

Comment le prouver ?

Daniel J_ Velleman

Table des matières

[Demi-page de titre](#)

[Page de titre](#)

[Page de droits d'auteur](#)

[Dévouement](#)

[Contenu](#)

[Préface de la troisième édition](#)

[Introduction](#)

[1 Logique phrasenelle](#)

[1.1 Raisonnement déductif et connecteurs logiques](#)

[1.2 Tables de vérité](#)

[1.3 Variables et ensembles](#)

[1.4 Opérations sur les ensembles](#)

[1.5 Les connecteurs conditionnels et biconditionnels](#)

[2 Logique quantificationnelle](#)

[2.1 Quantificateurs](#)

[2.2 Equivalences impliquant des quantificateurs](#)

[2.3 Autres opérations sur les ensembles](#)

[3 preuves](#)

[3.1 Stratégies de preuve](#)

[3.2 Preuves impliquant des négations et des conditionnels](#)

[3.3 Preuves impliquant des quantificateurs](#)

[3.4 Preuves impliquant des conjonctions et des biconditions](#)

[3.5 Preuves impliquant des disjonctions](#)

[3.6 Preuves d'existence et d'unicité](#)

[3.7 Autres exemples de preuves](#)

[4 Relations](#)

[4.1 Paires ordonnées et produits cartésiens](#)

[4.2 Relations](#)

[4.3 En savoir plus sur les relations](#)

[4.4 Relations de commande](#)

[4.5 Relations d'équivalence](#)

[5 fonctions](#)

[5.1 Fonctions](#)

[5.2 Un à un et sur](#)

[5.3 Inverses de fonctions](#)

[5.4 Fermetures](#)

[5.5 Images et images inversées : un projet de recherche](#)

[6 Induction mathématique](#)

[6.1 Preuve par induction mathématique](#)

[6.2 Autres exemples](#)

[6.3 Récursivité](#)

[6.4 Forte induction](#)

[6.5 Fermetures à nouveau](#)

[7 Théorie des nombres](#)

[7.1 Plus grands diviseurs communs](#)

[7.2 Factorisation en nombres premiers](#)

[7.3 Arithmétique modulaire](#)

[7.4 Théorème d'Euler](#)

[7.5 Cryptographie à clé publique](#)

[8 ensembles infinis](#)

[8.1 Ensembles équinombreux](#)

[8.2 Ensembles dénombrables et indénombrables](#)

[8.3 Le théorème de Cantor-Schröder-Bernstein](#)

[Annexe : Solutions aux exercices sélectionnés](#)

[Suggestions de lectures complémentaires](#)

[Résumé des techniques de preuve](#)

[Indice](#)

Comment le prouver

COMMENT LE PROUVER

Une approche structurée

Troisième édition

Daniel J. Velleman

*Département de mathématiques et de statistique
Collège Amherst*

*Département de mathématiques et de statistique
Université du Vermont*





Imprimerie universitaire, Cambridge CB2 8BS, Royaume-Uni
One Liberty Plaza, 20e étage, New York, NY 10006, États-Unis
477 Williamstown Road, Port Melbourne, VIC 3207, Australie
314–321, 3e étage, parcelle 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, Inde
79 Anson Road, #06–04/06, Singapour 079906

Cambridge University Press fait partie de l'Université de Cambridge.

Elle contribue à la mission de l'Université en diffusant les connaissances dans la poursuite de l'éducation, de l'apprentissage et de la recherche aux plus hauts niveaux d'excellence internationaux.

www.cambridge.org

Informations sur ce titre : www.cambridge.org/9781108424189

DOI : [10.1017/9781108539890](https://doi.org/10.1017/9781108539890)

© Daniel J. Velleman 2019

Cette publication est protégée par le droit d'auteur. Sous réserve des exceptions légales et des dispositions des accords de licence collective pertinents, toute reproduction, même partielle, est interdite sans l'autorisation écrite de Cambridge University Press.

Première publication en 1994

Deuxième édition 2006

Troisième édition 2019

Imprimé au Royaume-Uni par TJ International Ltd, Padstow Cornwall

Une notice de catalogue pour cette publication est disponible à la British Library .

Données de catalogage avant publication de la Bibliothèque du Congrès

Noms : Velleman, Daniel J., auteur.

Titre : Comment le prouver : une approche structurée / Daniel J. Velleman (Amherst College, Massachusetts).

Description : Troisième édition. | Cambridge ; New York, NY : Cambridge University Press, [2019] | Comprend un index.

Identifiants : LCCN 2019013488 | ISBN 9781108424189 (couverture rigide : papier alcalin) | ISBN 9781108439534 (livre broché : papier alcalin)

Matières : LCSH : Logique, symbolique et mathématique – Manuels scolaires. | Mathématiques – Manuels scolaires. | Théorie de la preuve – Manuels scolaires.

Classification : LCC QA9.V38 2019 | DDC 511.3–dc23

Enregistrement LC disponible sur <https://lccn.loc.gov/2019013488>

ISBN 978-1-108-42418-9 Couverture rigide

ISBN 978-1-108-43953-4 Broché

Cambridge University Press n'assume aucune responsabilité quant à la persistance ou à l'exactitude des URL des sites Internet externes ou tiers mentionnés dans cette publication et ne garantit pas que le contenu de ces sites Web est ou restera exact ou approprié.

A Shelley

Contenu

Préface de la troisième édition
Introduction

1 Logique phrasenelle

- 1.1 Raisonnement déductif et connecteurs logiques
- 1.2 Tables de vérité
- 1.3 Variables et ensembles
- 1.4 Opérations sur les ensembles
- 1.5 Les connecteurs conditionnels et biconditionnels

2 Logique quantificationnelle

- 2.1 Quantificateurs
- 2.2 Equivalences impliquant des quantificateurs
- 2.3 Autres opérations sur les ensembles

3 preuves

- 3.1 Stratégies de preuve
- 3.2 Preuves impliquant des négations et des conditionnels
- 3.3 Preuves impliquant des quantificateurs
- 3.4 Preuves impliquant des conjonctions et des biconditions
- 3.5 Preuves impliquant des disjonctions
- 3.6 Preuves d'existence et d'unicité
- 3.7 Autres exemples de preuves

4 Relations

- 4.1 Paires ordonnées et produits cartésiens
- 4.2 Relations
- 4.3 En savoir plus sur les relations

[4.4 Relations de commande](#)

[4.5 Relations d'équivalence](#)

5 fonctions

[5.1 Fonctions](#)

[5.2 Un à un et sur](#)

[5.3 Inverses de fonctions](#)

[5.4 Fermetures](#)

[5.5 Images et images inversées : un projet de recherche](#)

6 Induction mathématique

[6.1 Preuve par induction mathématique](#)

[6.2 Autres exemples](#)

[6.3 Récursivité](#)

[6.4 Forte induction](#)

[6.5 Fermetures à nouveau](#)

7 Théorie des nombres

[7.1 Plus grands diviseurs communs](#)

[7.2 Factorisation en nombres premiers](#)

[7.3 Arithmétique modulaire](#)

[7.4 Théorème d'Euler](#)

[7.5 Cryptographie à clé publique](#)

8 ensembles infinis

[8.1 Ensembles équinombreux](#)

[8.2 Ensembles dénombrables et indénombrables](#)

[8.3 Le théorème de Cantor-Schröder-Bernstein](#)

[Annexe : Solutions aux exercices sélectionnés](#)

[Suggestions de lectures complémentaires](#)

[Résumé des techniques de preuve](#)

[Indice](#)

Préface de la troisième édition

Les étudiants en mathématiques et en informatique ont souvent du mal la première fois qu'on leur demande de travailler sérieusement sur des preuves mathématiques, car ils ne connaissent pas les « règles du jeu ». Qu'attend-on de vous lorsqu'on vous demande de prouver quelque chose ? Qu'est-ce qui distingue une preuve correcte d'une preuve incorrecte ? Ce livre a pour but d'aider les étudiants à trouver les réponses à ces questions en expliquant les principes fondamentaux de la construction des preuves.

De nombreux élèves découvrent les preuves mathématiques lors d'un cours de géométrie au lycée. Malheureusement, on leur apprend généralement, en géométrie, à considérer une preuve comme une liste numérotée d'énoncés et de raisons, une vision des preuves trop restrictive pour être vraiment utile. Un parallèle avec l'informatique peut être instructif. Les premiers langages de programmation encourageaient une vision tout aussi restrictive des programmes informatiques, considérés comme des listes numérotées d'instructions. Aujourd'hui, les informaticiens se sont éloignés de ces langages et enseignent la programmation en utilisant des langages qui encouragent une approche dite de « programmation structurée ». L'analyse des preuves dans ce livre s'inspire de la conviction que nombre des considérations qui ont conduit les informaticiens à adopter l'approche structurée de la programmation s'appliquent également à la rédaction de preuves. On pourrait dire que ce livre enseigne la « démonstration structurée ».

En programmation structurée, un programme informatique est construit non pas en listant des instructions les unes après les autres, mais en combinant certaines structures de base, telles que la construction if-else et la boucle do-while du langage Java. Ces structures sont combinées, non seulement en les listant les unes après les autres, mais aussi en *les imbriquant* les unes dans les autres. Par exemple, un programme construit en imbriquant une construction if-else dans une boucle do-while ressemblerait à ceci :

faire

si [condition]

[La liste des instructions va ici.]

autre

[La liste alternative des instructions se trouve ici.]

pendant que [condition]

L'indentation dans ce plan de programme n'est pas absolument nécessaire, mais c'est une méthode pratique souvent utilisée en informatique pour afficher la structure sous-jacente d'un programme.

Les preuves mathématiques sont également construites en combinant certaines structures de preuve élémentaires. Par exemple, la preuve d'un énoncé de la forme « si P alors Q » utilise souvent la structure « supposer-jusqu'à » : on *suppose* que P est vrai *jusqu'à ce qu'on parvienne à la conclusion que Q est vrai*, après quoi on rétracte cette supposition et on conclut que l'énoncé « si P alors Q » est vrai. Un autre exemple est la structure « pour x arbitraire, prouver » : pour prouver un énoncé de la forme « pour tout x , $P(x)$ », on *déclare* x être *un objet arbitraire*, puis *prouver* $P(x)$. Une fois que nous concluons que $P(x)$ est vrai, nous retirons la déclaration de x comme arbitraire et concluons que l'affirmation « pour tout x , $P(x)$ » est vraie. De plus, pour prouver des affirmations plus complexes, ces structures sont souvent combinées, non seulement en les listant les unes après les autres, mais aussi en les imbriquant les unes dans les autres. Par exemple, pour prouver une affirmation de la forme « pour tout x , si $P(x)$ alors $Q(x)$ », nous imbriquerions probablement une structure « supposer-jusqu'à » dans une structure « pour prouver x arbitraire », ce qui donnerait une preuve de la forme suivante :

Soit x arbitraire.

Supposons que $P(x)$ soit vrai.

[La preuve de $Q(x)$ va ici.]

Ainsi, si $P(x)$ alors $Q(x)$.

Ainsi, pour tout x , si $P(x)$ alors $Q(x)$.

Comme précédemment, nous avons utilisé l'indentation pour rendre claire la structure sous-jacente de la preuve.

Bien sûr, les mathématiciens n'écrivent généralement pas leurs preuves sous cette forme indentée. Notre objectif dans ce livre est d'apprendre aux élèves à rédiger des preuves dans des paragraphes ordinaires, comme le font les mathématiciens, et non sous cette forme indentée. Néanmoins, notre approche repose sur la conviction que pour réussir à rédiger de telles preuves, les élèves doivent comprendre la structure sous-jacente de ces preuves. Ils doivent apprendre, par exemple, que des phrases comme « Soit x arbitraire » et « Supposons P

» ne sont pas des étapes isolées dans les preuves, mais servent à introduire les structures de preuve « pour x arbitraire, prouver » et « supposer jusqu'à ». C'est Il n'est pas rare que les étudiants débutants utilisent ces phrases de manière inappropriée. De telles erreurs sont comparables à l'erreur de programmation consistant à utiliser un « do » sans « while » correspondant.

Notez que dans nos exemples, le choix de la structure de preuve est guidé par la forme logique de l'énoncé à démontrer. C'est pourquoi le livre commence par la logique élémentaire afin de familiariser les étudiants avec les différentes formes que prennent les énoncés mathématiques. [Le chapitre 1 aborde les connecteurs logiques, et le chapitre 2](#) introduit les quantificateurs . Ces chapitres présentent également les bases de la théorie des ensembles, car il s'agit d'un sujet important qui est abordé dans le reste du livre (et tout au long des mathématiques), et aussi parce qu'il permet d'illustrer de nombreux points de logique abordés dans ces chapitres.

