,]\,.$$

Finalement, on applique simplement la définition de l'opérateur si et seulement si :

$$p \veebar q \stackrel{\text{def}}{=} \neg(p \Leftrightarrow q)\,.$$

Exercice 7

Démontrez chacune des propriétés suivantes à l'aide des deux techniques de démonstration vues jusqu'à maintenant : (*i*) par une table de vérité et (*ii*) par une succession d'équivalences :

a) $(\neg p \Leftrightarrow \neg q) \;\Leftrightarrow\; (p \Leftrightarrow q)$

Réponse (*i*) : Soit p et q deux expressions booléennes.

p	q	$\neg p$	$\neg q$	$(\neg p \Leftrightarrow \neg q)$	$(p \Leftrightarrow q)$	$(\neg p \Leftrightarrow \neg q) \;\Leftrightarrow\; (p \Leftrightarrow q)$
v	v	f	f	v	v	v
v	f	f	v	f	f	v
f	v	v	f	f	f	v
f	f	v	v	v	v	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$(\neg p \Leftrightarrow \neg q) \Leftrightarrow (p \Leftrightarrow q)$" est vraie.

C.Q.F.D.

Réponse (*ii*) : Soit p et q deux expressions booléennes.

$$
\begin{array}{ll}
 & p \Leftrightarrow q \\
\Leftrightarrow & \quad \langle\ \textit{Def 1.1.3 – Définition du si et seulement si}\ \rangle \\
 & (p \Rightarrow q) \wedge (q \Rightarrow p) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.9 – Contraposition, 2 fois}\ \rangle \\
 & (\neg q \Rightarrow \neg p) \wedge (\neg p \Rightarrow \neg q) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.6-d – Commutativité de la conjonction}\ \rangle \\
 & (\neg p \Rightarrow \neg q) \wedge (\neg q \Rightarrow \neg p) \\
\Leftrightarrow & \quad \langle\ \textit{Def 1.1.3 – Définition du si et seulement si}\ \rangle \\
 & \neg p \Leftrightarrow \neg q
\end{array}
$$

C.Q.F.D.

b) $(\neg p \Leftrightarrow q) \;\Leftrightarrow\; (p \Leftrightarrow \neg q)$

Réponse (*i*) : Soit p et q deux expressions booléennes.

p	q	$\neg p$	$\neg q$	$(\neg p \Leftrightarrow q)$	$(p \Leftrightarrow \neg q)$	$(\neg p \Leftrightarrow q) \;\Leftrightarrow\; (p \Leftrightarrow \neg q)$
v	v	f	f	f	f	v
v	f	f	v	v	v	v
f	v	v	f	v	v	v
f	f	v	v	f	f	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$(\neg p \Leftrightarrow q) \Leftrightarrow (p \Leftrightarrow \neg q)$" est vraie. **C.Q.F.D.**

Réponse (*ii*) : Soit p et q deux expressions booléennes.

$$
\begin{array}{ll}
 & \neg p \Leftrightarrow q \\
\Leftrightarrow & \quad \langle\ \textit{Résultat démontré en (a), avec } [p := (\neg p)]\ \rangle \\
 & \neg(\neg p) \Leftrightarrow \neg q \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.5-a – Double négation}\ \rangle \\
 & p \Leftrightarrow \neg q
\end{array}
$$

C.Q.F.D.

c) $(\neg p \Leftrightarrow q) \ \Leftrightarrow\ \neg(p \Leftrightarrow q)$

Réponse (*i*) : Soit p et q deux expressions booléennes.

p	q	$\neg p$	$(\neg p \Leftrightarrow q)$	$(p \Leftrightarrow q)$	$\neg(p \Leftrightarrow q)$	$(\neg p \Leftrightarrow q) \ \Leftrightarrow\ \neg(p \Leftrightarrow q)$
v	v	f	f	v	f	v
v	f	f	v	f	v	v
f	v	v	v	f	v	v
f	f	v	f	v	f	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$(\neg p \Leftrightarrow q) \Leftrightarrow \neg(p \Leftrightarrow q)$" est vraie.

C.Q.F.D.

Réponse (*ii*) : Soit p et q deux expressions booléennes.

$$
\begin{array}{ll}
 & \neg p \Leftrightarrow q \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.11 – Réécriture du si et seulement si}\ \rangle \\
 & (\neg p \wedge q) \vee (\neg(\neg p) \wedge \neg q) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.5-a – Double négation}\ \rangle \\
 & (\neg p \wedge \neg(\neg q)) \vee (\neg(\neg p) \wedge \neg q) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.4-b – Loi de De Morgan, 2 fois}\ \rangle \\
 & \neg(p \vee \neg q) \vee \neg(\neg p \vee q) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.4-a – Loi de De Morgan, avec } [p := (p \vee \neg q)] \textit{ et } [q := (\neg p \vee q)]\ \rangle \\
 & \neg(\,(p \vee \neg q) \wedge (\neg p \vee q)\,) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.6-d – Commutativité de la conjonction}\ \rangle \\
 & \neg(\,(\neg p \vee q) \wedge (p \vee \neg q)\,) \\
\Leftrightarrow & \quad \langle\ \textit{Def 1.1.2 – Définition de l'implication, 2 fois}\ \rangle \\
 & \neg(\,(p \Rightarrow q) \wedge (q \Rightarrow p)\,) \\
\Leftrightarrow & \quad \langle\ \textit{Def 1.1.3 – Définitions du si et seulement si}\ \rangle \\
 & \neg(\,p \Leftrightarrow q\,)
\end{array}
$$

C.Q.F.D.

d) $(\,\neg p \Rightarrow (p \Rightarrow q)\,)$

Réponse : Soit p et q deux expressions booléennes.

p	q	$\neg p$	$(p \Rightarrow q)$	$(\neg p \Rightarrow (p \Rightarrow q))$
v	v	f	v	v
v	f	f	f	v
f	v	v	v	v
f	f	v	v	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$(\neg p \Rightarrow (p \Rightarrow q))$" s'évalue à `vrai`.

C.Q.F.D.

Réponse (*ii*) : Soit p et q deux expressions booléennes.

$$
\begin{array}{ll}
 & \neg p \Rightarrow (p \Rightarrow q) \\
\Leftrightarrow & \quad \langle \textit{ Def 1.1.2 – Définition de l'implication } \rangle \\
 & \neg p \Rightarrow (\neg p \vee q) \\
\Leftrightarrow & \quad \langle \textit{ Def 1.1.2 – Définition de l'implication, avec } [p := \neg p] \textit{ et } [q := (\neg p \vee q)] \rangle \\
 & \neg(\neg p) \vee \neg p \vee q \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.5-a – Double négation } \rangle \\
 & p \vee \neg p \vee q \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.5-b – Tiers exclu } \rangle \\
 & \texttt{vrai} \vee q \\
\Leftrightarrow & \quad \left\langle \textit{ Prop 1.1.7-b – Élément absorbant } \right\rangle \\
 & \texttt{vrai}
\end{array}
$$

C.Q.F.D.

e) $(p \Rightarrow (\neg p \Rightarrow q))$

Réponse (*i*) :Soit p et q deux expressions booléennes.

p	q	$\neg p$	$(\neg p \Rightarrow q)$	$(p \Rightarrow (\neg p \Rightarrow q))$
v	v	f	v	v
v	f	f	v	v
f	v	v	v	v
f	f	v	f	v

Pour toutes les combinaisons de valeurs de vérité possibles attribuables aux expressions p et q, l'expression "$(p \Rightarrow (\neg p \Rightarrow q))$" s'évalue à `vrai`.

C.Q.F.D.

Réponse (*ii*) : Soit p et q deux expressions booléennes.

$$
\begin{array}{ll}
 & p \Rightarrow (\neg p \Rightarrow q) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.5-a – Double négation } \rangle \\
 & \neg(\neg p) \Rightarrow (\neg p \Rightarrow q) \\
\Leftrightarrow & \quad \langle \textit{ Résultat démontré en (d), avec } p := (\neg p)] \rangle \\
 & \texttt{vrai}
\end{array}
$$

C.Q.F.D.

f) $(p \Rightarrow \texttt{faux}) \Leftrightarrow \neg p$

Réponse (*i*) : Soit p une expression booléenne.

p	$p \Rightarrow \texttt{faux}$	$\neg p$	$(p \Rightarrow \texttt{faux}) \Leftrightarrow \neg p$
v	f	f	v
f	v	v	v

Pour les deux valeurs de vérité attribuables à l'expression p, l'expression $p \Rightarrow \texttt{faux} \Leftrightarrow \neg p$ est vraie.

C.Q.F.D.

Réponse (*ii*) : Soit p une expression booléenne.

$$
\begin{array}{ll}
 & p \Rightarrow \texttt{faux} \\
\Leftrightarrow & \quad \langle \textit{ Def 1.1.2 – Définition de l'implication } \rangle \\
 & \neg p \vee \texttt{faux} \\
\Leftrightarrow & \quad \left\langle \textit{ Prop 1.1.7-a – Élément neutre } \right\rangle \\
 & \neg p
\end{array}
$$

C.Q.F.D.

Exercice 8

Déterminez si les instances suivantes du problème SAT sont satisfiables. Pour les instances satisfiables, fournissez une assignation de variables telle que l'expression booléenne est vraie. Pour les instances insatisfiables, démontrez votre résultat à l'aide d'une table de vérité.

a) $\psi_a \;=\; (x_1 \vee x_2) \wedge x_3 \wedge (\neg x_1 \vee \neg x_3) \wedge (\neg x_2 \vee \neg x_3)$.

Réponse : L'instance ψ_a est insatisfiable, comme le montre la table de vérité suivante :

x_1	x_2	x_3	$\overbrace{x_1 \vee x_2}^{c_1}$	$\overbrace{x_3}^{c_2}$	$\overbrace{\neg x_1 \vee \neg x_3}^{c_3}$	$\overbrace{\neg x_2 \vee \neg x_3}^{c_4}$	$\overbrace{c_1 \wedge c_2 \wedge c_3 \wedge c_4}^{\psi_a}$
v	v	v	v	v	f	f	f
v	v	f	v	f	v	v	f
v	f	v	v	v	f	v	f
v	f	f	v	f	v	v	f
f	v	v	v	v	v	f	f
f	v	f	v	f	v	v	f
f	f	v	f	v	v	v	f
f	f	f	f	f	v	v	f

b) $\psi_b \;=\; (x_1 \vee x_2) \wedge x_3 \wedge (x_1 \vee \neg x_3) \wedge (\neg x_2 \vee \neg x_3)$.

Réponse : L'instance ψ_b est satisfiable. En effet, l'assignation de variables suivante satisfait ψ_b : $x_1 = \texttt{vrai},\ x_2 = \texttt{faux},\ x_3 = \texttt{vrai}$.

c) $\psi_c \;=\; (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_3)$.

Réponse : L'instance ψ_a est insatisfiable, comme le montre la table de vérité suivante :

x_1	x_2	x_3	$\overbrace{x_1 \vee x_2}^{c_1}$	$\overbrace{\neg x_1 \vee x_3}^{c_2}$	$\overbrace{x_1 \vee \neg x_2}^{c_3}$	$\overbrace{\neg x_2 \vee x_3}^{c_4}$	$\overbrace{\neg x_1 \vee \neg x_3}^{c_5}$	$\overbrace{c_1 \wedge c_2 \wedge c_3 \wedge c_4 \wedge c_5}^{\psi_c}$
v	v	v	v	v	v	v	f	f
v	v	f	v	f	v	f	v	f
v	f	v	v	v	v	v	f	f
v	f	f	v	f	v	v	v	f
f	v	v	v	v	f	v	v	f
f	v	f	v	v	f	f	v	f
f	f	v	f	v	v	v	v	f
f	f	f	f	v	v	v	v	f

d) $\psi_d \;=\; (\neg x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_2 \vee x_3 \vee \neg x_4)$.

Réponse : L'instance ψ_d est satisfiable. En effet, l'assignation de variables suivante satisfait ψ_d : $x_1 = \texttt{faux},\ x_2 = \texttt{faux},\ x_3 = \texttt{faux},\ x_4 = \texttt{faux}$.

Exercice 9

En utilisant les propriétés que nous avons vues dans cette section, réécrivez les expressions suivantes sous forme normale conjonctive :

a) $x_1 \Leftrightarrow x_2$

Réponse :

$$
\begin{array}{lll}
 & x_1 \Leftrightarrow x_2 & \\
\Leftrightarrow & (x_1 \Rightarrow x_2) \wedge (x_2 \Rightarrow x_1) & \langle \textit{ Def 1.1.3 – Définition du si et seulement si } \rangle \\
\Leftrightarrow & (\neg x_1 \vee x_2) \wedge (x_1 \vee \neg x_2) & \langle \textit{ Def 1.1.2 – Définition de l'implication (2 fois) } \rangle
\end{array}
$$

b) $(x_1 \vee x_2) \wedge (x_3 \vee x_4)$

Réponse : L'expression est déjà sous forme normale conjonctive !

c) $(x_1 \wedge x_2) \vee (x_3 \wedge x_4)$

Réponse :

$$
\begin{array}{ll}
 & (x_1 \wedge x_2) \vee (x_3 \wedge x_4) \\
\Leftrightarrow & \left\langle \begin{array}{l} \textit{Prop 1.1.7-f – Distributivité de la disjonction, avec } [p := x_1],\ [q := x_2] \\ \textit{et } [r := (x_3 \wedge x_4)] \end{array} \right\rangle \\
 & [x_1 \vee (x_3 \wedge x_4)] \wedge [x_2 \vee (x_3 \wedge x_4)] \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.7-f – Distributivité de la disjonction (2 fois) } \rangle \\
 & [(x_1 \vee x_3) \wedge (x_1 \vee x_4)] \wedge [(x_2 \vee x_3) \wedge (x_2 \vee x_4)] \\
\Leftrightarrow & \quad \langle \textit{ Priorité des opérateurs } \rangle \\
 & (x_1 \vee x_3) \wedge (x_1 \vee x_4) \wedge (x_2 \vee x_3) \wedge (x_2 \vee x_4)
\end{array}
$$

d) $(x_1 \Rightarrow x_2) \Rightarrow ((x_3 \Rightarrow x_4) \Rightarrow x_5)$

Réponse :

$$
\begin{array}{ll}
 & (x_1 \Rightarrow x_2) \Rightarrow ((x_3 \Rightarrow x_4) \Rightarrow x_5) \\
\Leftrightarrow & \quad \langle \textit{ Def 1.1.2 Définition de l'implication (2 fois) } \rangle \\
 & \neg(x_1 \Rightarrow x_2) \vee (\neg(x_3 \Rightarrow x_4) \vee x_5) \\
\Leftrightarrow & \quad \langle \textit{ Def 1.1.2 Définition de l'implication (2 fois) } \rangle \\
 & \neg(\neg x_1 \vee x_2) \vee (\neg(\neg x_3 \vee x_4) \vee x_5) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.4-b Deuxième loi de De Morgan (2 fois) } \rangle \\
 & (\neg\neg x_1 \wedge \neg x_2) \vee ((\neg\neg x_3 \wedge \neg x_4) \vee x_5) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.5-a Double négation (2 fois) } \rangle \\
 & (x_1 \wedge \neg x_2) \vee ((x_3 \wedge \neg x_4) \vee x_5) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.7-f Distributivité de la disjonction } \rangle \\
 & (x_1 \wedge \neg x_2) \vee ((x_3 \vee x_5) \wedge (\neg x_4 \vee x_5)) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.7-f Distributivité de la disjonction } \rangle \\
 & ((x_1 \wedge \neg x_2) \vee (x_3 \vee x_5)) \wedge ((x_1 \wedge \neg x_2) \vee (\neg x_4 \vee x_5)) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.1.7-f Distributivité de la disjonction (2 fois) } \rangle \\
 & ((x_1 \vee (x_3 \vee x_5)) \wedge (\neg x_2 \vee (x_3 \vee x_5))) \wedge ((x_1 \vee (\neg x_4 \vee x_5)) \wedge (\neg x_2 \vee (\neg x_4 \vee x_5))) \\
\Leftrightarrow & \quad \langle \textit{ Piorité des opérateurs } \rangle \\
 & (x_1 \vee x_3 \vee x_5) \wedge (\neg x_2 \vee x_3 \vee x_5) \wedge (x_1 \vee \neg x_4 \vee x_5) \wedge (\neg x_2 \vee \neg x_4 \vee x_5)
\end{array}
$$

Exercice 10

Imaginons qu'on vous demande d'écrire un "solveur SAT", c'est-à-dire un programme informatique qui reçoit en entrée une instance du problème SAT-CNF (soit une expression booléenne sous forme normale conjonctive) et détermine si cette instance est satisfiable.

a) Votre programme reçoit en entrée une instance du problème SAT-CNF décrite ainsi :
   — Un nombre n indiquant le nombre de variables du problème. On représente ces variables par $x_1, x_2, \ldots, x_n$;
   — Une collection de m clauses que l'on représente par $C_1, C_2, \ldots, C_m$.

   On vous fournit une fonction déjà programmée "`évaluerClause`$(C_j, a_1, a_2, \ldots, a_n)$" qui retourne le résultat de l'évaluation de la clause C_j (c'est-à-dire `vrai` ou `faux`) avec l'assignation de valeurs $x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$.

   Expliquez, en vos mots ou à l'aide d'un pseudo-code, la procédure que doit employer votre programme pour vérifier si une instance est satisfiable ou insatisfiable. Inspirez-vous de la méthode que vous utilisez pour bâtir une table de vérité.

Réponse (sous forme de texte) : Pour chacune des 2^n assignations possibles de valeurs de vérité aux variables $x_1, \ldots, x_n$, effectuer la procédure suivante :

— Vérifier à l'aide de la fonction `évaluerClause` si l'assignation de variables permet d'évaluer chacune des m clauses $C_1, \ldots, C_m$ à `vrai`.
— Si chacune des m clauses est vraie avec cette assignation de variables, alors le programme déclare que l'instance est *satisfiable*.

Si aucune des 2^n assignations de variables n'a permis d'évaluer à `vrai` l'ensemble des m clauses, alors le programme déclare que l'instance est *insatisfiable*.

Réponse (sous forme d'un pseudo-code) : Nous présentons ici le pseudo-code d'un algorithme, sous forme d'une fonction récursive. L'appel initial à la fonction doit respecter la forme "`solveurSAT`$(0, C_1, \ldots, C_m, a_1, \ldots, a_n)$", où $a_1, \ldots, a_n$ sont initialement des valeurs quelconques (elles sont initialisées au cours de l'exécution de l'algorithme). L'algorithme retourne la valeur `vrai` si l'instance est satisfiable et `faux` si l'instance est insatisfiable.

```
solveurSAT(i, C_1, ..., C_m, a_1, ..., a_n)
  i ← i + 1
  Si i > n alors
    Pour j = 1 à m Faire
      Si évaluerClause(C_j, a_1, ..., a_n) = faux alors
        Retourner faux
      Fin Si
    Fin Pour
    Retourner vrai
  Sinon
    a_i ← vrai
    eval_1 ← solveurSAT(i, C_1, ..., C_m, a_1, ..., a_n)
    a_i ← faux
    eval_2 ← solveurSAT(i, C_1, ..., C_m, a_1, ..., a_n)
    Retourner eval_1 ∨ eval_2
  Fin Si
```

b) Serait-il possible d'utiliser votre programme pour vérifier si une expression booléenne est toujours vraie ? Si oui, expliquez comment. Sinon, expliquez pourquoi.

Réponse : Oui ! Considérons une expression booléenne A. Pour déterminer si l'expression A est toujours vraie, il suffit d'exécuter le solveur SAT sur sa négation (c'est-à-dire $\neg A$).

Si le solveur détermine que l'instance $\neg A$ est insatisfiable, cela signifie qu'il n'existe

pas d'assignation de variables telles que l'expression $\neg A$ est vraie, donc l'expression $\neg A$ est toujours fausse, alors l'expression A est toujours vraie. De même, si le solveur détermine que l'instance $\neg A$ est satisfiable, cela signifie qu'il existe une assignation de variables telle que l'expression A est fausse.

Bien sûr, il faut transformer l'instance $\neg A$ sous forme normale conjonctive à l'aide des définitions et des propriétés des opérateurs booléens avant d'exécuter le solveur SAT.

Exercice 11

À la page 55 du présent document, la section 1.3 débute par une citation d'Eugène Ionesco, digne représentant du théâtre de l'absurde. Dans cette citation, un prétendu logicien affirme : "Tous les chats sont mortels. Socrate est mortel. Donc Socrate est un chat."

a) Expliquez dans vos propres mots pourquoi ce raisonnement est erroné ;

Réponse : Il est vrai que tous les chats sont mortels, mais cela ne signifie pas que tous les mortels sont des chats !

b) Réécrivez l'affirmation de l'aspirant logicien en utilisant les opérateurs booléens. Pour simplifier la tâche, considérez l'affirmation sous la forme : "Si Socrate est un chat, alors il est mortel. Socrate est mortel. Donc Socrate est un chat.". De même, utilisez les variables c et m pour représenter les expressions suivantes :

$$\begin{aligned} c &= \textit{Socrate est un chat}, \\ m &= \textit{Socrate est mortel}. \end{aligned}$$

Réponse : $[\,(c \Rightarrow m) \wedge m\,] \;\Rightarrow\; c\,.$

c) À partir de l'expression booléenne trouvée en (b), démontrez à l'aide d'une table de vérité que l'affirmation du pauvre logicien est fausse ;

Réponse :

c	m	$c \Rightarrow m$	$(c \Rightarrow m) \wedge m$	$[\,(c \Rightarrow m) \wedge m\,] \;\Rightarrow\; c$
v	v	v	v	v
v	f	f	f	v
f	v	v	v	f
f	f	v	f	v

La 3e ligne de la table de vérité montre que l'expression n'est pas vraie dans le cas où $c =$ `faux` et $m =$ `vrai`, c'est-à-dire si on pose comme hypothèse "Socrate n'est pas un chat" et "Socrate est mortel".

d) Suggérez une modification à l'affirmation du logicien afin qu'elle soit toujours vraie.

Réponse : On peut imaginer plusieurs solutions, notamment :

— “Tous les chats, et seulement les chats, sont mortels. Socrate est mortel. Donc Socrate est un chat.” :

$$[\,(c \Leftrightarrow m) \wedge m\,] \;\Rightarrow\; c\,.$$

— “Tous les chats sont mortels. Socrate est un chat. Donc Socrate est mortel.” :

$$[\,(c \Rightarrow m) \wedge c\,] \;\Rightarrow\; m\,.$$

— “Tous les mortels sont des chats. Socrate est mortel. Donc Socrate est un chat.” :

$$[\,(m \Rightarrow c) \wedge m\,] \;\Rightarrow\; c\,.$$

Ces affirmations peuvent sembler farfelues, mais il s’agit d’expressions booléennes valides, puisqu’elles sont toujours évaluées à `vrai` pour toutes les valeurs des expressions c et m. Par exemple, la dernière affirmation nous dit que *si on accepte les hypothèses* que “tous les mortels sont des chats” et que “Socrate est mortel”, *alors* on peut conclure que “Socrate est un chat”.

Section 1.2.7 – Exercices sur la logique du premier ordre

Exercice 1

Définissez des prédicats et fonctions appropriées (pensez-y d'abord sans l'indice[5]) et formalisez ensuite les phrases suivantes

1. Tout le monde aime Léo.
2. Léo aime quelqu'un.
3. Léo n'aime personne
4. Tout le monde aime tout le monde
5. Quelqu'un aime tout le monde
6. Tout le monde s'aime lui-même
7. Personne n'aime tout le monde
8. Quelqu'un n'aime personne

Réponses :

1. $(\forall x \in P \mid x \text{ aime Léo})$
2. $(\exists x \in P \mid \text{ Léo aime } x)$
3. $(\forall x \in P \mid \neg(\text{ Léo aime } x))$
4. $(\forall x \in P \mid (\forall y \in P \mid x \text{ aime } y))$
5. $(\exists x \in P \mid (\forall y \in P \mid x \text{ aime } y))$
6. $(\forall x \in P \mid x \text{ aime } x)$
7. $\neg(\exists x \in P \mid (\forall y \in P \mid x \text{ aime } y))$
8. $(\exists x \in P \mid (\forall y \in P \mid \neg(x \text{ aime } y)))$

Exercice 2

Est-ce que les situations suivantes sont possibles ? Justifiez.

1. $(\forall x \in E \mid P(x))$ est vrai, mais $\neg(\exists x \in E \mid \neg P(x))$ est faux
   Réponse : non car ils sont équivalents. En effet, par De Morgan, $\neg(\exists x \in E \mid \neg P(x))$ est équiv. à $(\forall x \in E \mid \neg(\neg P(x)))$ qui est équiv. à $(\forall x \in E \mid P(x))$
2. $(\exists x \in E \mid P(x))$ est vrai, mais $\neg(\forall x \in E \mid \neg P(x))$ est faux
   Réponse : non car ils sont équivalents. En effet, , par De Morgan, $\neg(\forall x \in E \mid \neg P(x))$ est équiv. à $(\exists x \in E \mid \neg\neg P(x))$, qui est équiv. à $(\exists x \in E \mid P(x))$
3. $(\forall x \in E \mid P(x)) \Rightarrow (\exists x \in E \mid P(x))$ est faux
   Réponse : Pour que ce soit faux, selon la table de vérité de l'implication, il faudrait que $(\forall x \in E \mid P(x))$ soit vrai mais $(\exists x \in E \mid P(x))$ soit faux. Il n'y a qu'une façon, c'est si E est vide. Ainsi, l'existence d'un x qui satisfait P est fausse, mais comme E est vide, le $\forall$ est vrai. C'est subtil...
4. $(\exists x \in E \mid P(x)) \Rightarrow (\forall x \in E \mid P(x))$ est vrai
   Réponse : Ceci n'est pas toujours vrai, mais ça peut être vrai, c'est tout ce qu'on nous demande, alors donnons un exemple. Posons $E := \mathbb{N}$, $P(x) := x \geq 0$. Cela rend l'expression vraie, tel que demandé. On aurait pu aussi rendre le $\exists$ faux, ce qui aurait rendu l'implication vraie... !

5. Prenons l'ensemble P des *Personnes*, précisons que Léo $\in P$ et prenons le prédicat à deux variables : $aime(x, y)$ qui pourrait aussi être écrit "x aime y"

Exercice 3
Trouvez un ensemble E et un prédicat P tel que $(\exists x \in E \mid P(x)) \Rightarrow \neg(\forall x \in E \mid P(x))$ est vrai. Est-ce que cette expression est toujours vraie ?
Réponse :

Pour rendre cette expression vraie, on peut prendre un ensemble E et un prédicat P qui rendent la partie de gauche fausse. Ainsi, l'expression sera nécessairement vraie. Par exemple, on peut choisir $E := \mathbb{N}$ et $P(x) := (x < 0)$.

Par contre, l'expression n'est pas *toujours* vraie. Prenons simplement $E := \mathbb{N}$ et $P(x) := (x \geq 0)$. Alors $(\exists x \in E \mid P(x))$ est vrai, mais $\neg(\forall x \in E \mid P(x))$, qui est équivalent à $(\exists x \in E \mid \neg P(x))$, est faux. L'implication est donc fausse.

Exercice 4
Quelle est la différence entre chaque paire d'expressions suivante ? s'il y a une différence, trouver un exemple de phrase, en français, qui l'illustre

1. $(\forall x \in E \mid \neg P(x))$ et $\neg(\forall x \in E \mid P(x))$?
   Réponse : C'est la différence entre *tout le monde est sans chat* et *ce n'est pas tout le monde qui a un chat*. (Remarquez, on n'a pas écrit pour le premier *tout le monde n'a pas de chat*, car en français ceci veut plutôt dire que ce n'est pas vrai que tout le monde a un chat : c'est l'ambigüité de la langue ! ! !)

2. $(\exists x \in E \mid \neg P(x))$ et $\neg(\exists x \in E \mid P(x))$?
   Réponse : C'est la différence entre *il existe quelqu'un qui n'a pas de chat* et *personne n'a de chat*

3. $(\forall x \mid x \in E \Rightarrow P(x))$ et $(\forall x \mid x \in E \wedge P(x))$?
   Réponse : Prenons E comme l'ensemble des *jeunes* (ce qui englobe de plus en plus de monde ! ! ! !) et $P(x)$ comme x *a un téléphone*. Le 1er veut dire *tous les jeunes ont un téléphone* et le 2e veut dire *tout le monde est jeune et a un téléphone*

4. $(\exists x \mid x \in E \Rightarrow P(x))$ et $(\exists x \mid x \in E \wedge P(x))$?
   Réponse : Prenons encore une fois E comme l'ensemble des *jeunes* et $P(x)$ comme x *a un téléphone*. S'il n'y a pas de jeune dans notre population (donc, si E est l'ensemble vide), alors la première expression est vraie, alors que la deuxième est fausse.

Confrontez 3 et 4 à la définition 1.2.2.

Exercice 5

Éliminez les négations devant les parenthèses

1. $\neg(\forall x \in E \mid P(x))$ — **Réponse :** $(\exists x \in E \mid \neg P(x))$
2. $\neg(\exists x \in E \mid \neg P(x))$ — **Réponse :** $(\forall x \in E \mid P(x))$
3. $\neg(\exists x \in E \mid x$ aime Léo$)$ — **Réponse :** $(\forall x \in E \mid x$ n'aime pas Léo$)$
4. $\neg((\forall x \in E \mid x > 3) \wedge (\exists x \in E \mid 5 - x > 0))$ — **Rép. :** $(\exists x \in E \mid x \leq 3) \vee (\forall x \in E \mid 5 - x \leq 0)$
5. $\neg(\forall x \in E \mid (\exists y \in F \mid x < y))$ — **Réponse :** $(\exists x \in E \mid (\forall y \in F \mid x \geq y))$

Exercice 6

Écrivez en logique :

— Un nombre pair multiplié par un nombre impair donne un nombre pair. Vous pouvez utiliser les prédicats pair(z) et impair(z) suivants, pour $z \in \mathbb{Z}$:

$$\text{pair}(z) \stackrel{\text{def}}{=} (\exists k \in \mathbb{Z} \mid z = 2k)$$
$$\text{impair}(z) \stackrel{\text{def}}{=} (\exists k \in \mathbb{Z} \mid z = 2k + 1)$$

— Un truc bien connu pour savoir si un nombre se divise par 9 : additionner les chiffres de sa représentation en base 10 et évaluer si ce nombre se divise par 9. Écrivez cet énoncé pour les nombres positifs de 2 chiffres (par exemple 21, 34, 99), c'est-à-dire : un nombre est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. Ces nombres s'écrivent sous la forme $10d+u$ où $d, u \in \{0, 1, 2, \ldots, 9\}$ (la dizaine et l'unité). Rappelons la définition du modulo, pour 9 (c.-à-d. le reste de la division par 9), pour un $n \in \mathbb{N}$:

$$(n \bmod 9 = r) \stackrel{\text{def}}{=} (r \in \{0, 1, 2, \ldots, 8\}) \wedge (\exists k \in \mathbb{N} \mid n = 9k + r).$$

Un nombre n est donc divisible par 9 si $n \bmod 9 = 0$. **Réponse** : $(\forall d, u \in \{0, 1, 2, \ldots, 9\} \mid ((10d + u) \bmod 9 = 0 \Leftrightarrow (d + u) \bmod 9 = 0))$.

Section 1.2.8 – Exercices sur les ensembles

Exercice 1 : Définissez les ensembles suivants par compréhension :

a) l'ensemble des entiers non négatifs plus petits que 4 ;
Réponse 1 : $\{n \in \mathbb{N} \mid n < 4\}$
Réponse 2 : $\{n \in \mathbb{Z} \mid 0 \leq n < 4\}$
(Ceci n'est pas en compréhension : $\{0, 1, 2, 3\}$.)

b) l'ensemble des entiers strictement positifs divisibles par 3 et plus petits que 4 ;
Réponse 1 : $\{i \in \mathbb{N} \mid 0 < i < 4 \wedge i \bmod 3 = 0\}$
Note : L'opérateur modulo " mod " correspond au reste de la division entière. Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$, nous avons : $a \bmod b \stackrel{\text{def}}{=} a - b \cdot \left\lfloor \frac{a}{b} \right\rfloor$
Réponse 2 : $\{3i \mid i \in \mathbb{N}^* \wedge 3i < 4\}$
(Ceci n'est pas en compréhension : $\{3\}$.)

c) l'ensemble des nombres impairs ;
Réponse 1 : $\{2i + 1 \mid i \in \mathbb{Z}\}$
Réponse 2 : $\{i \in \mathbb{Z} \mid i \bmod 2 = 1\}$
Réponse 3 : $\{n \mid (\exists i \in \mathbb{Z} \mid 2i + 1 = n)\}$
(Ceci n'est pas en compréhension : $\{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots\}$.)

d) l'ensemble des carrés dont la racine est située entre 10 et 22 ;
Réponse 1 : $\{i^2 \mid i \in \mathbb{N} \wedge 10 \leq i \leq 22\}$
Réponse 2 : $\{n \in \mathbb{N} \mid 10 \leq \sqrt{n} \leq 22\}$
(Ceci n'est pas en compréhension : $\{10^2, 11^2, 12^2, 13^2, \ldots, 22^2\}$.)

e) l'ensemble des puissances de 2.
Réponse 1 : $\{2^x \mid x \in \mathbb{N}\}$
Réponse 2 : $\{n \in \mathbb{N} \mid (\exists i \in \mathbb{N} \mid n = 2^i)\}$
(Ceci n'est pas en compréhension : $\{1, 2, 4, 8, 16, 32, 64, 128, \ldots\}$.)

Exercice 2 : Donnez une description en *langue française* des ensembles suivants :

a) $\{x \in \mathbb{Z} \mid 0 < x \wedge x \text{ est pair}\}$;
Réponse : L'ensemble des entiers strictement positifs pairs.

b) $\{x \in \mathbb{N}^* \mid 0 < x \wedge x \bmod 2 = 0\}$;
Réponse : Même réponse qu'en a)

c) $\{p \mid q \in \mathbb{Z} \wedge r = 2 \wedge p > 0 \wedge p = q \cdot r\}$;
Réponse : Même réponse qu'en a)

d) $\{z \in \mathbb{N}^* \mid (\exists y \in \mathbb{Z} \mid 2y = z)\}$;
Réponse : Même réponse qu'en a)

e) $\{z \in \mathbb{Z} \mid -1 < z \wedge (\exists x \in \mathbb{Z} \mid z = x \cdot y) \wedge (y = 2 \vee y = 3)\}$;
Réponse : L'ensemble des entiers non négatifs qui sont divisibles par 2 ou par 3.

f) $\{z \in \mathbb{Z} \mid -1 < x \wedge 1 < y < 4 \wedge z = x \cdot y\}$.
Réponse : Même réponse qu'en e)

Exercice 3 :

a) Définissez l'ensemble suivant par compréhension. L'ensemble des nombres premiers compris entre 10 et 30. Vous pouvez utiliser la fonction booléenne premier(i) qui retourne la valeur de l'expression "i est un nombre premier", c'est-à-dire `vrai` si i est premier, `faux` sinon.
Réponse : $\{i \in \mathbb{Z} \mid 10 \leq i \leq 30 \wedge \text{premier}(i)\}$. Si on avait demandé de donner l'ensemble en extension, la réponse serait $\{11, 13, 17, 19, 23, 29\}$.

b) Décrivez l'ensemble suivant en français.

$$\{x \mid y \in \mathbb{N} \wedge z \in \{2, 3\} \wedge x = y^z\}$$

Réponse : L'ensemble des entiers positifs ou nuls qui sont des carrés ou cubes. En extension :

$$\{0, 1, 4, 8, 9, 16, 25, 27, 36, 49, \ldots\}.$$

Exercice 4 : Soit l'ensemble de couleurs $C = \{\texttt{rouge}, \texttt{vert}, \texttt{bleu}\}$. Écrivez les ensembles suivants en extensions :

a) $\mathcal{P}(C)$;
Réponse :

$$\mathcal{P}(C) = \left\{ \begin{array}{l} \emptyset, \{\texttt{rouge}\}, \{\texttt{vert}\}, \{\texttt{bleu}\}, \{\texttt{rouge}, \texttt{vert}\}, \{\texttt{rouge}, \texttt{bleu}\}, \\ \{\texttt{vert}, \texttt{bleu}\}, \{\texttt{rouge}, \texttt{vert}, \texttt{bleu}\} \end{array} \right\}$$

b) $\mathcal{P}(C) \cap \emptyset$;
Réponse : $\mathcal{P}(C) \cap \emptyset \;=\; \emptyset$

c) $\mathcal{P}(C) \cap \mathcal{P}(\emptyset)$;
Réponse : $\mathcal{P}(C) \cap \mathcal{P}(\emptyset) \;=\; \mathcal{P}(C) \cap \{\emptyset\} \;=\; \{\emptyset\}$

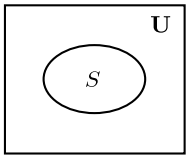
d) $\{c \in \mathcal{P}(C) \mid 2 > |c|\}$;
Réponse : { $\emptyset$, {`rouge`}, {`vert`}, {`bleu`} }

e) $\{c \in \mathcal{P}(C) \mid c \subseteq \{\texttt{rouge}, \texttt{bleu}\}\}$;
Réponse : { $\emptyset$, {`rouge`}, {`bleu`}, {`rouge`, `bleu`} }

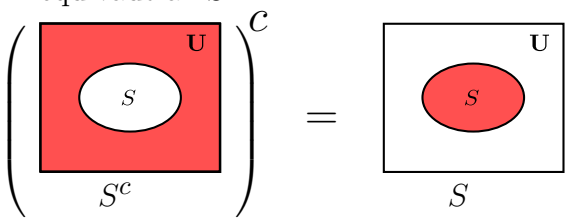
f) $\{c \in \mathcal{P}(C) \mid \{\texttt{rouge}, \texttt{bleu}\} \subseteq c\}$.
Réponse : { {`rouge`, `bleu`}, {`rouge`, `vert`, `bleu`} }

Exercice 5 : Démontrez chacune des propriétés suivantes à l'aide des deux techniques de démonstration vues jusqu'à maintenant, c'est-à-dire (*i*) à l'aide de diagrammes de Venn (démonstration par cas) et (*ii*) par une succession d'équivalences :

a) Complémentarité (Proposition 1.2.8-a) : $(S^c)^c = S$;
Réponse (*i*) : Soit S un ensemble. Démontrons "$(S^c)^c = S$" à l'aide de diagrammes de Venn. Considérons la représentation suivante :



Démontrons que "$(S^c)^c$" équivaut à "S" :



Les diagrammes de Venn obtenus montrent que les éléments appartenant à "$(S^c)^c$" sont les mêmes que les éléments appartenant à l'ensemble "S".

C.Q.F.D.

Réponse (*ii*) Soit S un ensemble. Par l'axiome d'extensionnalité (définition 1.2.1, avec $[S := (S^c)^c]$ et $[T := S]$), l'expression à démontrer est équivalente à :

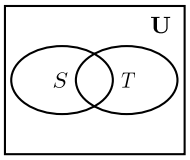
$$(\forall e \mid e \in (S^c)^c \Leftrightarrow e \in S\,)\,.$$

Démontrons donc "$e \in (S^c)^c \Leftrightarrow e \in S$" :
Soit e, un élément quelconque.

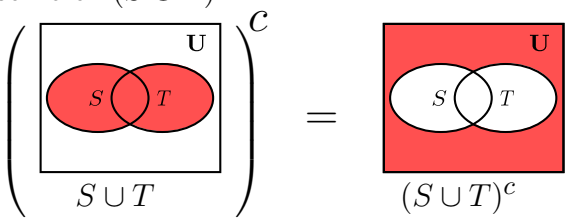
$$\begin{array}{ll} & e \in (S^c)^c \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-a – Complément, avec } [S := S^c]\ \rangle \\ & \neg(e \in S^c) \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-a – Complément}\ \rangle \\ & \neg\neg(e \in S) \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.1.5-a – Double négation}\ \rangle \\ & e \in S \end{array}$$

C.Q.F.D.