[Le chapitre 3](#) aborde les techniques de démonstration structurées de manière systématique, passant en revue les différentes formes que peuvent prendre les énoncés mathématiques et discutant des structures de démonstration appropriées à chaque forme. Les exemples de démonstration présentés dans ce chapitre sont généralement choisis non pour leur contenu mathématique, mais pour les structures de démonstration qu'ils illustrent. Cela est particulièrement vrai au début du chapitre, où seules quelques techniques de démonstration ont été abordées, et de ce fait, nombre des démonstrations présentées dans cette partie sont plutôt triviales. À mesure que le chapitre progresse, les démonstrations deviennent plus sophistiquées et plus intéressantes, mathématiquement parlant.

[Les chapitres 4 et 5](#), consacrés aux relations et aux fonctions, ont deux objectifs. Premièrement, ils fournissent aux élèves des éléments sur lesquels ils peuvent s'exercer aux techniques de rédaction de preuves du [chapitre 3](#). Deuxièmement, ils leur présentent quelques concepts fondamentaux utilisés dans toutes les branches des mathématiques.

[Le chapitre 6](#) est consacré à une méthode de preuve essentielle en mathématiques et en informatique : l'induction mathématique. La présentation s'appuie sur les techniques du [chapitre 3](#), que les élèves devraient maîtriser à ce stade du livre.

Après avoir terminé [le chapitre 6](#), les élèves devraient être prêts à aborder des sujets mathématiques plus approfondis. Deux de ces sujets sont présentés aux chapitres [7](#) et [8](#). [Le chapitre 7](#), nouveau dans cette troisième édition, propose une introduction à la théorie des nombres, et [le chapitre 8](#) aborde les cardinalités infinies. Ces chapitres permettent aux élèves de s'exercer davantage aux démonstrations

mathématiques et offrent également un aperçu des mathématiques plus avancées.

Chaque section de chaque chapitre se termine par une liste d'exercices. Certains exercices sont signalés par un astérisque ; les solutions ou les indices correspondants sont fournis en annexe. Les exercices signalés par le symbole P.D peuvent être réalisés à l'aide du logiciel Proof Designer, disponible gratuitement sur Internet.

Les principaux changements de cette troisième édition sont l'ajout d'un nouveau chapitre sur la théorie des nombres et de plus de 150 exercices supplémentaires. La section sur les fermetures réflexives, symétriques et transitives des relations a été supprimée du [chapitre 4](#) (bien que ces sujets soient désormais abordés dans certains exercices de [la section 4.4](#)) ; elle a été remplacée par une nouvelle section au [chapitre 5](#) sur les fermetures d'ensembles par des fonctions. De nombreux petits changements ont également été apportés au texte.

Je tiens à remercier tous ceux qui m'ont fait part de leurs commentaires sur les précédentes éditions de ce livre. John Corcoran et Raymond Boute ont notamment formulé plusieurs suggestions utiles. Je suis également reconnaissant à Jonathan Sands et à plusieurs relecteurs anonymes pour leurs conseils.

Introduction

Qu'est-ce que les mathématiques ? Au lycée, les mathématiques s'intéressent principalement à la résolution d'équations et au calcul des réponses à des questions numériques. À l'université, les mathématiques abordent une plus grande variété de questions, impliquant non seulement les nombres, mais aussi les ensembles, les fonctions et d'autres objets mathématiques. Leur point commun est l'utilisation du *raisonnement déductif* pour trouver les réponses aux questions. Résoudre une équation pour x , c'est utiliser les informations fournies par l'équation pour *déduire* la valeur de x . De même, lorsque les mathématiciens résolvent d'autres types de problèmes mathématiques, ils justifient toujours leurs conclusions par le raisonnement déductif.

Le raisonnement déductif en mathématiques se présente généralement sous la forme d'une *preuve*. L'un des principaux objectifs de ce livre est de vous aider à développer votre capacité de raisonnement mathématique en général, et en particulier votre capacité à lire et à écrire des preuves. Dans les chapitres suivants, nous étudierons en détail la construction des preuves, mais examinons d'abord quelques exemples.

Ne vous inquiétez pas si vous avez du mal à comprendre ces démonstrations. Elles ont simplement pour but de vous donner un aperçu de ce que sont les démonstrations mathématiques. Dans certains cas, vous pourrez suivre de nombreuses étapes de la démonstration, mais vous vous demanderez peut-être pourquoi elles sont combinées ainsi, ou comment quelqu'un a pu concevoir la démonstration. Si c'est le cas, nous vous demandons de faire preuve de patience. Nombre de ces questions trouveront des réponses plus loin dans ce livre, notamment au [chapitre 3](#).

Tous les exemples de démonstration de cette introduction porteront sur des nombres premiers. Rappelons qu'un entier supérieur à 1 est dit *premier* s'il ne peut pas s'écrire comme le produit de deux entiers positifs plus petits. S'il peut s'écrire comme le produit de deux entiers positifs plus petits, alors il est *composé*. Par exemple, 6 est un nombre composé, puisque $6 = 2 \cdot 3$, mais 7 est un nombre premier.

Avant de donner un exemple de preuve impliquant des nombres premiers, il nous faut trouver quelque chose à prouver : un fait concernant les nombres premiers dont l'exactitude peut être vérifiée par une preuve. On peut parfois découvrir des schémas mathématiques intéressants en effectuant un calcul sur quelques nombres. Prenons par exemple le tableau de [la figure I.1](#). Pour chaque entier n compris entre 2 et 10, le tableau indique si n et $2^n - 1$ sont tous deux premiers, et un schéma surprenant apparaît. Il apparaît que $2^n - 1$ est premier précisément dans les cas où n est premier !

n	Is n prime?	$2^n - 1$	Is $2^n - 1$ prime?
2	yes	3	yes
3	yes	7	yes
4	no: $4 = 2 \cdot 2$	15	no: $15 = 3 \cdot 5$
5	yes	31	yes
6	no: $6 = 2 \cdot 3$	63	no: $63 = 7 \cdot 9$
7	yes	127	yes
8	no: $8 = 2 \cdot 4$	255	no: $255 = 15 \cdot 17$
9	no: $9 = 3 \cdot 3$	511	no: $511 = 7 \cdot 73$
10	no: $10 = 2 \cdot 5$	1023	no: $1023 = 31 \cdot 33$

Figure I.1.

Cette tendance va-t-elle perdurer ? On est tenté de la supposer, mais ce n'est qu'une supposition. Les mathématiciens appellent ces suppositions des *conjectures*. Ainsi, nous avons les deux conjectures suivantes :

Conjecture 1. Supposer n est un entier supérieur à 1 et n est premier. Alors $2^n - 1$ est premier .

Conjecture 2. Supposer n est un entier supérieur à 1 et n n'est pas premier. Alors $2^n - 1$ n'est pas premier .

Malheureusement, si l'on poursuit le tableau de [la figure I.1](#), on constate immédiatement que la conjecture 1 est incorrecte. Il est facile de vérifier que 11 est premier, mais $2^{11} - 1 = 2047 = 23 \cdot 89$, donc $2^{11} - 1$ est composé. Ainsi, 11 est un *contre-exemple* à la conjecture 1. L'existence d'un seul contre-exemple suffit à prouver que la conjecture est incorrecte, mais il est intéressant de noter que dans ce cas, il existe de nombreux contre-exemples. Si l'on poursuit l'analyse des nombres jusqu'à 30, on trouve deux autres contre-exemples à la conjecture 1 : 23 et 29 sont tous deux premiers, mais $2^{23} - 1 = 8\ 388\ 607 = 47 \cdot 178\ 481$ et $2^{29} - 1 = 536\ 870\ 911 = 2\ 089 \cdot 256\ 999$. Cependant, aucun nombre jusqu'à 30 ne constitue un contre-exemple à la conjecture 2.

Pensez-vous que la conjecture 2 est correcte ? Ayant trouvé des contre-exemples à la conjecture 1, nous savons que cette conjecture est incorrecte, mais notre incapacité à trouver un contre-exemple à la conjecture 2 ne prouve pas qu'elle soit correcte. Il existe peut-être des

contre-exemples, mais le plus petit est supérieur à 30. Continuer à vérifier les exemples pourrait révéler un contre-exemple, ou, s'il n'en trouve pas, il pourrait le révéler. Augmenter notre confiance dans la conjecture. Cependant, nous ne pouvons jamais être sûrs de sa validité en nous contentant de vérifier des exemples. Quel que soit le nombre d'exemples vérifiés, il est toujours possible que le suivant soit le premier contre-exemple. La seule façon de garantir la validité de la conjecture 2 est de la prouver.

En fait, la conjecture 2 est correcte. Voici sa preuve :

Preuve de la conjecture 2. Puisque n n'est pas premier, il existe des entiers positifs a et b tels que $a < n$, $b < n$ et $n = ab$. Soit $x = 2^b - 1$ et $y = 1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}$. Alors

$$\begin{aligned} xy &= (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= 2^b \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= (2^b + 2^{2b} + 2^{3b} + \dots + 2^{ab}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= 2^{ab} - 1 \\ &= 2^n - 1. \end{aligned}$$

Puisque $b < n$, nous pouvons conclure que $x = 2^b - 1 < 2^n - 1$. De plus, puisque $ab = n > a$, il s'ensuit que $b > 1$. Par conséquent, $x = 2^b - 1 > 2^1 - 1 = 1$, donc $y < xy = 2^n - 1$. Ainsi, nous avons montré que $2^n - 1$ peut s'écrire comme le produit de deux entiers positifs x et y , tous deux plus petits que $2^n - 1$, donc $2^n - 1$ n'est pas premier.

□

Maintenant que la conjecture est prouvée, on peut la qualifier de *théorème*. Ne vous inquiétez pas si la preuve vous paraît un peu mystérieuse. Nous y reviendrons à la fin du [chapitre 3](#) pour analyser sa construction. Pour l'instant, le point le plus important à comprendre est que si n est un entier supérieur à 1 pouvant s'écrire comme un produit de deux entiers positifs plus petits a et b , alors la preuve donne une méthode (certes mystérieuse) pour écrire $2^n - 1$ comme un produit de deux entiers positifs plus petits x et y . Ainsi, si n n'est pas premier, alors $2^n - 1$ ne doit pas non plus l'être. Par exemple, supposons que $n = 12$, donc $2^n - 1 = 4095$. Puisque $12 = 3 \cdot 4$, on pourrait prendre $a = 3$ et $b = 4$ dans la preuve. Français Ensuite, selon les formules pour x et y données dans la preuve, nous aurions $x = 2^b - 1 = 2^4 - 1 = 15$ et $y = 1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b} = 1 + 2^4 + 2^8 = 273$. Et, tout comme les formules dans la preuve le prédisent, nous avons $xy = 15 \cdot 273 = 4095 = 2^n - 1$. Bien sûr, il existe d'autres façons de factoriser 12 en un produit de deux entiers plus petits, et celles-ci pourraient

conduire à d'autres façons de factoriser 4095. Par exemple, puisque $12 = 2 \cdot 6$, nous pourrions utiliser les valeurs $a = 2$ et $b = 6$. Essayez de calculer les valeurs correspondantes de x et y et assurez-vous que leur produit est 4095.

Bien que nous sachions déjà que la conjecture 1 est incorrecte, des questions intéressantes peuvent encore se poser à son sujet. Si nous continuons à vérifier si 2^{n-1} est premier pour les nombres premiers n , trouverons-nous encore des contre-exemples à cette conjecture – des exemples où $2^n - 1$ n'est pas premier ? Continuerons-nous à trouver des exemples où $2^n - 1$ est premier ? S'il n'existe qu'un nombre fini de nombres premiers, nous pourrions peut-être répondre à ces questions en vérifiant simplement $2^n - 1$ pour tout nombre premier n . Mais en réalité, il existe une infinité de nombres premiers. Euclide (vers 300 av. J.-C.) en a donné une preuve dans le livre IX de ses *Éléments*. Sa démonstration est l'une des plus célèbres de toutes les mathématiques :[1](#)

Théorème 3. *Il existe une infinité de nombres premiers.*

Preuve . Supposons qu'il n'y ait qu'un nombre fini de nombres premiers. Soit p_1, p_2, \dots, p_n une liste de tous les nombres premiers. Soit $m = p_1 p_2 \cdots p_n + 1$. Notons que m n'est pas divisible par p_1 , puisque diviser m par p_1 donne un quotient de $p_2 p_3 \cdots p_n$ et un reste de 1. De même, m n'est divisible par aucun des nombres p_2, p_3, \dots, p_n .

Nous utilisons maintenant le fait que tout entier supérieur à 1 est soit premier, soit peut s'écrire comme un produit de deux ou plusieurs nombres premiers. (Nous verrons une démonstration de ce fait au [chapitre 6](#) – voir [le théorème 6.4.2](#).) De toute évidence, m est supérieur à 1, donc m est soit premier, soit un produit de nombres premiers. Supposons d'abord que m soit premier. Notons que m est supérieur à tous les nombres de la liste p_1, p_2, \dots, p_n , nous avons donc trouvé un nombre premier qui ne figure pas dans cette liste. Mais cela contredit notre hypothèse selon laquelle il s'agissait d'une liste de *tous* les nombres premiers.