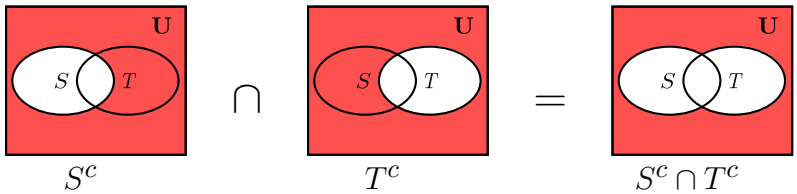
b) Deuxième loi de De Morgan appliquée aux ensembles (Proposition 1.2.7-b) :
$(S \cup T)^c = S^c \cap T^c$;
Réponse (*i*) : Soit S et T deux ensembles. Démontrons la deuxième loi de De Morgan à l'aide de diagrammes de Venn. Considérons la représentation suivante des ensembles S et T :



Bâtissons d'abord l'ensemble "$(S \cup T)^c$" :



Bâtissons ensuite l'ensemble "$S^c \cap T^c$" :



Les diagrammes de Venn obtenus montrent bien que les éléments appartenant à "$(S \cup T)^c$" sont les mêmes que les éléments appartenant à l'ensemble "$S^c \cap T^c$".

C.Q.F.D.

Réponse (*ii*) : Soit S et T deux ensembles. Par l'axiome d'extensionnalité (définition 1.2.1, avec $[S := (S \cup T)^c]$ et $[T := S^c \cap T^c]$), l'expression à démontrer est équivalente à :

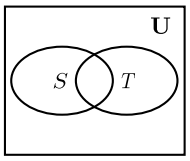
$$(\forall e \mid e \in (S \cup T)^c \Leftrightarrow e \in S^c \cap T^c\,)\,.$$

Démontrons donc "$e \in (S \cup T)^c \Leftrightarrow e \in S^c \cap T^c$" :
Soit e, un élément quelconque.

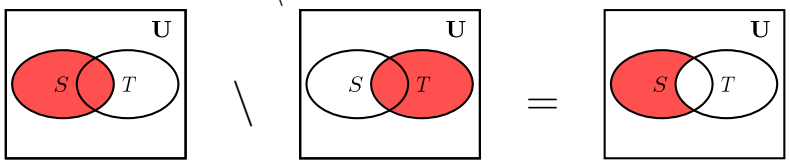
$$\begin{array}{ll} & e \in (S \cup T)^c \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-a – Complément}\ \rangle \\ & \neg(e \in (S \cup T)) \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-c – Union}\ \rangle \\ & \neg(e \in S \vee e \in T) \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.1.4-b – De Morgan, avec } [p := (e \in S)] \textit{ et } [q := (e \in T)]\ \rangle \\ & \neg(e \in S) \wedge \neg(e \in T) \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-a – Complément, 2 fois}\ \rangle \\ & e \in S^c \wedge e \in T^c \\ \Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-b – Intersection}\ \rangle \\ & e \in S^c \cap T^c \end{array}$$

C.Q.F.D.

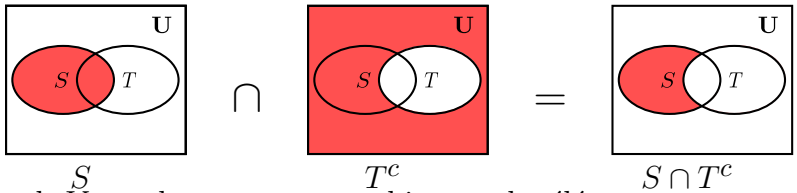
c) Réécriture de la différence (Proposition 1.2.11-b) : $S \setminus T = S \cap T^c$.
Réponse (*i*) : Soit S et T deux ensembles. Considérons la représentation suivante des ensembles S et T :



Bâtissons d'abord l'ensemble "$S \setminus T$" :



Bâtissons ensuite l'ensemble "$S \cap T^c$" :



Les diagrammes de Venn obtenus montrent bien que les éléments appartenant à "$S \setminus T$" sont les mêmes que les éléments appartenant à l'ensemble "$S \cap T^c$".

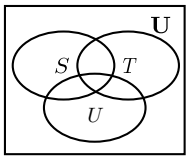
C.Q.F.D.

Réponse (*ii*) : Soit S et T deux ensembles. Par l'axiome d'extensionnalité, l'expression à démontrer est équivalente à : $(\forall e \mid e \in S \setminus T \Leftrightarrow e \in S \cap T^c)$.
Soit un élément e quelconque.

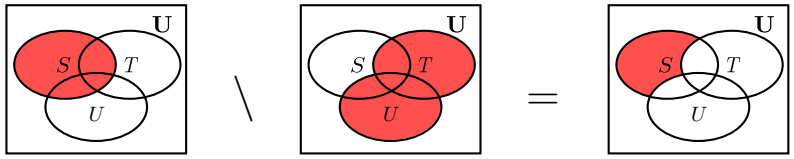
$$
\begin{array}{ll}
 & e \in S \setminus T \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-d – Différence } \rangle \\
 & e \in S \wedge \neg(e \in T) \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-a – Complément } \rangle \\
 & e \in S \wedge e \in T^c \\
\Leftrightarrow & \quad \langle \textit{ Prop 1.2.12-b – Intersection } \rangle \\
 & e \in S \cap T^c
\end{array}
$$

C.Q.F.D.

d) Différence d'une union (Proposition 1.2.11-e) : $S \setminus (T \cup U) = (S \setminus T) \cap (S \setminus U)$;
Réponse (*i*) : Soit S, T et U trois ensembles. Considérons la représentation suivante :

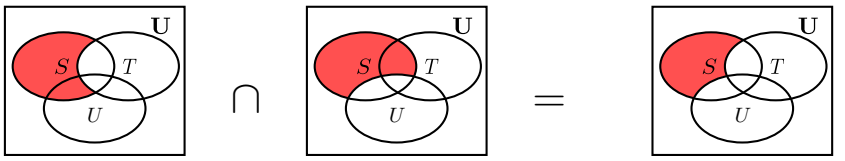


Bâtissons d'abord l'ensemble "$S \setminus (T \cup U)$" :



S $\qquad$ $T \cup U$ $\qquad$ $S \setminus (T \cup U)$

Bâtissons ensuite l'ensemble "$(S \setminus T) \cap (S \setminus U)$" :



$S \setminus T$ $\qquad$ $S \setminus U$ $\qquad$ $(S \setminus T) \cap (S \setminus U)$

Les diagrammes de Venn obtenus montrent que les éléments appartenant à "$S \setminus (T \cup U)$" sont les mêmes que les éléments appartenant à l'ensemble "$(S \setminus T) \cap (S \setminus U)$".

C.Q.F.D.

Réponse (*ii*) – Voici deux démonstrations possibles :

Démonstration 1 (Par l'axiome d'extensionnalité et les propriétés de l'algèbre booléenne) :
Soit S et T et U des ensembles. Par l'axiome d'extensionnalité (définition 1.2.1, avec $[S := S\setminus(T\cup U)]$ et $[T := (S\setminus T)\cap(S\setminus U)]$), l'expression à démontrer est équivalente à :

$$(\forall e \mid e \in S \setminus (T \cup U) \Leftrightarrow e \in (S \setminus T) \cap (S \setminus U)\,).$$

Démontrons donc "$e \in S \setminus (T \cup U) \Leftrightarrow e \in (S \setminus T) \cap (S \setminus U)$" :
Soit e, un élément quelconque. On a :

$$\begin{array}{ll}
& e \in S \setminus (T \cup U) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-d – Différence, avec } [T := T \cup U]\ \rangle \\
& e \in S \wedge \neg(e \in T \cup U) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-c – Union}\ \rangle \\
& e \in S \wedge \neg(e \in T \vee e \in U) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.4-b – De Morgan, avec } [p := e \in T] \textit{ et } [q := e \in U]\ \rangle \\
& e \in S \wedge \neg(e \in T) \wedge \neg(e \in U) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.6-c – Idempotence, avec } [p := e \in S]\ \rangle \\
& e \in S \wedge e \in S \wedge \neg(e \in T) \wedge \neg(e \in U) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.1.6-d – Commutativité}\ \rangle \\
& e \in S \wedge \neg(e \in T) \wedge e \in S \wedge \neg(e \in U) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-d – Différence, 2 fois}\ \rangle \\
& e \in (S \setminus T) \wedge e \in (S \setminus U) \\
\Leftrightarrow & \quad \langle\ \textit{Prop 1.2.12-b – Intersection}\ \rangle \\
& e \in (S \setminus T) \cap (S \setminus U)
\end{array}$$

C.Q.F.D.

Démonstration 2 (Utilisant directement les propriétés ensemblistes) :
Soit S et T des ensembles.

$$\begin{array}{ll}
& S \setminus (T \cup U) \\
= & \quad \langle\ \textit{Prop 1.2.11-b – Réécriture de la différence}\ \rangle \\
& S \cap (T \cup U)^c \\
= & \quad \langle\ \textit{Prop 1.2.7-b – De Morgan}\ \rangle \\
& S \cap T^c \cap U^c \\
= & \quad \langle\ \textit{Prop 1.2.9-c – Idempotence}\ \rangle \\
& S \cap S \cap T^c \cap U^c \\
= & \quad \langle\ \textit{Prop 1.2.9-d – Commutativité}\ \rangle \\
& S \cap T^c \cap S \cap U^c \\
= & \quad \langle\ \textit{Prop 1.2.11-b – Réécriture de la différence, 2 fois}\ \rangle \\
& (S \setminus T) \cap (S \setminus U)
\end{array}$$

C.Q.F.D.

Section 1.3.10 – Exercices sur les techniques de démonstrations

Pour cette série d'exercices, vous devez écrire vos démonstrations sous la forme d'un texte français, similairement aux démonstrations présentées tout au long de la section 1.3. Nous vous encourageons cependant à vous former une intuition en utilisant les diagrammes de Venn si les énoncés concernent des ensembles.

Exercice 1 :

a) Vous venez de démontrer qu'un élément quelconque d'un ensemble X est aussi élément d'un ensemble Y. Écrivez la phrase logique que vous venez de démontrer.
Réponse : $X \subseteq Y$.

b) Étant donnés deux ensembles A et B. En vous inspirant du numéro a), expliquez comment "classiquement" on démontrerait l'énoncé : A=B
Réponse : Une façon de faire serait de d'abord démontrer que $A \subseteq B$ (*en démontrant qu'un élément quelconque de l'ensemble A est aussi élément de l'ensemble B*) et ensuite de démontrer que $B \subseteq A$ (*en démontrant qu'un élément quelconque de l'ensemble B est aussi élément de l'ensemble A*),

c) Étant donné deux ensembles U et V. Vous venez de démontrer qu'un élément quelconque de l'ensemble V est aussi élément d'un ensemble U. Puis vous avez démontré qu'il existe un élément de l'ensemble U qui n'appartient pas à l'ensemble V. Écrivez la phrase logique que vous venez de démontrer.
Réponse : $V \subset U$.

Exercice 2 : Soit S et T des ensembles quelconques. Démontrez $S \setminus T = S \cap T^c$ à l'aide de l'antisymétrie de l'inclusion (Propriété 1.2.13-d) : $(\star\star)$ $S = T \;\Leftrightarrow\; S \subseteq T \wedge T \subseteq S$.
Réponse : Faisons-le à titre d'exercice, mais comme les arguments sont exactement les mêmes dans les 2 directions de l'antisymétrique, une démonstration par succession d'équivalence demande moins de caractères...
Soit S et T des ensembles. Utilisons l'antisymétrie de l'inclusion $(\star\star)$ et démontrons à tour de rôle $S \setminus T \subseteq S \cap T^c$ et $S \setminus T \supseteq S \cap T^c$.
$\boxed{\subseteq :}$ Soit un élément $e \in S \setminus T$ $\quad\langle$ *On veut* $e \in S \cap T^c$ $\rangle$
Par la définition de la différence, on a donc $e \in S$ et $e \notin T$.
Puisque $e \notin T$, on a $e \in T^c$.
On a donc à la fois $e \in S$ et $e \in T^c$, c'est-à-dire $e \in S \cap T^c$ $\quad\langle$ *Inclusion démontrée* $\rangle$

$\boxed{\supseteq :}$ Soit un élément $e \in S \cap T^c$ ⟨ *On veut* $e \in S \setminus T$ ⟩
On a $e \in S$ et $e \in T^c$.
Par la définition du complément, $e \in T^c \Leftrightarrow e \notin T$.
Puisque $e \in S$ et $e \notin T$, on a $e \in S \setminus T$ ⟨ *Inclusion inverse démontrée* ⟩
C.Q.F.D.

Exercice 3 : Supposons que S et T sont deux ensembles quelconques. Démontrez :

a) $S \cap T \subseteq T$
Réponse : Selon la définition de l'inclusion (définition 1.2.5-a), il faut démontrer :

$$(\forall e \mid e \in S \cap T \Rightarrow e \in T)\,.$$

Soit $e \in S \cap T$. ⟨ *On veut* $e \in T$ ⟩
Alors $e \in S$ et $e \in T$, ⟨ *Par la définition de l'intersection* ⟩
On a donc $e \in T$ comme désiré. **C.Q.F.D.**

b) $S \setminus T \subseteq S$.
Réponse : Selon la définition de l'inclusion, il faut démontrer :

$$(\forall e \mid e \in S \setminus T \Rightarrow e \in S)\,.$$

Soit $e \in S \setminus T$. ⟨ *On veut* $e \in S$ ⟩
Alors $e \in S$ et $e \notin T$, ⟨ *Par la définition de la différence entre deux ensembles* ⟩
On a donc $e \in S$ comme désiré. **C.Q.F.D.**

c) Transitivité de $\subseteq$: $\quad S \subseteq T \wedge T \subseteq U \Rightarrow S \subseteq U$;
Réponse : Supposons $(*)\, S \subseteq T$ et $(**)\, T \subseteq U$, et montrons $S \subseteq U$, c'est-à-dire :

$$(\forall e \mid e \in S \Rightarrow e \in U)\,.$$

Soit un élément $e \in S$. ⟨ *On veut* $e \in U$ ⟩
Comme $S \subseteq T$, on a $e \in T$. ⟨ *Voir (*)* ⟩
Comme $T \subseteq U$, on a $e \in U$. ⟨ *Voir (**)* ⟩
Ainsi, $S \subseteq U$. **C.Q.F.D.**

d) $(\forall x \mid P(x) \Rightarrow Q(x)\,) \;\Leftrightarrow\; \{x \mid P(x)\,\} \subseteq \{x \mid Q(x)\}$

Réponse : Démontrons successivement l'implication et l'implication inverse :

$\boxed{\Rightarrow :}$ Supposons **(1)** $(\forall x \mid P(x) \Rightarrow Q(x)\,)$ ⟨ *On veut* $\{x \mid P(x)\,\} \subseteq \{x \mid Q(x)\}$ ⟩
Démontrons $(\forall e \mid e \in \{x \mid P(x)\} \Rightarrow e \in \{x \mid Q(x)\}\,)$. ⟨ *Définition de l'inclusion* ⟩
Soit $e \in \{x \mid P(x)\}$.
Comme $e \in \{x \mid P(x)\}$, alors $P(e) = \texttt{vrai}$.
Donc $Q(e) = \texttt{vrai}$. ⟨ *Selon l'hypothèse* **(1)** ⟩
Donc $e \in \{x \mid Q(x)\}$. ⟨ *Implication démontrée* ⟩

$\boxed{\Leftarrow :}$ Supposons **(2)** $\{x \mid P(x)\,\} \subseteq \{x \mid Q(x)\}$ ⟨ *On veut* $(\forall x \mid P(x) \Rightarrow Q(x)\,)$ ⟩
Soit un élément e et supposons $P(e) = \texttt{vrai}$. ⟨ *Montrons* $Q(e) = \texttt{vrai}$ ⟩
Alors $e \in \{x \mid P(x)\,\}$
Donc $e \in \{x \mid Q(x)\,\}$ ⟨ *Selon l'hypothèse* **(2)** ⟩
Donc $Q(e) = \texttt{vrai}$. ⟨ *Implication inverse démontrée* ⟩

C.Q.F.D.

Exercice 4 : Supposons que S et T sont deux ensembles quelconques. Démontrez :

a) $S \subseteq T \;\Leftrightarrow\; S \cap T = S$;

Réponse : Démontrons successivement l'implication et l'implication inverse :

$\boxed{\Rightarrow :}$ Supposons $(\heartsuit)$ $S \subseteq T$ ⟨ *Montrons* $S \cap T = S$ ⟩
Démontrons successivement $S \cap T \subseteq S$ et $S \cap T \supseteq S$
⟨ *Par l'antisymétrie de l'inclusion* ⟩

$\boxed{\subseteq :}$ Soit $x \in S \cap T$ ⟨ *Montrons* $x \in S$ ⟩
Alors $x \in S$ et $x \in T$ ⟨ *Définition de l'intersection* ⟩
On a $x \in S$ comme désiré. ⟨ *Inclusion démontrée* ⟩

$\boxed{\supseteq :}$ Soit $x \in S$ ⟨ *Montrons* $x \in S \cap T$ ⟩
Comme $S \subseteq T$, on a que $x \in T$ ⟨ *Par l'hypothèse* $(\heartsuit)$ ⟩
Puisque $x \in S$ et $x \in T$, on a $x \in S \cap T$ ⟨ *Inclusion inverse démontrée* ⟩
On a montré $S \cap T \subseteq S$ et $S \cap T \supseteq S$, donc $S \cap T = S$. ⟨ *Implication démontrée* ⟩

$\boxed{\Leftarrow :}$ Supposons $(\heartsuit\heartsuit)$ $S \cap T = S$ ⟨ *On veut* $S \subseteq T$) ⟩
Soit $x \in S$. ⟨ *Montrons* $x \in T$ ⟩
Puisque $S = S \cap T$, on a $x \in S \cap T$. ⟨ *Par l'hypothèse* $(\heartsuit\heartsuit)$ ⟩
Alors $x \in S$ et $x \in T$.
Comme voulu, on a $e \in T$, donc $S \subseteq T$ ⟨ *Implication inverse démontrée* ⟩

C.Q.F.D.

b) $S \subseteq T \;\Leftrightarrow\; S \cup T = T$

Réponse : Démontrons successivement l'implication et l'implication inverse :

$\boxed{\Rightarrow :}$ Supposons $(\Diamond)$ $S \subseteq T$ ⟨ *Montrons* $S \cup T = T$ ⟩

Démontrons successivement $S \cup T \subseteq T$ et $S \cup T \supseteq T$

⟨ *Par l'antisymétrie de l'inclusion* ⟩

$\boxed{\subseteq :}$ Soit $x \in S \cup T$ ⟨ *Montrons* $x \in T$ ⟩

Alors $x \in S$ ou $x \in T$ ⟨ *Définition de l'union* ⟩

Examinons les deux cas possibles :

– Cas 1 : Si $x \in T$, on a le résultat désiré.

– Cas 2 : Si $x \in S$, comme $S \subseteq T$, on a aussi $x \in T$. ⟨ *Par l'hypothèse* $(\Diamond)$ ⟩

Ainsi, on a nécessairement $x \in T$. ⟨ $S \cup T \subseteq T$ *démontrée* ⟩

$\boxed{\supseteq :}$ $T \subseteq S \cup T$ a été démontré à la page 62

On a montré $S \cup T \subseteq T$ et $S \cup T \supseteq T$, donc $S \cup T = T$. ⟨ *Implication démontrée* ⟩

$\boxed{\Leftarrow :}$ Supposons $(\Diamond\Diamond)$ $S \cup T = T$ ⟨ *On veut* $S \subseteq T$ ⟩

Soit $x \in S$. ⟨ *Montrons* $x \in T$ ⟩

Alors $x \in S \cup T$.

Puisque $S \cup T = T$, on a $x \in T$. ⟨ *Par l'hypothèse* $(\Diamond\Diamond)$ ⟩

On a donc $S \subseteq T$. ⟨ *Implication inverse démontrée* ⟩

C.Q.F.D.

Exercice 5 : Donnez les grandes étapes d'une démonstration d'un énoncé qui se lirait comme suit :

$$\neg\big(\forall x \in X \mid P(x) \Rightarrow Q(x)\big).$$

Réponse : Transformons d'abord notre énoncé (on pourrait l'écrire aussi en succession d'équivalences).

	$\neg(\forall x \in X \mid P(x) \Rightarrow Q(x))$
est équivalent, par De Morgan, à	$(\exists x \in X \mid \neg(P(x) \Rightarrow Q(x)))$
ce qui est équivalent à	$(\exists x \in X \mid \neg(\neg P(x) \vee Q(x)))$
ce qui, par De Morgan, est équivalent à	$(\exists x \in X \mid \neg(\neg P(x)) \wedge \neg Q(x))$
ce qui est équivalent à	$(\exists x \in X \mid P(x) \wedge \neg Q(x))$,.

Nous allons démontrer qu'il existe un x dans X tel que $P(x) \wedge \neg Q(x)$ est vrai.

Prenons x choisi de telle façon (...) ; il existe pour telle raison (...) et appartient à X (car ...). Nous démontrons ensuite que $P(x)$ est vrai (car ...), et ensuite que $\neg Q(x)$ est vrai , c'est-à-dire que $Q(x)$ est faux (car ...).

Exercice 6 : Démontrez

1. $(\exists x \in \mathbb{N} \mid x^2 = x)$.
2. $(\exists x \in \mathbb{N} \mid x^2 = -1) \Rightarrow (\forall y \in \mathbb{N} \mid (\exists x \in \mathbb{N} \mid x^2 y + y = 0))$ [6].

Réponses : À voir en TD.

Exercice 7 : Démontrez que $(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$ est toujours faux. C'est-à-dire, démontrez $\neg(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$. Faites-le par contradiction.
Réponse : Démontrons $\neg(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$ par contradiction.

Démonstration.
Supposons le contraire de l'énoncé, c'est-à-dire que $(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$ est vrai.
Prenons $x \in \mathbb{N}$ tel que $4x^2 = 4x - 1$ ⟨ *Un tel x existe par la supposition de départ.* ⟩
On a donc $4x^2 - 4x + 1 = 0$;
donc $(2x - 1)^2 = 0$, donc $x = 1/2$. ⟨ *Arithmétique* ⟩
C'est une contradiction avec $x \in \mathbb{N}$.
Nous avons une contradiction, donc notre hypothèse est fausse,
c'est-à-dire $(\exists x \in \mathbb{N} \mid 4x^2 = 4x - 1)$ est faux, comme voulu. **C.Q.F.D.**

Exercice 8
Soit PAIRS $= \{i \in \mathbb{Z} \mid (\exists j \in \mathbb{Z} \mid i = 2j)\}$ et IMPAIRS $= \{i \in \mathbb{Z} \mid (\exists j \in \mathbb{Z} \mid i = 2j + 1)\}$.
Démontrez

6. Relisez la section sur l'utilisation de $\exists$, page 71. Bien sûr l'hypothèse est fausse, mais on s'amuse : à partir d'une hypothèse fausse, on peut démontrer n'importe quoi. Morale : gare aux démagogues !

1. $(\forall x \in \text{PAIRS} \mid x^2 + 1 \in \text{IMPAIRS})$.
2. $(\forall x, y \in \mathbb{Z} \mid x \in \text{PAIRS} \Rightarrow xy \in \text{PAIRS})$.

Réponses : À voir en TD.

Une note sur l'opérateur modulo. Le modulo est très important en informatique pour toutes les données cycliques. Un exemple courant : si un événement arrive tous les 16 jours, pour connaître le jour de la semaine associé à la prochaine occurrence, il suffit de calculer "16 mod 7", c'est-à-dire le reste de division de 16 par 7. Ce nombre est 2. Ainsi, il suffit d'ajouter 2 jours : si l'événement s'est produit un lundi, la prochaine occurrence sera un mercredi, puis ensuite un vendredi, etc. Les exercices suivants vous obligent à maîtriser le modulo...

Exercice 9 : Démontrons que la définition du modulo par 9 qui suit est correcte,

$$(n \bmod 9 = r) \stackrel{\text{def}}{=} (r \in \{0, 1, 2, \ldots, 8\}) \wedge (\exists k \in \mathbb{N} \mid n = 9k + r).$$

C'est-à-dire démontrez que le "r" est unique :

$$\begin{aligned}(\forall n, r_1, r_2 \in \mathbb{N} \mid [&(r_1 \in \{0, 1, 2, \ldots, 8\} \wedge (\exists k \in \mathbb{N} \mid n = 9k + r_1)) \\ &\wedge (r_2 \in \{0, 1, 2, \ldots, 8\} \wedge (\exists k \in \mathbb{N} \mid n = 9k + r_2)) \Rightarrow r_1 = r_2]\end{aligned}$$

Démonstration.
Soit $n, r_1, r_2 \in \mathbb{N}$.
Supposons la partie de gauche de l'implication ci-haut :

$$(r_1 \in \{0, 1, 2, \ldots, 8\} \wedge (\exists k \in \mathbb{N} \mid n = 9k + r_1)) \wedge (r_2 \in \{0, 1, 2, \ldots, 8\} \wedge (\exists k \in \mathbb{N} \mid n = 9k + r_2)),$$

$\langle$ *et montrons que* $r_1 = r_2$. $\rangle$

Par cette supposition, $r_1, r_2 \in \{0, 1, 2, \ldots, 8\}$.
Prenons $k_1, k_2 \in \mathbb{N}$ tels que $n = 9k_1 + r_1$ et $n = 9k_2 + r_2$.

$\langle$ k_1 *existe car* $(\exists k \in \mathbb{N} \mid n = 9k + r_1)$ $\rangle$
$\langle$ k_2 *existe car* $(\exists k \in \mathbb{N} \mid n = 9k + r_2)$ $\rangle$

Ainsi, on obtient $9k_1 + r_1 = 9k_2 + r_2$,
ce qui donne $9(k_1 - k_2) = r_1 - r_2$.
Comme $r_1, r_2 \in \{0, 1, 2, \ldots, 8\}$, on a $-8 \leq r_1 - r_2 \leq 8$ $\langle$ *Arithmétique* $\rangle$
Ainsi on obtient $\frac{-8}{9} \leq k_1 - k_2 \leq \frac{8}{9}$,
mais comme $k_1 - k_2$ est un entier, on a nécessairement $k_1 - k_2 = 0$.
Ainsi, on a $0 = 9(k_1 - k_2) = r_1 - r_2$,
Donc $r_1 - r_2 = 0$, et $r_1 = r_2$, comme voulu ! **C.Q.F.D.**

Exercice 10 : Un truc bien connu pour savoir si un nombre se divise par 9 : additionner les chiffres de sa représentation en base 10 et évaluer si ce nombre se divise par 9. Démontrons cet énoncé pour les nombres positifs de 2 chiffres (par exemple 21, 34, 99). Ces nombres s'écrivent sous la forme $10d + u$ où $d, u \in \{0, 1, 2, \ldots, 9\}$ (la dizaine et l'unité). Ainsi, démontrez :

$$\big(\forall d, u \in \{0, 1, 2, \ldots, 9\} \;\big|\; (10d + u) \bmod 9 = 0 \Leftrightarrow (d + u) \bmod 9 = 0\big).$$

Démonstration.

Soit $d, u \in \{0, 1, 2, \ldots, 9\}$.

$\boxed{\Rightarrow :}$ $(10d + u) \bmod 9 = 0 \Rightarrow (d + u) \bmod 9 = 0$

Supposons $(10d + u) \bmod 9 = 0$, c'est-à-dire $(\exists k \in \mathbb{N} \mid 10d + u = 9k)$.

⟨ *Montrons* $(d + u)$ *mod* $9 = 0$, *c'est-à-dire* $(\exists k' \in \mathbb{N} \mid d + u = 9k')$ ⟩

Prenons $k \in \mathbb{N}$ tel que $10d + u = 9k$. ⟨ *Un tel* k *existe par supposition* ⟩

Ceci implique $d + u = 9k - 9d$,

ce qui implique $d + u = 9(k - d)$. ⟨ *Arithmétique* ⟩

Notons alors que $k - d \geq 0$ puisque $d + u \geq 0$.

Pour conclure, nous devons démontrer $(\exists k' \in \mathbb{N} \mid d + u = 9k')$.

Prenons $k' = k - d$. ⟨ *Ce nombre existe et est dans* $\mathbb{N}$ *car* $k, d \in \mathbb{N}$ *et* $k - d \geq 0$. ⟩

Nous avons bien $d + u = 9(k - d) = 9k'$, comme voulu.

$\boxed{\Leftarrow :}$ $(10d + u) \bmod 9 = 0 \Leftarrow (d + u) \bmod 9 = 0$

(L'implication inverse se montre de façon similaire, mais au lieu de $k - d$ on sera amené à choisir $k + d$. On vous laisse le faire par vous-même !)

C.Q.F.D.

Section 1.4.6 – Exercices sur les relations et fonctions

Exercice 1 : (*Vous pouvez faire cet exercice en représentant vos relations par des graphes.*)

Étant données les trois relations $\rho, \sigma, \theta \subseteq \{1,2,3,4\} \times \{1,2,3,4\}$ suivantes :

— $\rho = \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 3,4\rangle, \langle 4,1\rangle\}$
— $\sigma = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,1\rangle, \langle 3,1\rangle, \langle 4,1\rangle\}$
— $\theta = \{\langle x,y\rangle \mid x \leq y\}$

1. Calculez $\rho \circ \sigma$, ρ^2, θ^c et θ^{-1}.
2. Déterminez la (ou les) propriété(s) que la relation ρ satisfait parmi les suivantes :
   (a) réflexivité (b) irréflexivité (c) symétrie
   (d) asymétrie (e) antisymétrie (f) transitivité
3. Même question pour la relation σ.
4. Même question pour la relation θ.
5. Existe-t-il un n pour lequel $\rho^n = \{1,2,3,4\} \times \{1,2,3,4\}$? Si oui, trouvez le plus petit de ces n.
6. Même question pour la relation σ.
7. Même question pour la relation θ.

Réponses :

1. $\rho \circ \sigma = \{\langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle, \langle 4,1\rangle, \langle 4,2\rangle, \langle 4,3\rangle, \langle 4,4\rangle\}$
   $\rho^2 = \{\langle 1,3\rangle, \langle 3,1\rangle, \langle 2,4\rangle, \langle 4,2\rangle\}$
   $\theta^c = \{\langle x,y\rangle \mid x > y\}$
   $\theta^{-1} = \{\langle y,x\rangle \mid x \leq y\}$ ou $\{\langle x,y\rangle \mid x \geq y\}$
2. (b), (d) et (e). 3. (c). 4. (a), (e) et (f)
5. NON. 6. OUI, $n = 2$. 7. NON.

Exercice 2 : (*Pour ce numéro, aucune justification n'est demandée.*)

Étant données les deux relations $\rho, \theta \subseteq \mathbb{Z} \times \mathbb{Z}$ suivantes :

— $\rho = \{\langle i,j\rangle \mid i+1 = j\}$
— $\theta = \{\langle x,y\rangle \mid (\exists z \in \mathbb{Z} \mid 2z = x - y)\}$

a) Donnez ρ^2, θ^c et θ^{-1}.

b) Déterminez la (ou les) propriété(s) que la relation ρ satisfait parmi les suivantes :
   (a) réflexivité (b) irréflexivité (c) symétrie
   (d) asymétrie (e) antisymétrie (f) transitivité

c) Même question pour la relation θ.

Réponses :

a) $\rho^2 = \{\langle i, j\rangle \in \mathbb{Z}^2 \mid i + 2 = j\}$
$\theta^c = \{\langle x, y\rangle \mid (\exists z \in \mathbb{Z} \mid 2z + 1 = x - y)\}$
$\theta^{-1} = \theta$

b) (b)irréflexivité, (d)asymétrie et (e)antisymétrie.

c) (a)réflexivité, (c)symétrie et (f)transitivité.

Exercice 3 : Quelles propriétés parmi : *réflexivité, irréflexivité, symétrie, asymétrie, antisymétrie et transitivité* les relations suivantes possèdent-elles ?

a) $b \mathcal{R} c$ ssi b et c sont des entiers tous deux négatifs ou tous deux positifs.

b) $b \mathcal{R} c$ ssi b et c sont des entiers tels que $b - c$ est un multiple de 5.

c) $\emptyset$, où $\emptyset$ est une relation sur un ensemble non vide B.

d) $\mathbf{I}_B$, la relation identité sur un ensemble non vide B.

e) $B \times B$ où B est un ensemble non vide contenant au moins deux éléments.

f) $=$ sur $\mathbb{Z}$.

g) $<$ sur $\mathbb{Z}$.

h) $\leq$ sur $\mathbb{Z}$.

i) $b \rho c$ ssi b est le père de c.

j) $b \rho c$ ssi b est le père de c ou vice-versa.

k) $b \rho c$ ssi b est c ou le père de c.

Réponses :

	réflexivité	irréflexivité	symétrie	asymétrie	antisymétrie	transitivité
a)	x		x			x
b)	x		x			x
c)		x	x	x	x	x
d)	x		x		x	x
e)	x		x			x
f)	x		x		x	x
g)		x		x	x	x
h)	x				x	x
i)		x		x	x	
j)		x	x			
k)	x				x	

Exercice 4 : Démontrez la définition équivalente de l'antisymétrie (Proposition 1.4.15-e) :

$$(\forall a, b \in S \mid a \mathcal{R} b \wedge b \mathcal{R} a \Rightarrow a = b) \;\Leftrightarrow\; \mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathbf{I}_S \,.$$

Réponses : On peut faire les démonstrations de chaque direction. Ça donne ceci :

$\boxed{\Rightarrow}$: Supposons $(\forall a, b \in S \mid a \mathcal{R} b \wedge b \mathcal{R} a \Rightarrow a = b)$ $(\heartsuit)$ $\langle$ *on veut* $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathbf{I}_S$ $\rangle$

Soit $\langle a, b \rangle \in \mathcal{R} \cap \mathcal{R}^{-1}$. Voir note [a]. $\langle$ *on veut* $\langle a, b \rangle \in \mathbf{I}_S$ $\rangle$

Donc $\langle a, b \rangle \in \mathcal{R}$ et $\langle a, b \rangle \in \mathcal{R}^{-1}$ $\langle$ *Def de* $\cap$ $\rangle$

Donc $\langle a, b \rangle \in \mathcal{R}$ et $\langle b, a \rangle \in \mathcal{R}$ $\langle$ *Def de* $\mathcal{R}^{-1}$ $\rangle$

Donc $a = b$ $\langle$ *Par hyp.* $(\heartsuit)$ $\rangle$

Donc $\langle a, b \rangle \in \mathbf{I}_S$ $\langle$ *Def de* $\mathbf{I}_S$ $\rangle$

$\Rightarrow$ est démontré

a. Puisqu'on a affaire à des ensembles, pourquoi ne dit-on pas : soit $x \in \mathcal{R} \cap \mathcal{R}^{-1}$? En fait on aurait pu, mais on voit que $\mathcal{R}$ est en fait une relation et qu'on a besoin d'utiliser ce fait ; dans ce cas, plus loin, on aurait été obligé de dire *donc* $x = \langle a, b \rangle$ *pour un* a *et un* b pour pouvoir continuer. Ça revient au même, on sauve une étape.

$\boxed{\Leftarrow}$: Supposons $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathbf{I}_S$ $(\heartsuit\heartsuit)$ $\langle$ *on veut* $(\forall a, b \in S \mid a \mathcal{R} b \wedge b \mathcal{R} a \Rightarrow a = b)$ $\rangle$

Soit a, b tels que $\langle a, b \rangle \in \mathcal{R}$ et $\langle b, a \rangle \in \mathcal{R}$ $\langle$ *On veut* $a = b$ $\rangle$

Donc $\langle a, b \rangle \in \mathcal{R}$ et $\langle a, b \rangle \in \mathcal{R}^{-1}$ $\langle$ *Def de* $\mathcal{R}^{-1}$ $\rangle$

Donc $\langle a, b \rangle \in \mathcal{R} \cap \mathcal{R}^{-1}$ $\langle$ *Def de* $\cap$ $\rangle$

Donc $\langle a, b \rangle \in \mathbf{I}_S$ $\langle$ *Par hyp.* $(\heartsuit\heartsuit)$ $\rangle$

Donc $a = b$ $\langle$ *Def de* $\mathbf{I}_S$ $\rangle$

$\Leftarrow$ est démontré

C.Q.F.D.

Toutefois en regardant la démonstration on réalise que les arguments sont exactement les mêmes dans les 2 directions. La démonstration suivante est moins longue et équivalente. Les deux démonstrations sont acceptables.

$(\forall a, b \in S \mid a \mathcal{R} b \wedge b \mathcal{R} a \Rightarrow a = b)$

$\Leftrightarrow (\forall a, b \in S \mid \langle a, b \rangle \in \mathcal{R} \wedge \langle b, a \rangle \in \mathcal{R} \Rightarrow a = b)$ $\langle$ *réécriture* $\rangle$

$\Leftrightarrow (\forall a, b \in S \mid \langle a, b \rangle \in \mathcal{R} \wedge \langle a, b \rangle \in \mathcal{R}^{-1} \Rightarrow a = b)$ $\langle$ *Def de* $\mathcal{R}^{-1}$ $\rangle$

$\Leftrightarrow (\forall a, b \in S \mid \langle a, b \rangle \in \mathcal{R} \cap \mathcal{R}^{-1} \Rightarrow a = b)$ $\langle$ *Def de* $\cap$ $\rangle$

$\Leftrightarrow (\forall a, b \in S \mid \langle a, b \rangle \in \mathcal{R} \cap \mathcal{R}^{-1} \Rightarrow \langle a, b \rangle \in \mathbf{I}_S)$ $\langle$ *Def de* $\mathbf{I}_S$ $\rangle$

$\Leftrightarrow \mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathbf{I}_S$.

C.Q.F.D.