Supposons maintenant que m soit un produit de nombres premiers. Soit q l'un des nombres premiers de ce produit. Alors m est divisible par q . Or, nous avons déjà vu que m n'est divisible par aucun des nombres de la liste p_1, p_2, \dots, p_n , ce qui contredit à nouveau l'hypothèse selon laquelle cette liste inclurait tous les nombres premiers.

Puisque l'hypothèse selon laquelle il existe un nombre fini de nombres premiers a conduit à une contradiction, il doit y avoir une infinité de nombres premiers.

□

Encore une fois, ne vous inquiétez pas si certains aspects de cette preuve vous semblent mystérieux. Après avoir lu [le chapitre 3](#), vous serez mieux préparé à la comprendre en détail. Nous y reviendrons ensuite et analyserons sa structure.

Nous avons vu que si n n'est pas premier, alors $2^n - 1$ ne peut pas l'être, mais si n est premier, alors $2^n - 1$ peut être premier ou composé. Puisqu'il existe une infinité de nombres premiers, il existe une infinité de nombres de la forme $2^n - 1$ qui, d'après nos connaissances actuelles, *pourraient* être premiers. Mais combien d'entre eux *sont* premiers ?

Les nombres premiers de la forme $2^n - 1$ sont appelés *nombre premiers de Mersenne*, du nom du père Marin Mersenne (1588–1648), moine et érudit français qui les a étudiés. Bien que de nombreux nombres premiers de Mersenne aient été découverts, on ignore encore s'il en existe une infinité. Nombre des plus grands nombres premiers connus sont des nombres premiers de Mersenne. À la date de rédaction de cet article (février 2019), le plus grand nombre premier connu est le nombre premier de Mersenne $2^{82\,589\,933} - 1$, un nombre à 24 862 048 chiffres.

Les nombres premiers de Mersenne sont apparentés aux nombres parfaits, sujet d'un autre célèbre problème mathématique non résolu. Un entier positif n est dit *parfait* si n est égal à la somme de tous les entiers positifs inférieurs à n qui divisent n . (Pour deux entiers m et n *quelconques*, on dit que m *divise* n si n est divisible par m ; autrement dit, s'il existe un entier q tel que $n = qm$.) Par exemple, les seuls entiers positifs inférieurs à 6 qui divisent 6 sont 1, 2 et 3, et $1 + 2 + 3 = 6$. Ainsi, 6 est un nombre parfait. Le nombre parfait immédiatement inférieur est 28. (Vous devriez vérifier par vous-même que 28 est parfait en trouvant tous les entiers positifs inférieurs à 28 qui divisent 28 et en les additionnant.)

Euclide a prouvé que si $2^n - 1$ est premier, alors $2^{n-1}(2^n - 1)$ est parfait. Ainsi, tout nombre premier de Mersenne donne naissance à un nombre parfait. De plus, environ 2000 ans après la démonstration d'Euclide, le mathématicien suisse Leonhard Euler (1707–1783), le mathématicien le plus prolifique de l'histoire, a prouvé que tout nombre pair parfait apparaît de cette manière. (Par exemple, notez que $6 = 2^1(2^2 - 1)$ et $28 = 2^2(2^3 - 1)$.) Comme on ne sait pas s'il existe une infinité de nombres premiers de Mersenne, on ne sait pas non plus s'il

existe une infinité de nombres pairs parfaits. On ne sait pas non plus s'il existe des nombres parfaits impairs. Pour les démonstrations des théorèmes d'Euclide et d'Euler, voir [les exercices 18 et 19 de la section 7.4](#).

Bien qu'il existe une infinité de nombres premiers, leur nombre diminue à mesure que l'on considère des nombres de plus en plus grands. Par exemple, il existe 25 nombres premiers entre 1 et 100, 16 nombres premiers entre 1 001 et 1 100, et seulement six nombres premiers entre 1 000 001 et 1 000 100. Comme dernier exemple introductif de démonstration, nous montrons qu'il existe de longues séquences d'entiers positifs consécutifs ne contenant aucun nombre premier. Dans cette démonstration, nous utiliserons la terminologie suivante : pour tout entier positif n , le produit de tous les entiers de 1 à n est appelé n . *factorielle et est notée $n!$* . Ainsi, $n! = 1 \cdot 2 \cdot 3 \cdots n$. Comme pour nos deux précédentes démonstrations, nous reviendrons sur cette démonstration à la fin du [chapitre 3](#) pour analyser sa structure.

Théorème 4. *Pour tout entier positif n , il existe une séquence de n consécutifs entiers positifs ne contenant aucun nombre premier.*

Preuve. Supposons que n soit un entier strictement positif. Soit $x = (n+1)! + 2$. Nous allons montrer qu'aucun des nombres $x, x+1, x+2, \dots, x+(n-1)$ n'est premier. Puisqu'il s'agit d'une suite de n entiers strictement positifs consécutifs, ceci démontrera le théorème.

Pour voir que x n'est pas premier, notez que

$$\begin{aligned} x &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 2 \\ &= 2 \cdot (1 \cdot 3 \cdot 4 \cdots (n+1) + 1). \end{aligned}$$

Ainsi, x peut être écrit comme un produit de deux entiers positifs plus petits, donc x n'est pas premier.

De même, nous avons

$$\begin{aligned} x+1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 3 \\ &= 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n+1) + 1), \end{aligned}$$

Donc $x+1$ n'est pas premier non plus. En général, considérons tout nombre $x+i$, où $0 \leq i \leq n-1$. On a alors

$$\begin{aligned} x+i &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + (i+2) \\ &= (i+2) \cdot (1 \cdot 2 \cdot 3 \cdots (i+1) \cdot (i+3) \cdots (n+1) + 1), \end{aligned}$$

donc $x+i$ n'est pas premier.

□

Le théorème 4 montre qu'il existe parfois de longs intervalles entre deux nombres premiers. Mais il arrive aussi que des nombres premiers

soient proches les uns des autres. Puisque 2 est le seul nombre premier pair, la seule paire d'entiers consécutifs qui soient tous deux premiers est 2 et 3. Or, de nombreuses paires de nombres premiers ne diffèrent que de deux, par exemple 5 et 7, 29 et 31, et 7949 et 7951. Ces paires de nombres premiers sont appelées *nombres premiers jumeaux*. On ignore s'il existe une infinité de nombres premiers jumeaux.

Récemment, des progrès significatifs ont été réalisés sur la question des nombres premiers jumeaux. En 2013, Yitang Zhang (1955-) a prouvé qu'il existe un entier positif $d \leq 70\,000\,000$ tel qu'il existe une infinité de paires de nombres premiers différant de d . Les travaux de nombreux autres mathématiciens en 2013-2014 ont réduit les possibilités pour d à $d \leq 246$. Bien sûr, si l'affirmation est vraie avec $d = 2$, alors il existe une infinité de nombres premiers jumeaux.

Exercices

Remarque : Les solutions ou indices pour les exercices marqués d'un astérisque (*) sont donnés en annexe.

- *1. (a) Factorisez $2^{15} - 1 = 32\,767$ en un produit de deux entiers positifs plus petits.
(b) Trouvez un entier x tel que $1 < x < 2^{32\,767} - 1$ et $2^{32\,767} - 1$ soit divisible par x .
- 2. Émettez des conjectures sur les valeurs de n pour lesquelles $3^n - 1$ est premier ou sur les valeurs de n pour lesquelles $3^n - 2^n$ est premier. (Vous pouvez commencer par créer un tableau similaire à [la figure I.1](#).)
- *3. La preuve du théorème 3 donne une méthode pour trouver un nombre premier différent de n'importe quel nombre premier dans une liste donnée de nombres premiers.
 - (a) Utilisez cette méthode pour trouver un nombre premier différent de 2, 3, 5 et 7.
 - (b) Utilisez cette méthode pour trouver un nombre premier différent de 2, 5 et 11.
- 4. Trouvez cinq entiers consécutifs qui ne sont pas premiers.
- 5. Utilisez le tableau de [la figure I.1](#) et la discussion de la p. 5 pour trouver deux autres nombres parfaits.
- 6. La suite 3, 5, 7 est une liste de trois nombres premiers tels que chaque paire de nombres adjacents diffère de deux. Existe-t-il d'autres nombres premiers triplets de ce type ?

7. Une paire d'entiers positifs distincts (m , n) est dite *amicale* si la somme de tous les entiers positifs inférieurs à n qui divisent n est égale à m , et la somme de tous les entiers positifs inférieurs à m qui divisent m est égale à n . Montrer que (220, 284) est amicale.

[Euclide](#) a formulé le théorème et la démonstration de manière quelque peu différente. Nous avons choisi d'adopter une approche plus moderne dans notre présentation.

1

Logique des phrases

1.1 Raisonnement déductif et connecteurs logiques

Comme nous l'avons vu dans l'introduction, les preuves jouent un rôle central en mathématiques, et le raisonnement déductif en est le fondement. Par conséquent, nous commençons notre étude du raisonnement et des preuves mathématiques en examinant le fonctionnement du raisonnement déductif.

Exemple 1.1.1. Voici trois exemples de raisonnement déductif :

1. Il pleuvra ou il neigera demain.
Il fait trop chaud pour qu'il neige.
Par conséquent, il pleuvra.
2. Si c'est dimanche aujourd'hui, je n'ai pas besoin d'aller travailler aujourd'hui.
Aujourd'hui est dimanche.
Je n'ai donc pas besoin d'aller travailler aujourd'hui.
3. J'irai travailler demain ou aujourd'hui.
Je vais rester à la maison aujourd'hui.
Donc, j'irai travailler demain.

Dans chaque cas, nous sommes arrivés à une *conclusion* en supposant que d'autres affirmations, appelées *prémisses*, sont vraies. Par exemple, les prémisses de l'argument 3 sont les affirmations « J'irai travailler demain ou aujourd'hui » et « Je resterai à la maison aujourd'hui ». La conclusion est « J'irai travailler demain », et elle semble nous être imposée d'une manière ou d'une autre par les prémisses.

Mais cette conclusion est-elle vraiment correcte ? Après tout, n'est-il pas possible que je reste à la maison aujourd'hui, puis que je me réveille malade demain et que je finisse par rester à nouveau à la maison ? Si cela se produisait, la conclusion se révélerait fausse. Mais remarquez que dans ce cas, la première prémissse, qui disait que j'irais travailler

demain ou aujourd'hui, serait également fausse ! Bien que nous n'ayons aucune garantie que la conclusion soit vraie, elle ne peut être fausse que si au moins une des prémisses est également fausse. Si les deux prémisses sont vraies, nous pouvons être sûrs que la conclusion l'est également. C'est en ce sens que la conclusion nous est imposée par les prémisses, et c'est le critère que nous utiliserons pour juger de la justesse du raisonnement déductif. Nous dirons qu'un argument est *valide* si les prémisses ne peuvent pas toutes être vraies sans que la conclusion ne le soit également. Les trois arguments de notre exemple sont des arguments valides.

Voici un exemple d'argument déductif invalide :

Soit le majordome est coupable, soit la femme de chambre est coupable.

Soit la femme de ménage est coupable, soit la cuisinière est coupable.

Par conséquent, soit le majordome est coupable, soit le cuisinier est coupable.

L'argument est invalide car la conclusion pourrait être fausse même si les deux prémisses sont vraies. Par exemple, si la servante était coupable, mais que le majordome et le cuisinier étaient tous deux innocents, alors les deux prémisses seraient vraies et la conclusion serait fausse.

On peut comprendre la validité d'un argument en comparant les trois arguments de [l'exemple 1.1.1](#). À première vue, les arguments 2 et 3 pourraient sembler les plus communs, car ils portent sur le même sujet : l'assiduité au travail. Mais en termes de raisonnement, les arguments 1 et 3 sont les plus similaires. Ils introduisent tous deux deux possibilités dans la première prémissé, excluent la seconde avec la seconde, puis concluent que la première possibilité doit être vérifiée. Autrement dit, les deux arguments ont la forme suivante :

P ou Q .

Pas Q .

Par conséquent, P .

C'est cette forme, et non le sujet, qui valide ces arguments. On peut constater que l'argument 1 a cette forme en considérant la lettre P comme « Il pleuvra demain » et la lettre Q comme « Il neigera demain ». Pour l'argument 3, P signifierait « J'irai travailler demain » et Q « J'irai travailler aujourd'hui ».