Exercice 5 : (*Pour cet exercice, aucune réponse n'a à être justifiée.*) Dites si chacune des relations suivantes est (*i*) déterministe, (*ii*) totale, (*iii*) injective, (*iv*) surjective, (*v*) une fonction, (*vi*) une fonction injective, (*vii*) une fonction surjective ou (*viii*) une fonction bijective.

a) $\rho = \{\langle i, j\rangle \in \mathbb{R}^2 \mid i + 1 = j\}$;
Réponse : ρ est une fonction (c.-à-d. : une relation déterministe et totale) qui est bijective (c.-à-d. : injective et surjective).

b) $\sigma = \{\langle i, j\rangle \in \mathbb{N}^2 \mid i + 1 = j\}$;
Réponse : σ est une fonction (c.-à-d. : une relation déterministe et totale) qui est injective, mais pas surjective (et donc pas bijective).

c) $\theta = \{\langle i, j\rangle \in \mathbb{N}^2 \mid i - 1 = j\}$;
Réponse : θ est une relation déterministe, mais pas totale (ρ n'est donc pas une fonction) qui est bijective (c.-à-d. : injective et surjective).

d) $d : \mathbb{R} \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $d(x) = x^2$;
Réponse : d est une fonction (c.-à-d. : une relation déterministe et totale) qui est ni injective ni surjective (et donc pas bijective).

e) la relation inverse de la relation d définie en d) ;
Réponse : d^{-1} est une relation qui est ni déterministe, ni totale (et donc pas une fonction) mais qui est injective et surjective (et donc bijective)

f) $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $f(x) = x^2$;
Réponse : f est une fonction (c.-à-d. : une relation déterministe et totale) qui est injective, mais pas surjective (et donc pas bijective).

g) $g : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$, définie par la règle de correspondance : $g(x) = x^2$;
Réponse : g est une fonction (c.-à-d. : une relation déterministe et totale) qui est injective et surjective (et donc bijective).

h) $h : \mathbb{R} \longrightarrow [-1, 1]$, définie par la règle de correspondance : $h(x) = sin(x)$;
Réponse : h est une fonction (c.-à-d. : une relation déterministe et totale) qui est surjective, mais pas injective (et donc pas bijective).

i) $i : \mathbb{R} \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $i(x) = x^3$;
Réponse : i est une fonction (c.-à-d. : une relation déterministe et totale) qui est injective et surjective (et donc bijective).

j) la relation inverse de la relation i définie en i) ;
Réponse : i^{-1} est une fonction (c.-à-d. : une relation déterministe et totale) qui est

injective et surjective (et donc bijective).
Notez que la relation inverse d'une fonction bijective est toujours elle aussi une fonction bijective.

k) $k : \mathbb{R} \longrightarrow \mathbb{R}^+$, définie par la règle de correspondance : $k(x) = 2^x$;
Réponse : k est une fonction (c.-à-d. : une relation déterministe et totale) qui est injective et surjective (et donc bijective).

l) $l : \mathbb{R} \longrightarrow \mathbb{R}^+$, définie par la règle de correspondance : $l(x) = log_2(x)$;
Réponse : l n'est pas bien défini, car la règle de correspondance $l(x) = log_2(x)$ qui la définie n'a pas de sens pour les valeurs de $x \leq 0$, on ne peut donc pas répondre à cette question.

m) $m : \mathbb{R}^+ \longrightarrow \mathbb{R}$, définie par la règle de correspondance : $m(x) = log_2(x)$.
Réponse : f est une fonction (c.-à-d. : une relation déterministe et totale) qui est injective et surjective (et donc bijective).
Notez que, $m = k^{-1}$

Exercice 6 : (*Pour ce numéro, seuls le c) et le g) nécessitent quelques justifications et vous pouvez définir toute relation par une représentation graphique.*)

a) Construisez une relation $\rho \subseteq A \times B$ qui soit une fonction bijective.

b) Construisez une relation $\theta \subseteq C \times D$ qui ne soit ni totale, ni déterministe, ni injective, ni surjective.

c) Dans votre réponse en a), est-ce que $|A| = |B|$? Si oui, recommencez la question a) de telle sorte que $|A| \neq |B|$. Si vous n'y arrivez pas, expliquez pourquoi.

d) Soit $E = \{1, 2, 3\}$. Construisez une fonction $f : E \longrightarrow \mathcal{P}(E)$.

e) À partir de la fonction f que vous avez fabriquée en d), construisez l'ensemble $T = \{e \in E \mid e \notin f(e)\}$.

f) Étant donné le f et le T que vous avez construits, est-ce que T appartient à l'ensemble d'arrivée de f ?

g) Étant donné le f et le T que vous avez construits, est-ce que $T \in \mathrm{Im}(f)$?
Si vous avez répondu non, refaites les numéros d) et e) de telle sorte que $T \in \mathrm{Im}(f)$.
Si vous n'y arrivez pas, expliquez brièvement pourquoi.

Solutions à venir

Exercice 7 : (*Pour cet exercice, toute réponse doit être pleinement justifiée.*)
Soit les cinq relations :

— $\rho \subseteq \mathbb{N} \times \mathbb{N}$, définie par : $\rho = \{\langle i, j\rangle \mid i + 1 = j\}$
— $\theta \subseteq \mathbb{Z} \times \mathbb{Z}$, définie par : $\theta = \{\langle x, y\rangle \mid (\exists z \in \mathbb{Z} \mid 2z = x - y)\}$
— $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, définie par la règle de correspondance : $f(x) = x + 3$
— $g : \mathbb{N} \longrightarrow \mathbb{N}$, définie par la règle de correspondance : $g(x) = x + 3$
— $h : \mathbb{Z} \longrightarrow \mathbb{Z}$, définie par la règle de correspondance : $h(x) = x^2$

A) Pour chacune d'elle, déterminez si oui ou non, il s'agit :

1) d'une relation déterministe
2) d'une fonction (c.-à-d. : déterministe et totale) ;
3) d'une fonction injective (c.-à-d. : déterministe, totale et injective) ;
4) d'une fonction surjective (c.-à-d. : déterministe, totale et surjective) ;
5) d'une fonction bijective (c.-à-d. : déterministe, totale, injective et surjective).

B) Donnez la fonction inverse de chacune des fonctions bijectives trouvées en A5).

Solutions de la question (A) :

[(1) – pour ρ] (*Intuitivement, ρ semble être une relation déterministe.*)
Démontrons donc que $(\forall a, b, b' \in \mathbb{N} \mid a\,\rho\,b \wedge a\,\rho\,b' \Rightarrow b = b')$.

Soit $a, b, b' \in \mathbb{N}$. Supposons que $a\,\rho\,b$ et $a\,\rho\,b'$. ⟨ *et montrons que* $b = b'$. ⟩
Comme $a\,\rho\,b$, alors par la définition de ρ, on a $b = a + 1$.
Comme $a\,\rho\,b'$, alors par la définition de ρ, on a $b' = a + 1$.
Donc, par la transitivité de $=$, on a $b = b'$.

C.Q.F.D.

ρ est donc une relation déterministe.

[(2) – pour ρ] (*Intuitivement, $\rho \subseteq \mathbb{N} \times \mathbb{N}$ semble être une relation totale.*)
Démontrons donc que $(\forall a \in \mathbb{N} \mid (\exists b \in \mathbb{N} \mid a\ \rho\ b))$

Soit $a \in \mathbb{N}$. ⟨ *Montrons* $(\exists b \in \mathbb{N} \mid a\ \rho\ b)$ ⟩
Prenons $b = a + 1$. ⟨ *Un tel b existe et appartient à $\mathbb{N}$, propriété de l'arithmétique.* ⟩
Alors, on a bien $a\,\rho\,b$. ⟨ *Définition de ρ.* ⟩

C.Q.F.D.

ρ est donc une relation totale et comme elle est aussi déterministe (Voir [(1)– pour ρ]), ρ est donc une fonction.

[(3) – pour ρ] (*On a déjà montré en (1) et (2) que ρ est une fonction, et intuitivement, elle semble être injective.*)

Comme ρ est une fonction, nous allons démontrer : $(\forall x, x' \in \mathbb{N} \mid \rho(x) = \rho(x') \Rightarrow x = x')$.

Soit $x, x' \in \mathbb{N}$ et supposons que $\rho(x) = \rho(x')$. ⟨ *Montrons $x = x'$* ⟩
Alors on a $x + 1 = x' + 1$. ⟨ *Définition de ρ.* ⟩
Alors on a $x + 1 - 1 = x' + 1 - 1$. ⟨ *Propriété de l'arithmétique.* ⟩
Alors on a $x = x'$. ⟨ *Propriété de l'arithmétique.* ⟩

C.Q.F.D.

ρ est bien une fonction injective.

[(4) – pour ρ] (*On a déjà montré en (1) et (2) que ρ est une fonction, et intuitivement, elle semble ne pas être surjective, car 0 ne semble pas faire partie de l'image de ρ.*)

Comme ρ est une fonction, nous devons donc démontrer :

$$\neg(\forall y \in \mathbb{N} \mid (\exists x \in \mathbb{N} \mid \rho(x) = y)) .$$

Ce qui est équivalent à démontrer $(\exists y \in \mathbb{N} \mid \neg(\exists x \in \mathbb{N} \mid \rho(x) = y))$. ⟨ *De Morgan.* ⟩
Ce qui est équivalent à démontrer $(\exists y \in \mathbb{N} \mid (\forall x \in \mathbb{N} \mid \rho(x) \neq y))$.
⟨ *De Morgan et définition de $\neq$.* ⟩

Démontrons donc $(\exists y \in \mathbb{N} \mid (\forall x \in \mathbb{N} \mid \rho(x) \neq y))$.
Prenons $y = 0$. ⟨ *Un tel y existe et/car clairement $0 \in \mathbb{N}$.* ⟩
Soit $x \in \mathbb{N}$. ⟨ *Montrons $\rho(x) \neq y$* ⟩
Alors clairement, $\rho(x) = x + 1 \neq 0$.

⟨ *Car si $x \in \mathbb{N}$ alors $x + 1 > 0$ et donc $x + 1 \neq 0$ – propriété de l'arithmétique.* ⟩

C.Q.F.D.

ρ n'est pas une fonction surjective.

[(5) – pour ρ] ρ n'est pas une fonction bijective parce qu'elle n'est pas surjective.

[(1) – pour θ] (*Intuitivement, θ semble ne pas être une relation déterministe.*)
Nous devons donc démontrer que $\neg(\forall a, b, b' \in \mathbb{Z} \mid a\,\theta\,b \wedge a\,\theta\,b' \Rightarrow b = b')$
Ce qui est équivalent à démontrer $(\exists a, b, b' \in \mathbb{Z} \mid \neg(a\,\theta\,b \wedge a\,\theta\,b' \Rightarrow b = b'))$.
⟨ *De Morgan.* ⟩
Ce qui est équivalent à démontrer $(\exists a, b, b' \in \mathbb{Z} \mid \neg(\neg(a\,\theta\,b \wedge a\,\theta\,b') \vee b = b'))$.

⟨ *Définition de* $\Rightarrow$. ⟩

Ce qui est équivalent à démontrer $(\exists a, b, b' \in \mathbb{Z} \mid \neg\neg(a\,\theta\,b \wedge a\,\theta\,b') \wedge \neg(b = b'))$.

⟨ *De Morgan.* ⟩

Ce qui est équivalent à démontrer $(\exists a, b, b' \in \mathbb{Z} \mid a\,\theta\,b \wedge a\,\theta\,b' \wedge b \neq b')$. ⟨ *Réécriture* ⟩

Démontrons donc que $(\exists a, b, b' \in \mathbb{Z} \mid a\,\theta\,b \wedge a\,\theta\,b' \wedge b \neq b')$.

Prenons $a = 2, b = 4, b' = 6$ ⟨ *Clairement, de tels a, b et b′ existent et appartiennent à* $\mathbb{Z}$. ⟩

Alors on a bien que $a\,\theta\,b$. ⟨ *Car* $2 \times -1 = 2 - 4$, *et -1 appartient à* $\mathbb{Z}$– *Définition de* θ. ⟩

Et que $a\,\theta\,b'$. ⟨ *Car* $2 \times -2 = 2 - 6$, *et -2 appartient à* $\mathbb{Z}$– *Définition de* θ. ⟩

Et que $b \neq b'$. ⟨ *Car* $4 \neq 6$. ⟩

C.Q.F.D.

θ n'est donc pas une relation déterministe.

[(2), (3), (4) et (5) – pour θ] Comme θ n'est pas déterministe, elle n'est donc pas une fonction. La réponse est donc négative pour (2), (3), (4) et (5).

[(1) et (2) – pour f] *f est nécessairement une fonction (à moins d'une erreur faite par le professeur dans l'énoncé) puisque c'est ce que signifie la notation* $f : \mathbb{Z} \longrightarrow \mathbb{Z}$.

[(3) – pour f] (*Intuitivement,* $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *semble être une fonction injective.*)

Comme f est une fonction, nous allons démontrer :

$$(\forall x, x' \in \mathbb{Z} \mid f(x) = f(x') \Rightarrow x = x')\,.$$

Soit $x, x' \in \mathbb{Z}$ et supposons que $f(x) = f(x')$. ⟨ *Montrons* $x = x'$ ⟩

Alors on a $x + 3 = x' + 3$. ⟨ *Définition de* f. ⟩

Alors on a $x + 3 - 3 = x' + 3 - 3$. ⟨ *Propriété de l'arithmétique.* ⟩

Alors on a $x = x'$. ⟨ *Propriété de l'arithmétique.* ⟩

C.Q.F.D.

f est bien une fonction injective.

[(4) – pour f] (*On a déjà montré en (1) et (2) que* f *est une fonction, et intuitivement, elle semble être surjective.*)

Comme f est une fonction, nous allons démontrer : $(\forall y \in \mathbb{Z} \mid (\exists x \in \mathbb{Z} \mid f(x) = y))$.

Soit $y \in \mathbb{Z}$. ⟨ *Montrons* $(\exists x \in \mathbb{Z} \mid f(x) = y)$ ⟩

Prenons $x = y - 3$. ⟨ *Un tel x existe et appartient à* $\mathbb{Z}$ – *Propriété de l'arithmétique.* ⟩

Alors on a $f(x) = f(y - 3) = (y - 3) + 3 = y$.

C.Q.F.D.

(5) – pour f Comme f est une fonction injective et surjective, elle est donc une fonction bijective.

(1), (2) et (3) – pour g De façon très similaire à ce qui a été fait pour f, on peut montrer que g est une fonction injective.

(4) – pour g (*Intuitivement g semble ne pas être surjective, car ni 0, ni 1, ni 2 ne semblent faire partie de l'image de g.*)

Comme g est une fonction de $\mathbb{N}$ vers $\mathbb{N}$, nous devons donc démontrer :

$$\neg(\forall y \in \mathbb{N} \mid (\exists x \in \mathbb{N} \mid g(x) = y)) .$$

Ce qui est équivalent à démontrer $(\exists y \in \mathbb{N} \mid \neg(\exists x \in \mathbb{N} \mid g(x) = y))$. ⟨ *De Morgan* ⟩

Ce qui est équivalent à démontrer $(\exists y \in \mathbb{N} \mid (\forall x \in \mathbb{N} \mid g(x) \neq y))$.

⟨ *De Morgan et déf de* $\neq$ ⟩

Démontrons donc $(\exists y \in \mathbb{N} \mid (\forall x \in \mathbb{N} \mid g(x) \neq y))$.

Prenons $y = 0$. ⟨ *Un tel y existe, car clairement* $0 \in \mathbb{N}$. ⟩

Soit $x \in \mathbb{N}$. ⟨ *Montrons* $g(x) \neq y$ ⟩

Alors clairement, $g(x) = x + 3 \neq 0$.

⟨ *Car si* $x \in \mathbb{N}$ *alors* $x + 3 > 0$ *et donc* $x + 3 \neq 0$ – *propriété de l'arithmétique.* ⟩

C.Q.F.D.

g n'est pas une fonction surjective.

(5) – pour g g n'est pas une fonction bijective parce qu'elle n'est pas surjective.

(1) et (2) – pour h *h est nécessairement une fonction (à moins d'une erreur faite par le professeur dans l'énoncé) puisque c'est ce que signifie la notation* $h : \mathbb{Z} \longrightarrow \mathbb{Z}$.

(3) – pour h (*Intuitivement,* $h : \mathbb{Z} \longrightarrow \mathbb{Z}$ *semble ne pas être une fonction injective.*)

Comme h est une fonction, nous devons donc démontrer :

$$\neg(\forall x, x' \in \mathbb{Z} \mid h(x) = h(x') \Rightarrow x = x') .$$

Ce qui est équivalent à démontrer $(\exists x, x' \in \mathbb{Z} \mid \neg(h(x) = h(x') \Rightarrow x = x'))$.

⟨ *De Morgan* ⟩

Ce qui est équivalent à démontrer $(\exists x, x' \in \mathbb{Z} \mid \neg(\neg(h(x) = h(x')) \vee x = x'))$.

⟨ *Def de* $\Rightarrow$ ⟩

Ce qui est équivalent à démontrer $(\exists x, x' \in \mathbb{Z} \mid \neg\neg(h(x) = h(x')) \wedge \neg(x = x'))$.

⟨ *De Morgan* ⟩

Démontrons donc $(\exists x, x' \in \mathbb{Z} \mid h(x) = h(x') \wedge x \neq x')$. ⟨ *Réécriture* ⟩

Prenons $x = 2$ et $x' = -2$.

⟨ *De tels* x *et* x' *existent et appartiennent à* $\mathbb{Z}$ *– Propriété de l'arithmétique.* ⟩

Alors on a bien que $h(x) = h(2) = 2^2 = (-2)^2 = h(-2) = h(x')$.

C.Q.F.D.

h n'est pas une fonction injective.

[(4) – pour h] (*Intuitivement, h semble ne pas être surjective, car les entiers négatifs ne semblent pas être dans l'image de h.*)

Comme h est une fonction, nous devons donc démontrer :

$$\neg(\forall y \in \mathbb{Z} \mid (\exists x \in \mathbb{Z} \mid h(x) = y)) .$$

Ce qui est équivalent à démontrer $(\exists y \in \mathbb{Z} \mid \neg(\exists x \in \mathbb{Z} \mid h(x) = y))$. ⟨ *De Morgan* ⟩

Ce qui est équivalent à démontrer $(\exists y \in \mathbb{Z} \mid (\forall x \in \mathbb{Z} \mid h(x) \neq y))$. ⟨ *De Morgan* ⟩

Démontrons donc $(\exists y \in \mathbb{Z} \mid (\forall x \in \mathbb{Z} \mid h(x) \neq y))$.

Prenons $y = -1$. ⟨ *Un tel* y *existe, et/car clairement* $-1 \in \mathbb{Z}$. ⟩

Soit $x \in \mathbb{Z}$ ⟨ *Montrons* $h(x) \neq y$ ⟩

Alors clairement, $h(x) = x^2 \geq 0$

⟨ *Car si* $x \in \mathbb{Z}$ *alors* $x^2 \geq 0$ *– propriété de l'arithmétique.* ⟩

On a donc que $h(x) \neq -1$.

h n'est pas une fonction surjective. **C.Q.F.D.**

[(5) – pour h] Comme h n'est ni une fonction injective ni une fonction surjective, elle n'est donc pas une fonction bijective.

Solution de la question (B) : Seule f est une fonction bijective. Nous présentons deux solutions possibles.

- **Solution 1 :** Par le corolaire 1.4.21-d, comme f est une fonction bijective, on sait que f^{-1} est aussi une fonction. On calcule l'ensemble f^{-1} à partir de la définition d'une relation inverse :

  $f^{-1} = \{\langle y, x\rangle \mid \langle x, y\rangle \in f\}$. ⟨ *Définition 1.4.12* ⟩

  C'est-à-dire que $f^{-1} = \{\langle f(x), x\rangle \mid \langle x, f(x)\rangle \in f\}$. ⟨ *Car* f *est une fonction.* ⟩

  C'est-à-dire que $f^{-1} = \{\langle x + 3, x\rangle \mid x \in \mathbb{Z}\}$. ⟨ *Définition de* f ⟩

C'est-à-dire que $f^{-1} = \{\langle (y-3)+3, (y-3)\rangle \mid (y-3) \in \mathbb{Z}\}$. ⟨ *On pose* $y := x+3$ ⟩
C'est-à-dire que $f^{-1} = \{\langle y, y-3\rangle \mid (y-3) \in \mathbb{Z}\}$. ⟨ *Propriété de l'arithmétique.* ⟩
C'est-à-dire que $f^{-1} = \{\langle y, y-3\rangle \mid y \in \mathbb{Z}\}$.
⟨ *Car* $(y-3) \in \mathbb{Z} \Leftrightarrow y \in \mathbb{Z}$ – *propriété de l'arithmétique.* ⟩

Réponse : La fonction inverse de f est $f^{-1} = \{\langle y, y-3\rangle \mid y \in \mathbb{Z}\}$.

- **Solution 2 :** Soit $k : \mathbb{Z} \longrightarrow \mathbb{Z}$, défini par la règle de correspondance $k(x) = x - 3$.

  Démontrons que k est la fonction inverse de f. Par le théorème 1.4.22, il suffit de démontrer $f \circ k = \mathbf{I}_{\mathbb{Z}}$ et $k \circ f = \mathbf{I}_{\mathbb{Z}}$

  A. $f \circ k = \mathbf{I}_{\mathbb{Z}}$

  Il faut ici démontrer que $(\forall x \in \mathbb{Z} \mid (f \circ k)(x) = \mathbf{I}_{\mathbb{Z}}(x))$.
  Autrement dit, démontrons que $(\forall x \in \mathbb{Z} \mid (f \circ k)(x) = x)$. ⟨ *Définition de* $\mathbf{I}_{\mathbb{Z}}$ ⟩
  Soit $x \in \mathbb{Z}$. ⟨ *On veut* $(f \circ k)(x) = x$ ⟩
  On a donc $(f \circ k)(x) = k(f(x)) = k(x+3) = (x+3) - 3 = x$.

  B. $k \circ f = \mathbf{I}_{\mathbb{Z}}$

  Il faut ici démontrer que $(\forall y \in \mathbb{Z} \mid (k \circ f)(y) = \mathbf{I}_{\mathbb{Z}}(y))$.
  Autrement dit, démontrons que $(\forall y \in \mathbb{Z} \mid (k \circ f)(y) = y)$. ⟨ *Définition de* $\mathbf{I}_{\mathbb{Z}}$ ⟩
  Soit $y \in \mathbb{Z}$. ⟨ *On veut* $(k \circ f)(y) = y$ ⟩
  On a donc $(k \circ f)(y) = f(k(y)) = f(y-3) = (y-3) + 3 = y$.

  k est bien la fonction inverse de f.

  C.Q.F.D.

Exercice 8 : Étant donnée une fonction $h : \mathbb{Z} \longrightarrow \mathbb{Z}$

- h est strictement croissante $\stackrel{\text{def}}{=} (\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow h(x) < h(x'))$
- h est strictement décroissante $\stackrel{\text{def}}{=} (\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow h(x) > h(x'))$

(A) Démontrez que la composition de deux fonctions est encore une fonction

Démonstration Soit deux fonctions f et g. ⟨ *On veut démontrer que* $f \circ g$ *est une fonction* ⟩
Comme f et g sont des fonctions, elles sont des relations totales et déterministes.
Par le théorème 1.4.18-a $f \circ g$ est donc totale.
Par le théorème 1.4.18-b, $f \circ g$ est donc déterministe.
Donc $f \circ g$ est une fonction.

C.Q.F.D.

(B) Démontrez l'énoncé suivant :

Si $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ et $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ sont deux fonctions strictement décroissantes alors $f \circ g$ est une fonction strictement croissante.

Démonstration

En supposant	:	$(\star)$	$(\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow f(x) > f(x'))$
et	:	$(\star\star)$	$(\forall y, y' \in \mathbb{Z} \mid y < y' \Rightarrow g(y) > g(y'))$
Nous allons démontrer	:		$(\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow (f \circ g)(x) < (f \circ g)(x'))$

Soit $x, x' \in \mathbb{Z}$. Supposons que $x < x'$
⟨ *montrons que $(f \circ g)(x) < (f \circ g)(x')$ ou, autrement dit, montrons que $g(f(x)) < g(f(x'))$.* ⟩

Alors, on a $f(x) > f(x')$. ⟨ *Voir $(\star)$.* ⟩

Ce qui est équivalent à $f(x') < f(x)$.

Ce qui implique $g\Big(f(x')\Big) > g\Big(f(x)\Big)$. ⟨ *Voir $(\star\star)$, avec $[y := f(x')]$ et $[y' := f(x)]$.* ⟩

Ce qui est équivalent à $(f \circ g)(x') > (f \circ g)(x)$. ⟨ *Voir la définition de $\circ$.* ⟩

Ce qui est équivalent à $(f \circ g)(x) < (f \circ g)(x')$.

$f \circ g$ est donc une fonction strictement croissante.

C.Q.F.D.

(C) Démontrez l'énoncé suivant :

Si $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ et $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ sont deux fonctions strictement croissantes alors $f \circ g$ est une fonction strictement croissante.

Démonstration

En supposant	:	$(\star)$	$(\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow f(x) < f(x'))$
et	:	$(\star\star)$	$(\forall y, y' \in \mathbb{Z} \mid y < y' \Rightarrow g(y) < g(y'))$
Nous allons démontrer	:		$(\forall x, x' \in \mathbb{Z} \mid x < x' \Rightarrow (f \circ g)(x) < (f \circ g)(x'))$

Soit $x, x' \in \mathbb{Z}$ et supposons que $x < x'$
⟨ *Montrons que $(f \circ g)(x) < (f \circ g)(x')$ ou autrement dit, montrons que $g(f(x)) < g(f(x'))$.* ⟩

Alors, on a $f(x) < f(x')$. ⟨ *Voir $(\star)$.* ⟩

Ce qui implique $g\Big(f(x)\Big) < g\Big(f(x')\Big)$. ⟨ *Voir $(\star\star)$, avec $[y := f(x)]$ et $[y' := f(x')]$.* ⟩

Ce qui est équivalent à $(f \circ g)(x) < (f \circ g)(x')$. ⟨ *Voir la définition de* $\circ$. ⟩

$f \circ g$ est donc une fonction strictement croissante.

C.Q.F.D.

Exercice 9 : On désire modéliser une base de données contenant des informations sur les étudiants et les cours de l'université à l'aide de relations. On considère les trois ensembles suivants :

— L'ensemble ETUDIANTS contenant les noms des étudiants de l'université.
— L'ensemble ENSEIGNANTS contenant les noms des enseignants.
— L'ensemble COURS contenant les sigles des cours offerts par l'université.

De plus, on modélise les tables de la base de données à l'aide des deux relations suivantes :

— La relation EtudCo $\subseteq$ ETUDIANTS $\times$ COURS qui associe les étudiants aux cours qu'ils suivent.
— La relation EnsCo $\subseteq$ ENSEIGNANTS $\times$ COURS qui associe les enseignants aux cours qu'ils donnent.

a) Écrivez l'ensemble des étudiants

1. inscrits au cours `MAT1919`. Bien sûr, on suppose ici que `MAT1919` $\in$ COURS.
2. qui ne sont inscrits qu'au cours `MAT1919`.
3. qui ne sont inscrits à aucun cours
4. qui sont inscrits à au moins un cours

Réponse : 1. $\{e \in \text{ETUDIANTS} \mid (e \,\text{EtudCo}\, \texttt{MAT1919})\}$. 2. voir b)-1. 3. $\{e \in \text{ETUDIANTS} \mid (\forall y \in \text{COURS} \mid \neg(e \,\text{EtudCo}\, y)\}$ ou complément de l'ensemble suivant. 4. Dom(EtudCo).

b) Que retournent les ensembles suivants ?

1. $\{e \in \text{ETUDIANTS} \mid (\forall y \in \text{COURS} \mid \langle e, y\rangle \in \text{EtudCo} \Rightarrow y = \texttt{MAT1919})\}$
2. $\{e \in \text{ETUDIANTS} \mid (\forall y \in \text{COURS} \mid \langle e, y\rangle \in \text{ETUDIANTS} \times \text{COURS} \Rightarrow y = \texttt{MAT1919})\}$
3. $\{e \in \text{ETUDIANTS} \mid (\exists \texttt{MAT1919} \in \text{COURS} \mid \langle e, \texttt{MAT1919}\rangle \in \text{EtudCo})\}$

Réponse : 1. les étudiants inscrits à Mat1919. 2. un ensemble vide s'il y a au moins un autre cours que MAT1919 dans l'ensemble COURS. 3. Les étudiants inscrits à au moins un cours, car $\exists$`MAT1919` utilise `MAT1919` comme une variable, comme si ♡ avait été utilisé à la place.

c) Dites à quoi correspond la relation EnsCo^{-1}.
Réponse : C'est une relation qui associe les cours aux enseignants qui les donnent.

d) En combinant les relations EnsCo et EtudCo à l'aide des opérateurs de relations appropriés, écrivez la définition d'une nouvelle relation qui associe les étudiants aux enseignants qu'ils subissent à cette session. Vous devez définir cette relation à partir de ces deux relations seulement (vous ne pouvez pas définir une relation intermédiaire).
Réponse : $\text{EtudCo} \circ (\text{EnsCo})^{-1}$

e) Dites quelle interprétation possède l'expression suivante :

$$(\exists x \in \text{ENSEIGNANTS} \mid (\forall y \in \text{COURS} \mid \neg(x \,\text{EnsCo}\, y)))\,.$$

Comment écrirait-on qu'il en existe plusieurs (au moins 2) ?
Réponse : Il y a (au moins) un enseignant qui ne donne aucun cours. Pour plus qu'un :
$(\exists x, y \in \text{ENSEIGNANTS} \mid x \neq y \wedge (\forall y \in \text{COURS} \mid \neg(x \,\text{EnsCo}\, y)))$
ou $|\{x \in \text{ENSEIGNANTS} \mid (\forall y \in \text{COURS} \mid \neg(x \,\text{EnsCo}\, y))\}| \geq 2$.

Exercice 10 : Sans justifier vos réponses, dites si les énoncés suivants sont VRAIS ou FAUX.

a) une relation asymétrique est toujours antisymétrique et irréflexive. $\_\_VRAI\_\_\_$.

b) Si $\rho = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x < y\}$, alors $\rho^{-1} = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x > y\}$ et $\rho^c = \{\langle x, y\rangle \in \mathbb{N}^2 \mid x \geq y\}$. $\_\_VRAI\_\_\_$.

c) Si $\theta = \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N})^2 \mid A \subset B\}$, alors $\theta^{-1} = \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N})^2 \mid A \supset B\}$ et $\theta^c = \{\langle A, B\rangle \in \mathcal{P}(\mathbb{N})^2 \mid A \supseteq B\}$. $\_\_FAUX\_\_\_$.

Exercice 11 : (*Pour fin de réflexion et de discussion*) Un hôtel a un nombre infini de chambres (pour chaque entier $i > 0$, il y a une chambre portant le numéro i). L'hôtel est plein (il y a un voyageur dans chaque chambre). Arrive un nouveau voyageur qui voudrait bien dormir à l'hôtel lui aussi. Alors l'hôtelier lui dit qu'il va lui trouver une chambre. Il ne mettra à la porte aucun voyageur, il ne mettra pas deux voyageurs dans une même chambre et il ne fera pas construire une nouvelle chambre. Alors comment l'hôtelier fera-t-il ?

Exercice 12 : (*Pour fin de réflexion et de discussions*) Une charrue enlève la neige le long d'une route qui s'étend jusqu'à l'infini. Tout au long de la route, il y a 15cm de neige. La pelle de la charrue laisse écouler un quinzième de la neige qui entre dans sa pelle (c.-à-d. : 1cm de neige sur les 15). Supposant que la pelle a une capacité infinie et que les flocons qu'elle laisse écouler sortent selon un principe "premier entré, premier sorti", quelle quantité de neige restera dans la pelle une fois le travail terminé ?

Exercice 13 : (*Pour fin de réflexion et de discussions*) Vous avez deux ensembles infinis, comment savoir lequel des deux a le plus grand nombre d'éléments ?

Section 1.5.7 – Exercices sur les ensembles infinis

Exercice 1

Démontrez que les ensembles suivants sont infinis dénombrables (c.-à-d. : qu'ils ont la même cardinalité que $\mathbb{N}$). *Pour ce numéro, vous pouvez, tout comme dans les notes de cours, donner des définitions en extension visuelle de toute fonction bijective dont le domaine est $\mathbb{N}$, et dans ce cas, vous n'avez pas à démontrer qu'il s'agit effectivement d'une fonction bijective.*

a) $\mathbb{N} \times \{5, 12, 789\}$.

Solution : Pour montrer la dénombrabilité de $\mathbb{N} \times \{5, 12, 789\}$, nous allons construire une fonction bijective $f : \mathbb{N} \longrightarrow \mathbb{N} \times \{5, 12, 789\}$, en la définissant en extension de la manière suivante :

$$\begin{array}{ccccccc}
\langle 0,5\rangle & \langle 1,5\rangle & \langle 2,5\rangle & \langle 3,5\rangle & \langle 4,5\rangle & & \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \cdots & \\
f(0) & f(3) & f(6) & f(9) & f(12) & & \\
\langle 0,12\rangle & \langle 1,12\rangle & \langle 2,12\rangle & \langle 3,12\rangle & \langle 4,12\rangle & & \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \cdots & \\
f(1) & f(4) & f(7) & f(10) & f(13) & & \\
\langle 0,789\rangle & \langle 1,789\rangle & \langle 2,789\rangle & \langle 3,789\rangle & \langle 4,789\rangle & & \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \cdots & \\
f(2) & f(5) & f(8) & f(11) & f(14) & &
\end{array}$$

On a donc que $\left|\mathbb{N}\right| = \left|\mathbb{N} \times \{5, 12, 789\}\right|$.

$\mathbb{N} \times \{5, 12, 789\}$ est donc un ensemble (infini) dénombrable.

C.Q.F.D.

b) $\mathbb{N} \setminus \{5, 12, 789\}$.

Solution : Pour montrer la dénombrabilité de $\mathbb{N} \setminus \{5, 12, 789\}$, nous allons construire une fonction bijective $f : \mathbb{N} \longrightarrow \mathbb{N} \setminus \{5, 12, 789\}$, en la définissant en extension de la maniére suivante :

$$\begin{array}{ccccccccccccccccc}
0 & 1 & 2 & 3 & 4 & & 6 & 7 & & 11 & & 13 & 14 & & 788 & & 790 & 791 & \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & \uparrow & \uparrow & \cdots & \uparrow & & \uparrow & \uparrow & \cdots & \uparrow & & \uparrow & \uparrow & \cdots \\
f(0) & f(1) & f(2) & f(3) & f(4) & & f(5) & f(6) & & f(10) & & f(11) & f(12) & & f(786) & & f(787) & f(788) &
\end{array}$$

On a donc que $\left|\mathbb{N}\right| = \left|\mathbb{N} \setminus \{5, 12, 789\}\right|$.

$\mathbb{N} \setminus \{5, 12, 789\}$ est donc un ensemble (infini) dénombrable.

C.Q.F.D.

c) $\mathbb{N} \times \mathbb{N}$.

Solution : Voir dans les notes de cours.

d) $\mathbb{Z} \times \mathbb{Z}$.

Solution : Pour montrer la dénombrabilité de $\mathbb{Z} \times \mathbb{Z}$,
nous allons construire une fonction bijective $f : \mathbb{N} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, en la définissant en extension de la manière suivante :

$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\iddots$
	$\langle 3,-3\rangle$ $\uparrow$ $f(36)$	$\langle 3,-2\rangle$ $\uparrow$ $f(35)$	$\langle 3,-1\rangle$ $\uparrow$ $f(34)$	$\langle 3,0\rangle$ $\uparrow$ $f(33)$	$\langle 3,1\rangle$ $\uparrow$ $f(32)$	$\langle 3,2\rangle$ $\uparrow$ $f(31)$	$\langle 3,3\rangle$ $\uparrow$ $f(30)$	
$\cdots$	$\langle 2,-3\rangle$ $\uparrow$ $f(37)$	$\langle 2,-2\rangle$ $\uparrow$ $f(16)$	$\langle 2,-1\rangle$ $\uparrow$ $f(15)$	$\langle 2,0\rangle$ $\uparrow$ $f(14)$	$\langle 2,1\rangle$ $\uparrow$ $f(13)$	$\langle 2,2\rangle$ $\uparrow$ $f(12)$	$\langle 2,3\rangle$ $\uparrow$ $f(29)$	$\cdots$
$\cdots$	$\langle 1,-3\rangle$ $\uparrow$ $f(38)$	$\langle 1,-2\rangle$ $\uparrow$ $f(17)$	$\langle 1,-1\rangle$ $\uparrow$ $f(4)$	$\langle 1,0\rangle$ $\uparrow$ $f(3)$	$\langle 1,1\rangle$ $\uparrow$ $f(2)$	$\langle 1,2\rangle$ $\uparrow$ $f(11)$	$\langle 1,3\rangle$ $\uparrow$ $f(28)$	$\cdots$
$\cdots$	$\langle 0,-3\rangle$ $\uparrow$ $f(39)$	$\langle 0,-2\rangle$ $\uparrow$ $f(18)$	$\langle 0,-1\rangle$ $\uparrow$ $f(5)$	$\langle 0,0\rangle$ $\uparrow$ $f(0)$	$\langle 0,1\rangle$ $\uparrow$ $f(1)$	$\langle 0,2\rangle$ $\uparrow$ $f(10)$	$\langle 0,3\rangle$ $\uparrow$ $f(27)$	$\cdots$
$\cdots$	$\langle -1,-3\rangle$ $\uparrow$ $f(40)$	$\langle -1,-2\rangle$ $\uparrow$ $f(19)$	$\langle -1,-1\rangle$ $\uparrow$ $f(6)$	$\langle -1,0\rangle$ $\uparrow$ $f(7)$	$\langle -1,1\rangle$ $\uparrow$ $f(8)$	$\langle -1,2\rangle$ $\uparrow$ $f(9)$	$\langle -1,3\rangle$ $\uparrow$ $f(26)$	$\cdots$
$\cdots$	$\langle -2,-3\rangle$ $\uparrow$ $f(41)$	$\langle -2,-2\rangle$ $\uparrow$ $f(20)$	$\langle -2,-1\rangle$ $\uparrow$ $f(21)$	$\langle -2,0\rangle$ $\uparrow$ $f(22)$	$\langle -2,1\rangle$ $\uparrow$ $f(23)$	$\langle -2,2\rangle$ $\uparrow$ $24(5)$	$\langle -2,3\rangle$ $\uparrow$ $f(25)$	$\cdots$
$\cdots$	$\langle -3,-3\rangle$ $\uparrow$ $f(42)$	$\langle -3,-2\rangle$ $\uparrow$ $f(43)$	$\langle -3,-1\rangle$ $\uparrow$ $f(44)$	$\langle -3,0\rangle$ $\uparrow$ $f(45)$	$\langle -3,1\rangle$ $\uparrow$ $f(46)$	$\langle -3,2\rangle$ $\uparrow$ $f(47)$	$\langle -3,3\rangle$ $\uparrow$ $f(48)$	$\cdots$
$\iddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

On a donc que $\left|\mathbb{N}\right| = \left|\mathbb{Z} \times \mathbb{Z}\right|$.

$\mathbb{Z} \times \mathbb{Z}$ est donc un ensemble (infini) dénombrable.

C.Q.F.D.

e) l'ensemble de toutes les puissances de 2.

Solution : Pour montrer la dénombrabilité de $\{2^n \mid n \in \mathbb{N}\}$, nous allons construire une fonction bijective $f : \mathbb{N} \longrightarrow \{2^n \mid n \in \mathbb{N}\}$, en la définissant en extension de la manière suivante :

1	2	4	8	16	32	64	128	256	
↑	↑	↑	↑	↑	↑	↑	↑	↑	...
$f(0)$	$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	$f(7)$	$f(8)$	

On a donc que $\left|\mathbb{N}\right| = \left|\{2^n \mid n \in \mathbb{N}\}\right|$.

$\{2^n \mid n \in \mathbb{N}\}$ est donc un ensemble (infini) dénombrable. **C.Q.F.D.**

f) l'ensemble de tous les mots qu'on peut construire avec un alphabet qui soit composé uniquement des lettres "a", "b" et "c".

Solution : Notons par $\mathcal{M}_{a,b,c}$, l'ensemble de tous les mots finis sur l'alphabet $\{$"a", "b", "c"$\}$. Soit $f : \mathbb{N} \longrightarrow \mathcal{M}_{a,b,c}$, une fonction bijective définie en extension de la manière suivante :

Longueur du mot	$\mathcal{M}_{finis}$									
0	ε									
	↑									
	$f(0)$									
1	a	b	c							
	↑	↑	↑							
	$f(1)$	$f(2)$	$f(3)$							
2	aa	ab	ac	ba	bb	bc	ca	cb	cc	
	↑	↑	↑	↑	↑	↑	↑	↑	↑	
	$f(4)$	$f(5)$	$f(6)$	$f(7)$	$f(8)$	$f(9)$	$f(10)$	$f(11)$	$f(12)$	
3	aaa	aab	aac	aba			...			ccc
	↑	↑	↑	↑						↑
	$f(13)$	$f(14)$	$f(15)$	$f(16)$						$f(39)$
⋮				⋮						

Ainsi, il existe une fonction bijective de $\mathbb{N}$ vers $\mathcal{M}_{a,b,c}$,
L'ensemble de tous les mots finis sur l'alphabet $\{$"a", "b", "c"$\}$ est donc dénombrable.
C.Q.F.D.

Exercice 2

a) Démontrez que la fonction $f : \mathbb{N} \longrightarrow \mathbb{N} \times \{2,3\}$,

définie par la règle de correspondance $f(i) = \begin{cases} \langle \frac{i}{2}, 2 \rangle & \text{si } i \text{ est pair} \\ \langle \frac{i-1}{2}, 3 \rangle & \text{si } i \text{ est impair} \end{cases}$

est surjective.

Démonstration.