Remplacer certaines affirmations de chaque argument par des lettres, comme nous l'avons fait pour la forme des arguments 1 et 3, présente deux avantages. Premièrement, cela nous évite d'être distraits par des aspects des arguments qui n'affectent pas leur validité. Il n'est

pas nécessaire d'avoir des connaissances en météorologie ou en habitudes de travail pour reconnaître la validité des arguments 1 et 3. En effet, les deux arguments ont la forme présentée précédemment, et on peut en déduire que cet argument est valide. La forme est valide sans même connaître les significations *de P et Q*. Si vous n'y croyez pas, considérez l'argument suivant :

Soit le widget framger ne fonctionne pas correctement, soit le mécanisme wrompal est mal aligné.

J'ai vérifié l'alignement du mécanisme wrompal, et tout va bien.

Par conséquent, le widget framger ne fonctionne pas correctement.

Si un mécanicien vous donnait cette explication après avoir examiné votre voiture, vous seriez peut-être encore perplexe quant à la raison pour laquelle la voiture ne démarre pas, mais vous n'auriez aucun mal à suivre sa logique !

Plus important encore, notre analyse des formes des arguments 1 et 3 met en évidence ce qui *est* important pour déterminer leur validité : les mots « *or* » et « *not* ». Dans la plupart des raisonnements déductifs, et en particulier dans le raisonnement mathématique, la signification de quelques mots seulement nous donne la clé pour comprendre ce qui rend un raisonnement valide ou invalide. (Quels sont les mots importants dans l'argument 2 de [l'exemple 1.1.1](#) ?) Les premiers chapitres de ce livre sont consacrés à l'étude de ces mots et à leur utilisation dans l'écriture et le raisonnement mathématiques.

Dans ce chapitre, nous nous concentrerons sur les mots utilisés pour combiner des affirmations et former des phrases plus complexes. Nous continuerons d'utiliser des lettres pour représenter des affirmations, mais uniquement pour les affirmations non ambiguës, vraies ou fausses. Les questions, les exclamations et les affirmations vagues seront interdites. Il sera également utile d'utiliser des symboles, parfois appelés *symboles de connexion*, pour représenter certains mots utilisés pour combiner des affirmations. Voici nos trois premiers symboles de connexion et les mots qu'ils représentent :

Symbol	Meaning
\vee	or
\wedge	and
\neg	not

Ainsi, si P et Q représentent deux énoncés, alors nous écrirons $P \vee Q$ pour représenter l'énoncé « P ou Q », $P \wedge Q$ pour « P et Q » et $\neg P$ pour « pas P » ou « P est faux ». L'énoncé $P \vee Q$ est parfois appelé la *disjonction* de P et Q , $P \wedge Q$ est appelé la *conjonction* de P et Q , et $\neg P$ est appelé la *négation* de P .

Exemple 1.1.2. Analyser les formes logiques des énoncés suivants :

1. Soit John est allé au magasin, soit nous n'avons plus d'œufs.
2. Joe va quitter la maison et ne pas revenir.
3. Soit Bill est au travail et Jane ne l'est pas, soit Jane est au travail et Bill ne l'est pas.

Solutions

1. Si nous laissons P représenter l'énoncé « John est allé au magasin » et Q « Nous n'avons plus d'œufs », alors cet énoncé pourrait être représenté symboliquement par $P \vee Q$.
2. Si l'on considère P comme l'affirmation « Joe va quitter la maison » et Q comme « Joe ne reviendra pas », on pourrait représenter symboliquement cette affirmation par $P \wedge Q$. Cependant, cette analyse omet une caractéristique importante de l'affirmation : elle n'indique pas que Q est une affirmation négative. On pourrait obtenir une meilleure analyse en considérant R comme l'affirmation « Joe va revenir », puis en écrivant Q sous la forme $\neg R$. En intégrant cela à notre première analyse de l'affirmation initiale, on obtient l'analyse améliorée $P \wedge \neg R$.
3. Soit B l'énoncé « Bill est au travail » et J l'énoncé « Jane est au travail ». La première moitié de l'énoncé, « Bill est au travail et Jane non », peut alors être représentée par $B \wedge \neg J$. De même, la seconde moitié est $J \wedge \neg B$. Pour représenter l'énoncé complet, il faut combiner ces deux équations avec *ou*, formant ainsi leur disjonction. La solution est donc $(B \wedge \neg J) \vee (J \wedge \neg B)$.

Notez qu'en analysant la troisième affirmation de l'exemple précédent, nous avons ajouté des parenthèses lors de la disjonction de $B \wedge \neg J$ et $J \wedge \neg B$ afin d'indiquer sans ambiguïté les affirmations combinées. Ceci est similaire à l'utilisation des parenthèses en algèbre : par exemple, le produit de $a + b$ par $a - b$ s'écrirait $(a + b) \cdot (a - b)$, les parenthèses servant à indiquer sans ambiguïté les quantités à multiplier. Comme en algèbre, il est pratique en logique d'omettre certaines parenthèses pour raccourcir et faciliter la lecture de nos expressions. Cependant, il est nécessaire de convenir de certaines conventions de lecture de ces expressions afin qu'elles restent sans ambiguïté. L'une d'elles est que le symbole \neg ne s'applique qu'à l'affirmation qui le suit immédiatement. Par exemple, $\neg P \wedge Q$ signifie $(\neg P) \wedge Q$ plutôt que $\neg(P \wedge Q)$. Nous verrons d'autres conventions concernant les parenthèses plus tard.

Exemple 1.1.3. Quelles phrases anglaises sont représentées par les expressions suivantes ?

1. $(\neg S \wedge L) \vee S$, où S signifie « John est intelligent » et L signifie « John a de la chance ».

2. $\neg S \wedge (L \vee S)$, où S et L ont les mêmes significations que précédemment.

3. $\neg(S \wedge L) \vee S$, avec S et L toujours comme avant.

Solutions

1. Soit John n'est pas intelligent et il a de la chance, soit il est intelligent.
2. John n'est pas intelligent, et soit il a de la chance, soit il est intelligent.
Remarquez comment la place du mot « *either* » en anglais change selon l'emplacement des parenthèses.
3. Soit John n'est ni intelligent ni chanceux, soit John est intelligent. Le mot « *both* » en anglais permet également de distinguer les différentes positions possibles des parenthèses.

Il est important de garder à l'esprit que les symboles \wedge , \vee et \neg ne correspondent pas vraiment à tous les usages des mots *and*, *or*, *and* en *anglais*. Par exemple, le symbole \wedge ne pourrait pas être utilisé pour représenter l'emploi du mot *and* dans la phrase « John et Bill sont amis », car dans cette phrase, le mot *and* n'est pas utilisé pour combiner deux énoncés. Les symboles \wedge et \vee ne peuvent être utilisés *qu'entre deux énoncés*, pour former leur conjonction ou leur disjonction, et le symbole \neg ne peut être utilisé *qu'avant un énoncé*, pour le nier. Cela signifie que certaines chaînes de lettres et de symboles sont tout simplement dénuées de sens. Par exemple, $P \neg \wedge Q$, $P \wedge \vee Q$ et $P \neg Q$ sont toutes des expressions « *agrammaticales* » en langage logique. Les expressions « *grammaticales* », comme celles des [exemples 1.1.2](#) et [1.1.3](#), sont parfois appelées *formules bien formées* ou simplement *formules*. Là encore, il peut être utile de faire une analogie avec l'algèbre : les symboles $+$, $-$, \cdot et \div peuvent être utilisés *entre deux nombres* comme opérateurs, et le symbole $-$ peut également être utilisé *devant un nombre* pour le nier. Ce sont les seules façons d'utiliser ces symboles en algèbre ; des expressions comme $x - \div y$ sont donc dénuées de sens.

Parfois, d'autres mots que *et*, *ou* et *non* sont utilisés pour exprimer les significations représentées par \wedge , \vee et \neg . Par exemple, considérons la première affirmation de [l'exemple 1.1.3](#). Bien que nous ayons donné la traduction anglaise « Soit John n'est pas intelligent et il a de la chance, soit il est intelligent », une autre façon de transmettre la même information serait de dire « Soit John n'est pas intelligent *mais* il a de la chance, soit il est intelligent ». Souvent, le mot « *mais* » est utilisé en anglais pour signifier *et*, surtout lorsqu'il existe un contraste ou un conflit entre les affirmations combinées. Pour un exemple plus frappant, imaginez un météorologue terminant ses prévisions par l'affirmation « La pluie et la neige sont les deux seules possibilités pour le temps de demain. » Il s'agit simplement d'une façon détournée de

dire qu'il pleuvra ou qu'il neigera demain. Ainsi, même si le météorologue a utilisé le mot *et*, le sens exprimé par son affirmation est une disjonction. La leçon de ces exemples est que pour déterminer la forme logique d'une déclaration, vous devez réfléchir à ce que signifie la déclaration, plutôt que de simplement traduire mot pour mot en symboles.

Parfois, des mots logiques sont cachés dans la notation mathématique. Prenons l'exemple de l'énoncé $3 \leq \pi$. Bien qu'il semble simple et ne contienne aucun mot de logique, sa lecture à voix haute permet d'entendre le mot *ou*. Si P représente l'énoncé $3 < \pi$ et Q l'énoncé $3 = \pi$, alors l'énoncé $3 \leq \pi$ s'écrirait $P \vee Q$. Dans cet exemple, les énoncés représentés par les lettres P et Q sont si courts qu'il semble peu utile de les abréger par une seule lettre. Dans ce cas, on ne se préoccupera pas toujours de les remplacer par des lettres ; on pourrait donc écrire cet énoncé ainsi : $(3 < \pi) \vee (3 = \pi)$.

Pour un exemple un peu plus compliqué, considérons l'énoncé $3 \leq \pi < 4$. Cet énoncé signifie $3 \leq \pi$ et $\pi < 4$, donc une fois de plus, un mot de logique a été caché dans la notation mathématique. En complétant le sens que nous venons de déterminer pour $3 \leq \pi$, nous pouvons écrire l'énoncé complet comme $[(3 < \pi) \vee (3 = \pi)] \wedge (\pi < 4)$. Savoir que l'énoncé a cette forme logique peut être important pour comprendre un raisonnement mathématique impliquant cet énoncé.

Exercices

*1. Analysez les formes logiques des énoncés suivants :

- (a) Nous aurons soit un devoir de lecture, soit des devoirs à faire à la maison, mais nous n'aurons pas à la fois des devoirs à faire à la maison et un test.
- (b) Tu n'iras pas skier, ou tu le feras et il n'y aura pas de neige.
- (c) $\sqrt{7} \leq 2$.

2. Analysez les formes logiques des énoncés suivants :

- (a) Soit John et Bill disent tous les deux la vérité, soit aucun des deux ne le dit.
- (b) Je prendrai soit du poisson, soit du poulet, mais je ne prendrai pas à la fois du poisson et de la purée de pommes de terre.
- (c) 3 est un diviseur commun de 6, 9 et 15.

3. Analysez les formes logiques des énoncés suivants :

- (a) Alice et Bob ne sont pas tous les deux dans la pièce.
- (b) Alice et Bob ne sont pas tous les deux dans la pièce.
- (c) Soit Alice, soit Bob n'est pas dans la pièce.
- (d) Ni Alice ni Bob ne sont dans la pièce.

4. Analysez les formes logiques des énoncés suivants :

- (a) Soit Ralph et Ed sont tous les deux grands, soit ils sont tous les deux beaux.
- (b) Ralph et Ed sont tous les deux grands ou beaux.
- (c) Ralph et Ed ne sont ni grands ni beaux.
- (d) Ni Ralph ni Ed ne sont à la fois grands et beaux.

5. Lesquelles des expressions suivantes sont des formules bien formées ?

- (a) $\neg(\neg P \vee \neg R)$.
- (b) $\neg(P, Q, \wedge R)$.
- (c) $P \wedge \neg P$.
- (d) $(P \wedge Q)(P \vee R)$.

*6. Soit P pour l'affirmation « J'achèterai le pantalon » et S pour l'affirmation « J'achèterai la chemise ». Quelles phrases anglaises sont représentées par les formules suivantes ?

- (a) $\neg(P \wedge \neg S)$.
- (b) $\neg P \wedge \neg S$.
- (c) $\neg P \vee \neg S$.

7. Soit S pour l'affirmation « Steve est heureux » et G pour « George est heureux ». Quelles phrases anglaises sont représentées par les formules suivantes ?

- (a) $(S \vee G) \wedge (\neg S \vee \neg G)$.
- (b) $[S \vee (G \wedge \neg S)] \vee \neg G$.
- (c) $S \vee [G \wedge (\neg S \vee \neg G)]$.

8. Soit T pour l'affirmation « Les impôts vont augmenter » et D pour « Le déficit va augmenter ». Quelles phrases anglaises sont représentées par les formules suivantes ?