- Pour montrer que f est une fonction, il suffit ici de montrer que la règle de correspondance est bien définie, autrement dit qu'à chaque i de l'ensemble de départ $\mathbb{N}$ correspond **un** et **un seul** élément de l'ensemble d'arrivée $\mathbb{N} \times \{2,3\}$.
  Comme un élément de $\mathbb{N}$ est soit pair soit impair (et jamais les deux en même temps), on a donc

  - si i est pair il y a $\langle \frac{i}{2}, 2 \rangle$ qui lui f-correspond, ce qui est bien un élément de l'ensemble d'arrivée et comme alors i n'est pas impair, il ne peut y en avoir d'autre.

  - si i est impair il y a $\langle \frac{i-1}{2}, 3 \rangle$ qui lui f-correspond, ce qui est bien un élément de l'ensemble d'arrivée et comme alors i n'est pas pair, il ne peut y en avoir d'autre.

- Comme f est une fonction, pour montrer que f est surjective, nous allons montrer que

$$(\forall j \in \mathbb{N} \times \{2,3\} \mid (\exists i \in \mathbb{N} \mid f(i) = j))$$

  Soit $j \in \mathbb{N} \times \{2,3\}$. $\quad \langle$ *Montrons* $(\exists i \in \mathbb{N} \mid f(i) = j)$ $\rangle$
  Il y a deux cas à considérer.

  Cas 1 : La deuxième composante de j est un 2.
  Alors $j = \langle k, 2 \rangle \quad$ pour un certain $k \in \mathbb{N}$.
  Posons $i = 2k$
  $\left\langle$ *Un tel i existe et appartient à $\mathbb{N}$, car un nombre naturel multiplié par 2 donne un nombre naturel – propriété de l'arithmétique.* $\right\rangle$
  Alors $f(i) = f(2k) = \langle \frac{2k}{2}, 2 \rangle = \langle k, 2 \rangle = j$.
  $\langle$ *Voir la déf. de f, $2k$ étant un nombre pair.* $\rangle$

  Cas 2 : la deuxième composante de j est un 3.
  Alors $j = \langle l, 3 \rangle \quad$ pour un certain $l \in \mathbb{N}$.
  Posons $i = 2l + 1$
  $\left\langle$ *Un tel i existe et appartient à $\mathbb{N}$, car multiplier par 2 un nombre naturel et y ajouter 1 donne un nombre naturel – propriété de l'arithmétique.* $\right\rangle$

Alors $f(i) = f(2l+1) = \langle \frac{(2l+1)-1}{2}, 2\rangle = \langle \frac{2l}{2}, 2\rangle = \langle l, 2\rangle = j$.

$\langle$ *Voir la déf. de f, 2l+1 étant un nombre impair.* $\rangle$

Dans tous les cas, nous avons trouvé un $i \in \mathbb{N}$ tel que $f(i) = j$.

f est donc une fonction surjective. **C.Q.F.D.**

b) En déduire que $\mathbb{N} \times \{2, 3\}$ est dénombrable.

Solution :

De a), on déduit que $\left|\mathbb{N}\right| \geq \left|\mathbb{N} \times \{2, 3\}\right|$.

L'ensemble $\mathbb{N} \times \{2, 3\}$ est donc dénombrable.

Exercice 3 : (*Pour ce numéro, aucune justification n'est demandée.*)

Étant donnés les ensembles A, B, C et D, que peut-on conclure sur leurs cardinalités ?

a) — il existe une fonction bijective de A vers C ;
— il existe une fonction surjective de A vers B ;
— il existe une fonction injective de A vers D.

Réponse : $|D| \geq |C| = |A| \geq |B|$.

b) — il existe une fonction bijective de A vers C ;
— il existe une fonction surjective de A vers B ;
— il existe une fonction injective de A vers D ;
— il existe une fonction surjective de B vers D.

Réponse : $|A| = |B| = |C| = |D|$.

c) — il existe une fonction surjective de A vers B ;
— il existe une fonction surjective de B vers C ;
— il existe une fonction surjective de C vers D ;
— il existe une fonction surjective de D vers $\mathbb{N}$.

Réponse : $|A| \geq |B| \geq |C| \geq |D| \geq |\mathbb{N}|$.

Et donc que A, B, C et D sont tous des ensembles infinis.

d) — il existe une fonction surjective de A vers B,
— il existe une fonction bijective de B vers C,
— il n'existe pas de fonction injective de C vers $\mathbb{N}$.

Réponse : $|A| \geq |B| = |C| > |\mathbb{N}|$.

Et donc que A, B et C sont tous trois non dénombrables.

Exercice 4

Rappel : *L'ensemble* $\mathbb{Q} \stackrel{\text{def}}{=} \left\{ \frac{x}{y} \;\middle|\; x \in \mathbb{Z}, y \in \mathbb{Z}^* \right\}$ *est l'ensemble des nombres rationnels.*

a) Démontrez que $\mathbb{Z} \times \mathbb{Z}^*$ est dénombrable en construisant en extension une fonction bijective entre $\mathbb{N}$ et cet ensemble..

Démonstration. Démontrons que $\mathbb{Z}^*$ est dénombrable en construisant la fonction bijective $f : \mathbb{N} \longrightarrow \mathbb{Z}^*$ suivante :

$$\begin{array}{ccccccccccc} \cdots & -4 & -3 & -2 & -1 & & 1 & 2 & 3 & 4 & \cdots \\ & \uparrow & \uparrow & \uparrow & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \\ \cdots & f(7) & f(5) & f(3) & f(1) & & f(0) & f(2) & f(4) & f(6) & \cdots \end{array}$$

- On sait déjà que $\mathbb{Z}$ est dénombrable (Voir l'exemple 1.5.4 à la page 112)
- $\mathbb{Z} \times \mathbb{Z}^*$ est donc dénombrable (Voir le théorème 1.5.16(2).) **C.Q.F.D.**

b) Démontrez que la relation F suivante est une fonction surjective :

$$\begin{array}{rccc} F : & \mathbb{Z} \times \mathbb{Z}^* & \longrightarrow & \mathbb{Q} \\ & \langle x, y \rangle & \longmapsto & \frac{x}{y} \end{array}$$

Démonstration. Comme F est une fonction, nous allons démontrer :

$$(\forall b \in \mathbb{Q} \mid (\exists a \in \mathbb{Z} \times \mathbb{Z}^* \mid F(a) = b)) .$$

Soit $b \in \mathbb{Q}$ ⟨ *Montrons* $(\exists a \in \mathbb{Z} \times \mathbb{Z}^* \mid F(a) = b)$ ⟩
Soit $a = \langle x, y \rangle \in \mathbb{Z} \times \mathbb{Z}^*$, choisis tels que $\frac{x}{y} = b$
⟨ *Ce* x *et ce* y *existent par définition de l'ensemble* $\mathbb{Q}$ ⟩
On a $F(a) = F(\langle x, y \rangle) = \frac{x}{y}$ ⟨ *Par choix de* a *et par la définition de* F ⟩
Et on a aussi $\frac{x}{y} = b$ ⟨ *Par choix de* x *et* y ⟩
Ainsi, on a bien $F(a) = b$. **C.Q.F.D.**

c) En utilisant a) et b), démontrez que $\mathbb{Q}$ est dénombrable.

Démonstration.

- De b), on conclut que $|\mathbb{Z} \times \mathbb{Z}^*| \geq |\mathbb{Q}|$.
- De a), on déduit que $|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}^*|$
- Donc $|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}^*| \geq |\mathbb{Q}|$.

$\mathbb{Q}$ est donc **dénombrable**. **C.Q.F.D.**

Exercice 5 : Complétez et justifiez brièvement.

a) S'il n'existe pas de fonction surjective de A vers $\mathbb{N}$, alors A est __$FINI$__.

Justification : Par le théorème 1.5.13 (*1↔9*), on sait que $\left|A\right| < \left|\mathbb{N}\right|$.
Comme en plus $\left|\mathbb{N}\right|$ est la plus petite cardinalité infinie (voir le théorème 1.5.11), on a donc que l'ensemble A doit être un ensemble fini.

b) S'il n'existe pas de fonction surjective de $\mathbb{N}$ vers A, alors A est __NON DÉNOMBRABLE__.

Justification : théorème 1.5.15 (*1↔3*).

c) Soit $(A_i)_{i\in\mathbb{N}}$, une famille d'ensembles finis, alors l'union de tous les ensembles de cette famille (notée $\bigcup_{i\in\mathbb{N}} A_i$) est __DÉNOMBRABLE__.

Justification : Notons n_i la cardinalité de l'ensemble A_i. Pour chaque A_i, on considère une fonction bijective $a_i : \{x \in \mathbb{N} | x < n_i\} \longrightarrow A_i$. Une telle fonction bijective existe, car $|\{x \in \mathbb{N} | x < n_i\}| = |A_i|$.
On peut construire en extension une fonction surjective $k : \mathbb{N} \longrightarrow \bigcup_{i\in\mathbb{N}} A_i$:

A_0	$a_0(0)$ $\uparrow$ $k(0)$	$a_0(1)$ $\uparrow$ $k(1)$	$a_0(2)$ $\uparrow$ $k(2)$	$\cdots$	$a_0(n_0-1)$ $\uparrow$ $k(n_0-1)$
A_1	$a_1(0)$ $\uparrow$ $k(n_0)$	$a_1(1)$ $\uparrow$ $k(n_0+1)$	$a_1(2)$ $\uparrow$ $k(n_0+2)$	$\cdots$	$a_1(n_1-1)$ $\uparrow$ $k(n_0+n_1-1)$
A_2	$a_2(0)$ $\uparrow$ $k(n_0+n_1)$	$a_2(1)$ $\uparrow$ $k(n_0+n_1+1)$	$a_2(2)$ $\uparrow$ $k(n_0+n_1+2)$	$\cdots$	$a_2(n_1-1)$ $\uparrow$ $k(n_0+n_1+n_2-1)$
A_3	$a_3(0)$ $\uparrow$ $k(n_0+n_1+n_2)$	$a_3(1)$ $\uparrow$ $k(n_0+n_1+n_2+1)$	$a_3(2)$ $\uparrow$ $k(n_0+n_1+n_2+2)$	$\cdots$	$a_3(n_1-1)$ $\uparrow$ $k(n_0+n_1+n_2+n_3-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

On en conclut que $|\mathbb{N}| \geq |\bigcup_{i\in\mathbb{N}} A_i|$, et donc que $\bigcup_{i\in\mathbb{N}} A_i$ est un ensemble dénombrable.
Notez que notre construction montre "seulement" que k est une fonction surjective (ce qui est suffisant pour démontrer que l'ensemble est dénombrable). On ne peut pas

conclure que k est bijective, car il peut y avoir des éléments communs à plusieurs ensembles A_i. Dans ce cas, il existe deux $y, y' \in \mathbb{N}$ tels que $k(y) = k(y')$ et $y \neq y'$, k n'est donc pas une fonction injective.

d) Soit $(A_i)_{i\in\mathbb{N}}$, une famille d'ensembles infinis dénombrables, alors $\bigcup_{i\in\mathbb{N}} A_i$ est
__INFINI DÉNOMBRABLE___.

Justification :

(1) L'ensemble $\bigcup_{i\in\mathbb{N}} A_i$ est dénombrable :

Pour chaque ensemble A_i, on considère une fonction bijective $a_i : \mathbb{N} \longrightarrow A_i$. Une telle fonction bijective existe, car $|A_i| = |\mathbb{N}|$.

On peut construire en extension une fonction surjective $k : \mathbb{N} \longrightarrow \bigcup_{i\in\mathbb{N}} A_i$:

A_0	$\underset{k(0)}{a_0(0)}$	$\underset{k(2)}{a_0(1)}$	$\underset{k(5)}{a_0(2)}$	$\underset{k(9)}{a_0(3)}$	$\underset{k(14)}{a_0(4)}$	$\cdots$
A_1	$\underset{k(1)}{a_1(0)}$	$\underset{k(4)}{a_1(1)}$	$\underset{k(8)}{a_1(2)}$	$\underset{k(13)}{a_1(3)}$	$\underset{k(19)}{a_1(4)}$	$\cdots$
A_2	$\underset{k(3)}{a_2(0)}$	$\underset{k(7)}{a_2(1)}$	$\underset{k(12)}{a_2(2)}$	$\underset{k(18)}{a_2(3)}$	$\underset{k(25)}{a_2(4)}$	$\cdots$
A_3	$\underset{k(6)}{a_3(0)}$	$\underset{k(11)}{a_3(1)}$	$\underset{k(17)}{a_3(2)}$	$\underset{k(24)}{a_3(3)}$	$\underset{k(32)}{a_3(4)}$	$\cdots$
A_4	$\underset{k(10)}{a_4(0)}$	$\underset{k(14)}{a_4(1)}$	$\underset{k(23)}{a_4(2)}$	$\underset{k(31)}{a_4(3)}$	$\underset{k(40)}{a_4(4)}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

On en conclut que $|\mathbb{N}| \geq |\bigcup_{i\in\mathbb{N}} A_i|$, et donc que $\bigcup_{i\in\mathbb{N}} A_i$ est un ensemble dénombrable.

(2) L'ensemble $\bigcup_{i\in\mathbb{N}} A_i$ est infini :

Soit A_k un ensemble de cette famille ($k \in \mathbb{N}$). On a nécessairement $A_k \subseteq \bigcup_{i\in\mathbb{N}} A_i$ et donc $|A_k| \leq |\bigcup_{i\in\mathbb{N}} A_i|$ (Voir la proposition 1.5.10). Comme A_k est un ensemble infini, on en conclut que $\bigcup_{i\in\mathbb{N}} A_i$ est aussi infini.

Exercice 6

Démontrez que l'ensemble de tous les sous-ensembles finis de $\mathbb{N}$ est dénombrable alors que l'ensemble de tous les sous-ensembles de $\mathbb{N}$ ne l'est pas.

Solution :

1.- $\mathcal{P}(\mathbb{N})$ est non dénombrable.

Par le théorème 1.5.17 (Cantor) [avec $A := \mathbb{N}$], on a que $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$.
$\mathcal{P}(\mathbb{N})$ est donc non dénombrable.

C.Q.F.D.

2.- L'ensemble de tous les sous-ensembles finis de $\mathbb{N}$ est dénombrable. On remarque facilement :

- qu'il n'y a qu'un nombre fini de sous-ensembles finis de $\mathbb{N}$ dont la somme des éléments est égale à 0. En fait il n'y en a que deux, $\emptyset$ et $\{0\}$.
- qu'il n'y a qu'un nombre fini de sous-ensembles finis de $\mathbb{N}$ dont la somme des éléments est égale à 1. En fait il n'y en a que deux, $\{1\}$ et $\{0, 1\}$.
- qu'en général pour chaque $n \in \mathbb{N}$, $\mathbb{N}$ ne contenant aucun nombre négatif, il n'y a qu'un nombre fini de sous-ensembles finis de $\mathbb{N}$ dont la somme des éléments est égale à n.

Notons par A, l'ensemble de tous les sous-ensembles finis de $\mathbb{N}$.
Soit $f : \mathbb{N} \longrightarrow A$, une fonction bijective définie en extension de la manière illustrée par le diagramme **(*)** à la page suivante.

Ainsi, il existe une fonction bijective de $\mathbb{N}$ vers A,
A est donc dénombrable.

C.Q.F.D.

Diagramme (*) : Illustration de la fonction $f : \mathbb{N} \longrightarrow A$.

Somme des éléments du sous-ensemble	A							
0	$\emptyset$ $\uparrow$ $f(0)$	$\{0\}$ $\uparrow$ $f(1)$						
1	$\{1\}$ $\uparrow$ $f(2)$	$\{0,1\}$ $\uparrow$ $f(3)$						
2	$\{2\}$ $\uparrow$ $f(4)$	$\{0,2\}$ $\uparrow$ $f(5)$						
3	$\{3\}$ $\uparrow$ $f(6)$	$\{0,3\}$ $\uparrow$ $f(7)$	$\{1,2\}$ $\uparrow$ $f(8)$	$\{0,1,2\}$ $\uparrow$ $f(9)$				
4	$\{4\}$ $\uparrow$ $f(10)$	$\{0,4\}$ $\uparrow$ $f(11)$	$\{1,3\}$ $\uparrow$ $f(12)$	$\{0,1,3\}$ $\uparrow$ $f(13)$				
5	$\{5\}$ $\uparrow$ $f(14)$	$\{0,5\}$ $\uparrow$ $f(15)$	$\{1,4\}$ $\uparrow$ $f(16)$	$\{0,1,4\}$ $\uparrow$ $f(17)$	$\{2,3\}$ $\uparrow$ $f(18)$	$\{0,2,3\}$ $\uparrow$ $f(19)$		
6	$\{6\}$ $\uparrow$ $f(20)$	$\{0,6\}$ $\uparrow$ $f(21)$	$\{1,5\}$ $\uparrow$ $f(22)$	$\{0,1,5\}$ $\uparrow$ $f(23)$	$\{2,4\}$ $\uparrow$ $f(24)$	$\{0,2,4\}$ $\uparrow$ $f(25)$	$\{1,2,3\}$ $\uparrow$ $f(26)$	$\{0,1,2,3\}$ $\uparrow$ $f(27)$
$\vdots$				$\vdots$				

Exercice 7 : Soit la fonction f, définie par $\begin{array}{rccc} f: & [1,100] & \longrightarrow & [0,1] \\ & x & \longmapsto & \frac{x-1}{100} \end{array}$

a) Démontrez que f est injective, mais pas surjective.

Démonstration.

f est injective.

Comme f est une fonction, il suffit de montrer :

$$(\forall x, x' \in [1,100] \mid f(x) = f(x') \Rightarrow x = x')$$

Soit $x, x' \in [1,100]$ et supposons que $f(x) = f(x')$. ⟨ *Montrons* $x = x'$ ⟩

Alors on a $\frac{x-1}{100} = \frac{x'-1}{100}$ ⟨ *Définition de* f ⟩

Donc $x - 1 = x' - 1$ ⟨ *Propriété de l'arithmétique* ⟩

Donc $x = x'$ ⟨ *Propriété de l'arithmétique* ⟩

f est donc une fonction injective.

f n'est pas surjective

Comme f est une fonction, il suffit de montrer :

$$\neg(\forall y \in [0,1] \mid (\exists x \in [1,100] \mid f(x) = y))$$

Ce qui par la loi de De Morgan (pour le $\forall$) est équivalent à montrer :

$$(\exists y \in [0,1] \mid \neg(\exists x \in [1,100] \mid f(x) = y))$$

Ce qui par la loi de De Morgan (pour le $\exists$) est équivalent à montrer :

$$(\exists y \in [0,1] \mid (\forall x \in [1,100] \mid f(x) \neq y))$$

Posons $y = 1$ ⟨ *Clairement, un tel* y *existe et appartient à* $[0,1]$. ⟩

Soit $x \in [1,100]$ ⟨ *Montrons* $f(x) \neq y$ ⟩

Alors,

$$\begin{array}{rcll} f(x) & = & \frac{x-1}{100} & \langle \text{Définition de } f. \rangle \\ & \leq & \frac{100-1}{100} & \langle \text{Car } f \text{ est un fonction croissante et } x \leq 100. \rangle \\ & = & \frac{99}{100} & \\ & < & 1 & \end{array}$$

Donc $f(x) \neq 1$ $\langle$ *car* $f(x) < 1$. $\rangle$
Donc $f(x) \neq y$

f n'est donc pas une fonction surjective.

C.Q.F.D.

b) Peut-on conclure de a) que $\Big|[1,100]\Big| \leq \Big|[0,1]\Big|$? Pourquoi ?
Solution : OUI, voir la définition 1.5.8.

c) Peut-on conclure de a) que $\Big|[1,100]\Big| < \Big|[0,1]\Big|$? Pourquoi ?
Solution :
NON, car ce n'est pas parce que la fonction $f : [1,100] \longrightarrow [0,1]$ n'est pas surjective qu'il n'existe pas de fonction surjective de $[1,100]$ vers $[0,1]$.

d) Est-ce que $[1,100]$ est dénombrable ? Justifiez.
Solution : NON. Nous allons démontrer que $[1,100]$ est non-dénombrable.

Démonstration.
(1) - Montrons d'abord que

$$\begin{array}{rccc} h : & [0,1[& \longrightarrow & [1,100] \\ & x & \longmapsto & x+1 \end{array}$$

est une fonction injective.

Pour montrer que h est une fonction, il suffit de monter que la règle de correspondance est bien définie, ce qui est clairement le cas, car :
— pour chaque élément x de l'ensemble de départ $[0,1[$ il existe **un** et **un seul** élément qui lui correspond, soit l'élément $x+1$,
— et cet élément $x+1$ est bien dans l'ensemble d'arrivée $[1,100]$ si $x \in [0,1[$.

Montrons donc que h est injectif en montrant :

$$(\forall x, x' \in [0,1[\ \mid \ h(x) = h(x') \Rightarrow x = x')$$

Soit $x, x' \in [0,1[$ et supposons que $h(x) = h(x')$. ⟨ *Montrons* $x = x'$ ⟩
Alors $x + 1 = x' + 1$ ⟨ *Définition de* h. ⟩
Donc $x = x'$ ⟨ *Propriété de l'arithmétique.* ⟩
h est donc une fonction injective.

(2) - De (1), on conclut que $\Big|[0,1[\Big| \leq \Big|[1,100]\Big|$.

(3) - Comme dans les notes on a démontré que $\Big|\mathbb{N}\Big| < \Big|[0,1[\Big|$.

On a donc que $\Big|\mathbb{N}\Big| < \Big|[0,1[\Big| \leq \Big|[1,100]\Big|$.

$[1,100]$ est donc un ensemble non dénombrable.

C.Q.F.D.

Section 1.6.3 – Exercices sur les ensembles de fonctions

Exercice 1

Sans justifier vos réponses, dites si les énoncés suivants sont VRAIS ou FAUX.

a) Tous les ensembles de fonctions non-dénombrables. __*FAUX*___.

b) $\left|\mathbb{N}^{\{0,1\}}\right| = \left|\{0,1\}^{\mathbb{N}}\right|$. __*FAUX*___.

c) $\mathbb{N}^{\mathbb{Z}}$ est dénombrable. __*FAUX*___.

Exercice 2

a) Démontrez que l'ensemble de tous les mots *finis* sur l'alphabet {"a", "b"} est dénombrable alors que l'ensemble de tous les mots *infinis* sur ce même alphabet ne l'est pas.

b) Est-ce que l'ensemble de tous les mots (*finis et infinis*) sur l'alphabet {"a", "b"} est dénombrable ? Justifiez brièvement.

Solution de 6a – partie I : Il y a un nombre dénombrable de mots finis sur l'alphabet à deux lettres

On remarque facilement que sur l'alphabet {"a", "b"},

— il n'y a qu'un nombre fini de mots de longueur 0. En fait il n'y en a qu'un, le *mot vide* qui est généralement noté par ε.

— il n'y a qu'un nombre fini de mots de longueur 1. En fait il n'y en a que deux, a et b.

— et en général pour chaque $n \in \mathbb{N}$, il n'y a qu'un nombre fini de mots de longueur n.

Notons par $\mathcal{M}_{finis}$, l'ensemble de tous les mots finis sur l'alphabet {"a", "b"}.
Soit $f : \mathbb{N} \longrightarrow \mathcal{M}_{finis}$, une fonction bijective définie en extension de la manière suivante :

Longueur du mot	$\mathcal{M}_{finis}$							
0	ε $\uparrow$ $f(0)$							
1	a $\uparrow$ $f(1)$	b $\uparrow$ $f(2)$						
2	aa $\uparrow$ $f(3)$	ab $\uparrow$ $f(4)$	ba $\uparrow$ $f(5)$	bb $\uparrow$ $f(6)$				
3	aaa $\uparrow$ $f(7)$	aab $\uparrow$ $f(8)$	aba $\uparrow$ $f(9)$	abb $\uparrow$ $f(10)$	baa $\uparrow$ $f(11)$	bab $\uparrow$ $f(12)$	bba $\uparrow$ $f(13)$	bbb $\uparrow$ $f(14)$
$\vdots$				$\vdots$				

Ainsi, il existe une fonction bijective de $\mathbb{N}$ vers $\mathcal{M}_{finis}$,

L'ensemble de tous les mots finis sur l'alphabet $\{$"a", "b"$\}$ est donc dénombrable.

C.Q.F.D.

Solution de 6a – partie II : Il y a un nombre non dénombrable de mots infinis sur l'alphabet à deux lettres

Notons par $\mathcal{M}_{infinis}$, l'ensemble de tous les mots infinis sur l'alphabet $\{$"a", "b"$\}$.

Ainsi un élément de $\mathcal{M}_{infinis}$ est un élément de la forme

$$\langle \alpha_0, \alpha_1, \alpha_2, \alpha_3, \ldots \rangle$$

où chacun des α_i est soit la lettre "a" soit la lettre "b".

Un mot infini $\langle \alpha_0, \alpha_1, \alpha_2, \alpha_3, \ldots \rangle$ est donc une fonction $f : \mathbb{N} \longrightarrow \{$"$a$", "$b$"$\}$ où $f(0) = \alpha_0$, $f(1) = \alpha_1$, $f(2) = \alpha_2$, $f(3) = \alpha_3$, ...
Et inversement, une fonction $f : \mathbb{N} \longrightarrow \{$"$a$", "$b$"$\}$ est le mot $\langle f(0), f(1), f(2), f(3), \ldots \rangle$

Ainsi, l'ensemble de tous les mots infinis sur l'alphabet $\{\text{“}a\text{”}, \text{“}b\text{”}\}$ **est égal** à l'ensemble $\{\text{“}a\text{”}, \text{“}b\text{”}\}^{\mathbb{N}}$.

Comme $\left|\{\text{“}a\text{”}, \text{“}b\text{”}\}\right| \geq 2$ et comme $\mathbb{N}$ est infini, par le théorème 1.6.4, on a donc que $\{\text{“}a\text{”}, \text{“}b\text{”}\}^{\mathbb{N}}$ est un ensemble non dénombrable.

L'ensemble de tous les mots infinis sur l'alphabet $\{\text{“}a\text{”}, \text{“}b\text{”}\}$ est donc non dénombrable.

C.Q.F.D.

Solution de 6b) Puisque $\mathcal{M}_{infinis} \subseteq \mathcal{M}_{finis} \cup \mathcal{M}_{infinis}$, on a donc par Proposition 1.5.10 que

$$\left|\mathcal{M}_{infinis}\right| \leq \left|\mathcal{M}_{finis} \cup \mathcal{M}_{infinis}\right|.$$

Comme on a démontré en (6a– partie II) que $\mathcal{M}_{infinis}$ est non dénombrable, on a donc que $\mathcal{M}_{finis} \cup \mathcal{M}_{infinis}$ est lui aussi un ensemble non dénombrable.

L'ensemble de tous les mots (finis et infinis) sur l'alphabet $\{\text{“}a\text{”}, \text{“}b\text{”}\}$ est donc non dénombrable.

C.Q.F.D.

Exercice 3

a) Les données d'entrée et de sortie d'un programme sont des séquences de bits. On peut donc considérer une séquence de bits comme un nombre naturel exprimé en binaire (en ajoutant un bit “1” au début de la séquence, de sorte que les “0” initiaux du programme soient significatifs). Donc un programme calcule une fonction de $\mathbb{N}$ vers $\mathbb{N}$.

L'ensemble de toutes les fonctions de $\mathbb{N}$ vers $\mathbb{N}$ est-il dénombrable ?

b) Un programme en JAVA est construit à partir d'un nombre fini de symboles et est de longueur finie. On peut donc considérer un programme comme un mot écrit à l'aide d'un certain alphabet.

L'ensemble de tous les programmes en JAVA est-il dénombrable ?

c) Si on suppose qu'on n'a aucun problème de mémoire, est-ce que n'importe quelle fonction de $\mathbb{N}$ vers $\mathbb{N}$ peut-être calculée en JAVA ? (Justifiez brièvement.)

Solution de a)

Par le théorème 1.6.4, on obtient directement que $\mathbb{N}^{\mathbb{N}}$, (l'ensemble de toutes les fonctions de $\mathbb{N}$ vers $\mathbb{N}$) est non dénombrable.

C.Q.F.D.

Solution de b)

Comme l'ensemble des symboles utilisables dans un programme JAVA est fini, On a donc que pour chaque $n \in \mathbb{N} \setminus \{0\}$, il y a au plus un nombre fini de programmes JAVA de longueur n.

- Soit n_1 le nombre de programmes JAVA de longueur 1.
  Et soit J_1^1, J_2^1, ... $J_{n_1}^1$, ces programmes de longueur 1.
- Soit n_2 le nombre de programmes JAVA de longueur 2.
  Et soit J_1^2, J_2^2, ... $J_{n_2}^2$, ces programmes de longueur 2.
- Soit n_3 le nombre de programmes JAVA de longueur 3.
  Et soit J_1^3, J_2^3, ... $J_{n_2}^3$, ces programmes de longueur 3.
- etc...

Soit $\mathcal{J}$, l'ensemble de tous les programmes JAVA.
Et soit f, une fonction bijective de $\mathbb{N}$ vers $\mathcal{J}$, définie en extension de la manière suivante :

Longueur du programme	$\mathcal{J}$					
1	J_1^1 ↑ $f(0)$	J_2^1 ↑ $f(1)$	...	$J_{n_1}^1$ ↑ $f(n_1-1)$		
2	J_1^2 ↑ $f(n_1)$	J_2^1 ↑ $f(n_1+1)$		...	$J_{n_1}^1$ ↑ $f(n_1+n_2-1)$	
3	J_1^3 ↑ $f(n_1+n_2)$	J_2^1 ↑ $f(n_1+n_2+1)$			...	$J_{n_1}^1$ ↑ $f(n_1+n_2+n_3-1)$
⋮				⋮		

Ainsi, il existe une fonction bijective de $\mathbb{N}$ vers l'ensemble de tous les programmes JAVA,
cet ensemble est donc dénombrable.

C.Q.F.D.

Solution de c) Non, parce que si chacune de ces fonctions était calculable en JAVA, il faudrait qu'il y ait au moins "autant" de programmes JAVA que de fonctions de $\mathbb{N}$

vers $\mathbb{N}$. Or il existe un nombre **non dénombrable** de fonctions de $\mathbb{N}$ vers $\mathbb{N}$, mais seulement un nombre **dénombrable** de programmes JAVA.

Exercice 4

Expliquez brièvement pourquoi $\{0,1,2\}^{\mathbb{N}}$ est non dénombrable.

Solution : Voir le théorème 1.6.4 et l'explication intuitive avant la démonstration de la proposition 1.6.5 (page 136).

Exercice 5

En construisant en extension une fonction bijective appropriée, démontrez la dénombrabilité de l'ensemble $\mathbb{Z}^{\{1,2\}}$. Notez que des théorèmes des notes de cours permettent de démontrer la dénombrabilité de cet ensemble, mais vous ne pouvez les utiliser pour cet exercice.

Astuce : *La difficulté est de représenter les éléments de cet ensemble. Écrivez $f_{i,j}$ pour la fonction qui envoie 1 sur le nombre i et 2 sur le nombre j (il faut toutefois définir cette nouvelle notation dans votre réponse avant de l'utiliser)*

Solution : *Voir la page suivante*

Démonstration. Écrivons $f_{i,j}$ pour la fonction qui envoie 1 sur le nombre i et 2 sur le nombre j.

Pour montrer la dénombrabilité de $\mathbb{Z}^{\{1,2\}}$, nous allons construire une fonction bijective $g : \mathbb{N} \longrightarrow \mathbb{Z}^{\{1,2\}}$, en la définissant en extension de la manière suivante :

$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$ $\cdots$
$\cdots$	$f_{3,-3}$ $\uparrow$ $g(36)$	$f_{3,-2}$ $\uparrow$ $g(35)$	$f_{3,-1}$ $\uparrow$ $g(34)$	$f_{3,0}$ $\uparrow$ $g(33)$	$f_{3,1}$ $\uparrow$ $g(32)$	$f_{3,2}$ $\uparrow$ $g(31)$	$f_{3,3}$ $\uparrow$ $g(30)$ $\cdots$
$\cdots$	$f_{2,-3}$ $\uparrow$ $g(37)$	$f_{2,-2}$ $\uparrow$ $g(16)$	$f_{2,-1}$ $\uparrow$ $g(15)$	$f_{2,0}$ $\uparrow$ $g(14)$	$f_{2,1}$ $\uparrow$ $g(13)$	$f_{2,2}$ $\uparrow$ $g(12)$	$f_{2,3}$ $\uparrow$ $g(29)$ $\cdots$
$\cdots$	$f_{1,-3}$ $\uparrow$ $g(38)$	$f_{1,-2}$ $\uparrow$ $g(17)$	$f_{1,-1}$ $\uparrow$ $g(4)$	$f_{1,0}$ $\uparrow$ $g(3)$	$f_{1,1}$ $\uparrow$ $g(2)$	$f_{1,2}$ $\uparrow$ $g(11)$	$f_{1,3}$ $\uparrow$ $g(28)$ $\cdots$
$\cdots$	$f_{0,-3}$ $\uparrow$ $g(39)$	$f_{0,-2}$ $\uparrow$ $g(18)$	$f_{0,-1}$ $\uparrow$ $g(5)$	$f_{0,0}$ $\uparrow$ $g(0)$	$f_{0,1}$ $\uparrow$ $g(1)$	$f_{0,2}$ $\uparrow$ $g(10)$	$f_{0,3}$ $\uparrow$ $g(27)$ $\cdots$
$\cdots$	$f_{-1,-3}$ $\uparrow$ $g(40)$	$f_{-1,-2}$ $\uparrow$ $g(19)$	$f_{-1,-1}$ $\uparrow$ $g(6)$	$f_{-1,0}$ $\uparrow$ $g(7)$	$f_{-1,1}$ $\uparrow$ $g(8)$	$f_{-1,2}$ $\uparrow$ $g(9)$	$f_{-1,3}$ $\uparrow$ $g(26)$ $\cdots$
$\cdots$	$f_{-2,-3}$ $\uparrow$ $g(41)$	$f_{-2,-2}$ $\uparrow$ $g(20)$	$f_{-2,-1}$ $\uparrow$ $g(21)$	$f_{-2,0}$ $\uparrow$ $g(22)$	$f_{-2,1}$ $\uparrow$ $g(23)$	$f_{-2,2}$ $\uparrow$ $24(5)$	$f_{-2,3}$ $\uparrow$ $g(25)$ $\cdots$
$\cdots$	$f_{-3,-3}$ $\uparrow$ $g(42)$	$f_{-3,-2}$ $\uparrow$ $g(43)$	$f_{-3,-1}$ $\uparrow$ $g(44)$	$f_{-3,0}$ $\uparrow$ $g(45)$	$f_{-3,1}$ $\uparrow$ $g(46)$	$f_{-3,2}$ $\uparrow$ $g(47)$	$f_{-3,3}$ $\uparrow$ $g(48)$ $\cdots$
$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$ $\ddots$

On a donc que $\left|\mathbb{N}\right| = \left|\mathbb{Z}^{\{1,2\}}\right|$.

$\mathbb{Z}^{\{1,2\}}$ est donc un ensemble (infini) dénombrable. **C.Q.F.D.**

Section 1.7.5 – Exercices sur les relations d'équivalences et d'ordres

Exercice 1 : Étant donné le tableau suivant, qui donne les propriétés de relations fictives, mais plausibles (toute ressemblance avec une relation existante est purement spéculative), dites lesquelles sont des relations d'équivalence, des ordres partiels, des ordres partiels stricts.

	réflexivité	irréflexivité	symétrie	asymétrie	antisymétrie	transitivité
a	x		x			x
b	x			x		x
c		x	x	x	x	x
d	x		x		x	x
e	x		x		x	x
f		x		x	x	x
g	x				x	x
h		x		x	x	
i		x	x			
j	x				x	

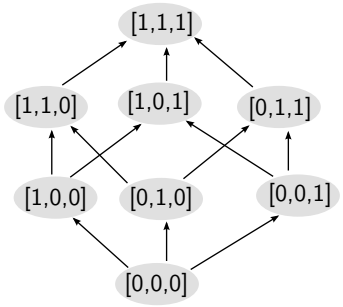
Exercice 2

Soit la relation suivante, qui est un ordre partiel sur l'ensemble de fonctions $\{0,1\}^{\{1,2,3\}}$.

$$\left\{ \langle f, g\rangle \in \{0,1\}^{\{1,2,3\}} \times \{0,1\}^{\{1,2,3\}} \;\middle|\; \big(\forall i \in \{1,2,3\} \mid f(i) \leq g(i)\big) \right\}.$$

Tracez le diagramme de Hasse de cet ordre.

Solution : Dans le diagramme qui suit, nous utilisons la notation $[\mathbf{a}, \mathbf{b}, \mathbf{c}]$ pour désigner la fonction $\{\langle 1, a\rangle, \langle 2, b\rangle, \langle 3, c\rangle\}$.



Section 2.1.4 – Exercices sur les suites

Exercice 1 : Évaluez la valeur de la somme suivante :

$$s \;=\; \sum_{i=1}^{3}\sum_{j=1}^{2}(\,i^2+j\,)\,.$$

Solution 1 : Comme les sommes comportent peu de termes, il est facile de les calculer "à la main" :

$$\begin{aligned}
s &= \sum_{i=1}^{3}\sum_{j=1}^{2}(\,i^2+j\,)\\
&= \sum_{i=1}^{3}(\,(i^2+1)+(i^2+2)\,)\\
&= \sum_{i=1}^{3}(\,2i^2+3\,)\\
&= (2\cdot 1^2+3)+(2\cdot 2^2+3)+(2\cdot 3^2+3)\\
&= 5+11+21\\
&= 37
\end{aligned}$$

Solution 2 : En utilisant les propriétés des sommes en notation sigma, on obtient :

$$\begin{aligned}
s &= \sum_{i=1}^{3}\sum_{j=1}^{2}(\,i^2+j\,)\\
&= \sum_{i=1}^{3}\left[\sum_{j=1}^{2}i^2+\sum_{j=1}^{2}j\right] && \langle\ \textit{Prop 2.1.2-c}\ \rangle\\
&= \sum_{i=1}^{3}\sum_{j=1}^{2}i^2\;+\;\sum_{i=1}^{3}\sum_{j=1}^{2}j && \langle\ \textit{Prop 2.1.2-c}\ \rangle\\
&= \sum_{i=1}^{3}2i^2\;+\;3\sum_{j=1}^{2}j && \langle\ \textit{Prop 2.1.2-b, cas particulier (2 fois)}\ \rangle\\
&= 2\sum_{i=1}^{3}i^2\;+\;3\sum_{j=1}^{2}j && \langle\ \textit{Prop 2.1.2-b}\ \rangle\\
&= 2\cdot\frac{(2\cdot 3+1)\cdot(3+1)\cdot 3}{6}\;+\;3\sum_{j=1}^{2}j && \langle\ \textit{Prop 2.1.2-e}\ \rangle\\
&= 2\cdot\frac{(2\cdot 3+1)\cdot(3+1)\cdot 3}{6}\;+\;3\cdot\frac{2\cdot(2+1)}{2} && \langle\ \textit{Prop 2.1.2-d}\ \rangle\\
&= 7\cdot 4\;+\;3\cdot 3 && \langle\ \textit{Arithmétique}\ \rangle\\
&= 37
\end{aligned}$$

Exercice 2 : En vous servant de la notation en extension des sommes, illustrez les égalités suivantes (la réponse du premier exercice vous est donnée à titre d'exemple) :

a) $\sum_{i=1}^{n} i \;=\; 1 + \sum_{i=2}^{n} i$

Solution :

$$\begin{aligned}\sum_{i=1}^{n} i &= 1 + 2 + 3 + \ldots + n \\ &= 1 + (2 + 3 + \ldots + n) \\ &= 1 + \sum_{i=2}^{n} i\end{aligned}$$

b) $\sum_{i=0}^{n} i \;=\; \sum_{i=1}^{n} i$

Solution :

$$\begin{aligned}\sum_{i=0}^{n} i &= 0 + 1 + 2 + 3 + \ldots + n \\ &= 1 + 2 + 3 + \ldots + n \\ &= \sum_{i=1}^{n} i\end{aligned}$$

c) $\sum_{i=1}^{n} (n - i) \;=\; \sum_{i=1}^{n-1} i$

Solution :

$$\begin{aligned}\sum_{i=1}^{n} (n - i) &= (n-1) + (n-2) + \ldots + (n-(n-2)) + (n-(n-1)) + (n-n) \\ &= (n-1) + (n-2) + \ldots + 2 + 1 + 0 \\ &= 0 + 1 + 2 + \ldots + (n-2) + (n-1) \\ &= 1 + 2 + \ldots + (n-2) + (n-1) \\ &= \sum_{i=1}^{n-1} i\end{aligned}$$

»

d) $\displaystyle\sum_{i=1}^{n} k\sqrt{i} \;=\; k \cdot \sum_{i=1}^{n} \sqrt{i}\;,$ pour tout $k \in \mathbb{R}$

Solution :

$$\begin{aligned}\sum_{i=1}^{n} k\sqrt{i} &= k\sqrt{1} + k\sqrt{2} + k\sqrt{3} + \ldots + k\sqrt{n} \\ &= k \cdot (\sqrt{1} + \sqrt{2} + \sqrt{3} + \ldots + \sqrt{n}) \\ &= k \cdot \sum_{i=1}^{n} \sqrt{i}.\end{aligned}$$

e) $\displaystyle\sum_{i=0}^{n-1} 2i + 1 \;=\; \sum_{i=1}^{n} 2i - 1$

Solution :

$$\begin{aligned}\sum_{i=0}^{n-1} 2i + 1 &= (2 \cdot 0 + 1) + (2 \cdot 1 + 1) + (2 \cdot 2 + 1) + \ldots + (2 \cdot (n-1) + 1) \\ &= (2 \cdot 1 - 2 + 1) + (2 \cdot 2 - 2 + 1) + (2 \cdot 3 - 2 + 1) + \ldots + (2 \cdot n - 2 + 1) \\ &= (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + (2 \cdot 3 - 1) + \ldots + (2 \cdot n - 1) \\ &= \sum_{i=1}^{n} 2i - 1\,.\end{aligned}$$

f) $\displaystyle\sum_{i=1}^{n-1}\sum_{j=1}^{n}\sum_{k=1}^{n} 1 \;=\; n^3 - n^2$

Solution :

$$\begin{aligned}\sum_{i=1}^{n-1}\sum_{j=1}^{n}\sum_{k=1}^{n} 1 &= \sum_{i=1}^{n-1}\sum_{j=1}^{n}(\underbrace{1 + 1 + \ldots + 1}_{n \text{ fois}}) \\ &= \sum_{i=1}^{n-1}\sum_{j=1}^{n} n \\ &= \sum_{i=1}^{n-1}(\underbrace{n + n + \ldots + n}_{n \text{ fois}}) \\ &= \sum_{i=1}^{n-1} n \cdot n \\ &= \sum_{i=1}^{n-1} n^2 \\ &= \underbrace{n^2 + n^2 + \ldots + n^2}_{(n-1) \text{ fois}} \\ &= (n-1) \cdot n^2 \\ &= n^3 - n^2\end{aligned}$$

Exercice 3 : Soit la suite $\langle v_n \rangle_{n\in\mathbb{N}^*}$ dont le $n$ième terme correspond à la valeur retournée par l'algorithme suivant exécuté avec le paramètre n en entrée (avec $n \geq 1$).

```
Algo_Jouet_Trois ( n )
  v ← 0
  Pour i = 1 à n Faire
      Pour j = i + 1 à n Faire
          v ← v + 1
      Fin Pour
  Fin Pour
  Retourner v
```

a) À l'aide de la notation sigma, donnez l'expression permettant de calculer un terme v_n quelconque (avec $n \in \mathbb{N}^*$).

Solution :

$$v_n \;=\; \sum_{i=1}^{n} \sum_{j=i+1}^{n} 1\,.$$

b) À partir de la réponse précédente, calculez le terme général de la suite $\langle v_n \rangle_{n\in\mathbb{N}^*}$. Pour ce faire, utilisez les propriétés arithmétiques des sommes en notation sigma.

Solution :

$$\begin{aligned}
v_n &= \sum_{i=1}^{n} \sum_{j=i+1}^{n} 1 \\
&= \sum_{i=1}^{n} (n-i) && \langle\ \textit{Prop 2.1.2-a}\ \rangle \\
&= \sum_{i=1}^{n-1} i && \langle\ \textit{Voir l'exercice 2-c ci-haut}\ \rangle \\
&= \frac{(n-1)\cdot\big((n-1)+1\big)}{2} && \langle\ \textit{Prop 2.1.2-d}\ \rangle \\
&= \frac{n(n-1)}{2} && \langle\ \textit{Arithmétique}\ \rangle
\end{aligned}$$

c) Donnez la définition par récurrence de la suite $\langle v_n \rangle_{n\in\mathbb{N}^*}$.

Solution :

$$\begin{cases} v_1 \;=\; 0 \\ v_n \;=\; v_{n-1} + (n-1) \quad \forall n \in \mathbb{N}^* \setminus \{1\}\,. \end{cases}$$

d) Calculez les 5 premiers termes de la suite $\langle v_n \rangle_{n \in \mathbb{N}^*}$ à l'aide de chacune des trois expressions trouvées en (a), (b) et (c). Assurez-vous que les réponses sont identiques.

Solution :

$$\langle v_n \rangle_{n \in \mathbb{N}^*} \;=\; \langle 0, 1, 3, 6, 10, \ldots \rangle \; .$$

Section 2.2.3 – Exercices sur la méthode des substitutions à rebours

Exercice 1 : Calculez le terme général des récurrences suivantes à l'aide de la méthode des substitutions à rebours :

a) $\begin{cases} x_1 &= 0 \\ x_n &= x_{n-1} + 5 \quad \forall n \in \mathbb{N}^* \setminus \{1\} \end{cases}$

Solution :

$$\begin{aligned}
x_n &= x_{n-1} + 5 && \langle \textit{ Définition par récurrence de } x_n \rangle \\
&= x_{n-2} + 5 + 5 && \langle \textit{ Car } x_{n-1} = x_{n-2} + 5 \rangle \\
&= x_{n-3} + 5 + 5 + 5 && \langle \textit{ Car } x_{n-2} = x_{n-3} + 5 \rangle \\
&= x_{n-4} + 5 + 5 + 5 + 5 && \langle \textit{ Car } x_{n-3} = x_{n-4} + 5 \rangle \\
&= \dots \\
&= x_{n-i} + \underbrace{5 + 5 + \dots + 5}_{i \text{ fois}} && \langle\ \forall i \in \{1, \dots, n-1\}\ \rangle \\
&= x_{n-i} + 5i \\
&= x_1 + 5 \cdot (n-1) && \langle \textit{ Avec } [i := n-1] \rangle \\
&= 5 \cdot (n-1) && \langle \textit{ Car } x_1 = 0 \rangle \\
&= 5n - 5
\end{aligned}$$

b) $\begin{cases} y(1) &= 4 \\ y(n) &= 3 \cdot y(n-1) \quad \forall n \in \mathbb{N}^* \setminus \{1\} \end{cases}$

Solution :

$$\begin{aligned}
y(n) &= 3 \cdot y(n-1) && \langle \textit{ Définition par récurrence de } y_n \rangle \\
&= 3 \cdot 3 \cdot y(n-2) && \langle \textit{ Car } y(n-1) = 3 \cdot y(n-2) \rangle \\
&= 3 \cdot 3 \cdot 3 \cdot y(n-3) && \langle \textit{ Car } y(n-2) = 3 \cdot y(n-3) \rangle \\
&= 3 \cdot 3 \cdot 3 \cdot 3 \cdot y(n-4) && \langle \textit{ Car } y(n-3) = 3 \cdot y(n-4) \rangle \\
&= \dots \\
&= \underbrace{3 \cdot 3 \cdot \dots \cdot 3}_{i \text{ fois}} \cdot y(n-i) && \langle \textit{ Pour tout } i \in \{1, \dots, n-1\} \rangle \\
&= 3^i \cdot y(n-i) \\
&= 3^{n-1} \cdot y(1) && \langle \textit{ Avec } [i := n-1] \rangle \\
&= 4 \cdot 3^{n-1} && \langle \textit{ Car } y(1) = 4 \rangle
\end{aligned}$$

c) $\begin{cases} z(0) &= 0 \\ z(n) &= z(n-1) + 2n - 1 \quad \forall n \in \mathbb{N}^* \end{cases}$

Solution :

$$
\begin{array}{lll}
& z(n) & \\
= & z(n-1) + 2n - 1 & \langle \textit{ Définition de } z_n \rangle \\
= & z(n-2) + 2(n-1) - 1 + 2n - 1 & \langle \textit{ Substitution de } z(n-1) \rangle \\
= & z(n-2) + 2(n-1) + 2n - 2 & \langle \textit{ Arithmétique} \rangle \\
= & z(n-3) + 2(n-2) - 1 + 2(n-1) + 2n - 2 & \langle \textit{ Substitution de } z(n-2) \rangle \\
= & z(n-3) + 2(n-2) + 2(n-1) + 2n - 3 & \langle \textit{ Arithmétique} \rangle \\
= & z(n-4) + 2(n-3) - 1 + 2(n-2) + 2(n-1) + 2n - 3 & \langle \textit{ Substitution de } z(n-3) \rangle \\
= & z(n-4) + 2(n-3) + 2(n-2) + 2(n-1) + 2n - 4 & \langle \textit{ Arithmétique} \rangle \\
= & z(n-4) + 2\,[\,(n-3) + (n-2) + (n-1) + n\,] - 4 & \langle \textit{ Arithmétique} \rangle \\
& \ldots & \\
= & z(n-i) + 2\,[\,(n-(i-1)) + (n-(i-2)) + \ldots + (n-1) + n\,] - i & \langle\, \forall i \in \{1, \ldots, n\} \,\rangle \\
= & z(0) + 2\,[\,(n-(n-1)) + (n-(n-2)) + \ldots + (n-1) + n\,] - n & \langle \textit{ Avec } [i := n] \rangle \\
= & z(0) + 2\,[\,1 + 2 + \ldots + (n-1) + n\,] - n & \langle \textit{ Arithmétique} \rangle \\
= & z(0) + n + 2\,[\,1 + 2 + \ldots + (n-1)\,] & \langle \textit{ Car } 2n - n = n \rangle \\
= & n + 2\,[\,1 + 2 + \ldots + (n-1)\,] & \langle \textit{ Car } z(0) = 0 \rangle \\
= & n + 2 \cdot \displaystyle\sum_{j=1}^{n-1} j & \langle \textit{ Notation sigma} \rangle \\
= & n + 2 \cdot \dfrac{(n-1) \cdot (\,(n-1) + 1\,)}{2} & \langle \textit{ Prop 2.1.2-d, avec } [n := n-1] \rangle \\
= & n + 2 \cdot \dfrac{(n-1) \cdot n}{2} & \langle \textit{ Arithmétique} \rangle \\
= & n + n^2 - n & \\
= & n^2 &
\end{array}
$$

Section 2.3.5 – Exercices sur l'induction mathématique

Exercice 1 : Étant donnée la formule :

$$\sum_{i=0}^{n} 2i \;=\; n(n+1)\,.$$

a) Vérifiez cette formule pour $n = 1$, 2, 5 et 10.

b) Démontrez par induction que cette formule est vraie pour tout $n \in \mathbb{N}$.

Démonstration

Prenons le prédicat $P(n)$: $\displaystyle\sum_{i=0}^{n} 2i \;=\; n(n+1)$.

Alors nous devons démontrer que $(\forall n \in \mathbb{N} \mid P(n))$.

Et par le principe d'induction mathématique,

il suffit de démontrer que $P(0) \;\wedge\; (\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n))$.

Montrons $P(0)$. $\left\langle$ *C'est-à-dire, montrons* $\displaystyle\sum_{i=0}^{0} 2i = 0 \cdot (0+1)$. $\right\rangle$

$\displaystyle\sum_{i=0}^{0} 2i \;=\; 2 \cdot 0$, ce qui est bien égal à $0 \cdot (0+1)$.

Montrons $(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n))$.

Soit $n \in \mathbb{N}^*$, et supposons $P(n-1)$ vrai.

$\left\langle$ *C'est-à-dire, n satisfait* $\displaystyle\sum_{i=0}^{n-1} 2i = (n-1)((n-1)+1)$ $\right\rangle$

Montrons $P(n)$. $\left\langle$ *C'est à dire* $\displaystyle\sum_{i=0}^{n} 2i \;=\; n(n+1)$ $\right\rangle$

$$\begin{aligned}
&\sum_{i=0}^{n} 2i \\
=\quad & \qquad \langle \textit{ Passage de l'écriture en notation sigma à l'écriture en extension } \rangle \\
&2 \cdot 0 + 2 \cdot 1 + 2 \cdot 2 + \ldots + 2 \cdot n \\
= \quad & \\
&2 \cdot 0 + 2 \cdot 1 + 2 \cdot 2 + \ldots + 2 \cdot (n-1) + 2 \cdot n \\
= \quad & \\
&\Big(2 \cdot 0 + 2 \cdot 1 + 2 \cdot 2 + \ldots + 2 \cdot (n-1)\Big) + 2 \cdot n \\
= \quad & \qquad \langle \textit{ Passage de l'écriture en extension à l'écriture notation sigma. } \rangle \\
&\left(\sum_{i=0}^{n-1} 2i\right) + 2 \cdot n
\end{aligned}$$

$$
\begin{aligned}
&= && \langle \textit{ Par l'hypothèse d'induction. } \rangle \\
&\quad (n-1)((n-1)+1) + 2 \cdot n \\
&= && \langle \textit{ Développement de l'expression. } \rangle \\
&\quad (n^2 - n) + 2n \\
&= \\
&\quad n^2 + n \\
&= && \langle \textit{ Mise en évidence. } \rangle \\
&\quad n(n+1)\,.
\end{aligned}
$$

On a démontré $(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n))$.

Conclusion : on a bien $\Big(\forall n \in \mathbb{N} \mid P(n)\Big)$,

c'est à dire : $\displaystyle\sum_{i=0}^{n} 2i = n(n+1)$.

C.Q.F.D.

Exercice 2 : Soit $f : \mathbb{N} \longrightarrow \mathbb{R}$, une fonction qui satisfait la règle de récurrence suivante :

$$
\begin{cases}
f(0) &= 3 \\
f(k+1) &= 2 \cdot f(k) + 2k - 4 \quad \forall k \in \mathbb{N}\,.
\end{cases}
$$

a) Évaluez $f(0)$, $f(1)$, $f(2)$, $f(5)$ et $f(10)$.
Réponse : $f(0) = 3$, $f(1) = 2$, $f(2) = 2$, $f(5) = 24$ et $f(10) = 1006$.

b) Démontrez par induction que $f(n) = 2^n - 2n + 2 \quad \forall n \in \mathbb{N}$.

Démonstration
Prenons le prédicat $P(n) : \quad f(n) = 2^n - 2n + 2$.
Alors nous devons démontrer que $(\forall n \in \mathbb{N} \mid P(n))$.
Et par le principe d'induction mathématique,
il suffit de démontrer que $P(0) \ \wedge \ (\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1))$.[7]

Montrons $P(0)$. $\langle$ *C'est-à-dire, montrons* $f(0) = 2^0 - 2 \cdot 0 + 2$. $\rangle$

$2^0 - 2 \cdot 0 + 2 \ = \ 1 - 0 + 2 \ = \ 3$, ce qui est bien égal à la définition de $f(0)$.

7. Notez que nous avons choisi cette forme du principe d'induction, car elle est mieux adaptée à ce problème.

Montrons $(\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1))$**.**

Soit $n \in \mathbb{N}$, et supposons $P(n)$ vrai. ⟨ *C'est-à-dire, n satisfait $f(n) = 2^n - 2n + 2$.* ⟩

Et montrons $P(n+1)$. ⟨ *c'est à dire $f(n+1) = 2^{n+1} - 2(n+1) + 2$.* ⟩

$$
\begin{array}{ll}
& f(n+1) \\
= & \qquad \langle \textit{ Définition de } f, \textit{ car } n \in \mathbb{N}. \rangle \\
& 2 \cdot f(n) + 2n - 4 \\
= & \qquad \langle \textit{ Par l'hypothèse d'induction. } \rangle \\
& 2(2^n - 2n + 2) + 2n - 4 \\
= & \qquad \langle \textit{ Simplifications algébriques. } \rangle \\
& 2 \cdot 2^n - 4n + 4 + 2n - 4 \\
= & \qquad \langle \textit{ Simplifications algébriques. } \rangle \\
& 2^{n+1} - 2n - 2 + 2 \\
= & \qquad \langle \textit{ Mise en évidence. } \rangle \\
& 2^{n+1} - 2(n+1) + 2\,.
\end{array}
$$

On a démontré $(\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1))$.

Conclusion : on a bien $\Big(\forall n \in \mathbb{N} \mid P(n)\Big)$,
c'est à dire : $f(n) = 2^n - 2n + 2 \quad \forall n \in \mathbb{N}$.

C.Q.F.D.

Exercice 3 : Soit la suite $\langle a_n \rangle_{n \in \mathbb{N}}$ définie par récurrence par :

$$
\left\{ \begin{array}{lcl} a_0 & = & 2 \\ a_n & = & 3a_{n-1} + 2 \quad \forall n \in \mathbb{N}^*\,. \end{array} \right.
$$

Montrez par induction que le terme général de la suite $\langle a_n \rangle_{n \in \mathbb{N}}$ est :

$$a_n \;=\; 3^{n+1} - 1 \quad \forall n \in \mathbb{N}\,.$$

Démonstration
Prenons le prédicat $\quad P(n) : \; a_n = 3^{n+1} - 1.$
Alors nous devons démontrer que $(\forall n \in \mathbb{N} \mid P(n))$.
Et par le principe d'induction mathématique,
il suffit de démontrer que $\quad P(0) \;\wedge\; (\forall n \in \mathbb{N}^\star \mid P(n-1) \Rightarrow P(n))$.

Montrons $P(0)$**.** ⟨ *C'est-à-dire, montrons $a_0 = 3^{0+1} - 1$.* ⟩

$3^{0+1} - 1 \;=\; 3 - 1 \;=\; 2$, ce qui est bien égal à la définition de a_0.

Montrons $(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n))$**.**

Soit $n \in \mathbb{N}^\star$, et supposons $P(n-1)$ vrai. (*C'est-à-dire que* $a_{n-1} = 3^{(n-1)+1} - 1$.)

⟨ Et montrons $P(n)$. (*c'est à dire* $a_n = 3^{n+1} - 1$.)

$$
\begin{aligned}
& a_n \\
= \quad & \qquad \langle \textit{ Définition de la suite } \langle a_n \rangle_{n\in\mathbb{N}}, \textit{ car } n \in \mathbb{N}^\star. \rangle \\
& 3\,a_{n-1} + 2 \\
= \quad & \qquad \langle \textit{ Par l'hypothèse d'induction.} \rangle \\
& 3(3^{(n-1)+1} - 1) + 2 \\
= \quad & \qquad \langle \textit{ Simplification algébrique.} \rangle \\
& 3(3^n - 1) + 2 \\
= \quad & \qquad \langle \textit{ Par distributivité.} \rangle \\
& 3 \cdot 3^n - 3 + 2 \\
= \quad & \qquad \langle \textit{ Simplifications algébriques.} \rangle \\
& 3^{n+1} - 1\,.
\end{aligned}
$$

On a démontré $(\forall n \in \mathbb{N}^\star \mid P(n-1) \Rightarrow P(n))$.

Conclusion : on a bien $\Big(\forall n \in \mathbb{N} \mid P(n)\Big)$, c'est à dire : $a_n = 3^{n+1} - 1 \quad \forall n \in \mathbb{N}$.

C.Q.F.D.

Exercice 4 : Soit la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par :

$$
\begin{cases}
b_0 &= -4 \\
b_n &= 3\,b_{n-1} + 4n + 4 \quad \forall n \in \mathbb{N}^*\,.
\end{cases}
$$

Montrez par induction que le terme général de la suite $\langle b_n \rangle_{n\in\mathbb{N}}$ est :

$$b_n = 3^n - 2n - 5 \quad \forall n \in \mathbb{N}\,.$$

Démonstration

Prenons le prédicat $P(n) :\ b_n = 3^n - 2n - 5$.
Alors nous devons démontrer que $(\forall n \in \mathbb{N} \mid P(n))$.
Et par le principe d'induction mathématique,
il suffit de démontrer que $P(0) \ \wedge\ (\forall n \in \mathbb{N}^\star \mid P(n-1) \Rightarrow P(n))$.

Montrons $P(0)$**.** ⟨ *C'est-à-dire, montrons* $b_0 = 3^0 - 2 \cdot 0 - 5$. ⟩

$3^0 - 2 \cdot 0 - 5 \ = \ 1 - 0 - 5 \ = \ -4$, ce qui est bien égal à la définition de b_0.

Montrons $(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n))$**.**

Soit $n \in \mathbb{N}^\star$ et supposons $P(n-1)$ vrai.
(*C'est-à-dire que* $b_{n-1} = 3^{n-1} - 2(n-1) - 5$.)

Montrons $P(n)$. (*c'est à dire* $b_n = 3^n - 2n - 5$.)

$$
\begin{array}{ll}
& b_n \\
= & \qquad \langle \textit{ Définition de la suite } \langle b_n \rangle_{n\in\mathbb{N}}\textit{, car car } n \in \mathbb{N}^\star. \rangle \\
& 3\, b_{n-1} + 4n + 4 \\
= & \qquad \langle \textit{ Par l'hypothèse d'induction. } \rangle \\
& 3(3^{n-1} - 2(n-1) - 5) + 4n + 4 \\
= & \qquad \langle \textit{ Simplification algébrique. } \rangle \\
& 3 \cdot 3^{n-1} - 6n + 6 - 15 + 4n + 4 \\
= & \qquad \langle \textit{ Simplifications algébriques. } \rangle \\
& 3^n - 2n - 5\,.
\end{array}
$$

On a démontré $(\forall n \in \mathbb{N}^\star \mid P(n-1) \Rightarrow P(n))$.

Conclusion : on a bien $\Big(\forall n \in \mathbb{N} \mid P(n)\Big)$,
c'est à dire : $b_n = 3^n - 2n - 5 \quad \forall n \in \mathbb{N}$.

C.Q.F.D.

Exercice 5 : Soit la suite $\langle c_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par :

$$
\left\{
\begin{array}{lcl}
c_0 & = & 1 \\
c_1 & = & 1 \\
c_n & = & 4 \cdot c_{n-1} - 4 \cdot c_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\}\,.
\end{array}
\right.
$$

Montrez par induction que le terme général de la suite $\langle c_n \rangle_{n\in\mathbb{N}}$ est :

$$c_n \;=\; 2^{n-1} \cdot (2-n) \quad \forall n \in \mathbb{N}\,.$$

Démonstration
Prenons le prédicat $\quad P(n) : \quad c_n = 2^{n-1} \cdot (2-n)$.
Alors nous devons démontrer que $(\forall n \in \mathbb{N} \mid P(n))$.
Et par le principe d'induction mathématique à deux cas de base,
il suffit de démontrer que $\; P(0) \;\wedge\; P(1) \;\wedge\; (\forall n \in \mathbb{N}\setminus\{0,1\} \mid P(n-2) \wedge P(n-1) \Rightarrow P(n))$.
Montrons $P(0)$**.** $\qquad \langle$ *C'est-à-dire, montrons* $c_0 = 2^{0-1} \cdot (2-0)$. $\rangle$

$2^{0-1} \cdot (2-0) \;=\; \frac{1}{2} \cdot 2 \;=\; 1$, ce qui est bien égal à la définition de c_0.

Montrons $P(1)$**.** ⟨ *C'est-à-dire, montrons* $c_1 = 2^{1-1} \cdot (2-1)$*.* ⟩

$2^{1-1} \cdot (2-1) \;=\; 1 \cdot 1 \;=\; 1$, ce qui est bien égal à la définition de c_1.

Montrons $(\forall n \in \mathbb{N}\backslash\{0,1\} \mid P(n-2) \wedge P(n-1) \Rightarrow P(n))$**.**

Soit $n \in \mathbb{N}^\star$, et supposons $P(n-2)$ et $P(n-1)$ vrais.

Nous avons donc :

$$\begin{cases} c_{n-2} &=& 2^{(n-2)-1} \cdot (2-(n-2)) \\ c_{n-1} &=& 2^{(n-1)-1} \cdot (2-(n-1)) \end{cases}$$

Montrons $P(n)$. (*c'est à dire* $c_n = 2^{n-1} \cdot (2-n)$.)

$$\begin{array}{ll} & c_n \\ = & \qquad \langle \textit{ Définition de la suite } \langle c_n \rangle_{n\in\mathbb{N}}\textit{, car } n \in \mathbb{N}\backslash\{0,1\}. \rangle \\ & 4 \cdot c_{n-1} - 4 \cdot c_{n-2} \\ = & \qquad \langle \textit{ Par l'hypothèse d'induction.} \rangle \\ & 4\Big(2^{(n-1)-1} \cdot (2-(n-1))\Big) \;-\; 4\Big(2^{(n-2)-1} \cdot (2-(n-2))\Big) \\ = & \qquad \langle \textit{ Simplification algébrique.} \rangle \\ & 4\Big(2^{n-2} \cdot (3-n)\Big) \;-\; 4\Big(2^{n-3} \cdot (4-n)\Big) \\ = & \qquad \langle \textit{ Simplifications algébriques.} \rangle \\ & 12 \cdot 2^{n-2} - 4n \cdot 2^{n-2} - 16 \cdot 2^{n-3} + 4n \cdot 2^{n-3} \\ = & \qquad \langle \textit{ Réécriture de l'expression.} \rangle \\ & 6 \cdot 2 \cdot 2^{n-2} - 2n \cdot 2 \cdot 2^{n-2} - 4 \cdot 4 \cdot 2^{n-3} + n \cdot 4 \cdot 2^{n-3} \\ = & \qquad \langle \textit{ Simplifications algébriques.} \rangle \\ & 6 \cdot 2^{n-1} - 2n \cdot 2^{n-1} - 4 \cdot 2^{n-1} + n \cdot 2^{n-1} \\ = & \qquad \langle \textit{ Mise en évidence.} \rangle \\ & 2^{n-1} \cdot (6 - 2n - 4 + n)) \\ = & \qquad \langle \textit{ Simplifications algébriques.} \rangle \\ & 2^{n-1} \cdot (2-n)\,. \end{array}$$

On a démontré $\Big(\forall n \in \mathbb{N}\backslash\{0,1\} \mid P(n-2) \wedge P(n-1) \Rightarrow P(n)\Big)$.

Conclusion : on a bien $\Big(\forall n \in \mathbb{N} \mid P(n)\Big)$,

c'est à dire : $c_n = 2^{n-1} \cdot (2-n) \quad \forall n \in \mathbb{N}$.

C.Q.F.D.

Exercice 6 : Démontrez par induction que les deux fonctions suivantes sont équivalentes à la fonction exponentielle, c.-à-d. qu'elles sont égales à e^n pour tout $n \in \mathbb{N}$:

a) — $\texttt{exp}(0) = 1$
   — $\texttt{exp}(n) = e \cdot \exp(n-1)$ pour $n > 0$

b) — $\texttt{expBin}(0) = 1$
   — $\texttt{expBin}(n) = \texttt{expBin}(\frac{n}{2})^2$ si $n > 0$ est pair,
   — $\texttt{expBin}(n) = e \cdot (\texttt{expBin}(\frac{n-1}{2}))^2$ si n est impair.

c) Sans lien avec l'induction : laquelle des deux façons de calculer e^n est la plus "efficace" ?

Exercice 7 : Démontrez par induction sur n que la méthode suivante est équivalente à l'exponentiation de b par n modulo m, c.-à-d. qu'elle est égale à $b^n \bmod m$ pour tout $b, n, m \in \mathbb{N}$ (Quand on dit "par induction sur n", on dit qu'on va démontrer une proposition de la forme $(\forall n \mid P(n))$, donc que b et m seront fixés ; pour un indice sur quel P choisir, voir note [8]. Ensuite suivre les étapes) :

$\texttt{expmod}(b, n, m)$ On suppose $b, n, m \in \mathbb{N},\ m \geq 2; n \geq 0$

Si $n = 0$ **alors**
    retourner 1
Sinon
    Si n est pair **alors**
        Retourner $\texttt{expmod}(b, n/2, m)^2 \bmod m$
    Sinon
        Retourner $((\texttt{expmod}(b, \frac{n-1}{2}, m)^2 \bmod m) \cdot (b \bmod m)) \bmod m$
    Fin Si
Fin Si

8. Prenons $P(n) := (\forall b, m \in \mathbb{N} \mid b^n \bmod m = \mathit{expmod}(b, n, m))$

Section 2.4.4 – Exercices sur les cas particuliers de récurrences

Exercice 1 :

a) Est-ce que la suite $\langle c_n \rangle_{n\in\mathbb{N}}$, définie par le terme général $c_n = 5n-6 \quad \forall n \in \mathbb{N}$, est une suite arithmétique ?
Réponse : oui, voir le théorème 2.4.2 (3. $\Rightarrow$ 1.)

b) Donnez c_0, c_1 et c_{200}.
Réponse : $c_0 = -6$, $c_1 = -1$ et $c_{200} = 994$.

c) Soit la suite $\langle S_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par : $\begin{cases} S_0 &= -6 \\ S_n &= S_{n-1} + 5n - 6 \quad \forall n \in \mathbb{N}^* . \end{cases}$
Montrez (sans utiliser l'induction) que le terme général de la suite $\langle S_n \rangle_{n\in\mathbb{N}}$ est

$$S_n = \frac{(n+1)(5n-12)}{2} \quad \forall n \in \mathbb{N} .$$

Démonstration

Comme la suite $\langle c_n \rangle_{n\in\mathbb{N}}$ est une suite arithmétique (voir a)), S_n est donc une suite de somme de premiers termes d'une suite arithmétique, par le théorème 2.4.6, on obtient donc

$$S_n = \frac{(a_0 + a_n)(n+1)}{2} = \frac{(-6+5n-6)(n+1)}{2} = \frac{(n+1)(5n-12)}{2} \qquad \forall n \in \mathbb{N} .$$

C.Q.F.D.

Exercice 2 : Trouvez le terme général des suites suivantes :

a) $\begin{cases} b_0 &= 0 \\ b_n &= b_{n-1} + n \quad \forall n \in \mathbb{N}^* . \end{cases}$

Solution :
On remarque que $\langle b_n \rangle_{n\in\mathbb{N}}$ est *une suite sommes de premiers termes* d'une suite arithmétique. (Voir le théorème 2.4.6 et la définition 2.4.5.)

Soit $\langle a_n \rangle_{n\in\mathbb{N}}$, la suite définie par le terme général $a_n = 0 + n \cdot 1 \quad \forall n \in \mathbb{N}$.
Alors,

(1) par le théorème 2.4.2, on a que $\langle a_n \rangle_{n\in\mathbb{N}}$ est **une suite arithmétique** de 1$^{\text{er}}$ terme $a = 0$ et de différence $d = 1$.

(2) Et en plus, **on a bien que** $\begin{cases} b_0 &= a_0 \\ b_n &= b_{n-1} + a_n \quad \forall n \in \mathbb{N}^* \end{cases}$

$\langle$ *Car* $a_0 = 0$ *et* $a_n = 0 + n \cdot 1 = n.$ $\rangle$

Donc, par le théorème 2.4.6, on a $b_n = \dfrac{(a_0 + a_n)(n+1)}{2} \qquad \forall n \in \mathbb{N}\,.$

Réponse : $b_n = \dfrac{(0 + 0 + n \cdot 1)(n+1)}{2} = \dfrac{n(n+1)}{2} \qquad \forall n \in \mathbb{N}\,.$

b) $w_n = 1 + 3 + 5 + 7 + 9 + \cdots + (2n+1) \quad \forall n \in \mathbb{N}\,.$

Réponse : $w_n = (n+1)^2 \quad \forall n \in \mathbb{N}\,.$

c) $\begin{cases} p_0 &= -2 \\ p_n &= p_{n-1} + 5n - 2 \qquad \forall n \in \mathbb{N}^*\,. \end{cases}$

Réponse : $p_n = \dfrac{(5n-4)(n+1)}{2} \quad \forall n \in \mathbb{N}\,.$

Exercice 3 : Soit la suite $\langle d_n \rangle_{n\in\mathbb{N}}$ définie par récurrence par :

$$\begin{cases} d_0 &= 5 \cdot 2^3 \\ d_n &= d_{n-1} + 5 \cdot 2^{n+3} \quad \forall n \in \mathbb{N}^*\,. \end{cases}$$

Montrez (sans utiliser l'induction) que le terme général de la suite $\langle d_n \rangle_{n\in\mathbb{N}}$ est

$$d_n = \frac{5 \cdot 2^3 \,(1 - 2^{n+1})}{-1} \quad \forall n \in \mathbb{N}\,.$$

Démonstration

Soit la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ définie par le terme général $a_n = 5 \cdot 2^{n+3} \quad \forall n \in \mathbb{N}$.

Comme $5 \cdot 2^{n+3} = (5 \cdot 2^3) \cdot 2^n$ et comme $a_0 = 5 \cdot 2^3$, par le théorème 2.4.4 (3. $\Rightarrow$ 1.) on remarque que la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ est une suite géométrique de premier terme $a = 5 \cdot 2^3$ et de raison $r = 2$.

On a donc que la suite $\langle d_n \rangle_{n\in\mathbb{N}}$ est une suite de sommes de premiers termes d'une suite géométrique, par le théorème 2.4.7, on obtient donc

$d_n = \dfrac{5 \cdot 2^3 \cdot (1 - 2^{n+1})}{1 - 2} = \dfrac{5 \cdot 2^3 \cdot (1 - 2^{n+1})}{-1} \qquad \forall n \in \mathbb{N}\,.$

C.Q.F.D.

Exercice 4 : Vous placez $\$1000.^{00}$ dans un compte à intérêt composé de 5% par année.

Ainsi, après un an il y aura dans votre compte, $\$1000.^{00} + (5\%$ *de* $\$1000.^{00})$*, c'est-à-dire, en tout* $\$1050.^{00}$*. Après deux ans, il y aura dans votre compte,* $\$1050.^{00} + (5\%$ *de* $\$1050.^{00})$*, etc...*

Soit $\langle \$_n \rangle_{n\in\mathbb{N}}$, la suite qui donne le montant d'argent qu'il y a dans votre compte après n années.

a) Définissez $\langle \$_n \rangle_{n\in\mathbb{N}}$ par récurrence.

Réponse : $\begin{cases} \$_0 &= 1000 \\ \$_n &= \$_{n-1} + 0.05 \cdot \$_{n-1} \qquad \forall n \in \mathbb{N}^\star \end{cases}$

ou encore

Réponse : $\begin{cases} \$_0 &= 1000 \\ \$_n &= 1.05 \cdot \$_{n-1} \qquad \forall n \in \mathbb{N}^\star \end{cases}$

b) Trouvez le terme général de $\langle \$_n \rangle_{n\in\mathbb{N}}$.

Démonstration

En se basant sur la deuxième réponse du numéro b) et sur le théorème 2.4.4(2. $\Rightarrow$ 1.), on constate que $\langle \$_n \rangle_{n\in\mathbb{N}}$ est une suite géométrique de premier terme $a_0 = 1000$ et de raison $r = 1.05$.

Par le (2. $\Rightarrow$ 3.) de ce théorème on obtient donc que le terme général de cette suite est :

$$\$_n = 1000 \cdot 1.05^n \quad \forall n \in \mathbb{N}$$

C.Q.F.D.

c) Après 10 ans, combien d'argent y aura-t-il dans le compte ?

Réponse : $\$_{10} = 1000 \cdot 1.05^{10} = 1628.89$ dollars.

Exercice 5 : Évaluez la somme suivante :

$$32 + 8 + 2 + \frac{1}{2} + \ldots + \frac{1}{524288}\,.$$

Réponse : $\dfrac{32 \cdot \left(1 - \left(\frac{1}{4}\right)^{12+1}\right)}{1 - \frac{1}{4}} = \cdots$

Section 2.5.5 – Exercices sur la méthode des séries génératrices

Exercice 1 : Exprimez les séries génératrices des suites suivantes sous forme de fonctions rationnelles :

$a)$ $\begin{cases} a_0 &= 1 \\ a_n &= 2 \cdot a_{n-1} + 3^n \quad \forall n \in \mathbb{N}^* \end{cases}$ $b)$ $\begin{cases} b_0 &= 1 \\ b_n &= b_{n-1} + n \quad \forall n \in \mathbb{N}^* \end{cases}$

$c)$ $\begin{cases} c_0 &= 1 \\ c_1 &= 1 \\ c_n &= c_{n-1} + c_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$ $d)$ $\begin{cases} d_0 &= 1 \\ d_1 &= 1 \\ d_n &= 4 \cdot d_{n-1} - 4 \cdot d_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

Réponses : a) $G(x) = \frac{1}{(1-2x)(1-3x)}$ **b)** $G(x) = \frac{x^2-x+1}{(1-x)^3}$ **c)** $G(x) = \frac{1}{1-x-x^2}$ **d)** $G(x) = \frac{1-3x}{(1-2x)^2}$.

Exercice 2 : Décomposez en fractions partielles les fonctions rationnelles suivantes :

$a)$ $a(x) = \dfrac{1}{(x+4)(x+3)}$ $b)$ $b(x) = \dfrac{x}{(1-x)^2(1+x)}$ $c)$ $c(x) = \dfrac{x}{(x-1)(x-2)(x-3)}$

$d)$ $d(x) = \dfrac{1-3x}{1-4x+4x^2}$ $e)$ $e(x) = \dfrac{1-3x}{(1-2x)^2}$ $f)$ $f(x) = \dfrac{x^2+2x+3}{(x-1)^2\,(x-2)}$

Réponses :
a) $a(x) = \dfrac{A}{(x+4)} + \dfrac{B}{(x+3)}$ **b)** $b(x) = \dfrac{A}{1-x} + \dfrac{B}{(1-x)^2} + \dfrac{C}{(1+x)}$ **c)** $c(x) = \dfrac{A}{x-1} + \dfrac{B}{x-2} + \dfrac{C}{x-3}$

d) Voir 2e) **e)** $e(x) = \dfrac{A}{1-2x} + \dfrac{B}{(1-2x)^2}$ **f)** $f(x) = \dfrac{A}{x-1} + \dfrac{B}{(x-1)^2} + \dfrac{C}{x-2}$.

Exercice 3 : Trouvez la série de puissances associée à chacune des fonctions suivantes.

$a)$ $a(x) = \dfrac{1}{(1-5x)}$ $b)$ $b(x) = \dfrac{3}{x-5}$ $c)$ $c(x) = \dfrac{\frac{3}{2}}{1-2x} + \dfrac{\frac{-1}{2}}{(1-2x)^2}$

Réponses en extension :
a) $1 + 5 \cdot x + 5^2 \cdot x^2 + 5^3 \cdot x^3 + \cdots + 5^n \cdot x^n + \cdots$
b) $\frac{\frac{-3}{5}}{1-\frac{1}{5}x} = \frac{-3}{5} + \frac{-3}{5}\frac{1}{5} \cdot x + \frac{-3}{5}(\frac{1}{5})^2 \cdot x^2 + \frac{-3}{5}(\frac{1}{5})^3 \cdot x^3 + \cdots + \frac{-3}{5}(\frac{1}{5})^n \cdot x^n + \cdots$
c) $1 + 1 \cdot x + (2^2 - 2 \cdot 2^1) \cdot x^2 + (2^3 - 3 \cdot 2^2) \cdot x^3 + (2^4 - 4 \cdot 2^3) \cdot x^4 + \cdots + (2^n - n \cdot 2^{n-1}) \cdot x^n + \cdots$

Réponses en notation sigma :

a) $\displaystyle\sum_{i=0}^{\infty} 5^i\, x^i$ **b)** $\displaystyle\sum_{i=0}^{\infty} \left(-\frac{3}{5}\right) \cdot \left(\frac{1}{5}\right)^i \cdot x^i$ **c)** $\displaystyle\sum_{i=0}^{\infty} \left[2^i - i \cdot 2^{i-1}\right] \cdot x^i$

Exercice 4 : Pour chacune des suites définies par récurrence suivantes, résolvez la récurrence par la méthode des séries génératrices.

a) $\begin{cases} a_0 &= 2 \\ a_n &= 3a_{n-1} + 2^n \quad \forall n \in \mathbb{N}^* \end{cases}$

Solution :

Étape 1 : (on exprime la série génératrice sous la forme d'une fonction rationnelle)

- On remarque que : $a_n \; - \; 3 \cdot a_{n-1} - (2^n) \; = \; 0 \quad \forall n \in \mathbb{N}^*$;
- ce qui en extension donne :
$$\begin{aligned} a_1 - 3 \cdot a_0 - 2 &= 0 \\ a_2 - 3 \cdot a_1 - 2^2 &= 0 \\ a_3 - 3 \cdot a_2 - 2^3 &= 0 \\ a_4 - 3 \cdot a_3 - 2^4 &= 0 \\ &\text{etc...} \end{aligned}$$
- Posons $G(x) \; = \; a_0 \; + \; a_1\, x \; + \; a_2\, x^2 \; + \; a_3\, x^3 \; + \; \cdots \; + \; a_n\, x^n \; + \; \cdots$.