- (a) $T \vee D$.
- (b) $\neg(T \wedge D) \wedge \neg(\neg T \wedge \neg D)$.
- (c) $(T \wedge \neg D) \vee (D \wedge \neg T)$.

9. Identifiez les prémisses et les conclusions des arguments déductifs suivants et analysez leurs formes logiques. Pensez-vous que le raisonnement est valide ? (Bien que votre seule intuition vous guide pour répondre à cette dernière question, nous développerons dans la section suivante quelques techniques pour déterminer la validité des arguments.)

- (a) Jane et Pete ne gagneront pas tous les deux le prix de mathématiques. Pete gagnera soit le prix de mathématiques, soit le prix de chimie. Jane gagnera le prix de mathématiques. Par conséquent, Pete gagnera le prix de chimie.
- (b) Le plat principal sera soit du bœuf, soit du poisson. Le légume sera soit des petits pois, soit du maïs. Nous ne mangerons pas à la fois

du poisson et du maïs. Par conséquent, nous ne mangerons pas à la fois du bœuf et des petits pois.

- (c) Soit John, soit Bill dit la vérité. Soit Sam, soit Bill ment. Par conséquent, soit John dit la vérité, soit Sam ment.
- (d) Soit les ventes augmenteront et le patron sera content, soit les dépenses augmenteront et le patron ne sera pas content. Par conséquent, les ventes et les dépenses n'augmenteront pas toutes les deux.

1.2 Tables de vérité

Nous avons vu dans [la section 1.1](#) qu'un argument est valide si les prémisses ne peuvent pas toutes être vraies sans que la conclusion ne le soit également. Ainsi, pour comprendre comment des mots tels que *et*, *ou*, et *n'affectent pas* la validité des arguments, nous devons voir comment ils contribuent à la véracité ou à la fausseté des énoncés qui les contiennent.

Lorsqu'on évalue la véracité ou la fausseté d'une affirmation, on lui attribue l'une des étiquettes « *vrai* » ou « *faux* », appelée *valeur de vérité*. On comprend clairement comment le mot « *et* » contribue à la valeur de vérité d'une affirmation qui le contient. Une affirmation de la forme $P \wedge Q$ ne peut être vraie que si P et Q sont tous deux vrais ; si P ou Q est faux, alors $P \wedge Q$ le sera également. Puisque nous avons supposé que P et Q représentent tous deux des affirmations vraies ou fausses, nous pouvons résumer toutes les possibilités à l'aide du tableau de [la figure 1.1](#). C'est ce qu'on appelle une *vérité*. *Tableau de vérité* pour la formule $P \wedge Q$. Chaque ligne du tableau de vérité représente l'une des quatre combinaisons possibles de valeurs de vérité pour les énoncés P et Q . Bien que ces quatre possibilités puissent apparaître dans le tableau dans n'importe quel ordre, il est préférable de les lister systématiquement afin de s'assurer qu'aucune possibilité n'a été omise. Le tableau de vérité pour $\neg P$ est également assez facile à construire, car pour que $\neg P$ soit vrai, P doit être faux. Le tableau est présenté dans [la figure 1.2](#).

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

Figure 1.1.

P	$\neg P$
F	T
T	F

Figure 1.2.

La table de vérité pour $P \vee Q$ est un peu plus complexe. Les trois premières lignes doivent être complétées comme illustré à [la figure 1.3](#), mais la dernière ligne peut poser problème. $P \vee Q$ doit-elle être vraie ou fausse dans le cas où P et Q sont toutes deux vraies ? Autrement dit, $P \vee Q$ signifie-t-il « P ou Q , ou les deux » ou « P ou Q , mais pas les deux » ? La première interprétation du mot « *ou* » est appelée « *ou inclusif* » (car elle *inclus* la possibilité que les deux affirmations soient vraies), et la seconde « *ou exclusif* ». En mathématiques, « *ou* » signifie toujours « *ou inclusif* », sauf indication contraire, nous interpréterons donc \vee comme « *ou inclusif* ». Nous complétons donc la table de vérité pour $P \vee Q$ comme illustré à [la figure 1.4](#). Voir [l'exercice 3](#) pour plus d'informations sur le « *ou exclusif* ».

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	?

Figure 1.3.

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

Figure 1.4.

En utilisant les règles résumées dans ces tables de vérité, nous pouvons maintenant élaborer des tables de vérité pour des formules plus complexes. Il suffit de calculer les valeurs de vérité des composantes d'une formule, en commençant par les lettres individuelles et en progressant progressivement vers des formules plus complexes.

Exemple 1.2.1. Créer une table de vérité pour la formule $\neg(P \vee \neg Q)$.

Solution

P	Q	$\neg Q$	$P \vee \neg Q$	$\neg(P \vee \neg Q)$
F	F	T	T	F
F	T	F	F	T
T	F	T	T	F
T	T	F	T	F

Les deux premières colonnes de ce tableau listent les quatre combinaisons possibles de valeurs de vérité de P et Q . La troisième colonne, listant les valeurs de vérité pour la formule $\neg Q$, est trouvée en niant simplement les valeurs de vérité pour Q dans la deuxième colonne. La quatrième colonne, pour la formule $P \vee \neg Q$, est trouvée en combinant les valeurs de vérité pour P et $\neg Q$ listées dans les première et troisième colonnes, selon la règle de la valeur de vérité pour \vee résumée dans [la Figure 1.4](#). Selon cette règle, $P \vee \neg Q$ ne sera faux que si P et $\neg Q$ sont tous deux faux. En regardant dans les première et

troisième colonnes, nous voyons que cela ne se produit que dans la deuxième ligne du tableau, donc la quatrième colonne contient un F dans la deuxième ligne et des T dans toutes les autres lignes. Enfin, les valeurs de vérité pour la formule $\neg(P \vee \neg Q)$ sont listées dans la cinquième colonne, qui est trouvée en niant les valeurs de vérité dans la quatrième colonne. (Notez que ces colonnes devaient être calculées dans l'ordre, car chacune était utilisée dans le calcul de la suivante.)

Exemple 1.2.2. Créer une table de vérité pour la formule $\neg(P \wedge Q) \vee \neg R$.

Solution

P	Q	R	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg R$	$\neg(P \wedge Q) \vee \neg R$
F	F	F	F	T	T	T
F	F	T	F	T	F	T
F	T	F	F	T	T	T
F	T	T	F	T	F	T
T	F	F	F	T	T	T
T	F	T	F	T	F	T
T	T	F	T	F	T	T
T	T	T	T	F	F	F

Notez que, comme cette formule contient trois lettres, il faut huit lignes pour lister toutes les combinaisons possibles de valeurs de vérité pour ces lettres. (Si une formule contient n lettres différentes, combien de lignes sa table de vérité comportera-t-elle ?)

Voici une méthode pour rendre les tables de vérité plus compactes. Au lieu d'utiliser des colonnes séparées pour lister les valeurs de vérité des composantes d'une formule, il suffit de les lister sous le symbole connecteur correspondant dans la formule d'origine. Ceci est illustré à [la Figure 1.5](#), pour la formule de [l'Exemple 1.2.1](#). Dans la première étape, nous avons listé les valeurs de vérité de P et Q sous ces lettres, là où elles apparaissent dans la formule. Dans la deuxième étape, les valeurs de vérité de $\neg Q$ ont été ajoutées sous le symbole \neg de $\neg Q$. Dans la troisième étape, nous avons combiné les valeurs de vérité de P et $\neg Q$ pour obtenir les valeurs de vérité de $P \vee \neg Q$, qui sont listées sous le symbole \vee . Enfin, dans la dernière étape, ces valeurs de vérité sont inversées et listées sous le symbole \neg initial. Les valeurs de vérité ajoutées à la dernière étape donnent la valeur de vérité pour toute la formule ; nous appellerons donc le symbole sous lequel elles sont listées (le premier symbole \neg dans ce cas) le *connecteur principal* de la formule. Notez que les valeurs de vérité répertoriées sous le connecteur principal dans ce cas concordent avec les valeurs que nous avons trouvées dans [l'exemple 1.2.1](#).

Step 1				Step 2			
P	Q	$\neg(P \vee \neg Q)$		P	Q	$\neg(P \vee \neg Q)$	
F	F	F	F	F	F	F	TF
F	T	F	T	F	T	F	FT
T	F	T	F	T	F	T	TF
T	T	T	T	T	T	T	FT

Step 3				Step 4			
P	Q	$\neg(P \vee \neg Q)$		P	Q	$\neg(P \vee \neg Q)$	
F	F	F	TTF	F	F	F	TTTF
F	T	F	FT	F	T	T	FFFT
T	F	T	TTF	T	F	F	TTTF
T	T	T	FT	T	T	F	TTFT

Figure 1.5.

Maintenant que nous savons créer des tables de vérité pour des formules complexes, nous sommes prêts à revenir à l'analyse de la validité des arguments. Reprenons notre premier exemple d'argument déductif :

Il pleuvra ou il neigera demain.
Il fait trop chaud pour qu'il neige.
Par conséquent, il pleuvra.

Comme nous l'avons vu, si nous posons P pour l'affirmation « Il pleuvra demain » et Q pour l'affirmation « Il neigera demain », alors nous pouvons représenter l'argument symboliquement comme suit :

$$\frac{P \vee Q}{\therefore P} \quad (\text{The symbol } \therefore \text{ means } \textit{therefore}.)$$

Nous pouvons maintenant voir comment utiliser les tables de vérité pour vérifier la validité de cet argument. [La figure 1.6](#) présente une table de vérité pour les prémisses et la conclusion de l'argument. Rappelons que nous avons décidé de qualifier un argument de valide si les prémisses ne peuvent pas toutes être vraies sans que la conclusion ne le soit également. En examinant [la figure 1.6](#), nous constatons que la seule ligne du tableau où les deux prémisses sont vraies est la ligne trois, et que la conclusion y est également vraie. Ainsi, la table de vérité confirme que si les prémisses sont toutes vraies, la conclusion doit l'être également, et donc l'argument est valide.

Premises			Conclusion	
P	Q	$P \vee Q$	$\neg Q$	P
F	F	F	T	F
F	T	T	F	F
T	F	T	T	T
T	T	T	F	T

Figure 1.6.

Exemple 1.2.3. Déterminer si les arguments suivants sont valides.

- Soit John n'est pas intelligent et il a de la chance, soit il est intelligent.

John est intelligent.

John n'a donc pas de chance.

2. Le majordome et le cuisinier ne sont pas tous deux innocents.

Soit le majordome ment, soit le cuisinier est innocent.

Par conséquent, le majordome ment ou est coupable.

Solutions

1. Comme dans [l'exemple 1.1.3](#), supposons que S représente l'affirmation « Jean est intelligent » et L « Jean a de la chance ». L'argument est alors de la forme suivante :

$$\frac{S}{\therefore \neg L}$$

Nous allons maintenant établir une table de vérité pour les prémisses et la conclusion. (Vous devrez effectuer les étapes intermédiaires de la dérivation de la troisième colonne de ce tableau pour confirmer son exactitude.)

S	L	$(\neg S \wedge L) \vee S$	Premises		Conclusion	
			S	$\neg L$	S	$\neg L$
F	F	F	F	T		
F	T	T	F	F		
T	F	T	T	T		
T	T	T	T	F		

Les deux prémisses sont vraies aux lignes trois et quatre de ce tableau. La conclusion est également vraie à la ligne trois, mais fausse à la ligne quatre. Ainsi, il est possible que les deux prémisses soient vraies et la conclusion fausse, et que l'argument soit donc invalide. En fait, le tableau nous montre précisément pourquoi l'argument est invalide. Le problème se pose à la quatrième ligne du tableau, où S et L sont toutes deux vraies ; autrement dit, John est à la fois intelligent et chanceux. Ainsi, si John est à la fois intelligent et chanceux, alors les deux prémisses seront vraies, mais la conclusion sera fausse. Il serait donc erroné de déduire que la conclusion doit être vraie en supposant que les prémisses sont vraies.

2. Soit B l'affirmation « Le majordome est innocent », C l'affirmation « Le cuisinier est innocent » et L l'affirmation « Le majordome ment ». L'argument est alors de la forme suivante :

$$\frac{\neg(B \wedge C)}{L \vee C}$$

Voici la table de vérité pour les prémisses et la conclusion :

B	C	L	Premises		Conclusion $L \vee \neg B$
			$\neg(B \wedge C)$	$L \vee C$	
F	F	F	T	F	T
F	F	T	T	T	T
F	T	F	T	T	T
F	T	T	T	T	T
T	F	F	T	F	F
T	F	T	T	T	T
T	T	F	F	T	F
T	T	T	F	T	T

Les prémisses ne sont vraies qu'aux lignes deux, trois, quatre et six, et dans chacun de ces cas, la conclusion est également vraie. Par conséquent, l'argument est valide.