Alors,

$$\begin{array}{rcccccccccc} G(x) &=& a_0 &+& a_1x + & a_2x^2 + & a_3x^3 + \cdots + & a_nx^n + \cdots & & \\ -3x \cdot G(x) &=& & + & -3 \cdot a_0x + & -3 \cdot a_1x^2 + & -3 \cdot a_2x^3 + \cdots + & -3 \cdot a_{n-1}x^n + \cdots & & \\ -\frac{1}{1-2x} &=& -1 &+& -2x + & -(2^2)x^2 + & -(2^3)x^3 + \cdots + & -(2^n)x^n + \cdots & & (\bigstar) \\ \hline G(x) - 3xG(x) - \frac{1}{1-2x} &=& a_0 - 1 + & & 0x + & 0x^2 + & 0x^3 + \cdots + & 0x^n + \cdots & & \end{array}$$

$\langle$ *La ligne* $(\bigstar)$ *est obtenue par le théorème 2.5.1-a, avec* $[a := -1]$ *et* $[b := 2]$ $\rangle$

Ce qui donne $G(x) - 3x\, G(x) - \frac{1}{1-2x} \; = \; 1$ $\quad\quad$ $\langle$ *Car* $\quad a_0 - 1 \; = \; 2 - 1 \; = \; 1.$ $\rangle$

Donc, on a $\quad G(x)(1 - 3x) \; = \; 1 + \frac{1}{1-2x}$

Donc, on a $\quad G(x)(1 - 3x) \; = \; \frac{1-2x+1}{1-2x}$

Donc, on a $\quad G(x)(1 - 3x) \; = \; \frac{2-2x}{1-2x}$

Donc, on a $\quad G(x) \; = \; \frac{2-2x}{(1-3x)(1-2x)}$

Donc, on a $\quad G(x) \; = \; \frac{-2x+2}{(1-3x)(1-2x)}$,

Étape 2 : (on trouve la série de puissances associée à G)

$$\begin{aligned} G(x) &= \frac{A}{1-3x} + \frac{B}{1-2x} && \langle \textit{ Théorème 2.5.3-a } \rangle \\ &= \sum_{i=0}^{\infty} A \cdot 3^i\, x^i \;+\; \sum_{i=0}^{\infty} B \cdot 2^i\, x^i && \langle \textit{ Théorème 2.5.1-a (2 fois) } \rangle \\ &= \sum_{i=0}^{\infty} \left[A \cdot 3^i + B \cdot 2^i \right] x^i && \langle \textit{ Arithmétique } \rangle \end{aligned}$$

Étape 3 : (on trouve le terme général de la suite)

Le terme général de la suite $\langle a_n \rangle_{n\in\mathbb{N}}$ est donné par : $a_n \;=\; A \cdot 3^n + B \cdot 2^n$.
Par la définition de la récurrence, nous savons que $a_0 = 2$ et $a_1 = 3 \cdot a_0 + 2^1 = 8$.
Donc :

$$\begin{aligned} & a_0 \;=\; 3^0\, A + 2^0\, B \;=\; A + B \;=\; 2 \\ \Leftrightarrow\; & B \;=\; 2 - A\,, && (*) \\ & a_1 \;=\; 3^1\, A + 2^1\, B \;=\; 3\,A + 2\,B \;=\; 8 \\ \Leftrightarrow\; & 3\,A \;=\; 8 - 2\,B\,, && (**) \\ & 3\,A \;=\; 8 - 2\,(2 - A) \;=\; 4 + 2\,A && \langle \textit{ Substitutions de (*) dans (**) } \rangle \\ \Leftrightarrow\; & A \;=\; 4\,, && (***) \\ & B \;=\; 2 - 4 \;=\; -2\,. && \langle \textit{ Substitutions de (***) dans (*) } \rangle \end{aligned}$$

Avec ces valeurs de A et B, on obtient le terme général suivant :

$$\begin{aligned} a_n &= 4 \cdot 3^n + (-2) \cdot 2^n \\ &= 4 \cdot 3^n - 2^{n+1}. \end{aligned}$$

Réponse : La définition par terme général est $\quad a_n \;=\; 4 \cdot 3^n \;-\; 2^{n+1} \quad \forall n \in \mathbb{N}$.

b) $\begin{cases} b_0 &= 0 \\ b_n &= b_{n-1} + n \quad \forall n \in \mathbb{N}^* \end{cases}$

Solution :

Étape 1 : (on exprime la série génératrice sous la forme d'une fonction rationnelle)

- On remarque que : $b_n \;-\; b_{n-1} - n \;=\; 0 \quad \forall n \in \mathbb{N}^*$;

- ce qui en extension donne :
$$\begin{aligned} b_1 - b_0 - 1 &= 0 \\ b_2 - b_1 - 2 &= 0 \\ b_3 - b_2 - 3 &= 0 \\ b_4 - b_3 - 4 &= 0 \\ &\text{etc...} \end{aligned}$$

- Posons $G(x) = b_0 + b_1\,x + b_2\,x^2 + b_3\,x^3 + \cdots + b_n\,x^n + \cdots$.

Alors,

$$\begin{array}{rcccccccccc} G(x) & = & b_0 + & b_1\,x + & b_2\,x^2 + & b_3\,x^3 + \cdots + & b_n\,x^n + \cdots & & \\ -x\cdot G(x) & = & + & -b_0\,x + & -b_1\,x^2 + & -b_2\,x^3 + \cdots + & -b_{n-1}\,x^n + \cdots & & \\ -\frac{x}{(1-x)^2} & = & 0 + & (-1)\cdot x + & (-2)\cdot x^2 + & (-3)\cdot x^3 + \cdots + & (-n)\cdot x^n + \cdots & & (\bigstar) \\ \hline G(x) - xG(x) - \frac{x}{(1-x)^2} & = & b_0 + & 0x + & 0x^2 + & 0x^3 + \cdots + & 0x^n + \cdots & & \end{array}$$

⟨ *La ligne* (★) *est obtenue par le corollaire 2.5.2-d* ⟩

Ce qui donne $G(x) - x\,G(x) - \dfrac{x}{(1-x)^2} = 0$ ⟨ *Car* $b_0 = 0$. ⟩

Donc, on a $G(x)(1-x) = \dfrac{x}{(1-x)^2}$

Donc, on a $G(x) = \dfrac{x}{(1-x)^3}$.

Étape 2 : (on trouve la série de puissances associée à G)

$$\begin{aligned} G(x) &= \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{(1-x)^3} && \langle\ \textit{Théorème 2.5.3-e}\ \rangle \\ &= \sum_{i=0}^{\infty} A\cdot x^i \ + \ \sum_{i=0}^{\infty}(i+1)B\cdot x^i \ + \ \sum_{i=0}^{\infty}\frac{(i+1)(i+2)}{2}\,C\cdot x^i && \langle\ \textit{Théorème 2.5.1-a,b,d}\ \rangle \\ &= \sum_{i=0}^{\infty}\left[A + (i+1)B + \frac{(i+1)(i+2)}{2}\,C\right]x^i && \langle\ \textit{Arithmétique}\ \rangle \end{aligned}$$

Étape 3 : (on trouve le terme général de la suite)

Le terme général de la suite $\langle b_n\rangle_{n\in\mathbb{N}}$ est donné par :

$$b_n = A + (n+1)B + \frac{(n+1)(n+2)}{2}\,C\,.$$

Par la définition de la récurrence, nous savons que $b_0 = 0$ et $b_1 = 1$ et $b_2 = 3$. Donc :

$$\begin{array}{rrcll}
 & 0 & = & A + B + C & \langle\ \textit{Car } b_0 = 0\ \rangle \\
\Leftrightarrow & A & = & -B - C\,, & (*) \\
 & 1 & = & A + 2\,B + 3\,C & \langle\ \textit{Car } b_1 = 1\ \rangle \\
 & & = & -B - C + 2\,B + 3\,C & \langle\ \textit{Par l'équation (*)}\ \rangle \\
\Leftrightarrow & B & = & 1 - 2\,C\,, & (**) \\
 & 3 & = & A + 3\,B + 6\,C & \langle\ \textit{Car } b_2 = 3\ \rangle \\
 & & = & -B - C + 3\,B + 6\,C & \langle\ \textit{Par l'équation (*)}\ \rangle \\
 & & = & 2\,B + 5\,C & \\
 & & = & 2\,(1 - 2\,C) + 5\,C & \langle\ \textit{Par l'équation (**)}\ \rangle \\
\Leftrightarrow & C & = & 1\,, & \\
 & B & = & 1 - 2 \cdot 1 \;=\; -1\,, & \langle\ \textit{Substitution de } C \textit{ dans (**)}\ \rangle \\
 & A & = & -(-1) - (1) \;=\; 0\,. & \langle\ \textit{Substitution de } B \textit{ et } C \textit{ dans (*)}\ \rangle
\end{array}$$

Avec ces valeurs de A et B, on obtient le terme général suivant :

$$\begin{aligned}
b_n &= -(n+1) + \frac{(n+1)(n+2)}{2} \\
&= \frac{(n+1)\cdot[\,-2 + (n+2)\,]}{2} \\
&= \frac{n\cdot(n+1)}{2}\,.
\end{aligned}$$

Réponse : La définition par terme général est $b_n = \dfrac{n\,(n+1)}{2} \quad \forall n \in \mathbb{N}$.

c) $\left\{\begin{array}{rcl} c_0 &=& 1 \\ c_1 &=& 8 \\ c_n &=& 6 \cdot c_{n-1} - 9 \cdot c_{n-2} + 2^n \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{array}\right.$

Solution :

Étape 1 : (on exprime la série génératrice sous la forme d'une fonction rationnelle)

- On remarque que : $c_n \;-\; 6 \cdot c_{n-1} + 9 \cdot c_{n-2} - 2^n \;=\; 0 \quad \forall n \in \mathbb{N} \setminus \{0,1\}$;

- ce qui en extension donne :
$$\begin{aligned} c_2 - 6\cdot c_1 + 9\cdot c_0 - 2^2 &= 0\\ c_3 - 6\cdot c_2 + 9\cdot c_1 - 2^3 &= 0\\ c_4 - 6\cdot c_3 + 9\cdot c_2 - 2^4 &= 0\\ c_5 - 6\cdot c_4 + 9\cdot c_3 - 2^5 &= 0\\ &\text{etc...} \end{aligned}$$

- Posons $G(x) \;=\; c_0 \,+\, c_1\,x \,+\, c_2\,x^2 \,+\, c_3\,x^3 \,+\, \cdots \,+\, c_n\,x^n \,+\, \cdots$.

Alors,

$$\begin{array}{rcccccccccc} G(x) &=& c_0 &+& c_1\,x &+& c_2\,x^2 &+& c_3\,x^3 + \cdots + & c_n\,x^n + \cdots \\ -6x\cdot G(x) &=& & + & -6\,c_0\,x &+& -6\,c_1\,x^2 &+& -6\,c_2\,x^3 + \cdots + & -6\,c_{n-1}\,x^n + \cdots \\ +9x^2\cdot G(x) &=& & & & + & 9\,c_0\,x^2 &+& 9\,c_1\,x^3 + \cdots + & 9\,c_{n-2}\,x^n + \cdots \\ -\frac{1}{1-2x} &=& -1 &+& -2x &+& -(2^2)x^2 &+& -(2^3)x^3 + \cdots + & -(2^n)x^n + \cdots \quad (\bigstar) \end{array}$$

$$\begin{array}{l} G(x) - 6xG(x) \\ \quad +9x^2G(x) - \frac{1}{(1-2x)} \end{array} \;=\; (c_0-1) + (c_1-6c_0-2)x \,+\, 0x^2 \,+\, 0x^3 + \cdots + 0x^n + \cdots$$

$\langle$ *La ligne* $(\bigstar)$ *est obtenue par le théorème 2.5.1-a, avec* $[a := -1]$ *et* $[b := 2]$ $\rangle$

Ce qui donne $G(x) - 6x\,G(x) + 9x^2\,G(x) - \frac{1}{(1-2x)} \;=\; 0$

$\langle$ *Car* $\quad c_0 - 1 \,=\, 1 - 1 = 0 \quad$ *et* $\quad c_1 - 6c_0 - 2 \,=\, 8 - 6\cdot 1 - 2 = 0.$ $\rangle$

Donc, on a $\quad G(x)(1 - 6x + 9x^2) \;=\; \frac{1}{(1-2x)}$

Donc, on a $\quad G(x)(1 - 3x)^2 \;=\; \frac{1}{(1-2x)}$

Donc, on a $\quad G(x) \;=\; \frac{1}{(1-3x)^2\,(1-2x)}$.

Étape 2 : (on trouve la série de puissances associée à G)

$$\begin{aligned} G(x) \;&=\; \frac{A}{1-3x} + \frac{B}{(1-3x)^2} + \frac{C}{(1-2x)} && \langle\ \textit{Théorème 2.5.3-d}\ \rangle\\ &=\; \sum_{i=0}^{\infty} A\,3^i\cdot x^i \;+\; \sum_{i=0}^{\infty}(i+1)\,B\,3^i\cdot x^i \;+\; \sum_{i=0}^{\infty} C\,2^i\cdot x^i && \langle\ \textit{Théorème 2.5.1-a,b}\ \rangle\\ &=\; \sum_{i=0}^{\infty}\Big[3^i\,A + 3^i(i+1)B + 2^i\,C\Big]\,x^i && \langle\ \textit{Arithmétique}\ \rangle \end{aligned}$$

Étape 3 : (on trouve le terme général de la suite)

Le terme général de la suite $\langle c_n\rangle_{n\in\mathbb{N}}$ est donné par :

$$c_n \;=\; 3^n\,A + 3^n(n+1)B + 2^n\,C\,.$$

Par la définition de la récurrence, nous savons que :
$c_0 = 1$ et $c_1 = 8$ et $c_2 = 6 \cdot 8 - 9 \cdot 1 + 2^2 = 43$.

Donc :

$$\begin{array}{rrcll}
 & 1 & = & A + B + C & \langle\ \textit{Car } c_0 = 1\ \rangle \\
\Leftrightarrow & A & = & 1 - B - C\,, & (*) \\
 & 8 & = & 3\,A + 6\,B + 2\,C & \langle\ \textit{Car } c_1 = 8\ \rangle \\
 & & = & 3(1 - B - C) + 6\,B + 2\,C & \langle\ \textit{Par l'équation (*)}\ \rangle \\
 & & = & 3 - 3\,B - C & \\
\Leftrightarrow & C & = & 3\,B - 5\,, & (**) \\
 & 43 & = & 9\,A + 27\,B + 4\,C & \langle\ \textit{Car } c_2 = 43\ \rangle \\
 & & = & 9\,(1 - B - C) + 27\,B + 4\,C & \langle\ \textit{Par l'équation (*)}\ \rangle \\
 & & = & 9 + 18\,B - 5\,C & \\
 & & = & 9 + 18\,B - 5\,(3\,B - 5) & \langle\ \textit{Par l'équation (**)}\ \rangle \\
 & & = & 34 + 3\,B & \\
\Leftrightarrow & 9 & = & 3\,B & \\
\Leftrightarrow & B & = & 3\,, & \\
 & C & = & 3 \cdot 3 - 5 \;=\; 4\,, & \langle\ \textit{Substitution de } B \textit{ dans (**)}\ \rangle \\
 & A & = & 1 - 3 - 4 \;=\; -6\,. & \langle\ \textit{Substitution de } B \textit{ et } C \textit{ dans (*)}\ \rangle
\end{array}$$

Avec ces valeurs de A et B, on obtient le terme général suivant :

$$\begin{array}{rcl}
c_n & = & (-6) \cdot 3^n + 3(n+1) \cdot 3^n + 4 \cdot 2^n \\
 & = & (-2) \cdot 3^{n+1} + (n+1) \cdot 3^{n+1} + 2^{n+2} \\
 & = & (n-1) \cdot 3^{n+1} + 2^{n+2}\,.
\end{array}$$

Réponse : La définition par terme général est :

$$c_n \;=\; (n-1) \cdot 3^{n+1} + 2^{n+2} \quad \forall n \in \mathbb{N}\,.$$

Exercice 5 : Trouvez le terme général de la suite suivante :

$$\begin{cases} d_0 &= 1 \\ d_1 &= 8 \\ d_n &= 6 \cdot d_{n-1} - 9 \cdot d_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0, 1\} \, . \end{cases}$$

Solution : (*Nous utilisons la méthode des récurrences linéaires homogènes*)

Nous allons appliquer le théorème 2.5.7.

Soit $p(x) = x^2 - 6x + 9$, le polynôme caractéristique de la suite $\langle d_n \rangle_{n \in \mathbb{N}}$.
Par la formule quadratique, on constate facilement que les zéros de du polynôme p sont $x_1 = 3$ et $x_2 = 3$.

Comme $x_1 = x_2$, on a donc, par le théorème 2.5.7, que le terme général de la suite $\langle d_n \rangle_{n \in \mathbb{N}}$ est de la forme

$$d_n = C_1 \cdot (3)^n + C_2 \cdot n \cdot (3)^n \qquad \forall n \in \mathbb{N}$$

où C_1 et C_2 sont deux constantes.

Déterminons les valeurs de ces deux constantes :

On sait que $d_0 = 1$ et $d_1 = 8$.

$$\begin{array}{lll} \text{Donc on a} & C_1 \cdot (3)^0 + C_2 \cdot 0 \cdot (3)^0 &= 1 \\ & C_1 \cdot (3)^1 + C_2 \cdot 1 \cdot (3)^1 &= 8 \end{array}$$

$$\begin{array}{lll} \text{Donc on a} & C_1 \cdot 1 + 0 &= 1 \\ & C_1 \cdot (3) + C_2 \cdot 1 \cdot (3) &= 8 \end{array}$$

$$\begin{array}{lll} \text{Donc on a} & C_1 &= 1 \\ & 3 \cdot C_1 + C_2 \cdot 1 \cdot 3 &= 8 \end{array}$$

$$\begin{array}{lll} \text{Donc} & C_1 &= 1 \\ & C_2 &= \frac{8 - 3 \cdot C_1}{3} \end{array}$$

$$\begin{array}{lll} \text{Donc} & C_1 &= 1 \\ & C_2 &= \frac{5}{3} \end{array}$$

Réponse : Le terme général de la suite $\langle d_n \rangle_{n \in \mathbb{N}}$ est

$$d_n = 3^n + 5n \cdot 3^{n-1} \qquad \forall n \in \mathbb{N}$$

Exercice 6 : En utilisant le théorème sur les récurrences linéaires homogènes d'ordre 2, exprimez les suites suivantes sous forme de fonctions rationnelles :

a) $\begin{cases} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$ *b)* $\begin{cases} b_0 &= 2 \\ b_1 &= 6 \\ b_n &= b_{n-1} + b_{n-2} \quad \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

c) $\begin{cases} c_0 &= 1 \\ c_1 &= 4 \\ c_n &= 4 \cdot c_{n-1} - 4 \cdot c_{n-2} \ \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$ *d)* $\begin{cases} d_0 &= 1 \\ d_1 &= 1 \\ d_n &= 4 \cdot d_{n-1} - 4 \cdot d_{n-2} \ \forall n \in \mathbb{N} \setminus \{0,1\} \end{cases}$

Réponses :

a) $f_n = \dfrac{1}{\sqrt{5}} \left(\dfrac{1+\sqrt{5}}{2} \right)^n - \dfrac{1}{\sqrt{5}} \left(\dfrac{1-\sqrt{5}}{2} \right)^n \quad \forall n \in \mathbb{N}$

b) $b_n = (1+\sqrt{5}) \left(\dfrac{1+\sqrt{5}}{2} \right)^n + (1-\sqrt{5}) \left(\dfrac{1-\sqrt{5}}{2} \right)^n \quad \forall n \in \mathbb{N}$

c) $c_n = 2^n \cdot (n+1) \quad \forall n \in \mathbb{N}$

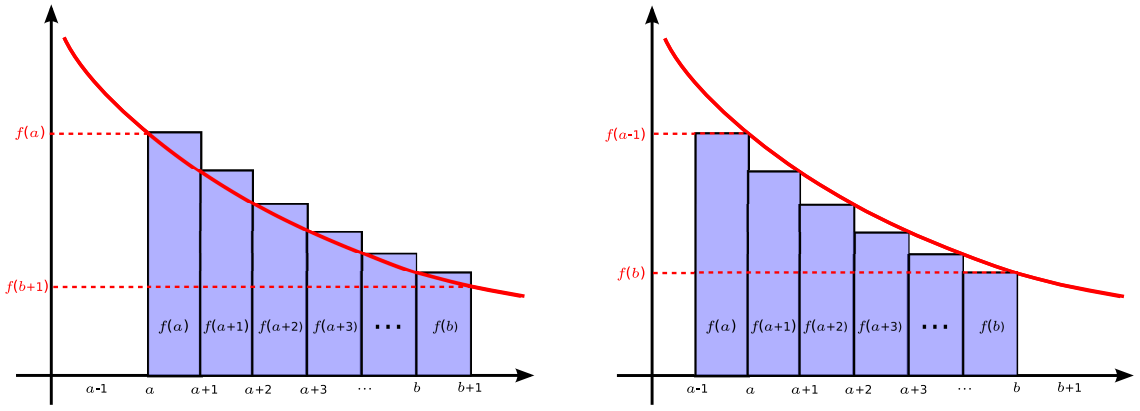
d) $d_n = 2^{n-1} \cdot (2-n) \quad \forall n \in \mathbb{N}$

Section 2.6.4 – Exercices sur l'approximation par une intégrale

Exercice 1 : En vous inspirant de la figure 2.3 (page 215), illustrez le théorème 2.6.2-b qui permet de borner une somme possédant la forme suivante :

$$\sum_{i=a}^{b} f(i), \quad \text{où } f \text{ est une fonction } \textit{non croissante} \text{ sur l'intervalle } [a-1, b+1]\,.$$

Solution :



(a) Borne inférieure de la somme.

(b) Borne supérieure de la somme.

Exercice 2 : En appliquant la méthode d'approximation par une intégrale, trouvez une borne inférieure et une borne supérieure des suites suivantes.

a) $a_n = 5 \cdot \sum_{i=1}^{n} i^4 \quad \forall n \in \mathbb{N}^*\,.$

Solution : Considérons la fonction $f(x) = x^4$. Cette fonction est non décroissante sur l'intervalle $[0, n+1]$ pour tout $n \geq 1$. Calculons l'intégrale selon la variable x de la fonction $f(x)$:

$$\int x^4 \cdot dx = \frac{x^5}{5} + C\,.$$

En appliquant le théorème 2.6.2-a, nous obtenons :

$$\begin{array}{rcccccl} & \left[\frac{x^5}{5}\right]_0^n & \leq & \sum_{i=1}^{n} i^4 & \leq & \left[\frac{x^5}{5}\right]_1^{n+1} \\ \Leftrightarrow & \frac{n^5}{5} - \frac{0^5}{5} & \leq & \sum_{i=1}^{n} i^4 & \leq & \frac{(n+1)^5}{5} - \frac{1^5}{5} \\ \Leftrightarrow & \frac{n^5}{5} & \leq & \sum_{i=1}^{n} i^4 & \leq & \frac{(n+1)^5 - 1}{5} \\ \Leftrightarrow & n^5 & \leq & 5 \cdot \sum_{i=1}^{n} i^4 & \leq & (n+1)^5 - 1 \end{array}$$

Ainsi, $\quad n^5 \;\leq\; a_n \;\leq\; (n+1)^5 - 1 \quad \forall n \in \mathbb{N}^*$.

b) $\; b_n \;=\; 5 \cdot \sum_{i=-2}^{n} i^4 \quad \forall n \in \mathbb{N}^*$.

Solution : La fonction $f(x) = x^4$ est décroissante pour $x \leq 0$ et croissante pour $x \geq 0$. Pour pouvoir appliquer l'approximation par une intégrale, réécrivons b_n ainsi :

$$b_n \;=\; 5 \cdot \left[(-2)^4 + (-1)^4 + 0^4 + \sum_{i=1}^{n} i^4\right] \;=\; 85 + 5 \cdot \sum_{i=1}^{n} i^4 \;=\; 85 + a_n\,,$$

où a_n est correspond au $n$ième terme de la suite définie à l'exercice précédent. Nous pouvons donc réutiliser directement le résultat de l'exercice précédent :

$$85 + n^5 \;\leq\; b_n \;\leq\; 84 + (n+1)^5 \quad \forall n \in \mathbb{N}^*\,.$$

c) $\; c_n \;=\; \sum_{i=1}^{n} i^k \quad \forall n \in \mathbb{N}^*$ (où $k \in \mathbb{N}^*$ est une constante).

Solution : Considérons la fonction $f(x) = x^k$. Cette fonction est non décroissante sur l'intervalle $[0, n+1]$ pour tout $n \geq 1$, peu importe la valeur de la constante $k \in \mathbb{N}^*$. L'intégrale de $f(x)$ selon la variable x est :

$$\int x^k \cdot dx \;=\; \frac{x^{k+1}}{k+1} + C\,.$$

En appliquant le théorème 2.6.2-a, nous obtenons :

$$\begin{array}{rcccl} & \left[\dfrac{x^{k+1}}{k+1}\right]_0^n & \leq & \displaystyle\sum_{i=1}^{n} i^k & \leq & \left[\dfrac{x^{k+1}}{k+1}\right]_1^{n+1} \\ \Leftrightarrow & \dfrac{n^{k+1}}{k+1} - \dfrac{0^{k+1}}{k+1} & \leq & \displaystyle\sum_{i=1}^{n} i^k & \leq & \dfrac{(n+1)^{k+1}}{k+1} - \dfrac{1^{k+1}}{k+1} \\ \Leftrightarrow & \dfrac{n^{k+1}}{k+1} & \leq & \displaystyle\sum_{i=1}^{n} i^k & \leq & \dfrac{(n+1)^{k+1}-1}{k+1} \end{array}$$

Ainsi, $\dfrac{n^{k+1}}{k+1} \leq c_n \leq \dfrac{(n+1)^{k+1}-1}{k+1} \quad \forall n, k \in \mathbb{N}^*$.

d) $d_n = \displaystyle\sum_{i=1}^{n} \frac{1}{i^2} \quad \forall n \in \mathbb{N}^*$..

Solution : Réécrivons d'abord d_n ainsi : $d_n = 1 + \displaystyle\sum_{i=2}^{n} \frac{1}{i^2} \quad \forall n \in \mathbb{N}^*$.

Considérons la fonction $f(x) = \dfrac{1}{x^2}$, qui est non croissante sur l'intervalle $[1, n+1]$ pour tout $n \geq 1$. L'intégrale de $f(x)$ selon la variable x est :

$$\int \frac{1}{x^2} \cdot dx = \int x^{-2} \cdot dx = \frac{x^{-1}}{-1} + C = -\frac{1}{x} + C\,.$$

En appliquant le théorème 2.6.2-b, nous obtenons :

$$\begin{array}{rcccl} & 1 + \left[-\dfrac{1}{x}\right]_2^{n+1} & \leq & 1 + \displaystyle\sum_{i=2}^{n} \frac{1}{i^2} & \leq & 1 + \left[-\dfrac{1}{x}\right]_1^{n} \\ \Leftrightarrow & 1 - \dfrac{1}{n+1} + \dfrac{1}{2} & \leq & 1 + \displaystyle\sum_{i=2}^{n} \frac{1}{i^2} & \leq & 1 - \dfrac{1}{n} + \dfrac{1}{1}\,. \end{array}$$

Ainsi, $\dfrac{3}{2} - \dfrac{1}{n+1} \leq d_n \leq 2 - \dfrac{1}{n} \quad \forall n \in \mathbb{N}^*$.

e) $e_n = \displaystyle\sum_{i=1}^{n} (i + \ln i - 1) \quad \forall n \in \mathbb{N}^*$.

Solution : Récrivons e_n ainsi :

$$e_n = 1 + \ln 1 - 1 + \sum_{i=2}^{n} (i + \ln i - 1) = \sum_{i=2}^{n} (i + \ln i - 1) \quad \forall n \in \mathbb{N}^*\,.$$

Considérons la fonction $f(x) = x + \ln x - 1$, qui est non décroissante sur l'intervalle

$[1, n+1]$ pour tout $n \geq 1$. L'intégrale de $f(x)$ selon la variable x est :

$$\int (x + \ln x - 1) \cdot dx \;=\; \int x \cdot dx + \int \ln x \cdot dx - \int 1 \cdot dx \;=\; \frac{x^2}{2} + x \cdot \ln x - 2x + C\,.$$

En appliquant le théorème 2.6.2-a, nous obtenons :

$$\begin{array}{rcccl} & \left[\frac{x^2}{2} + x \cdot \ln x - 2x\right]_1^n & \leq & \sum_{i=2}^{n} (i + \ln i - 1) & \leq \left[\frac{x^2}{2} + x \cdot \ln x - 2x\right]_2^{n+1} \\ \Leftrightarrow & \frac{n^2}{2} + n \cdot \ln n - 2n + \frac{3}{2} & \leq & \sum_{i=2}^{n} (i + \ln i - 1) & \leq \frac{(n+1)^2}{2} + (n+1) \cdot \ln(n+1) - 2(n + \ln 2) \end{array}$$

Ainsi, $\quad \frac{n^2 - 4n + 3}{2} + n \cdot \ln n \;\leq\; e_n \;\leq \frac{n^2 - 2n + 1}{2} + (n+1) \cdot \ln(n+1) - 2 \ln 2 \quad \forall n \in \mathbb{N}^*\,.$

f) $f_n \;=\; \log(n!) \quad \forall n \in \mathbb{N}^*\,.$
Rappels : $n! \stackrel{\text{def}}{=} 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ et $\log(a \cdot b) = \log a + \log b \;\; \forall a, b > 0$
Solution : Récrivons f_n ainsi :

$$f_n \;=\; \sum_{i=1}^{n} \log(i) \;=\; \log(1) + \sum_{i=2}^{n} \log(i) \;=\; \sum_{i=2}^{n} \log(n) \quad \forall n \in \mathbb{N}^*\,.$$

Considérons la fonction $g(x) = \log(x)$, qui est non décroissante sur l'intervalle $[1, n+1]$ pour tout $n \geq 1$. L'intégrale de $g(x)$ selon la variable x est :

$$\int \log(x) \cdot dx \;=\; x \log(x) - \frac{x}{\ln(10)}\,.$$

En appliquant le théorème 2.6.2-a, nous obtenons :

$$\begin{array}{rcccl} & \left[x \log(x) - \frac{x}{\ln(10)}\right]_1^n & \leq & f_n & \leq \left[n \log(n) - \frac{n}{\ln(10)}\right]_2^{n+1} \\ \Leftrightarrow & n \log(n) - \frac{n}{\ln(10)} + \frac{1}{\ln(10)} & \leq & f_n & \leq (n+1) \log(n+1) - \frac{n+1}{\ln(10)} - 2 \log(2) + \frac{2}{\ln(10)} \end{array}$$

Donc, $\quad n \log(n) - \frac{n-1}{\ln(10)} \;\leq\; f_n \;\leq\; (n+1) \log(n+1) - \log(4) - \frac{n-1}{\ln(10)} \quad \forall n \in \mathbb{N}^*\,.$

Exercice 3 : Décrivez une circonstance où la méthode d'approximation par une intégrale donne la valeur exacte de la somme. Autrement dit, exprimez une fonction f pour laquelle les bornes inférieure et supérieure obtenues par le théorème 2.6.2 sont égales à la valeur de la somme.

Solution : Lorsque la fonction f est constante.

En effet, considérons une constante $k \in \mathbb{R}$ et une fonction $f(x) = k$. On veut calculer :

$$\sum_{i=a}^{b} f(i)\,.$$

On constate que f est non décroissant pour n'importe quel intervalle $[a-1, b+1]$. Ainsi, par le théorème 2.6.2-a, on obtient :

$$\begin{aligned}
& \int_{a-1}^{b} k \cdot dx \;\leq\; \sum_{i=a}^{b} k \;\leq\; \int_{a}^{b+1} k \cdot dx \\
\Leftrightarrow \quad & [k \cdot x]_{a-1}^{b} \;\leq\; \sum_{i=a}^{b} k \;\leq\; [k \cdot x]_{a}^{b+1} \\
\Leftrightarrow \quad & k \cdot b - k \cdot (a-1) \;\leq\; \sum_{i=a}^{b} k \;\leq\; k \cdot (b+1) - k \cdot a \\
\Leftrightarrow \quad & k \cdot (b-a+1) \;\leq\; \sum_{i=a}^{b} k \;\leq\; k \cdot (b-a+1)
\end{aligned}$$

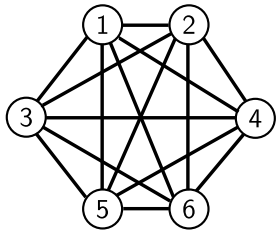
Ainsi, on conclut que : $\displaystyle\sum_{i=a}^{b} f(i) \;=\; k \cdot (b-a+1)\,.$

Section 3.1.8 – Exercices sur les éléments de base de la théorie des graphes

Exercice 1 : Six équipes sont inscrites à un tournoi de Hockey de garage. Dans la première phase du tournoi, chaque équipe doit affronter toutes les autres une et une seule fois.

a) Construisez un graphe représentant toutes les parties possibles.

Solution : Dans le graphe suivant, chaque équipe est représentée par un sommet et une partie entre l'équipe x et y est représentée par une arête $[x, y]$.



b) Quel type de graphe obtenez-vous ?

Solution : Il s'agit du graphe complet à 6 sommets, noté K_6.

c) Combien de parties comporte la première phase du tournoi ?

Solution : Pour connaître le nombre de parties, on compte le nombre d'arêtes. Un peu plus loin dans les notes, le théorème 3.3.1 (voir page 236) nous permettra de calculer directement le nombre d'arêtes d'un graphe complet :

$$|E(K_6)| \;=\; \frac{6 \cdot (6-1)}{2} \;=\; 15\,.$$

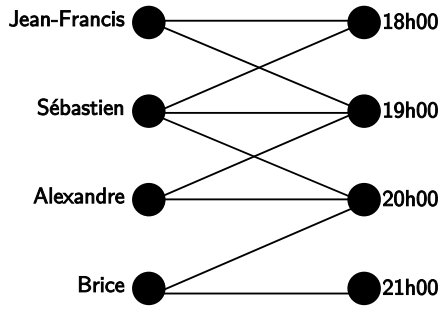
La première phase du tournoi comporte donc 15 parties.

Exercice 2 : Le représentant d'une compagnie de balayeuses centrales doit visiter quatre résidants d'un même immeuble en une même soirée. Chaque visite dure une heure et le représentant a suggéré aux résidents quatre plages horaires : 18h00, 19h00, 20h00 et 21h00. Voici les disponibilités des résidents :

Résident	18h00	19h00	20h00	21h00
Sébastien	✓	✓	✓	
Jean-Francis	✓	✓		
Brice			✓	✓
Alexandre		✓	✓	

a) Représentez cette situation par un graphe.

Solution :

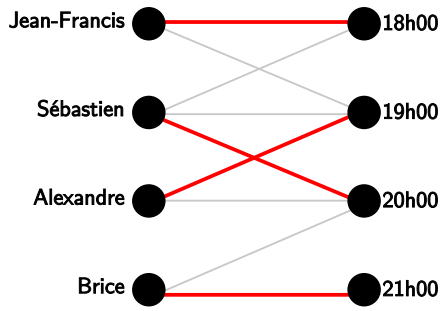


b) Quel type de graphe obtenez-vous ?

Solution : Il s'agit d'un graphe biparti.

c) Expliquez comment déduire du graphe un horaire possible pour le représentant (notez qu'on peut voir un horaire comme une fonction bijective entre l'ensemble des résidents et l'ensemble des plages horaires).

Solution : Il suffit de sélectionner quatre arêtes de telle sorte qu'aucune de ces quatre arêtes ne partage un même sommet. Le graphe suivant donne un exemple :



d) Donnez tous les horaires possibles pour ce problème.

Solution : Il y a trois horaires possibles :

(1) $\{\langle$Jean-Francis, 18h00$\rangle, \langle$Sébastien, 19h00$\rangle, \langle$Alexandre, 20h00$\rangle, \langle$Brice, 21h00$\rangle\}$

(2) $\{\langle$Jean-Francis, 18h00$\rangle, \langle$Sébastien, 20h00$\rangle, \langle$Alexandre, 19h00$\rangle, \langle$Brice, 21h00$\rangle\}$

(3) $\{\langle$Jean-Francis, 19h00$\rangle, \langle$Sébastien, 18h00$\rangle, \langle$Alexandre, 20h00$\rangle, \langle$Brice, 21h00$\rangle\}$

Exercice 3 :

a) Sept étudiants vont en vacances. Chacun va envoyer une carte postale à exactement trois des autres étudiants. Est-ce possible que pour chaque étudiant x, les étudiants qui écrivent à x soient exactement ceux à qui x a écrit ?

b) Qu'arrive-t-il si on remplace "trois" par un autre nombre entre 0 et 6 (inclusivement) à l'exercice précédent ?

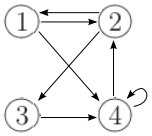
La solution à l'exercice 3 sera discutée en classe.

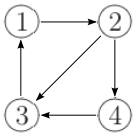
Exercice 4 : Considérons la matrice d'adjacence M_1 d'un digraphe G_1 et la matrice d'adjacence M_2 d'un digraphe G_2 :

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

a) Donnez une représentation graphique des digraphes G_1 et G_2.

Solution :





b) Calculez le produit matriciel suivant [9] : $M_3 = M_1 \times M_2$.

Réponse :

$$M_3 = \begin{pmatrix} 0 & 0 & 2 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix}$$

c) En examinant la matrice M_3 calculée précédemment, dites comment on peut interpréter le produit matriciel de deux matrices d'adjacence.

Solution : Le produit matriciel des matrices d'adjacence de deux graphes G_1 et G_2 correspond à la matrice d'adjacence de la composition $G_1 \circ G_2$ (voir la discussion à la fin de la section 3.2.1 pour plus de détails.)

9. Pour un rappel sur le produit matriciel, voir : http://fr.wikipedia.org/wiki/Produit_matriciel

Section 3.2.3 – Exercices sur les graphes en tant que relations

Exercice 1 : Considérez l'ensemble de sommets $S = \{1, 2, 3, 4\}$ et les deux digraphes suivants :

$$\begin{aligned} G &= \{\langle 2,3\rangle, \langle 3,3\rangle, \langle 4,3\rangle\} \subset S^2, \\ H &= \{\langle 1,2\rangle, \langle 2,4\rangle, \langle 3,1\rangle, \langle 4,3\rangle\} \subset S^2. \end{aligned}$$

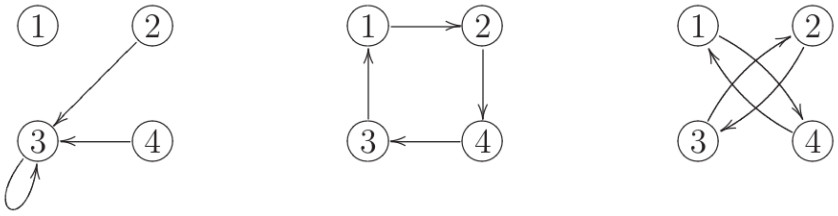
a) Calculez $G \cup H$, $G \cap H$, G^c, H^{-1}, $G \circ H$, G^2 et H^2.

Solution :

$$\begin{aligned} G \cup H &= \{\langle 2,3\rangle, \langle 3,3\rangle, \langle 4,3\rangle, \langle 1,2\rangle, \langle 2,4\rangle, \langle 3,1\rangle\} \\ G \cap H &= \{\langle 4,3\rangle\} \\ G^c &= \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,4\rangle, \\ &\quad \langle 3,1\rangle, \langle 3,2\rangle, \langle 3,4\rangle, \langle 4,1\rangle, \langle 4,2\rangle, \langle 4,4\rangle\} \\ H^{-1} &= \{\langle 2,1\rangle, \langle 4,2\rangle, \langle 1,3\rangle, \langle 3,4\rangle\} \\ G \circ H &= \{\langle 2,1\rangle, \langle 3,1\rangle, \langle 4,1\rangle\} \\ G^2 &= G \\ H^2 &= \{\langle 1,4\rangle, \langle 2,3\rangle, \langle 3,2\rangle, \langle 4,1\rangle\} \end{aligned}$$

b) Donnez la représentation graphique des digraphes G, H et H^2.

Solution :



c) Donnez la matrice d'adjacence des digraphes G, H et H^2.

Solution :

$$M_G = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad M_H = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad M_{H^2} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

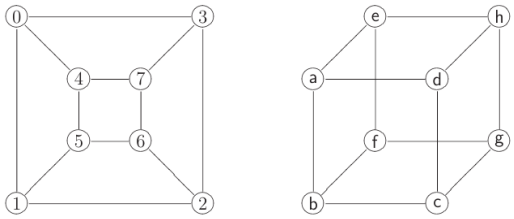
d) Dites lesquelles des propriétés suivantes les relations G et H possèdent :

réflexivité, irréflexivité, symétrie, antisymétrie, asymétrie, transitivité, équivalence, totalité, surjectivité, déterminisme, injectivité, fonction partielle, fonction, fonction bijective, ordre partiel, ordre partiel strict, ordre total.

Propriétés de G : antisymétrie, transitivité, déterminisme, fonction partielle.

Propriétés de H : irréflexivité, antisymétrie, asymétrie, totalité, surjectivité, déterminisme, injectivité, fonction, fonction bijective.

Exercice 2 : Montrez que les deux graphes suivants sont isomorphes.



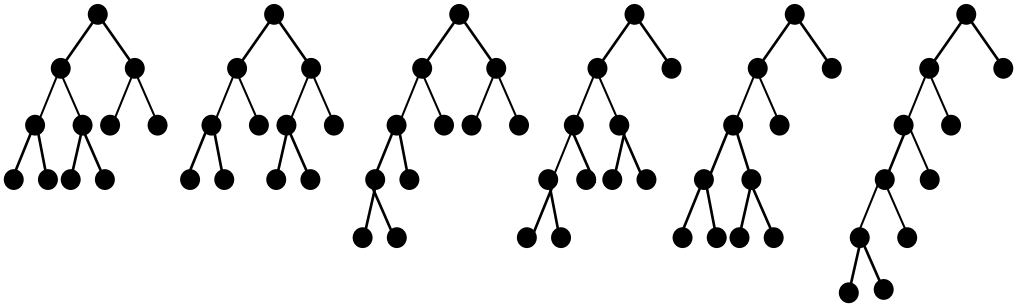
Solution : Désignons le graphe de gauche par G et le graphe de droite par D. Pour montrer que G et D sont isomorphes, construisons une fonction bijective $f : V(G) \longrightarrow V(D)$:

$$f \;=\; \{\, \langle 0, a\rangle\,, \langle 1, b\rangle\,, \langle 2, c\rangle\,, \langle 3, d\rangle\,, \langle 4, e\rangle\,, \langle 5, f\rangle\,, \langle 6, g\rangle\,, \langle 7, h\rangle\,\}\,.$$

Section 3.4.3 – Exercices sur les arbres

Exercice 1 : (*Aucune justification n'est demandée pour ce numéro.*)

a) Énumérez (à isomorphisme près) tous les arbres binaires ayant exactement 6 feuilles.
Solution : Il y a 6 arbres possibles :



b) Combien de sommets peut avoir un arbre binaire ayant exactement 6 feuilles.
Solution : 11 sommets.

c) Combien de sommets peut avoir un arbre binaire ayant exactement k feuilles (avec $k \geq 2$).

Solution : Considérons un arbre binaire T comportant n sommets, dont k feuilles.

1. Calculons d'abord la somme des degrés des sommets de T. Par la définition des arbres binaires (définition 3.1.14) on sait que T compte exactement k sommets de degré 1 (les feuilles), 1 sommet de degré 2 (la racine), et que les autres $(n-k-1)$ sommets sont de degré 3. Aussi, par le théorème 3.3.3, on sait que la somme des degrés de T est égale à deux fois le nombre d'arêtes. Donc :

$$|E(T)| \;=\; \frac{1\cdot k + 2\cdot 1 + 3\cdot(n-k-1)}{2} \;=\; \frac{3n-2k-1}{2}\,.$$

2. Par le théorème 3.4.2, puisque T est un arbre, on sait que $|V(T)| = |E(T)|+1$. Ainsi :

$$\begin{aligned} n &= \frac{3n-2k-1}{2}+1 = \frac{3n-2k+1}{2} \\ \Leftrightarrow \quad 2n &= 3n-2k+1 \\ \Leftrightarrow \quad n &= 2k-1\,. \end{aligned}$$

Exercice 2 : Définissons un *arbre trinaire* comme un arbre qui contient un sommet de degré 3 (la *racine*) et dont tous les autres sommets sont de degré 1 (les *feuilles*) ou de degré 4. Comme pour un arbre binaire, le *niveau* d'un sommet x d'un arbre trinaire équivaut à la longueur de l'unique chaîne allant de la racine au sommet x et la *hauteur* d'un arbre trinaire est égale au niveau maximal de ses feuilles. Finalement, un *arbre trinaire complet* est un arbre trinaire dont toutes les feuilles sont au même niveau.

a) Dessinez trois arbres : un arbre trinaire complet de hauteur 2, un arbre trinaire complet de hauteur 3 et un arbre trinaire complet de hauteur 4.

b) Donnez l'expression du nombre de feuilles d'un arbre trinaire complet en fonction de sa hauteur.

Solution : Considérons la suite $L(h)$ donnant le nombre de feuilles d'un arbre trinaire en fonction de sa hauteur $L(h)$. La suite se définit naturellement de façon récursive :

$$\begin{cases} L(0) &= 1 \\ L(h) &= 3 \cdot L(h-1) \quad \forall h \in \mathbb{N}^* \end{cases}$$

Par le théorème 2.4.4, on constate qu'il s'agit d'une somme géométrique de premier terme 1 et de raison 3. Le terme général est donc :

$$L(h) \;=\; 3^h \,.$$

c) Donnez l'expression du nombre de noeuds d'un arbre trinaire complet en fonction de sa hauteur. (Indice : Vous pouvez vous servir du résultat obtenu en (b) et des résultats présentés à la section 2.4.3 sur les *suites des sommes de premiers termes d'une suite*.)

Solution : Le nombre de noeuds $N(h)$ d'un arbre trinaire complet de hauteur h sera égale à la somme du nombre de feuilles des $h+1$ arbres trinaires complets de hauteur 0 à h. Ainsi :

$$N(h) \;=\; L(0) + L(1) + L(2) + \ldots + L(h) \;= \sum_{i=0}^{h} L(i) \,.$$

La suite $N(h)$ est donc la suite des sommes des premiers termes de la suite géométrique $L(h)$ définie en (b). Par le théorème 2.4.7, on obtient :

$$N(h) \;=\; \frac{1 \cdot (1 - 3^{h+1})}{1 - 3} \;=\; \frac{3^{h+1} - 1}{2} \,.$$

Exercice 3 : Un arbre est toujours un graphe biparti. Décrivez une méthode pour créer une bipartition à partir de n'importe quel arbre (Rappel : les concepts de *graphe biparti* et de *bipartition* ont été introduits par la définition 3.1.3-c).

Solution : Soit T un arbre non vide et $x \in V(T)$ un sommet quelconque de cet arbre. Voici comment on peut séparer les sommets de T en bipartition A et B :

$$\begin{aligned} A &= \{y \in V(T) \mid \text{La longueur de la chaîne élémentaire entre } x \text{ et } y \text{ est de longueur paire } \} \\ B &= \{y \in V(T) \mid \text{La longueur de la chaîne élémentaire entre } x \text{ et } y \text{ est de longueur impaire } \} \end{aligned}$$

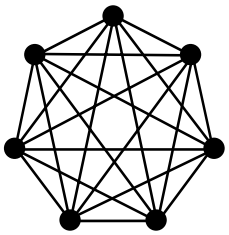
Notez qu'il y a toujours qu'une seule chaîne élémentaire entre x et y (voir le théorème 3.4.4-*3*).

Section 3.6.4 – Exercices sur les chaînes et chemins

Exercice 1 : Pour chacun des graphes ci-dessous, dites s'il s'agit d'un graphe

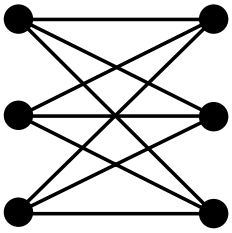
a) eulérien. Si oui, exhibez un cycle eulérien.

b) hamiltonien. Si oui, exhibez un cycle hamiltonien.

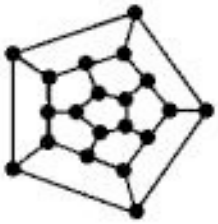


K_7

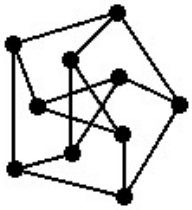
$K_{4,2}$



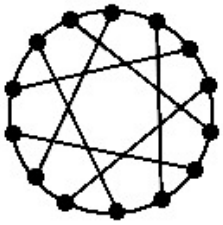
$K_{3,3}$



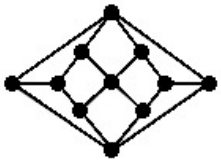
Le dodécaèdre



Le graphe de Petersen



Le graphe d'Heawood

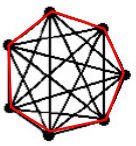


Le graphe d'Herschel

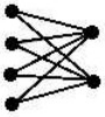
Solution :

a) Seuls les deux graphes K_7 et $K_{4,2}$ sont eulériens :

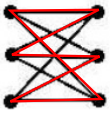
b) Les graphes K_7, $K_{3,3}$, le dodécaèdre et le graphe d'Heawood sont Hamiltoniens. Voici un cycle hamiltonien pour chacun d'eux :



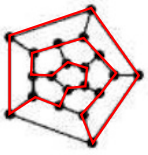
K_7



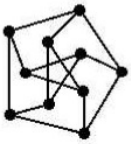
$K_{4,2}$



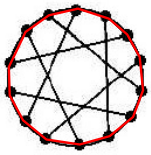
$K_{3,3}$



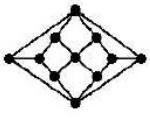
Le dodécaèdre



Le graphe de Petersen



Le graphe d'Heawood



Le graphe d'Herschel

Exercice 2 : On veut asseoir cinq couples autour d'une table ronde de telle sorte que pour chaque deux couples, au moins un des membres du premier couple soit assis à côté d'au moins un membre du deuxième couple. Est-ce possible ?

Solution : Oui ! Voici un raisonnement qui le montre :

1. On considère un graphe G où chaque sommet correspond à un couple (donc, $|V(G)| = 5$) et chaque arête $\langle x, y\rangle \in E(G)$ correspond à la relation "un des membres du couple x est assis à côté d'un des membres du couple y". Le graphe G comporte une arête entre chaque sommet. Il s'agit donc du graphe K_5, c'est-à-dire le graphe complet à 5 sommets.
2. Il y a une solution au problème si et seulement si il existe un cycle eulérien dans le graphe G.
3. Un tel cycle eulérien existe car aucun des sommets de G n'est de degré impair (théorème 3.6.5). Plus précisément, $\deg_G(x) = 4 \quad \forall x \in V(G)$.
4. De plus, il suffit de parcourir un cycle eulérien de G pour obtenir l'ordre dans lequel on peut asseoir les membres des couples autour de la table ronde pour satisfaire le problème.

Exercice 3 : L'algorithme de Dijkstra présenté à la page 252 retourne la longueur du plus court chemin entre le sommet d'origine et le sommet de destination z, mais ne permet pas de connaître la nature de ce chemin. Suggérez une modification à l'algorithme afin qu'il retourne le chemin le plus court (sous la forme, par exemple, d'une liste de sommets).

Solution : Dans le pseudo-code ci-dessous, le texte en rouge indique les lignes modifiées et/ou ajoutées par rapport à l'algorithme original. La fonction **fusionner** effectue la jonction entre deux listes, de telle sorte que : **fusionner**$(\,[u_0],[u_1,u_2,\ldots,u_n]\,) \stackrel{\text{def}}{=} [u_0,u_1,u_2,\ldots,u_n]\,.$

```
Algorithme_Dijkstra_Modifié ( Digraphe G, valeurs w, origine a, destination z )
  Initialiser :
  • Q ← V(G)                          ⟨ Pendant l'exécution, Q contient les sommets non visités ⟩
  • dist(v) ← ∞  ∀v ∈ Q \ {a}         ⟨ La distance de tous les sommets (sauf a) est inconnue ⟩
  • dist(a) ← 0                       ⟨ Le sommet source est à une distance nulle de lui-même ⟩

  Tant que |Q| > 0 Faire              ⟨ Tant qu'il reste des sommets à visiter... ⟩

      u ← Un élément de Q dont la valeur dist(u) est minimale
      Q ← Q \ {u}                     ⟨ On sélectionne le sommet u à visiter ⟩

      Si u = z alors
          chemin ← [u]                ⟨ Reconstruit le chemin en sens inverse ⟩
          Tant que u ≠ a Faire
              u ← prec(u)
              chemin ← fusionner( [u], chemin )
          Fin Tant que
          Retourner chemin
      Fin Si

      Pour tout v ∈ 𝒩(u) ∩ Q Faire    ⟨ Mise à jour de la distance des voisins de u ⟩
          Si dist(u) + w(⟨u,v⟩) < dist(v) alors
              dist(v) ← dist(u) + w(⟨u,v⟩)
              prec(v) ← u             ⟨ Le sommet u précède le sommet v ⟩
          Fin Si
      Fin Pour
  Fin Tant que
  Retourner [ ]                       ⟨ Aucun chemin trouvé (retourne une liste vide) ⟩
```

Définitions et théorèmes, chapitre 1

(ceci est une version complète, la version annexée à l'examen est plus loin)

Définition 1.1.1 Opérateurs booléens de base.

Négation :

p	$\neg p$
v	f
f	v

Conjonction :

p	q	$p \wedge q$
v	v	v
v	f	f
f	v	f
f	f	f

Disjonction :

p	q	$p \vee q$
v	v	v
v	f	v
f	v	v
f	f	f

Définition 1.1.2 Opérateur d'implication

$p \Rightarrow q \quad \stackrel{\text{def}}{=} \quad \neg p \vee q$

Définition 1.1.3 Opérateur si et seulement si.

$p \Leftrightarrow q \quad \stackrel{\text{def}}{=} \quad (p \Rightarrow q) \wedge (q \Rightarrow p)$

Proposition 1.1.4 Lois de De Morgan.

a : $\neg(p \wedge q) \quad \Leftrightarrow \quad \neg p \vee \neg q$ (1ière loi de De Morgan)

b : $\neg(p \vee q) \quad \Leftrightarrow \quad \neg p \wedge \neg q$ (2e loi de De Morgan)

Proposition 1.1.5 Propriétés de la négation.

a : $\neg(\neg p) \quad \Leftrightarrow \quad p$ (Double négation)

b : $p \vee \neg p \quad \Leftrightarrow \quad \texttt{vrai}$ (Tiers exclu)

c : $p \wedge \neg p \quad \Leftrightarrow \quad \texttt{faux}$ (Contradiction)

Proposition 1.1.6 Propriétés de la conjonction.

a : $p \wedge \texttt{vrai} \quad \Leftrightarrow \quad p$ (Él. neutre)

b : $p \wedge \texttt{faux} \quad \Leftrightarrow \quad \texttt{faux}$ (Él. absorbant)

c : $p \wedge p \quad \Leftrightarrow \quad p$ (Idempotence)

d : $p \wedge q \quad \Leftrightarrow \quad q \wedge p$ (Commutativité)

e : $(p \wedge q) \wedge r \quad \Leftrightarrow \quad p \wedge (q \wedge r)$ (Associativité)

f : $(p \vee q) \wedge r \quad \Leftrightarrow \quad (p \wedge r) \vee (q \wedge r)$ (Distributivité)

Proposition 1.1.7 Propriétés de la disjonction.

a : $p \vee \texttt{faux} \quad \Leftrightarrow \quad p$ (Él. neutre)

b : $p \vee \texttt{vrai} \quad \Leftrightarrow \quad \texttt{vrai}$ (Él. absorbant)

c : $p \vee p \quad \Leftrightarrow \quad p$ (Idempotence)

d : $p \vee q \quad \Leftrightarrow \quad q \vee p$ (Commutativité)

e : $(p \vee q) \vee r \quad \Leftrightarrow \quad p \vee (q \vee r)$ (Associativité)

f : $(p \wedge q) \vee r \quad \Leftrightarrow \quad (p \vee r) \wedge (q \vee r)$ (Distributivité)

Proposition 1.1.8 Transitivité du "si et seulement si"

$(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \quad \Rightarrow \quad (p \Leftrightarrow r)$

Proposition 1.1.9 Contraposition.

$p \Rightarrow q \quad \Leftrightarrow \quad \neg q \Rightarrow \neg p$

Proposition 1.1.10 Affaiblissement et renforcement.

a : $p \wedge q \quad \Rightarrow \quad p$ (Affaiblissement de la conjonction)

b : $p \quad \Rightarrow \quad p \vee q$ (Renfoncement de la disjonction)

Proposition 1.1.11 Réécriture du "si et seulement si"

$(p \Leftrightarrow q) \quad \Leftrightarrow \quad (p \wedge q) \vee (\neg p \wedge \neg q)$

Définition 1.2.1 Axiome d'extensionnalité

$S = T \stackrel{\text{def}}{=} (\forall e \mid e \in S \Leftrightarrow e \in T)$.

Définition 1.2.2 Notation abrégée des quantificateurs

a : $(\forall x \in T \mid P(x)) \stackrel{\text{def}}{=} (\forall x \mid x \in T \Rightarrow P(x))$

b : $(\exists x \in T \mid P(x)) \stackrel{\text{def}}{=} (\exists x \mid x \in T \wedge P(x))$

Proposition 1.2.3 Lois de De Morgan (Quantificateurs).

a : $\neg(\forall x \in T \mid P(x)) \quad \Leftrightarrow \quad (\exists x \in T \mid \neg P(x))$ (1ière loi)

b : $\neg(\exists x \in T \mid P(x)) \quad \Leftrightarrow \quad (\forall x \in T \mid \neg P(x))$ (2e loi)

Définition 1.2.4 Opérateurs de composition d'ensembles.

a : $S^c \stackrel{\text{def}}{=} \{e \mid e \notin S\}$ (Complément)

b : $S \cap T \stackrel{\text{def}}{=} \{e \mid e \in S \wedge e \in T\}$ (Intersection)

c : $S \cup T \stackrel{\text{def}}{=} \{e \mid e \in S \vee e \in T\}$ (Union)

d : $S \setminus T \stackrel{\text{def}}{=} \{e \mid e \in S \wedge e \notin T\}$ (Différence)

Définition 1.2.5 Opérateurs d'inclusions.

a : $T \subseteq S \stackrel{\text{def}}{=} (\forall e \mid e \in T \Rightarrow e \in S)$ (Incl.)

b : $T \subset S \stackrel{\text{def}}{=} T \subseteq S \wedge (\exists e \mid e \in S \wedge e \notin T)$ (Incl. stricte)

Définition 1.2.6 Ensemble puissance.

$\mathcal{P}(S) \stackrel{\text{def}}{=} \{E \mid E \subseteq S\}$.

Proposition 1.2.7 Lois de De Morgan (version ensembliste).

a : $(S \cap T)^c = S^c \cup T^c$ (Première loi de De Morgan)

b : $(S \cup T)^c = S^c \cap T^c$ (Deuxième loi de De Morgan)

Proposition 1.2.8 Propriétés du complément.

a : $(S^c)^c = S$ (Complémentarité)

b : $S \cup S^c = \mathbf{U}$ (Tiers exclu)

c : $S \cap S^c = \emptyset$ (Contradiction)

Proposition 1.2.9 Propriétés de l'intersection.

a : $S \cap \mathbf{U} = S$ (Él. neutre)

b : $S \cap \emptyset = \emptyset$ (Él. absorbant)

c : $S \cap S = S$ (Idempotence)

d : $S \cap T = T \cap S$ (Commutativité)

e : $(S \cap T) \cap U = S \cap (T \cap U)$ (Associativité)

f : $(S \cup T) \cap U = (S \cap U) \cup (T \cap U)$ (Distributivité)

Proposition 1.2.10 Propriétés de l'union.

a : $S \cup \emptyset = S$ (Él. neutre)

b : $S \cup \mathbf{U} = \mathbf{U}$ (Él. absorbant)

c : $S \cup S = S$ (Idempotence)

d : $S \cup T = T \cup S$ (Commutativité)

e : $(S \cup T) \cup U = S \cup (T \cup U)$ (Associativité)

f : $(S \cap T) \cup U = (S \cup U) \cap (T \cup U)$ (Distributivité)

Proposition 1.2.11 Propriétés de la différence.

a :	$S \setminus \emptyset$	$=$	S	(Élément neutre)
b :	$S \setminus T$	$=$	$S \cap T^c$	(Réécriture de "\")
c :	$S \cup (T \setminus S)$	$=$	$S \cup T$	(Union de "\")
d :	$S \cap (T \setminus S)$	$=$	$\emptyset$	(Intersection de "\")
e :	$S \setminus (T \cup U)$	$=$	$(S \setminus T) \cap (S \setminus U)$	(Différence de "∪")
f :	$S \setminus (T \cap U)$	$=$	$(S \setminus T) \cup (S \setminus U)$	(Différence de "∩")

Proposition 1.2.12 Appartenance d'un élément à un ensemble obtenu par composition.

a :	$e \in S^c$	$\Leftrightarrow$	$\neg(e \in S)$	(Complément)
b :	$e \in S \cap T$	$\Leftrightarrow$	$e \in S \wedge e \in T$	(Intersection)
c :	$e \in S \cup T$	$\Leftrightarrow$	$e \in S \vee e \in T$	(Union)
d :	$e \in S \setminus T$	$\Leftrightarrow$	$e \in S \wedge \neg(e \in T)$	(Différence)

Proposition 1.2.13 Propriétés d'équivalences de l'inclusion.

a :	$\emptyset \subseteq S$			(Omniprésence de "∅")
b :	$S \subseteq S$			(Réflexivité)
c :	$\neg(S \subset S)$			(Irréflexivité)
d :	$S = T$	$\Leftrightarrow$	$S \subseteq T \wedge T \subseteq S$	(Antisymétrie)
e :	$S \subseteq T$	$\Leftrightarrow$	$S \subset T \vee S = T$	(Réécriture de "⊆")
f :	$S \subset T$	$\Leftrightarrow$	$S \subseteq T \wedge T \neq S$	(Réécriture de "⊂")

Proposition 1.2.14 Propriétés d'implications de l'inclusion.

a :	$S \subset T$	$\Rightarrow$	$S \subseteq T$	
b :	$S \subset T$	$\Rightarrow$	$T \not\subseteq S$	
c :	$S \subset T$	$\Rightarrow$	$T \not\subset S$	
d :	$S \subset T \wedge U \not\subseteq T$	$\Rightarrow$	$U \not\subseteq S$	
e :	$S \subseteq T \wedge T \subseteq U$	$\Rightarrow$	$S \subseteq U$	(Transitivité (1))
f :	$S \subseteq T \wedge T \subset U$	$\Rightarrow$	$S \subset U$	(Transitivité (2))
g :	$S \subset T \wedge T \subseteq U$	$\Rightarrow$	$S \subset U$	(Transitivité (3))
h :	$S \subset T \wedge T \subset U$	$\Rightarrow$	$S \subset U$	(Transitivité (4))

Définition 1.4.1 Produit cartésien de deux ensembles

$S \times T \stackrel{\text{def}}{=} \{\langle a, b\rangle \mid a \in S \wedge b \in T\}$.

Définition 1.4.2 Produit cartésien de n ensembles

- $S_1 \times S_2 \times \ldots \times S_n \stackrel{\text{def}}{=} \{\langle e_1, e_2, \ldots, e_n\rangle \mid e_1 \in S_1 \wedge e_2 \in S_2 \wedge \ldots \wedge e_n \in S_n\}$.
- $S^n \stackrel{\text{def}}{=} S \times S \times \ldots \times S$ (n fois) .

Proposition 1.4.3 Propriétés du produit cartésien

a :	$S \times T = T \times S$	$\Leftrightarrow$	$S = \emptyset \vee T = \emptyset \vee S = T$	
b :	$S \times (T \cup U)$	$=$	$(S \times T) \cup (S \times U)$	(Dist. sur "∪")
c :	$S \times (T \cap U)$	$=$	$(S \times T) \cap (S \times U)$	(Dist. sur "∩")
d :	$S \times (T \setminus U)$	$=$	$(S \times T) \setminus (S \times U)$	(Dist. sur "\")
e :	$S \subseteq U \wedge T \subseteq V$	$\Rightarrow$	$S \times T \subseteq U \times V$	
f :	$S \times T \subseteq S \times U$	$\Rightarrow$	$S = \emptyset \vee T \subseteq U$	
g :	$(S \cap T) \times (U \cap V)$	$=$	$(S \times U) \cap (T \times V)$	
h :	$\lvert S \times T\rvert$	$=$	$\lvert S\rvert \cdot \lvert T\rvert$	si S et T sont finis.

Définition 1.4.4 Appartenance d'un couple à une relation

$a \ \rho \ b \stackrel{\text{def}}{=} \langle a, b\rangle \in \rho$.

Définition 1.4.5 Domaine et image d'une relation

a :	$\mathrm{Dom}(\rho)$	$\stackrel{\text{def}}{=}$	$\{a \in S \mid (\exists b \in T \mid a \ \rho \ b)\}$	(Domaine)
b :	$\mathrm{Im}(\rho)$	$\stackrel{\text{def}}{=}$	$\{b \in T \mid (\exists a \in S \mid a \ \rho \ b)\}$	(Image)

Définition 1.4.6 Relation identité

$\mathbf{I}_S \stackrel{\text{def}}{=} \{\langle a, a\rangle \in S^2 \mid a \in S\}$,

De manière équivalente : $\langle a, a\rangle \in \mathbf{I}_S \ \Leftrightarrow \ a \in S$.

Définition 1.4.7 Composition de deux relations

$\rho \circ \sigma \stackrel{\text{def}}{=} \{\langle a, c\rangle \mid (\exists b \mid \langle a, b\rangle \in \rho \wedge \langle b, c\rangle \in \sigma)\}$

Proposition 1.4.8 Propriétés de la composition

a :	$\mathbf{I}_S \circ \rho$	$=$	$\rho \circ \mathbf{I}_T$	$=$	ρ	(Él. neutre)
b :	$\emptyset \circ \rho$	$=$	$\rho \circ \emptyset$	$=$	$\emptyset$	(Él. absorbant)
c :	$(\rho \circ \sigma) \circ \theta$			$=$	$\rho \circ (\sigma \circ \theta)$	(Associativité)
d :	$\rho \subseteq \sigma$			$\Rightarrow$	$\rho \circ \theta \subseteq \sigma \circ \theta$	(Monotonie)

Définition 1.4.9 Puissance d'une relation

Si $n \geq 1$: $\rho^n \stackrel{\text{def}}{=} \rho \circ \rho \circ \ldots \circ \rho$ (n fois),

sinon ($n = 0$) : $\rho^0 \stackrel{\text{def}}{=} \mathbf{I}_S$.

Proposition 1.4.10 Propriétés de l'opérateur puissance

a :	$\rho^m \circ \rho^n$	$=$	ρ^{m+n}	(Somme des exposants)
b :	$(\rho^m)^n$	$=$	$\rho^{m \cdot n}$	(Produit des exposants)

Définition 1.4.11 Clôtures d'une relation

a :	ρ^+	$\stackrel{\text{def}}{=}$	$\rho^1 \cup \rho^2 \cup \rho^3 \cup \ldots$	(Clôture transitive)
b :	ρ^*	$\stackrel{\text{def}}{=}$	$\rho^0 \cup \rho^1 \cup \rho^2 \cup \rho^3 \cup \ldots$	(Cl. transitive et réflexive)

Définition 1.4.12 Inverse d'une relation

$\rho^{-1} \stackrel{\text{def}}{=} \{\langle b, a\rangle \mid \langle a, b\rangle \in \rho\}$.

Proposition 1.4.13 Propriétés de la relation inverse

a :	$\mathrm{Dom}(\rho^{-1})$	$=$	$\mathrm{Im}(\rho)$	(Domaine d'une rel. inv.)
b :	$\mathrm{Im}(\rho^{-1})$	$=$	$\mathrm{Dom}(\rho)$	(Image d'une rel. inverse.)
c :	$\emptyset^{-1}$	$=$	$\emptyset$	(Inverse de la rel. vide)
d :	$(\rho \circ \sigma)^{-1}$	$=$	$\sigma^{-1} \circ \rho^{-1}$	(Inverse de la composition)
e :	$(\rho \cup \sigma)^{-1}$	$=$	$\sigma^{-1} \cup \rho^{-1}$	(Inverse de l'union)
f :	$(\rho \cap \sigma)^{-1}$	$=$	$\sigma^{-1} \cap \rho^{-1}$	(Inverse de l'intersection)

Définition 1.4.14 Familles de relation (1)

a :	ρ est réflexif	$\Leftrightarrow$	$(\forall a \in S \mid a \ \rho \ a)$
b :	ρ est irréflexif	$\Leftrightarrow$	$(\forall a \in S \mid \neg(a \ \rho \ a))$
c :	ρ est symétrique	$\Leftrightarrow$	$(\forall a, b \in S \mid a \ \rho \ b \Rightarrow b \ \rho \ a)$
d :	ρ est asymétrique	$\Leftrightarrow$	$(\forall a, b \in S \mid a \ \rho \ b \Rightarrow \neg(b \ \rho \ a))$
e :	ρ est antisymétrique	$\Leftrightarrow$	$(\forall a, b \in S \mid a \ \rho \ b \wedge b \ \rho \ a \Rightarrow a = b)$
f :	ρ est transitif	$\Leftrightarrow$	$(\forall a, b, c \in S \mid a \ \rho \ b \wedge b \ \rho \ c \Rightarrow a \ \rho \ c)$

Proposition 1.4.15 Définitions équivalentes à 1.4.14

a :	ρ est réflexif	$\Leftrightarrow$	$\mathbf{I}_S \subseteq \rho$
b :	ρ est irréflexif	$\Leftrightarrow$	$\mathbf{I}_S \cap \rho = \emptyset$
c :	ρ est symétrique	$\Leftrightarrow$	$\rho^{-1} = \rho$
d :	ρ est asymétrique	$\Leftrightarrow$	$\rho \cap \rho^{-1} = \emptyset$
e :	ρ est antisymétrique	$\Leftrightarrow$	$\rho \cap \rho^{-1} \subseteq \mathbf{I}_S$
f :	ρ est transitif	$\Leftrightarrow$	$\rho^2 \subseteq \rho$

Définition 1.4.16 Familles de relation (2)

a : ρ est total $\Leftrightarrow$ $(\forall a \in S \mid (\exists b \in T \mid a\ \rho\ b))$

b : ρ est surjectif $\Leftrightarrow$ $(\forall b \in T \mid (\exists a \in S \mid a\ \rho\ b))$

c : ρ est déterministe

$\Leftrightarrow$ $(\forall a \in S, b, b' \in T \mid a\ \rho\ b \wedge a\ \rho\ b' \Rightarrow b = b')$

d : ρ est injectif

$\Leftrightarrow$ $(\forall a, a' \in S, b \in T \mid a\ \rho\ b \wedge a'\ \rho\ b \Rightarrow a = a')$

Théorème 1.4.17 Dualité totalité–surjectivité et dualité déterminisme–injectivité

a : ρ est total $\Leftrightarrow$ ρ^{-1} est surjectif ;

b : ρ est déterministe $\Leftrightarrow$ ρ^{-1} est injectif ;

c : ρ est injectif $\Leftrightarrow$ ρ^{-1} est déterministe ;

d : ρ est surjectif $\Leftrightarrow$ ρ^{-1} est total.

Théorème 1.4.18 Composition de relations totales, surjectives, déterministes et injectives.

a : ρ et σ sont totaux $\Rightarrow$ $\rho \circ \sigma$ est total ;

b : ρ et σ sont déterministes $\Rightarrow$ $\rho \circ \sigma$ est déterministe ;

c : ρ et σ sont injectifs $\Rightarrow$ $\rho \circ \sigma$ est injectif ;

d : ρ et σ sont surjectifs $\Rightarrow$ $\rho \circ \sigma$ est surjectif.

Proposition 1.4.19 Définitions équivalentes d'une fonction surjective

a : $(\forall b \in T \mid (\exists a \in S \mid a\ f\ b))$

b : $(\forall b \in T \mid (\exists a \in S \mid f(a) = b))$

Proposition 1.4.20 Définitions équivalentes d'une fonction injective

a : $(\forall a \in S, a' \in S, b \in T \mid a\ f\ b \wedge a'\ f\ b \Rightarrow a = a')$

b : $(\forall a \in S, a' \in S \mid f(a) = f(a') \Rightarrow a = a')$

c : $(\forall a \in S, a' \in S \mid a \neq a' \Rightarrow f(a) \neq f(a'))$

Corollaire 1.4.21 Inverses de fonctions et de relations

a : f est une fonction

$\Leftrightarrow$ f^{-1} est une relation bijective ;

b : f est une fonction injective

$\Leftrightarrow$ f^{-1} est une relation bijective et déterministe ;

c : f est une fonction surjective

$\Leftrightarrow$ f^{-1} est une relation bijective et totale ;

d : f est une fonction bijective

$\Leftrightarrow$ f^{-1} est une fonction bijective.

Théorème 1.4.22 Composition de fonctions inverses
Les relations $\rho \subseteq S \times T$ et $\sigma \subseteq T \times S$ sont deux fonctions bijectives et $\rho^{-1} = \sigma$ si et seulement si :

$$\rho \circ \sigma = \mathbf{I}_S \quad \text{et} \quad \sigma \circ \rho = \mathbf{I}_T .$$

Théorème 1.5.1 Deux ensembles finis A et B ont le même nombre d'éléments ssi il existe une fonction bijective $f : A \longrightarrow B$.

Définition 1.5.2 On dit que A a *autant d'éléments* que B (ou que *la cardinalité de A est égale à la cardinalité de B*) ssi il existe une fonction bijective de A vers B.

Définition 1.5.3 Un ensemble A est dit *dénombrable* s'il est fini ou de la même cardinalité que l'ensemble $\mathbb{N}$.

Proposition 1.5.4 L'ensemble $\mathbb{Z}$ est dénombrable.

Proposition 1.5.5 L'ensemble $\mathbb{N} \times \mathbb{N}$ est dénombrable.

Lemme 1.5.6 Étant donné un ensemble infini B. Alors,
B est dénombrable
$\Leftrightarrow (\exists A \mid A$ est infini dénombrable $\Rightarrow |A| = |B|)$.

Théorème 1.5.7 Soit A et B, deux ensembles non vides.
$\exists$ fonction injective $f : A \longrightarrow B$
ssi $\exists$ fonction surjective $g : B \longrightarrow A$.

Définition 1.5.8 On dit que A a *une cardinalité plus petite ou égale à* la cardinalité de B ssi il existe une fonction injective de A vers B. (ou, ce qui est équivalent, ssi il existe une fonction surjective de B vers A.)

Axiome 1.5.9 (Axiome du choix) Soit $(A_i)_{i \in I}$, une famille infinie d'ensembles non vides. Alors il existe une famille d'éléments $(a_i)_{i \in I}$ telle que pour chaque $i \in I$, $a_i \in A_i$.

Proposition 1.5.10 Si $A \subseteq B$ alors la fonction $I_{A \subseteq B} : \begin{array}{ccc} A & \longrightarrow & B \\ a & \longmapsto & a \end{array}$ est bien définie et est injective.

Théorème 1.5.11 Soit A un ensemble infini. Alors $|A| \geq |\mathbb{N}|$.

Théorème 1.5.12 Les énoncés suivants sont équivalents :

1. $|A| = |B|$.
2. $\exists$ fonction bijective $f : A \longrightarrow B$.
3. $\exists$ fonction bijective $g : B \longrightarrow A$.
4. $|A| \leq |B|$ et $|A| \geq |B|$.
5. $\exists$ fonction injective $f : A \longrightarrow B$
   et $\exists$ fonction injective $g : B \longrightarrow A$.
6. $\exists$ fonction injective $f : A \longrightarrow B$
   et $\exists$ fonction surjective $h : A \longrightarrow B$.
7. $\exists$ fonction surjective $k : B \longrightarrow A$
   et $\exists$ fonction surjective $h : A \longrightarrow B$.
8. $\exists$ fonction surjective $k : B \longrightarrow A$
   et $\exists$ fonction injective $g : B \longrightarrow A$.

Théorème 1.5.13 Les énoncés suivants sont équivalents :

1. $|A| < |B|$.
2. $|A| \leq |B|$ et $|A| \neq |B|$.
3. $\exists$ fonction injective, $f : A \longrightarrow B$ mais $\nexists$ fonction bijective $g : B \longrightarrow A$.
4. $|A| \leq |B|$ et $|A| \not\geq |B|$.
5. $\exists$ fonction injective, $f : A \longrightarrow B$ mais $\nexists$ fonction injective $g : B \longrightarrow A$.
6. $\exists$ fonction injective, $f : A \longrightarrow B$ mais $\nexists$ fonction surjective $g : A \longrightarrow B$.
7. $|A| \not\geq |B|$.
8. $\nexists$ fonction injective $g : B \longrightarrow A$.
9. $\nexists$ fonction surjective $g : A \longrightarrow B$.

Théorème 1.5.14 Les résultats suivants sont équivalents :

1. A est dénombrable.
2. $|A| \leq |\mathbb{N}|$
3. $\exists$ fonction surjective $f : \mathbb{N} \longrightarrow A$.
4. $\exists$ fonction injective $f : A \longrightarrow \mathbb{N}$.
5. $|A| < |\mathbb{N}|$ ou $|A| = |\mathbb{N}|$
6. A est fini ou $\exists$ fonction bijective $f : A \longrightarrow \mathbb{N}$.
7. A est fini ou $\exists$ fonction bijective $f : \mathbb{N} \longrightarrow A$.

Théorème 1.5.15 Les résultats suivants sont équivalents :

1. A est non dénombrable
2. $|A| > |\mathbb{N}|$.
3. $\nexists$ fonction surjective $f : \mathbb{N} \longrightarrow A$.
4. $\nexists$ fonction injective $f : A \longrightarrow \mathbb{N}$.
5. A est infini et $|A| \neq |\mathbb{N}|$.
6. A est infini et $\nexists$ fonction bijective $f : A \longrightarrow \mathbb{N}$.
7. A est infini et $\nexists$ fonction bijective $f : \mathbb{N} \longrightarrow A$.