Si vous pensiez que le premier argument de [l'exemple 1.2.3](#) serait valide, c'est probablement parce que la première prémissse vous a embrouillé. C'est une affirmation assez compliquée, que nous avons représentée symboliquement par la formule $(\neg S \wedge L) \vee S$. D'après notre table de vérité, cette formule est fausse si S et L sont tous deux faux, et vraie sinon. Mais remarquez qu'elle est exactement la même que la table de vérité pour la formule plus simple $L \vee S$! De ce fait, nous disons que les formules $(\neg S \wedge L) \vee S$ et $L \vee S$ sont *équivalentes*. Des formules équivalentes ont toujours la même valeur de vérité, quelles que soient les affirmations que leurs lettres représentent et quelles que soient les valeurs de vérité de ces affirmations. L'équivalence de la prémissse $(\neg S \wedge L) \vee S$ et de la formule plus simple $L \vee S$ peut vous aider à comprendre pourquoi l'argument est invalide. En traduisant la formule $L \vee S$ en anglais, on constate que la première prémissse aurait pu être formulée plus simplement comme « John est soit chanceux, soit intelligent (ou les deux). » Mais de cette prémissse et de la seconde prémissse (que John est intelligent), il ne s'ensuit clairement pas qu'il n'a pas de chance, car il pourrait être à la fois intelligent et chanceux.

Exemple 1.2.4. Lesquelles de ces formules sont équivalentes ?

$$\neg(P \wedge Q), \neg P \wedge \neg Q, \neg P \vee \neg Q.$$

Solution

Voici un tableau de vérité pour les trois affirmations. (Vous devriez le vérifier vous-même !)

P	Q	$\neg(P \wedge Q)$	$\neg P \wedge \neg Q$	$\neg P \vee \neg Q$
F	F	T	T	T
F	T	T	F	T
T	F	T	F	T
T	T	F	F	F

Les troisième et cinquième colonnes de ce tableau sont identiques, mais diffèrent de la quatrième. Par conséquent, les formules $\neg(P \wedge Q)$ et $\neg P \vee \neg Q$ sont équivalentes, mais aucune n'est équivalente à la formule $\neg P \wedge \neg Q$. Cela devrait être logique si l'on considère la

signification de tous les symboles. Par exemple, supposons que P représente l'affirmation « Les Yankees ont gagné hier soir » et Q « Les Red Sox ont gagné hier soir ». Alors $\neg(P \wedge Q)$ représenterait l'affirmation « Les Yankees et les Red Sox n'ont pas tous les deux gagné hier soir », et $\neg P \vee \neg Q$ représenterait « *Les Yankees ou les Red Sox ont perdu hier soir* » ; ces affirmations véhiculent clairement la même information. En revanche, $\neg P \wedge \neg Q$ représenterait « Les Yankees et les Red Sox ont tous les deux perdu hier soir », ce qui signifie quelque chose de complètement différent.

Vous pouvez vérifier par vous-même en créant une table de vérité que la formule $\neg P \wedge \neg Q$ de [l'exemple 1.2.4](#) est équivalente à la formule $\neg(P \vee Q)$. (Pour voir que cette équivalence est logique, remarquez que les affirmations « Les Yankees et les Red Sox ont tous deux perdu hier soir » et « Il n'est pas vrai que les Yankees ou les Red Sox aient gagné hier soir » signifient la même chose.) Cette équivalence et celle découverte dans [l'exemple 1.2.4](#) sont appelées *lois de De Morgan*. Elles doivent leur nom au mathématicien britannique Augustus De Morgan (1806–1871).

Pour analyser les arguments déductifs et leurs énoncés, il est utile de se familiariser avec un certain nombre d'équivalences fréquentes. Vérifiez vous-même les équivalences de la liste suivante en créant des tables de vérité et assurez-vous qu'elles sont cohérentes en traduisant les formules en anglais, comme dans [l'exemple 1.2.4](#).

Les lois de De Morgan

$\neg(P \wedge Q)$ is equivalent to $\neg P \vee \neg Q$.
 $\neg(P \vee Q)$ is equivalent to $\neg P \wedge \neg Q$.

Lois commutatives

$P \wedge Q$ is equivalent to $Q \wedge P$.
 $P \vee Q$ is equivalent to $Q \vee P$.

Lois associatives

$P \wedge (Q \wedge R)$ is equivalent to $(P \wedge Q) \wedge R$.
 $P \vee (Q \vee R)$ is equivalent to $(P \vee Q) \vee R$.

Lois idempotentes

$P \wedge P$ is equivalent to P .
 $P \vee P$ is equivalent to P .

Lois distributives

$P \wedge (Q \vee R)$ is equivalent to $(P \wedge Q) \vee (P \wedge R)$.
 $P \vee (Q \wedge R)$ is equivalent to $(P \vee Q) \wedge (P \vee R)$.

Lois d'absorption

$P \vee (P \wedge Q)$ is equivalent to P .
 $P \wedge (P \vee Q)$ is equivalent to P .

Loi de double négation

$\neg\neg P$ is equivalent to P .

Notez qu'en raison des lois associatives, nous pouvons omettre les parenthèses dans les formules de la forme $P \wedge Q \wedge R$ et $P \vee Q \vee R$ sans craindre que la formule résultante soit ambiguë, car les deux manières possibles de remplir les parenthèses conduisent à des formules équivalentes.

Plusieurs des équivalences de cette liste devraient vous rappeler des règles similaires impliquant $+$, \cdot et $-$ en algèbre. Comme en algèbre, ces règles peuvent être appliquées à des formules plus complexes et combinées pour obtenir des équivalences plus complexes. N'importe quelle lettre de ces équivalences peut être remplacée par une formule plus complexe, et l'équivalence résultante sera toujours vraie. Par exemple, en remplaçant P dans la loi de double négation par la formule $Q \vee \neg R$, vous pouvez constater que $\neg\neg(Q \vee \neg R)$ est équivalent à $Q \vee \neg R$. De plus, si deux formules sont équivalentes, vous pouvez toujours substituer l'une à l'autre dans n'importe quelle expression et les résultats seront équivalents. Par exemple, puisque $\neg\neg P$ est équivalent à P , si $\neg\neg P$ apparaît dans une formule, vous pouvez toujours le remplacer par P et la formule résultante sera équivalente à l'originale.

Exemple 1.2.5. Trouver des formules plus simples équivalentes à celles-ci :

1. $\neg(P \vee \neg Q)$.
2. $\neg(Q \wedge \neg P) \vee P$.

Solutions

1. $\neg(P \vee \neg Q)$

is equivalent to $\neg P \wedge \neg\neg Q$ (De Morgan's law),
which is equivalent to $\neg P \wedge Q$ (double negation law).

Vous pouvez vérifier que cette équivalence est correcte en créant une table de vérité pour $\neg P \wedge Q$ et en constatant qu'elle est la même que la table de vérité pour $\neg(P \vee \neg Q)$ trouvée dans [l'exemple 1.2.1](#).

2. $\neg(Q \wedge \neg P) \vee P$

is equivalent to $(\neg Q \vee \neg\neg P) \vee P$ (De Morgan's law),
which is equivalent to $(\neg Q \vee P) \vee P$ (double negation law),
which is equivalent to $\neg Q \vee (P \vee P)$ (associative law),
which is equivalent to $\neg Q \vee P$ (idempotent law).

Certaines équivalences sont basées sur le fait que certaines formules sont soit toujours vraies, soit toujours fausses. Par exemple, vous pouvez vérifier en créant une table de vérité que la formule $Q \wedge (P \vee \neg P)$ est équivalente à Q . Mais même avant de créer la table de vérité, vous pouvez probablement voir pourquoi elles sont équivalentes. Dans chaque ligne de la table de vérité, $P \vee \neg P$ sera vraie, et donc $Q \wedge (P \vee \neg P)$ sera vraie lorsque Q est également vraie, et fausse lorsque Q est fausse. Les formules qui sont toujours vraies, telles que $P \vee \neg P$, sont appelées *tautologies*. De même, les formules qui sont toujours fausses sont appelées *contradictions*. Par exemple, $P \wedge \neg P$ est une contradiction.

Exemple 1.2.6. Ces formules sont-elles des tautologies, des contradictions ou ni l'une ni l'autre ?

$$P \vee (Q \vee \neg P), P \wedge \neg (Q \vee \neg Q), P \vee \neg (Q \vee \neg Q).$$

Solution

Nous créons d'abord une table de vérité pour les trois formules.

P	Q	$P \vee (Q \vee \neg P)$	$P \wedge \neg (Q \vee \neg Q)$	$P \vee \neg (Q \vee \neg Q)$
F	F	T	F	F
F	T	T	F	F
T	F	T	F	T
T	T	T	F	T

deuxième une contradiction et la troisième ni l'une ni l'autre. En fait, la dernière colonne étant identique à la première, la troisième formule est équivalente à P .

Nous pouvons maintenant énoncer quelques lois utiles supplémentaires impliquant des tautologies et des contradictions. Vous devriez être en mesure de vous convaincre de leur exactitude en réfléchissant à ce à quoi ressembleraient les tables de vérité des affirmations concernées.

Lois de tautologie

$P \wedge (\text{une tautologie})$ est équivalent à P .

$P \vee (\text{une tautologie})$ est une tautologie.

$\neg(\text{une tautologie})$ est une contradiction.

Lois de contradiction

$P \wedge (\text{une contradiction})$ est une contradiction.

$P \vee (\text{une contradiction})$ est équivalent à P .

$\neg(\text{une contradiction})$ est une tautologie.

Exemple 1.2.7. Trouver des formules plus simples équivalentes à celles-ci :

1. $P \vee (Q \wedge \neg P)$.
2. $\neg(P \vee (Q \wedge \neg R)) \wedge Q$.

Solutions

1. $P \vee (Q \wedge \neg P)$

is equivalent to $(P \vee Q) \wedge (P \vee \neg P)$ (distributive law),
which is equivalent to $P \vee Q$ (tautology law).

La dernière étape utilise le fait que $P \vee \neg P$ est une tautologie.

2. $\neg(P \vee (Q \wedge \neg R)) \wedge Q$

is equivalent to $(\neg P \wedge \neg(Q \wedge \neg R)) \wedge Q$ (De Morgan's law),
which is equivalent to $(\neg P \wedge (\neg Q \vee \neg \neg R)) \wedge Q$ (De Morgan's law),
which is equivalent to $(\neg P \wedge (\neg Q \vee R)) \wedge Q$ (double negation law),
which is equivalent to $\neg P \wedge ((\neg Q \vee R) \wedge Q)$ (associative law),
which is equivalent to $\neg P \wedge (Q \wedge (\neg Q \vee R))$ (commutative law),
which is equivalent to $\neg P \wedge ((Q \wedge \neg Q) \vee (Q \wedge R))$ (distributive law),
which is equivalent to $\neg P \wedge (Q \wedge R)$ (contradiction law).

La dernière étape utilise le fait que $Q \wedge \neg Q$ est une contradiction. Finalement, grâce à la loi associative pour \wedge , on peut supprimer les parenthèses sans rendre la formule ambiguë, de sorte que la formule originale est équivalente à la formule $\neg P \wedge Q \wedge R$.

Exercices

*1. Créez des tables de vérité pour les formules suivantes :

- (a) $\neg P \vee Q$.
- (b) $(S \vee G) \wedge (\neg S \vee \neg G)$.

2. Créez des tables de vérité pour les formules suivantes :

- (a) $\neg[P \wedge (Q \vee \neg P)]$.
- (b) $(P \vee Q) \wedge (\neg P \vee R)$.

3. Dans cet exercice, nous utiliserons le symbole $+$ pour signifier « ou exclusif ». Autrement dit, $P + Q$ signifie « P ou Q , mais pas les deux ».

- (a) Créez une table de vérité pour $P + Q$.
- (b) Trouvez une formule utilisant uniquement les connecteurs \wedge , \vee et \neg qui est équivalente à $P + Q$. Justifiez votre réponse avec une table de vérité.