Théorème 1.5.16 Soit A et B, deux ensembles dénombrables (finis ou infinis). Alors

1. $A \cup B$ est dénombrable,
2. $A \times B$ est dénombrable.

Théorème 1.5.17 (Cantor)
Pour tout ensemble A, $|A| < |\mathcal{P}(A)|$.

Rappel 1.5.18 La représentation base 10 d'un nombre réel est de la forme $b_n\, b_{n-1} \ldots b_1\, b_0,\ a_0\, a_1\, a_2\, a_3\, a_4 \ldots$ où les b_j et les a_i sont des chiffres de 0 à 9.

Théorème 1.5.19 $\mathbb{R}$ est non dénombrable.

Définition 1.6.1 Étant donnés deux ensembles A et B, on définit B^A comme étant l'ensemble de *toutes* les fonctions de A vers B. Autrement dit : $B^A = \{f : A \longrightarrow B \mid \ \}$.

Proposition 1.6.2 Pour tout ensemble A, on a $|\mathcal{P}(A)| = |\{0,1\}^A|$.

Corollaire 1.6.3 $\{0,1\}^{\mathbb{N}}$ est un ensemble non dénombrable.

Théorème 1.6.4 Soit A un ensemble ayant au moins deux éléments et B un ensemble infini.
Alors A^B est un ensemble non dénombrable.

Proposition 1.6.5 $\{0,1,2\}^{\mathbb{N}}$ est non dénombrable.

Définition 1.7.1 Relation d'équivalence
La relation relation $\simeq$ est une relation d'équivalence si elle possède les propriétés suivantes :

- Réflexivité : $(\forall a \in S \mid a \simeq a)$;
- Symétrie : $(\forall a, b \in S \mid a \simeq b \Rightarrow b \simeq a)$;
- Transitivité : $(\forall a, b, c \in S \mid a \simeq b \wedge b \simeq c \Rightarrow a \simeq c)$.

Proposition 1.7.2 Soit A un ensemble, la relation $\mathbf{I}_A$ est une fonction bijective.

Théorème 1.7.3 Soit $f \subseteq A \times B$. Alors la relation f est une fonction bijective ssi la relation inverse $f^{-1} \subseteq B \times A$ est une fonction bijective.

Théorème 1.7.4 Soit $f \subseteq A \times B$ et $g \subseteq B \times C$. Si f et g sont deux fonctions bijectives, alors $f \circ g$ sera une fonction bijective de A vers C.

Définition 1.7.5 Ordre partiel
Une relation $\preceq$ est un ordre partiel sur l'ensemble S si elle possède les trois propriétés suivantes :

- Réflexivité : $(\forall a \in S \mid a \preceq a)$;
- Antisymétrie : $(\forall a, b \in S \mid a \preceq b \wedge b \preceq a \Rightarrow a = b)$;
- Transitivité : $(\forall a, b, c \in S \mid a \preceq b \wedge b \preceq c \Rightarrow a \preceq c)$.

Définition 1.7.6 Ordre partiel strict
Une relation $\prec$ est un ordre partiel strict sur l'ensemble S si elle possède les trois propriétés suivantes :

- Irréflexivité : $(\forall a \in S \mid \neg(a \prec a)$;
- Asymétrie : $(\forall a, b \in S \mid a \prec b \Rightarrow \neg(b \prec a))$;
- Transitivité : $(\forall a, b, c \in S \mid a \prec b \wedge b \prec c \Rightarrow a \prec c)$.

Théorème 1.7.7 (Bernstein-Schröder) S'il existe une fonction injective de A vers B et une fonction injective de B vers A, alors il existera une fonction bijective de A vers B.
Autrement dit : $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$.

MAT 1919 – Toutes les définitions et quelques propositions des notes... annexée à l'examen

Définition 1.1.2 Opérateur d'implication

$p \Rightarrow q \quad \stackrel{\text{def}}{=} \quad \neg p \vee q$

Définition 1.1.3 Opérateur si et seulement si.

$p \Leftrightarrow q \quad \stackrel{\text{def}}{=} \quad (p \Rightarrow q) \wedge (q \Rightarrow p)$

Proposition 1.1.4 Lois de De Morgan.

a : $\neg(p \wedge q) \quad \Leftrightarrow \quad \neg p \vee \neg q$ (1ère loi de De Morgan)

b : $\neg(p \vee q) \quad \Leftrightarrow \quad \neg p \wedge \neg q$ (2e loi de De Morgan)

Proposition 1.1.5 Propriétés de la négation.

a : $\neg(\neg p) \quad \Leftrightarrow \quad p$ (Double négation)

b : $p \vee \neg p \quad \Leftrightarrow \quad \texttt{vrai}$ (Tiers exclu)

c : $p \wedge \neg p \quad \Leftrightarrow \quad \texttt{faux}$ (Contradiction)

Proposition 1.1.8 Transitivité du "si et seulement si"

$(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \quad \Rightarrow \quad (p \Leftrightarrow r)$

Proposition 1.1.9 Contraposition.

$p \Rightarrow q \quad \Leftrightarrow \quad \neg q \Rightarrow \neg p$

Définition 1.2.2 Notation abrégée des quantificateurs

a : $(\forall x \in T \mid P(x)) \quad \stackrel{\text{def}}{=} \quad (\forall x \mid x \in T \Rightarrow P(x))$

b : $(\exists x \in T \mid P(x)) \quad \stackrel{\text{def}}{=} \quad (\exists x \mid x \in T \wedge P(x))$

Proposition 1.2.3 Lois de De Morgan Généralisées

a : $\neg(\forall x \in T \mid P(x)) \quad \Leftrightarrow \quad (\exists x \in T \mid \neg P(x))$ (1ère loi)

b : $\neg(\exists x \in T \mid P(x)) \quad \Leftrightarrow \quad (\forall x \in T \mid \neg P(x))$ (2e loi)

Techniques de démonstration

$\boxed{P \Rightarrow Q}$ On suppose P ; *puis* on montre Q.

$\boxed{P \Leftrightarrow Q}$ Succession d'équivalences ou

Démonstration de $P \Rightarrow Q$ *ET* Démonstration de $P \Leftarrow Q$.

$\boxed{(\forall x \in X \mid P(x))}$

– Démonstration directe : soit $x \in X$, et on démontre $P(x)$.

– Démonstration par cas : On choisit des ensembles $X_1, \ldots X_n$ dont l'union donne X. On montre ensuite chaque cas : $(\forall x \in X_1 \mid P(x)), \ldots, (\forall x \in X_n \mid P(x))$.

$\boxed{(\exists x \in X \mid P(x))}$ Prenons $x \in X$, choisi de telle façon. On montre que x existe, est bien dans X, puis que $P(x)$ est vrai.

$\boxed{P \wedge Q}$ Démonstration de P *ET* Démonstration de Q.

$\boxed{P \vee Q}$ Démonstration par cas (*Cas 1* : P est vrai (cas terminé) ; *Cas 2* : P est faux et on montre que Q est vrai).

Définition 1.2.1 Axiome d'extensionnalité

$S = T \quad \stackrel{\text{def}}{=} \quad (\forall e \mid e \in S \Leftrightarrow e \in T)$.

Définition 1.2.4 Opérateurs de composition d'ensembles.

a : $S^c \quad \stackrel{\text{def}}{=} \quad \{e \mid e \notin S\}$ (Complément)

b : $S \cap T \quad \stackrel{\text{def}}{=} \quad \{e \mid e \in S \wedge e \in T\}$ (Intersection)

c : $S \cup T \quad \stackrel{\text{def}}{=} \quad \{e \mid e \in S \vee e \in T\}$ (Union)

d : $S \setminus T \quad \stackrel{\text{def}}{=} \quad \{e \mid e \in S \wedge e \notin T\}$ (Différence)

Définition 1.2.5 Opérateurs d'inclusions.

a : $T \subseteq S \quad \stackrel{\text{def}}{=} \quad (\forall e \mid e \in T \Rightarrow e \in S)$ (Incl.)

b : $T \subset S \quad \stackrel{\text{def}}{=} \quad T \subseteq S \wedge (\exists e \mid e \in S \wedge e \notin T)$ (Incl. stricte)

Définition 1.2.6 Ensemble puissance.

$\mathcal{P}(S) \quad \stackrel{\text{def}}{=} \quad \{E \mid E \subseteq S\}$.

Proposition 1.2.13 Propriétés de l'inclusion.

d : $S = T \quad \Leftrightarrow \quad S \subseteq T \wedge T \subseteq S$ (Antisymétrie)

Définition 1.4.1 et 1.4.2 Produit cartésien d'ensembles

$S \times T \quad \stackrel{\text{def}}{=} \quad \{\langle a, b\rangle \mid a \in S \wedge b \in T\}$.

$S_1 \times \ldots \times S_n \quad \stackrel{\text{def}}{=} \quad \{\langle e_1, \ldots, e_n\rangle \mid e_1 \in S_1 \wedge \ldots \wedge e_n \in S_n\}$.

$S^n \quad \stackrel{\text{def}}{=} \quad S \times S \times \ldots \times S$ (n fois) .

Pour la suite, posons $\mathcal{R}, f \subseteq S \times T$, $\mathcal{L} \subseteq T \times U$, $\theta \subseteq T \times W$

Définition 1.4.4 Notation infixe pour les relations

$a \mathcal{R} b \quad \stackrel{\text{def}}{=} \quad \langle a, b\rangle \in \mathcal{R}$.

Définition 1.4.5 Domaine et image d'une relation

a : $\text{Dom}(\mathcal{R}) \quad \stackrel{\text{def}}{=} \quad \{a \in S \mid (\exists b \in T \mid a \mathcal{R} b)\}$ (Domaine)

b : $\text{Im}(\mathcal{R}) \quad \stackrel{\text{def}}{=} \quad \{b \in T \mid (\exists a \in S \mid a \mathcal{R} b)\}$ (Image)

Définition 1.4.6 Relation identité

$\mathbf{I}_S \quad \stackrel{\text{def}}{=} \quad \{\langle a, a\rangle \in S^2 \mid a \in S\}$

Définition 1.4.7 Composition de deux relations

$\mathcal{R} \circ \mathcal{L} \quad \stackrel{\text{def}}{=} \quad \{\langle a, c\rangle \in S \times U \mid (\exists b \in T \mid \langle a, b\rangle \in \mathcal{R} \wedge \langle b, c\rangle \in \mathcal{L})\}$.

Ainsi : $a \ (\mathcal{R} \circ \mathcal{L}) \ c \quad \stackrel{\text{def}}{=} \quad (\exists b \in T \mid a \mathcal{R} b \wedge b \mathcal{L} c)$

Définition 1.4.9 Puissance d'une relation

Si $n \geq 1$: $\quad \mathcal{R}^n \quad \stackrel{\text{def}}{=} \quad \mathcal{R} \circ \mathcal{R} \circ \ldots \circ \mathcal{R}$ (n fois) ,

sinon ($n = 0$) : $\quad \mathcal{R}^0 \quad \stackrel{\text{def}}{=} \quad \mathbf{I}_S$.

Définition 1.4.11 Clôtures d'une relation

a : $\mathcal{R}^+ \quad \stackrel{\text{def}}{=} \quad \mathcal{R}^1 \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \ldots$ (Clôture transitive)

b : $\mathcal{R}^* \quad \stackrel{\text{def}}{=} \quad \mathcal{R}^0 \cup \mathcal{R}^1 \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \ldots$ (Cl. transitive et réflexive)

Définition 1.4.12 Inverse d'une relation

$\mathcal{R}^{-1} \quad \stackrel{\text{def}}{=} \quad \{\langle b, a\rangle \in T \times S \mid \langle a, b\rangle \in \mathcal{R}\}$.

Définition 1.4.14, Familles de relations 1 **et Prop. 1.4.15**

Soit $\mathcal{R} \subseteq S^2$; $\mathcal{R}$ est

réflexif	$\stackrel{\text{def}}{=} (\forall a \in S \mid a \mathcal{R} a)$	$\Leftrightarrow \mathbf{I}_S \subseteq \mathcal{R}$
irréflexif	$\stackrel{\text{def}}{=} (\forall a \in S \mid \neg(a \mathcal{R} a))$	$\Leftrightarrow \mathbf{I}_S \cap \mathcal{R} = \emptyset$
symétrique	$\stackrel{\text{def}}{=} (\forall a, b \in S \mid a \mathcal{R} b \Rightarrow b \mathcal{R} a)$	$\Leftrightarrow \mathcal{R}^{-1} = \mathcal{R}$
asymétrique	$\stackrel{\text{def}}{=} (\forall a, b \in S \mid a \mathcal{R} b \Rightarrow \neg(b \mathcal{R} a))$	$\Leftrightarrow \mathcal{R} \cap \mathcal{R}^{-1} = \emptyset$
antisymétrique	$\stackrel{\text{def}}{=} (\forall a, b \in S \mid a \mathcal{R} b \wedge b \mathcal{R} a \Rightarrow a = b)$	$\Leftrightarrow \mathcal{R} \cap \mathcal{R}^{-1} \subseteq \mathbf{I}_S$
transitif	$\stackrel{\text{def}}{=} (\forall a, b, c \in S \mid a \mathcal{R} b \wedge b \mathcal{R} c \Rightarrow a \mathcal{R} c)$	$\Leftrightarrow \mathcal{R}^2 \subseteq \mathcal{R}$

Définition 1.4.16 Familles de relations 2.

Soit $\mathcal{R} \subseteq S \times T$; $\mathcal{R}$ est

a : $\mathcal{R}$ total $\quad \stackrel{\text{def}}{=} (\forall a \in S \mid (\exists b \in T \mid a \mathcal{R} b))$

b : $\mathcal{R}$ surjectif $\quad \stackrel{\text{def}}{=} (\forall b \in T \mid (\exists a \in S \mid a \mathcal{R} b))$

c : $\mathcal{R}$ déterministe $\stackrel{\text{def}}{=} (\forall a \in S, b, b' \in T \mid a \mathcal{R} b \wedge a \mathcal{R} b' \Rightarrow b = b')$

d : $\mathcal{R}$ injectif $\quad \stackrel{\text{def}}{=} (\forall a, a' \in S, b \in T \mid a \mathcal{R} b \wedge a' \mathcal{R} b \Rightarrow a = a')$

e : $\mathcal{R}$ bijectif $\quad \stackrel{\text{def}}{=} \mathcal{R}$ est injectif et surjectif.

Déf. une *fonction* est une relation totale et déterministe.

Théorème 1.4.17 Dualités...

a : $\mathcal{R}$ est total $\Leftrightarrow$ $\mathcal{R}^{-1}$ est surjectif ;

b : $\mathcal{R}$ est déterministe $\Leftrightarrow$ $\mathcal{R}^{-1}$ est injectif ;

c : $\mathcal{R}$ est injectif $\Leftrightarrow$ $\mathcal{R}^{-1}$ est déterministe ;

d : $\mathcal{R}$ est surjectif $\Leftrightarrow$ $\mathcal{R}^{-1}$ est total.

Théorème 1.4.18 Sur la composition de relations

a : $\mathcal{R}$ et $\mathcal{L}$ sont totaux $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est total ;

b : $\mathcal{R}$ et $\mathcal{L}$ sont déterministes $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est déterministe ;

c : $\mathcal{R}$ et $\mathcal{L}$ sont injectifs $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est injectif ;

d : $\mathcal{R}$ et $\mathcal{L}$ sont surjectifs $\Rightarrow$ $\mathcal{R} \circ \mathcal{L}$ est surjectif.

Proposition 1.4.19 Définition équiv. fonction surjective

b : $(\forall b \in T \mid (\exists a \in S \mid f(a) = b)$

Proposition 1.4.20 Définitions équiv. fonction injective

a : $(\forall a \in S, a' \in S, b \in T \mid a \ f \ b \wedge a' \ f \ b \Rightarrow a = a')$

b : $(\forall a \in S, a' \in S \mid f(a) = f(a') \Rightarrow a = a')$

c : $(\forall a \in S, a' \in S \mid a \neq a' \Rightarrow f(a) \neq f(a'))$

Corollaire 1.4.21 Inverses de fonctions et de relations

a : f est une fonction $\Leftrightarrow$ f^{-1} est une relation bijective ;

b : f est une fonction injective
$\Leftrightarrow$ f^{-1} est une relation bijective et déterministe ;

c : f est une fonction surjective
$\Leftrightarrow$ f^{-1} est une relation bijective et totale ;

d : f est une fonction bijective
$\Leftrightarrow$ f^{-1} est une fonction bijective.

Pour la suite, soit A et B des ensembles, et soit $f \subseteq A \times B$ et $g \subseteq B \times C$ des fonctions. La "cardinalité de A" se note $|A|$.

Définition 1.5.2 A et B *ont autant d'éléments* (c.-à-d. $|A| = |B|$) ssi $\exists$ une fonction bijective $h : A \longrightarrow B$.

Définition 1.5.3 Un ensemble A est dit *dénombrable* s'il est fini ou de la même cardinalité que l'ensemble $\mathbb{N}$.

Prop. 1.5.4, 1.5.5 Les ens. $\mathbb{Z}$ et $\mathbb{N} \times \mathbb{N}$ sont dénombrables.

Lemme 1.5.6 L'ensemble B est dénombrable ssi $(\exists A \mid A$ est dénombrable et $|A| = |B|)$.

Théorème 1.5.7 Pour A et B non vides, $\exists$ une fonction injective $f : A \longrightarrow B$ ssi $\exists$ une fonction surjective $g : B \longrightarrow A$.

Définition 1.5.8 $|A| \leq |B| \stackrel{\text{def}}{=} \exists$ une fonct. injective $f : A \longrightarrow B$. (est équivalent à $\exists$ une fonct. surjective $g : B \longrightarrow A$.)

Proposition 1.5.10 Si $A \subseteq B$ alors la fonction $I_{A \subseteq B} : \begin{array}{ccc} A & \longrightarrow & B \\ a & \longmapsto & a \end{array}$ est bien définie et est injective.

Théorème 1.5.11 Soit A un ensemble infini. Alors $|A| \geq |\mathbb{N}|$.

Théorème 1.5.12 Les énoncés suivants sont équivalents :

- $|A| = |B|$.
- $\exists$ fonction bijective $f : A \longrightarrow B$.
- $\exists$ fonction bijective $g : B \longrightarrow A$.
- $|A| \leq |B|$ et $|A| \geq |B|$.
- $\exists$ fonct. injective $f : A \longrightarrow B$ et $\exists$ fonct. injective $g : B \longrightarrow A$.
- $\exists$ fonct. inject. $f : A \longrightarrow B$ et $\exists$ fonct. surjective $h : A \longrightarrow B$.

Théorème 1.5.13 Les énoncés suivants sont équivalents :

- $|A| < |B|$.
- $|A| \leq |B|$ et $|A| \neq |B|$.
- $\exists$ fonct. inject. $f : A \longrightarrow B$ mais $\nexists$ fonct. biject. $g : B \longrightarrow A$.
- $|A| \leq |B|$ et $|A| \not\geq |B|$.
- $\exists$ fonct. inject. $f : A \longrightarrow B$ mais $\nexists$ fonct. inject. $g : B \longrightarrow A$.
- $\exists$ fonct. inject. $f : A \longrightarrow B$ mais $\nexists$ fonct. surject. $g : A \longrightarrow B$.
- $|A| \not\geq |B|$.

Théorème 1.5.14 Les énoncés suivants sont équivalents :

- A est dénombrable.
- $|A| \leq |\mathbb{N}|$
- $\exists$ fonction surjective $f : \mathbb{N} \longrightarrow A$.
- $\exists$ fonction injective $f : A \longrightarrow \mathbb{N}$.
- $|A| < |\mathbb{N}|$ ou $|A| = |\mathbb{N}|$
- A est fini ou $\exists$ fonction bijective $f : A \longrightarrow \mathbb{N}$.
- A est fini ou $\exists$ fonction bijective $f : \mathbb{N} \longrightarrow A$.

Théorème 1.5.16 Si A et B sont dénombrables, alors

1. $A \cup B$ est dénombrable,
2. $A \times B$ est dénombrable.

Théorème 1.5.17 (Cantor) Pour tout A, $|A| < |\mathcal{P}(A)|$.

Théorème 1.5.19 $\mathbb{R}$ est non dénombrables.

Définition 1.6.1 B^A est l'ensemble de *toutes* les fonctions de A vers B. Autrement dit : $B^A = \{f : A \longrightarrow B \mid \ \}$.

Proposition 1.6.2 Pour tout A, on a $|\mathcal{P}(A)| = |\{0,1\}^A|$.

Corollaire 1.6.3 $\{0,1\}^{\mathbb{N}}$ est non dénombrables.

Théorème 1.6.4 Si A a au moins deux éléments et B est infini, alors A^B est un ensemble non dénombrable.

Définition 1.7.1 Relation d'équivalence
La relation $\simeq$ est une relation d'équivalence si elle est :

- Réflexive : $(\forall a \in S \mid a \simeq a)$;
- Symétrique : $(\forall a, b \in S \mid a \simeq b \Rightarrow b \simeq a)$;
- Transitive : $(\forall a, b, c \in S \mid a \simeq b \wedge b \simeq c \Rightarrow a \simeq c)$.

Proposition 1.7.2 La relation $\mathbf{I}_A$ est une fonction bijective.

Théorème 1.7.3 La relation f est une fonction bijective ssi la relation inverse $f^{-1} \subseteq B \times A$ est une fonction bijective.

Théorème 1.7.4 Si f et g sont deux fonctions bijectives, alors $f \circ g$ est une fonction bijective de A vers C.

Définition 1.7.5 Ordre partiel
La relation $\preceq$ est un ordre partiel sur l'ensemble S si elle est :

- Réflexive : $(\forall a \in S \mid a \preceq a)$;
- Antisymétrique : $(\forall a, b \in S \mid a \preceq b \wedge b \preceq a \Rightarrow a = b)$;
- Transitive : $(\forall a, b, c \in S \mid a \preceq b \wedge b \preceq c \Rightarrow a \preceq c)$.

Définition 1.7.6 Ordre partiel strict
La relation $\prec$ est un ordre partiel strict sur l'ens. S si elle est :

- Irréflexive : $(\forall a \in S \mid \neg(a \prec a)$;
- Asymétrique : $(\forall a, b \in S \mid a \prec b \Rightarrow \neg(b \prec a))$;
- Transitive : $(\forall a, b, c \in S \mid a \prec b \wedge b \prec c \Rightarrow a \prec c)$.

Définition 2.1.1 Notation sigma : $\displaystyle\sum_{i=n_0}^{n} g(i) \stackrel{\text{def}}{=} g(n_0) + g(n_0+1) + g(n_0+2) + \ldots + g(n)\,.$

Proposition 2.1.2 Propriétés arithmétiques des sommes en notation sigma.

a : $\displaystyle\sum_{i=n_0}^{n} 1 = n - n_0 + 1$ (En particulier, $\displaystyle\sum_{i=1}^{n} 1 = n$)

b : $\displaystyle\sum_{i=n_0}^{n} k \cdot g(i) = k \cdot \sum_{i=n_0}^{n} g(i)$ (En particulier, $\displaystyle\sum_{i=1}^{n} k = k \cdot n$)

c : $\displaystyle\sum_{i=n_0}^{n} g(i) + h(i) = \sum_{i=n_0}^{n} g(i) + \sum_{i=n_0}^{n} h(i)$

d : $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

e : $\displaystyle\sum_{i=1}^{n} i^2 = \frac{(2n+1)(n+1)n}{6}$

Théorèmes 2.3.1 et 2.3.2 Principes d'induction mathématique faible, cas de base 0 ou n_0.

a : $\Big[\, P(0) \wedge \big(\forall n \in \mathbb{N} \mid P(n) \Rightarrow P(n+1)\big) \,\Big] \Rightarrow \big(\forall n \in \mathbb{N} \mid P(n)\big)$

b : $\Big[\, P(0) \wedge \big(\forall n \in \mathbb{N}^* \mid P(n-1) \Rightarrow P(n)\big) \,\Big] \Rightarrow \big(\forall n \in \mathbb{N} \mid P(n)\big)$

2.3.2 : $\Big[\, P(n_0) \wedge \big(\forall n \in \mathbb{I}\backslash\{n_0\} \mid P(n-1) \Rightarrow P(n)\big) \,\Big] \Rightarrow \big(\forall n \in \mathbb{I} \mid P(n)\big)\,,$ où $\mathbb{I} \stackrel{\text{def}}{=} \{n_0, n_0+1, n_0+2, \ldots\}$.

Théorème 2.3.3 Principe d'induction mathématique à deux cas de base.

$\Big[\, P(0) \wedge P(1) \wedge \big(\forall n \in \mathbb{N} \setminus \{0,1\} \mid P(n-2) \wedge P(n-1) \Rightarrow P(n)\big) \,\Big] \Rightarrow \big(\forall n \in \mathbb{N} \mid P(n)\big)\,.$

Théorèmes 2.3.4, 2.3.5 Principes d'induction forte, cas de base 0 ou n_0. Posons $\mathbb{I} \stackrel{\text{def}}{=} \{n_0, n_0+1, n_0+2, \ldots\}$

2.3.4 : $\Big[\, P(0) \wedge \big(\forall n \in \mathbb{N}^* \;\big|\; \big(\forall k \in \{0,1,2,\ldots,n-1\} \;\big|\; P(k)\big) \Rightarrow P(n)\big) \,\Big] \Rightarrow \big(\forall n \in \mathbb{N} \mid P(n)\big)\,.$

2.3.5 : $\Big[P(n_0) \wedge \big(\forall n \in \mathbb{I} \setminus \{n_0\} \;\big|\; \big(\forall k \in \{n_0, n_0+1, \ldots, n-1\} \;\big|\; P(k)\big) \Rightarrow P(n)\big)\Big] \Rightarrow \big(\forall n \in \mathbb{I} \mid P(n)\big)\,.$

Théorème 2.4.2 Terme général d'une suite arithmétique. Les énoncés suivants sont équivalents :

1. $\langle a_n \rangle_{n\in\mathbb{N}}$ est une suite arithmétique de premier terme a et de différence d.
2. $\langle a_n \rangle_{n\in\mathbb{N}}$ est définie par récurrence comme : $a_0 = a$ et $a_n = a_{n-1} + d \;\; \forall n \in \mathbb{N}^*$.
3. $\langle a_n \rangle_{n\in\mathbb{N}}$ est définie par terme général comme : $a_n = a + nd \;\; \forall n \in \mathbb{N}\,.$

Théorème 2.4.4 Terme général d'une suite géométrique. Les énoncés suivants sont équivalents :

1. $\langle a_n \rangle_{n\in\mathbb{N}}$ est une suite géométrique de premier terme a et de raison r.
2. $\langle a_n \rangle_{n\in\mathbb{N}}$ est définie par récurrence comme : $a_0 = a$ et $a_n = a_{n-1} \cdot r \;\; \forall n \in \mathbb{N}^*\,.$
3. $\langle a_n \rangle_{n\in\mathbb{N}}$ est définie par terme général comme : $a_n = a \cdot r^n \;\; \forall n \in \mathbb{N}\,.$

Définition 2.4.5 Suite des sommes de premiers termes d'une suite.

$S_n = \displaystyle\sum_{i=0}^{n} a_i \qquad \forall n \in \mathbb{N}\,.$

Théorème 2.4.6 Sommes de premiers termes d'une suite arithmétique

$S_n = \dfrac{(a_0 + a_n)(n+1)}{2} \qquad \forall n \in \mathbb{N}\,.$

Théorème 2.4.7 Sommes de premiers termes d'une suite géométrique

$S_n = \dfrac{a_0 \cdot (1 - r^{n+1})}{1 - r} \qquad \forall n \in \mathbb{N}\,.$

Méthode des substitutions à rebours

1. Substituer à rebours
2. Déduire l'expression après i subtitutions.
3. Substituer la valeur du cas de base
4. Calculer le terme général

Méthode des séries génératrices

1. Exprimer la série génératrice G sous la forme d'une fonction rationnelle
2. Trouver la série de puissance associée à G
3. Trouver le terme général de la suite

Théorème 2.5.1 Modèles de séries de puissances

a : $\dfrac{a}{1-bx} = \displaystyle\sum_{i=0}^{\infty} a\,b^i\,x^i = a + a\,b\,x + a\,b^2\,x^2 + a\,b^3\,x^3 + \cdots + a\,b^n\,x^n + \cdots$

b : $\dfrac{a}{(1-bx)^2} = \displaystyle\sum_{i=0}^{\infty} (i+1)a\,b^i\,x^i = a + 2a\,b\,x + 3a\,b^2 \cdot x^2 + \cdots + (n+1)a\,b^n\,x^n + \cdots$

c : $\dfrac{ax}{(1-bx)^2} = \displaystyle\sum_{i=0}^{\infty} i\,a\,b^{i-1}\,x^i = 0 + a\,x + 2a\,b\,x^2 + 3a\,b^2\,x^3 + \cdots + n\,a\,b^{n-1}\,x^n + \cdots$

d : $\dfrac{a}{(1-bx)^3} = \displaystyle\sum_{i=0}^{\infty} \frac{(i+2)(i+1)\,a\,b^i}{2}\,x^i = \frac{2\cdot 1\,a}{2} + \frac{3\cdot 2\,a\,b}{2}x + \frac{4\cdot 3\,a\,b^2}{2}x^2 + \frac{5\cdot 4\,a\,b^3}{2}x^3 + \cdots + \frac{(n+2)(n+1)\,a\,b^n}{2}\,x^n + \cdots$

Corollaire 2.5.2 Cas particuliers des modèles de séries de puissances

$$\texttt{a}: \quad \frac{1}{1-x} = \sum_{i=0}^{\infty} x^i = 1 + x + x^2 + x^3 + x^4 + \cdots + x^n + \cdots$$

$$\texttt{b}: \quad \frac{1}{1+x} = \sum_{i=0}^{\infty} (-1)^i\, x^i = 1 + (-1)x + (-1)^2x^2 + (-1)^3x^3 + \cdots$$

$$\texttt{c}: \quad \frac{1}{(1-x)^2} = \sum_{i=0}^{\infty} (i+1)\, x^i = 1 + 2x + 3x^2 + 4x^3 + \cdots + (n+1)\, x^n + \cdots$$

$$\texttt{d}: \quad \frac{x}{(1-x)^2} = \sum_{i=0}^{\infty} i\, x^i = 0 + x + 2x^2 + 3x^3 + 4x^4 + \cdots + n\, x^n + \cdots$$

$$\texttt{e}: \quad \frac{1}{(1-x)^3} = \sum_{i=0}^{\infty} \frac{(i+2)(i+1)}{2}\, x^i = \frac{2\cdot 1}{2} + \frac{3\cdot 2}{2}\, x + \frac{4\cdot 3}{2}\, x^2 + \cdots + \frac{(n+2)(n+1)}{2}\, x^n + \cdots$$

Théorème 2.5.3 Décomposition en fractions partielles

$$\texttt{a}: \quad \frac{ax+b}{(cx+d)(ex+f)} = \frac{A}{cx+d} + \frac{B}{ex+f}$$

$$\texttt{b}: \quad \frac{ax+b}{(cx+d)^2} = \frac{A}{cx+d} + \frac{B}{(cx+d)^2}$$

$$\texttt{c}: \quad \frac{ax^2+bx+c}{(dx+e)(fx+g)(hx+i)} = \frac{A}{dx+e} + \frac{B}{fx+g} + \frac{C}{hx+i}$$

$$\texttt{d}: \quad \frac{ax^2+bx+c}{(dx+e)^2(fx+g)} = \frac{A}{dx+e} + \frac{B}{(dx+e)^2} + \frac{C}{fx+g}$$

$$\texttt{e}: \quad \frac{ax^2+bx+c}{(dx+e)^3} = \frac{A}{dx+e} + \frac{B}{(dx+e)^2} + \frac{C}{(dx+e)^3}$$

Proposition 2.5.4 Propriétés des zéros d'un polynôme de degré 2

Soit $p(x) = ax^2+bx+c$, un polynôme de degré deux. Soit $\rho_1 \stackrel{\text{def}}{=} \dfrac{-b+\sqrt{b^2-4ac}}{2a}$ et $\rho_2 \stackrel{\text{def}}{=} \dfrac{-b-\sqrt{b^2-4ac}}{2a}$.

Alors,

- ρ_1 et ρ_2 sont appelés les **zéros du polynôme** p parce que $\quad p(\rho_1) = 0, \quad p(\rho_2) = 0 \quad$ et $\quad p(x) \neq 0 \quad \forall x \neq \rho_1, \rho_2$.
- Le polynôme p se factorise toujours ainsi : $p(x) = a(x-\rho_1)(x-\rho_2)$
- De plus, si le polynôme est unitaire (c'est-à-dire si $a = 1$), on a toujours que $\begin{cases} (*) & \rho_1 + \rho_2 = -b \\ (**) & \rho_1 \cdot \rho_2 = c. \end{cases}$

Proposition 2.5.5 Factorisation d'un polynôme de degré 2

Soit $q(x) = 1 - rx - sx^2$, un polynôme de degré deux dont la constante est 1. Considérons le polynome $p(x) = x^2 - rx - s$; soit ρ_1 et ρ_2 les deux zéros (peut-être égaux) du polynôme p. Alors $q(x)$ se factorise ainsi :

$$1 - rx - sx^2 = (1-\rho_1 x)\,(1-\rho_2 x)\,.$$

Théorème 2.5.7 Récurrences linéaires, homogènes d'ordre 2

$$\begin{cases} a_0 = a & \text{si } \rho_1 \neq \rho_2 : \; a_n = A\cdot(\rho_1)^n + B\cdot(\rho_2)^n \quad n \in \mathbb{N}. \\ a_1 = b & \text{si } \rho_1 = \rho_2 : \; a_n = A\cdot(\rho_1)^n + B\cdot n\cdot(\rho_1)^n \quad n \in \mathbb{N}. \\ a_n = r\cdot a_{n-1} + s\cdot a_{n-2} \quad \forall n \in \mathbb{N}\setminus\{0,1\} & \text{Où } \rho_1 \text{ et } \rho_2 \text{ sont les zéros du polynôme } p(x) = x^2 - rx - s. \end{cases}$$

Définition 2.6.1 Fonctions non décroissantes et fonctions croissantes.

$\texttt{a}: \quad f$ est non décroissant sur $[a,b] \quad \Leftrightarrow \quad (\forall x, y \in [a,b] \mid x < y \Rightarrow f(x) \leq f(y))$

$\texttt{b}: \quad f$ est non croissant sur $[a,b] \quad \Leftrightarrow \quad (\forall x, y \in [a,b] \mid x < y \Rightarrow f(x) \geq f(y))$

Théorème 2.6.2 Bornes d'une somme.

$$\texttt{a}: \quad \int_{a-1}^{b} f(x)\,dx \leq \sum_{i=a}^{b} f(i) \leq \int_{a}^{b+1} f(x)\,dx \quad \text{si } f \text{ est non décroissant sur } [a-1, b+1]$$

$$\texttt{b}: \quad \int_{a}^{b+1} f(x)\,dx \leq \sum_{i=a}^{b} f(i) \leq \int_{a-1}^{b} f(x)\,dx \quad \text{si } f \text{ est non croissant sur } [a-1, b+1]$$

Formules d'intégration En notant $F = \int f(x)\,dx$, on a : $\int_a^b f(x)\,dx = \Big[F(x)\Big]_a^b = F(b) - F(a)$.

a : $\int k\,dx = k\,x + C$	b : $\int x^a dx = \frac{x^{a+1}}{a+1} + C$ si $a \neq -1$	d : $\int \frac{c}{a\,x+b} dx = \frac{c}{a}\ln\lvert a\,x+b\rvert + C$	
c : $\int \frac{1}{x} dx = \ln\lvert x\rvert + C$	e : $\int e^x dx = e^x + C$	f : $\int a^x dx = \frac{a^x}{\ln a} + C$	
g : $\int \ln x\,dx = x\ln x - x + C$	h : $\int \log_a x\,dx = x\log_a x - \frac{x}{\ln a} + C$	i : $\int \Big(f(x)+g(x)\Big)dx = \int f(x)dx + \int g(x)dx$	

Lexique de la théorie des graphes

- Un **graphe** (ou **graphe non orienté**) est une relation binaire symétrique et irreflexive.
- Un **digraphe** (ou **graphe orienté**) est une relation binaire.
- Un **graphe régulier** d'ordre k est un graphe dont tous les sommets sont de degré k.
- Un **graphe complet** d'ordre n (noté K_n) est un graphe qui a exactement n sommets et où pour tout $x, y \in V(K_n)$ tels que $x \neq y$, on a $[x, y] \in E(K_n)$.
- Un graphe G est un **graphe biparti** de bipartition A et B si A et B forment une bipartition de $V(G)$ (c.-à-d. : $A \cap B = \emptyset$ et $V(G) = A \cup B$), et pour toute arête de G, une extrémité appartient à A et l'autre à B.
- Un graphe H est dit **sous-graphe** d'un graphe G (noté : $H \lhd G$) si $V(H) \subseteq V(G)$ et $E(H) \subseteq E(G)$.
- Un graphe H est un **sous-graphe couvrant** d'un graphe G si : $H \lhd G$ et $V(H) = V(G)$.
- Un graphe H est un **sous-graphe induit** d'un graphe G si $H \lhd G$ et $(\forall x, y \in V(H) \mid [x, y] \in E(G) \Rightarrow [x, y] \in E(H))$.
- Un **arbre** est un graphe qui est connexe et ne contient aucun cycle.
- Un **arbre binaire** est un arbre qui contient un sommet de degré 2 et dont tous les autres sommets sont de degrés 1 ou 3.
- Un **arbre binaire complet** est un arbre binaire dont toutes les feuilles sont toutes au même niveau.
- Un **isomorphisme** entre les graphes G_1 et G_2 est une fonction bijective $f : V(G_1) \longrightarrow V(G_2)$ telle que
$$\big(\forall x, y \mid [x, y] \in E(G_1) \;\Leftrightarrow\; [f(x), f(y)] \in E(G_2)\big).$$
- Un **cycle eulérien** d'un graphe est un cycle passant par chacune des arêtes du graphe. Un graphe qui contient un tel cycle est un **graphe eulérien**.
- Un **cycle hamiltonien** d'un graphe est un cycle élémentaire passant par chacun des sommets du graphe. Un graphe qui contient un tel cycle est un **graphe hamiltonien**.
- Un **graphe planaire** est un graphe qui peut être tracé dans un plan sans qu'aucune de ses arêtes en croise une autre.
- Une **représentation planaire** est une représentation dans le plan $\mathbb{R}^2$ d'un graphe planaire.

Théorème 3.4.2 Nombre de sommets d'un arbre.
Soit G un graphe connexe, alors : G est un arbre $\Leftrightarrow \Big|V(G)\Big| = \Big|E(G)\Big| + 1$.

Proposition 3.3.3 et 3.3.4 Somme des degrés d'un graphe et nombre de sommets de degré impair
Soit G un graphe et $V(G) = \{x_1, x_2, \ldots, x_{|V(G)|}\}$ l'ensemble de ses sommets. Alors : $\sum_{i=1}^{|V(G)|} \deg_G(x_i) = 2\Big|E(G)\Big|$.
Ainsi si G a un nombre fini de sommets alors G contient un nombre pair de sommets de degré impair.

Lemme 3.5.2 Représentations planaires et cycles.
Soit une représentation planaire G et $e \in E(G)$.

a : Si e appartient à un cycle de G, alors e fait partie de la frontière d'exactement deux régions de G.
b : Si e n'est dans aucun cycle de G, alors e fait partie de la frontière d'exactement une région de G.

Théorème 3.5.3 Formule d'Euler
Soit G une représentation planaire connexe. Alors $\Big|V(G)\Big| + \Big|F(G)\Big| - \Big|E(G)\Big| = 2$.

Proposition 3.5.4 Nombre d'arêtes maximal d'un graphe planaire.
Soit G un graphe planaire connexe tel que $\Big|V(G)\Big| \geq 4$, alors $\Big|E(G)\Big| \leq 3\Big|V(G)\Big| - 6$.

Proposition 3.5.5 Tout graphe planaire a un sommet de degré ≤ 5.