4. Trouvez une formule utilisant uniquement les connecteurs \wedge et \neg qui est équivalente à $P \vee Q$. Justifiez votre réponse avec une table de vérité.
- *5. Certains mathématiciens utilisent le symbole \downarrow pour signifier *ni*. Autrement dit, $P \downarrow Q$ signifie « ni P ni Q ».
- Créez une table de vérité pour $P \downarrow Q$.
 - Trouvez une formule utilisant uniquement les connecteurs \wedge , \vee et \neg qui est équivalente à $P \downarrow Q$.
 - Trouvez des formules utilisant uniquement le connecteur \downarrow qui sont équivalentes à $\neg P$, $P \vee Q$ et $P \wedge Q$.
6. Certains mathématiciens écrivent $P | Q$ pour signifier « P et Q ne sont pas tous les deux vrais ». (Ce connecteur est appelé *nand* et est utilisé dans l'étude des circuits en informatique.)
- Créez une table de vérité pour $P | Q$.
 - Trouvez une formule utilisant uniquement les connecteurs \wedge , \vee et \neg qui est équivalente à $P | Q$.
 - Trouvez des formules utilisant uniquement le connecteur $|$ qui sont équivalentes à $\neg P$, $P \vee Q$ et $P \wedge Q$.
- *7. Utilisez les tables de vérité pour déterminer si les arguments de [l'exercice 9 de la section 1.1 sont valides](#) ou non .
8. Utilisez les tables de vérité pour déterminer lesquelles des formules suivantes sont équivalentes :
- $(P \wedge Q) \vee (\neg P \wedge \neg Q)$.
 - $\neg P \vee Q$.
 - $(P \vee \neg Q) \wedge (Q \vee \neg P)$.
 - $\neg(P \vee Q)$.
 - $(Q \wedge P) \vee \neg P$.
- *9. Utilisez les tables de vérité pour déterminer lesquelles de ces affirmations sont des tautologies, lesquelles sont des contradictions et lesquelles ne sont ni l'une ni l'autre :
- $(P \vee Q) \wedge (\neg P \vee \neg Q)$.
 - $(P \vee Q) \wedge (\neg P \wedge \neg Q)$.
 - $(P \vee Q) \vee (\neg P \vee \neg Q)$.
 - $[P \wedge (Q \vee \neg R)] \vee (\neg P \vee R)$.
10. Utilisez les tables de vérité pour vérifier ces lois :
- La deuxième loi de De Morgan. (La première a été vérifiée dans le texte.)
 - Les lois distributives.
11. Utilisez les lois énoncées dans le texte pour trouver des formules plus simples équivalentes à ces formules. (Voir [exemples 1.2.5](#) et [1.2.7](#).)
- $\neg(\neg P \wedge \neg Q)$.
 - $(P \wedge Q) \vee (P \wedge \neg Q)$.
 - $\neg(P \wedge \neg Q) \vee (\neg P \wedge Q)$.

12. Utilisez les lois énoncées dans le texte pour trouver des formules plus simples équivalentes à ces formules. (Voir [exemples 1.2.5](#) et [1.2.7.](#))

- (a) $\neg(\neg P \vee Q) \vee (P \wedge \neg R)$.
- (b) $\neg(\neg P \wedge Q) \vee (P \wedge \neg R)$.
- (c) $(P \wedge R) \vee [\neg R \wedge (P \vee Q)]$.

13. Utilisez la première loi de De Morgan et la loi de double négation pour dériver la deuxième loi de De Morgan.

14. Notez que les lois associatives indiquent seulement que les parenthèses sont inutiles lorsqu'on combine *trois* énoncés avec \wedge ou \vee . En fait, ces lois peuvent servir à justifier l'omission des parenthèses lorsque plus de trois énoncés sont combinés. Utilisez les lois associatives pour montrer que $[P \wedge (Q \wedge R)] \wedge S$ est équivalent à $(P \wedge Q) \wedge (R \wedge S)$.

15. Combien de lignes y aura-t-il dans la table de vérité pour une instruction contenant n lettres ?

16. Trouvez une formule impliquant les connecteurs \wedge , \vee et \neg qui possède la table de vérité suivante :

P	Q	???
F	F	T
F	T	F
T	F	T
T	T	T

17. Trouvez une formule impliquant les connecteurs \wedge , \vee et \neg qui a la table de vérité suivante :

P	Q	???
F	F	F
F	T	T
T	F	T
T	T	F

18. Supposons que la conclusion d'un argument soit une tautologie. Que pouvez-vous conclure sur la validité de l'argument ? Et si la conclusion est une contradiction ? Et si l'une des prémisses est soit une tautologie, soit une contradiction ?

1.3 Variables et ensembles

En raisonnement mathématique, il est souvent nécessaire de formuler des affirmations sur des objets représentés par des lettres appelées *variables*. Par exemple, si la variable x représente un nombre dans un problème, l'affirmation « x est un nombre premier » pourrait nous intéresser. Bien qu'une seule lettre, par exemple P , puisse parfois représenter cette affirmation, nous modifierons légèrement cette notation et écrirons $P(x)$ pour souligner qu'il s'agit d'une affirmation *sur x* . Cette dernière notation facilite l'attribution d'une valeur à x dans l'énoncé. Par exemple, $P(7)$ représenterait l'énoncé « 7 est un nombre premier », et $P(a+b)$ signifierait « $a+b$ est un nombre premier ». Si une instruction contient plusieurs variables, notre abréviation inclura la liste de toutes les variables impliquées. Par exemple, nous pourrions représenter l'instruction « p est divisible par q » par $D(p, q)$. Dans ce cas, $D(12, 4)$ signifierait « 12 est divisible par 4 ».

Bien que vous ayez probablement déjà vu des variables utilisées pour représenter des nombres, elles peuvent représenter n'importe quoi. Par exemple, on pourrait utiliser $M(x)$ pour représenter l'affirmation « x est un homme » et $W(x)$ pour « x est une femme ». Dans ce cas, la variable x représente une personne. Une affirmation peut même contenir plusieurs variables représentant différents types d'objets. Par exemple, dans l'affirmation « x a y enfants », la variable x représente une personne et y représente un nombre.

Les instructions impliquant des variables peuvent être combinées à l'aide de connecteurs, tout comme les instructions sans variables.

Exemple 1.3.1. Analyser les formes logiques des énoncés suivants :

1. x est un nombre premier et y ou z est divisible par x .
2. x est un homme et y est une femme et x aime y , mais y n'aime pas x .

Solutions

1. On pourrait remplacer P par l'énoncé « x est un nombre premier », D par « y est divisible par x » et E par « z est divisible par x ». L'énoncé complet serait alors représenté par la formule $P \wedge (D \vee E)$. Mais cette analyse, bien que correcte, ne rend pas compte de la relation entre les énoncés D et E . Une meilleure analyse serait de remplacer $P(x)$ par « x est un nombre premier » et $D(y, x)$ par « y est divisible par x ». Alors $D(z, x)$ signifierait « z est divisible par x », de sorte que l'énoncé complet serait $P(x) \wedge (D(y, x) \vee D(z, x))$.

2. Soit $M(x)$ pour « x est un homme », $W(y)$ pour « y est une femme » et $L(x, y)$ pour « x aime y ». Alors $L(y, x)$ signifierait « y aime x ». (Remarquez que l'ordre des variables après le L fait une différence !) L'énoncé entier serait alors représenté par la formule $M(x) \wedge W(y) \wedge L(x, y) \wedge \neg L(y, x)$.

Dans la section précédente, nous avons introduit l'idée d'attribuer des valeurs de vérité aux énoncés. Cette idée ne pose aucun problème pour les énoncés ne contenant pas de variables, car ces énoncés sont soit vrais, soit faux. En revanche, si un énoncé contient des variables, on ne peut plus le décrire simplement comme vrai ou faux. Sa valeur de vérité peut dépendre des valeurs des variables impliquées. Par exemple, si $P(x)$ représente l'énoncé « x est un nombre premier », alors $P(x)$ serait vrai si $x = 23$, mais faux si $x = 22$. Pour résoudre cette complication, nous allons définir *des ensembles de vérité* pour les énoncés contenant des variables. Avant de donner cette définition, il pourrait toutefois être utile de revoir quelques définitions de base de la théorie des ensembles.

Un *ensemble* est une collection d'objets. Les objets de la collection sont appelés ses *éléments*. La façon la plus simple de spécifier un ensemble particulier est d'en lister les éléments entre accolades. Par exemple, $\{3, 7, 14\}$ est l'ensemble dont les éléments sont les trois nombres 3, 7 et 14. On utilise le symbole \in pour signifier *qu'il est un élément de*. Par exemple, si l'on considère A comme l'ensemble $\{3, 7, 14\}$, on peut écrire $7 \in A$ pour indiquer que 7 est un élément de A . Pour indiquer que 11 n'est pas un élément de A , on écrit $11 \notin A$.

Un ensemble est entièrement déterminé une fois ses éléments spécifiés. Ainsi, deux ensembles contenant exactement les mêmes éléments sont toujours égaux. De plus, lorsqu'un ensemble est défini par la liste de ses éléments, seul comptent les objets figurant dans la liste, et non leur ordre d'apparition. Un élément peut même apparaître plusieurs fois dans la liste. Ainsi, $\{3, 7, 14\}$, $\{14, 3, 7\}$ et $\{3, 7, 14, 7\}$ sont trois noms différents pour le même ensemble.

Il peut être difficile de définir un ensemble contenant un très grand nombre d'éléments en listant tous ses éléments, et il serait impossible de donner une telle définition pour un ensemble contenant une infinité d'éléments. On peut souvent contourner ce problème en listant quelques éléments suivis d'un point de suspension (...), si la suite de la liste est claire. Par exemple, supposons que nous définissions un ensemble B en disant que $B = \{2, 3, 5, 7, 11, 13, 17, \dots\}$. Une fois que vous avez reconnu que les nombres listés dans la définition de B sont des nombres premiers, vous savez alors que, par exemple, $23 \in B$, même s'il n'était pas explicitement listé lors de la définition de B . Mais cette méthode nécessite de reconnaître le motif dans la liste des nombres de la définition de B , ce qui introduit un élément d'ambiguïté

et de subjectivité dans notre notation qu'il vaut mieux éviter en écriture mathématique. Il est donc généralement préférable de définir un tel ensemble en précisant le motif qui détermine ses éléments.

Dans ce cas, nous pourrions être explicites en définissant B comme suit :

$$B = \{ x \mid x \text{ est un nombre premier}\}.$$

Cela se lit comme suit : « B est égal à l'ensemble de tous les x tels que x est un nombre premier », ce qui signifie que les éléments de B sont les valeurs de x qui rendent l'affirmation « x est un nombre premier » vraie. Il faut considérer l'affirmation « x est un nombre premier » comme un test d'élémentarité pour l'ensemble. Toute valeur de x qui rend cette affirmation vraie passe le test et est un élément de l'ensemble. Toute autre valeur échoue au test et n'est pas un élément. Bien sûr, dans ce cas, les valeurs de x qui rendent l'affirmation vraie sont précisément les nombres premiers ; cette définition dit donc que B est l'ensemble dont les éléments sont les nombres premiers, exactement comme précédemment.

Exemple 1.3.2. Réécrire ces définitions d'ensemble à l'aide de tests d'élémentarité :

1. $E = \{2, 4, 6, 8, \dots\}$.
2. $P = \{\text{George Washington, John Adams, Thomas Jefferson, James Madison, ...}\}$.

Solutions

Bien qu'il puisse y avoir d'autres façons de continuer ces listes d'éléments, les plus naturelles sont probablement celles données par les définitions suivantes :

1. $E = \{n \mid n \text{ est un entier pair positif}\}$.
2. $P = \{z \mid z \text{ était président des États-Unis}\}$.

Français Si un ensemble a été défini en utilisant un test d'élémentarité, alors ce test peut être utilisé pour déterminer si quelque chose est ou non un élément de l'ensemble. Par exemple, considérons l'ensemble $\{x \mid x^2 < 9\}$. Si nous voulons savoir si 5 est un élément de cet ensemble, nous appliquons simplement le test d'élémentarité dans la définition de l'ensemble - en d'autres termes, nous vérifions si $5^2 < 9$ ou non. Puisque $5^2 = 25 > 9$, il échoue au test, donc $5 \notin \{x \mid x^2 < 9\}$. D'autre part, $(-2)^2 = 4 < 9$, donc $-2 \in \{x \mid x^2 < 9\}$. Le même raisonnement s'appliquerait à tout autre nombre. Pour tout

nombre y , pour déterminer si $y \in \{x \mid x^2 < 9\}$ ou non, nous vérifions simplement si $y^2 < 9$ ou non. En fait, nous pourrions penser à l'énoncé $y \in \{x \mid x^2 < 9\}$ est simplement une manière détournée de dire $y^2 < 9$.

Notez que, puisque l'énoncé $y \in \{x \mid x^2 < 9\}$ signifie la même chose que $y^2 < 9$, il s'agit d'un énoncé sur y , mais pas sur x ! Pour déterminer si $y \in \{x \mid x^2 < 9\}$ ou non, vous devez connaître la valeur de y (afin de pouvoir comparer son carré à 9), mais pas celle de x . On dit que dans l'énoncé $y \in \{x \mid x^2 < 9\}$, y est une variable *libre*, tandis que x est une variable *liée* (ou une variable *muette*). Les variables libres d'une instruction représentent les objets dont l'énoncé parle. Insérer différentes valeurs pour une variable libre affecte le sens d'un énoncé et peut modifier sa valeur de vérité. Le fait de pouvoir insérer différentes valeurs pour une variable libre signifie qu'elle est libre de représenter n'importe quoi. Les variables liées, en revanche, sont simplement des lettres utilisées pour exprimer une idée et ne doivent pas être considérées comme représentant un objet particulier. Une variable liée peut toujours être remplacée par une nouvelle variable sans modifier le sens de l'énoncé, et souvent, celui-ci peut être reformulé de manière à éliminer complètement les variables liées. Par exemple, les énoncés $y \in \{x \mid x^2 < 9\}$ et $y \in \{w \mid w^2 < 9\}$ ont la même signification, car ils signifient tous deux « y est un élément de l'ensemble de tous les nombres dont les carrés sont inférieurs à 9 ». Dans ce dernier cas, Dans l'instruction, toutes les variables liées ont été éliminées et la seule variable qui apparaît dans l'instruction est la variable libre y .

Notez que x est une variable liée dans l'instruction $y \in \{x \mid x^2 < 9\}$, même si elle est une variable libre dans l'instruction $x^2 < 9$. Cette dernière affirmation concernant x serait vraie pour certaines valeurs de x et fausse pour d'autres. Ce n'est que lorsque cette affirmation est utilisée dans la notation du test d'élémentarité que x devient une variable liée. On pourrait dire que la notation $\{x \mid \dots\}$ *lie* la variable x .

Tout ce que nous avons dit sur l'ensemble $\{x \mid x^2 < 9\}$ s'appliquerait à tout ensemble défini par un test d'élémentarité. En général, l'énoncé $y \in \{x \mid P(x)\}$ signifie la même chose que $P(y)$, qui est un énoncé sur y mais pas sur x . De même, $y \notin \{x \mid P(x)\}$ signifie la même chose que $\neg P(y)$. Bien sûr, l'expression $\{x \mid P(x)\}$ n'est pas du tout un énoncé ; c'est le nom d'un ensemble. À mesure que vous apprendrez davantage la notation mathématique, il deviendra de plus en plus important de

veiller à bien distinguer les expressions qui sont des énoncés mathématiques de celles qui sont des noms d'objets mathématiques.

Exemple 1.3.3. Que signifient ces instructions ? Quelles sont les variables libres dans chaque instruction ?

1. $a + b \notin \{x \mid x \text{ est un nombre pair}\}$.
2. $y \in \{x \mid x \text{ est divisible par } w\}$.
3. $2 \in \{w \mid 6 \notin \{x \mid x \text{ est divisible par } w\}\}$.

Solutions

1. Cette affirmation indique que $a + b$ n'est pas un élément de l'ensemble des nombres pairs, autrement dit, $a + b$ n'est pas un nombre pair. a et b sont des variables libres, mais x est une variable liée. L'affirmation sera vraie pour certaines valeurs de a et b et fausse pour d'autres.
2. Cette affirmation stipule que y est divisible par w . Y et w sont des variables libres, mais x est une variable liée. Cette affirmation est vraie pour certaines valeurs de y et w et fausse pour d'autres.
3. Cela paraît compliqué, mais en procédant étape par étape, on peut le déchiffrer. Notons d'abord que l'énoncé $6 \notin \{x \mid x \text{ est divisible par } w\}$, qui apparaît dans l'énoncé donné, signifie la même chose que « 6 n'est pas divisible par w ». En le substituant dans l'énoncé donné, on constate que l'énoncé original est équivalent à l'énoncé plus simple $2 \in \{w \mid 6 \text{ n'est pas divisible par } w\}$. Mais cela signifie simplement la même chose que « 6 n'est pas divisible par 2 ». Ainsi, l'énoncé n'a pas de variables libres, et x et w sont tous deux des variables liées. Comme il n'y a pas de variables libres, la valeur de vérité de l'affirmation ne dépend pas de la valeur des variables. En fait, puisque 6 est divisible par 2, l'affirmation est fausse.

Vous avez peut-être deviné comment la théorie des ensembles peut nous aider à comprendre les valeurs de vérité des énoncés contenant des variables libres. Comme nous l'avons vu, un énoncé, par exemple $P(x)$, contenant une variable libre x , peut être vrai pour certaines valeurs de x et faux pour d'autres. Pour distinguer les valeurs de x qui rendent $P(x)$ vrai de celles qui le rendent faux, nous pourrions former l'ensemble des valeurs de x pour lesquelles $P(x)$ est vrai. Nous appellerons cet ensemble l'*ensemble de vérité* de $P(x)$.

Définition 1.3.4. L'*ensemble de vérité* d'une affirmation $P(x)$ est l'ensemble de toutes les valeurs de x qui rendent l'affirmation $P(x)$ vraie. Autrement dit, il s'agit de l'ensemble défini en utilisant l'affirmation $P(x)$ comme test d'élémentarité : $\{x \mid P(x)\}$.

Notez que nous avons défini des ensembles de vérité uniquement pour les instructions contenant *une* variable libre. Nous aborderons les ensembles de vérité pour les instructions comportant plusieurs variables libres au [chapitre 4](#).

Exemple 1.3.5. Quels sont les ensembles de vérité des affirmations suivantes ?

1. Shakespeare a écrit x .
2. n est un nombre premier pair.

Solutions

1. $\{x \mid \text{Shakespeare a écrit } x\} = \{\text{Hamlet, Macbeth, La Nuit des rois, ...}\}$.
2. $\{n \mid n \text{ est un nombre premier pair}\}$. Puisque le seul nombre premier pair est 2, cet ensemble est $\{2\}$. Notez que 2 et $\{2\}$ ne sont pas identiques ! Le premier est un nombre, et le second est un ensemble dont le seul élément est un nombre. Ainsi, $2 \in \{2\}$, mais $2 = \{2\}$.

Supposons que A soit l'ensemble de vérité d'une instruction $P(x)$. Selon la définition d'ensemble de vérité, cela signifie que $A = \{x \mid P(x)\}$. Nous avons déjà vu que pour tout objet y , l'énoncé $y \in \{x \mid P(x)\}$ signifie la même chose que $P(y)$. En substituant dans A par $\{x \mid P(x)\}$, il s'ensuit que $y \in A$ signifie la même chose que $P(y)$. Ainsi, nous voyons qu'en général, si A est l'ensemble de vérité de $P(x)$, alors dire que $y \in A$ signifie la même chose que dire $P(y)$.

Lorsqu'une instruction contient des variables libres, le contexte indique souvent clairement que ces variables représentent des objets d'un type particulier. L'ensemble de tous les objets de ce type – autrement dit, l'ensemble de toutes les valeurs possibles des variables – est On appelle *univers de discours* l'énoncé, et on dit que les variables *s'étendent sur* cet univers. Par exemple, dans la plupart des contextes, l'univers de l'énoncé $x^2 < 9$ serait l'ensemble de tous les nombres réels ; l'univers de l'énoncé « x est un homme » pourrait être l'ensemble de toutes les personnes.

Certains ensembles apparaissent fréquemment en mathématiques comme univers de discours, et il est pratique de leur attribuer des noms fixes. Voici quelques-uns des plus importants :

$$\mathbb{R} = \{x \mid x \text{ est un nombre réel}\}.$$

$$\mathbb{Q} = \{x \mid x \text{ est un nombre rationnel}\}.$$

(Rappelons qu'un nombre *réel* est n'importe quel nombre sur la droite numérique, et qu'un nombre *rationnel* est un nombre qui peut être écrit sous la forme d'une fraction p/q , où p et q sont des entiers.)

$$\mathbb{Z} = \{x \mid x \text{ est un entier}\} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

$$\mathbb{N} = \{ x \mid x \text{ est un nombre naturel} \} = \{0, 1, 2, 3, \dots\}.$$

(Certains livres incluent 0 comme nombre naturel et d'autres non. Dans ce livre, nous considérons 0 comme un nombre naturel.)

Les lettres \mathbb{R} , \mathbb{Q} et \mathbb{Z} peuvent être suivies d'un exposant + ou - pour indiquer que seuls les nombres positifs ou négatifs doivent être inclus dans l'ensemble. Par exemple, $\mathbb{R}^+ = \{x \mid x \text{ est un nombre réel positif}\}$ et $\mathbb{Z}^- = \{x \mid x \text{ est un entier négatif}\}$.

Bien que l'univers du discours puisse généralement être déterminé à partir du contexte, il est parfois utile de l'identifier explicitement. Considérons un énoncé $P(x)$ avec une variable libre x qui s'étend sur un univers U . Bien que nous ayons écrit l'ensemble de vérité de $P(x)$ comme $\{x \mid P(x)\}$, s'il y avait une possibilité de confusion sur ce qu'est l'univers, nous pourrions le spécifier explicitement en écrivant $\{x \in U \mid P(x)\}$; cela se lit « l'ensemble de tous les x dans U tels que $P(x)$ ». Cette notation indique que seuls les éléments de U doivent être considérés comme élémentaux dans cet ensemble de vérité, et parmi les éléments de U , seuls ceux qui passent le test d'élémentalité $P(x)$ seront réellement dans l'ensemble de vérité. Par exemple, considérons à nouveau l'énoncé $x^2 < 9$. Si l'univers du discours pour cet énoncé était l'ensemble de tous les nombres réels, alors son ensemble de vérité serait $\{x \in \mathbb{R} \mid x^2 < 9\}$, autrement dit, l'ensemble de tous les nombres réels compris entre -3 et 3. Mais si l'univers était l'ensemble de tous les entiers, alors l'ensemble de vérité serait $\{x \in \mathbb{Z} \mid x^2 < 9\} = \{-2, -1, 0, 1, 2\}$. Ainsi, par exemple, $1,58 \in \{x \in \mathbb{R} \mid x^2 < 9\}$ mais $1,58 \notin \{x \in \mathbb{Z} \mid x^2 < 9\}$. De toute évidence, le choix de l'univers peut parfois faire la différence !

Parfois, cette notation explicite est utilisée non pas pour spécifier l'univers du discours, mais pour restreindre l'attention à une partie seulement de celui-ci. Par exemple, dans le cas de l'énoncé $x^2 < 9$, nous pourrions vouloir considérer l'univers du discours comme l'ensemble de tous les nombres réels, mais au cours d'un raisonnement impliquant cet énoncé, nous pourrions vouloir restreindre temporairement notre attention aux seuls nombres réels positifs. On pourrait alors s'intéresser à l'ensemble $\{x \in \mathbb{R}^+ \mid x^2 < 9\}$. Comme précédemment, cette notation indique que seuls les nombres réels positifs seront considérés comme élémentaux dans cet ensemble, et parmi les nombres réels positifs, seuls ceux dont le carré est inférieur à 9 seront dans l'ensemble. Ainsi, pour qu'un nombre soit un élément de cet ensemble, il doit passer deux tests : il doit être un nombre réel positif, et son carré doit être inférieur à 9. En d'autres termes, l'énoncé $y \in \{x \in$

$\mathbb{R}^+ | x^2 < 9\}$ signifie la même chose que $y \in \mathbb{R}^+ \wedge y^2 < 9$. En général, $y \in \{x \in A | P(x)\}$ signifie la même chose que $y \in A \wedge P(y)$.

Lorsqu'un nouveau concept mathématique a été défini, les mathématiciens s'intéressent généralement à l'étude de tous les extrêmes possibles de ce concept. Par exemple, lorsque nous avons discuté des tables de vérité, les extrêmes que nous avons étudiés étaient des énoncés dont les tables de vérité ne contenaient que des T (tautologies) ou que des F (contradictions). Pour le concept d'ensemble de vérité d'un énoncé contenant une variable libre, les extrêmes correspondants seraient les ensembles de vérité des énoncés qui sont toujours vrais ou toujours faux. Supposons que $P(x)$ soit un énoncé contenant une variable libre x qui s'étend sur un univers U . Il devrait être clair que si $P(x)$ est vrai pour toute valeur de x dans U , alors l'ensemble de vérité de $P(x)$ sera l'univers entier U . Par exemple, puisque l'énoncé $x_2 \geq 0$ est vrai pour tout nombre réel x , l'*ensemble* de vérité de cet énoncé est $\{x \in R | x_2 \geq 0\} = \mathbb{R}$. Bien sûr, cela n'est pas sans rapport avec le concept de tautologie ↗ Par exemple, puisque $P \vee \neg P$ est une tautologie, l'énoncé $P(x) \vee \neg P(x)$ sera vrai pour tout $x \in U$, quelle que soit l'énoncé que $P(x)$ représente ou quel que soit l'univers U , et donc l'ensemble de vérité de l'énoncé $P(x) \vee \neg P(x)$ sera U .

Pour un énoncé $P(x)$ qui est faux pour toute valeur possible de x , rien dans l'univers ne peut passer le test d'élémentarité pour l'ensemble de vérité de $P(x)$, et donc cet ensemble de vérité doit être nul. L'idée d'un ensemble sans éléments peut paraître étrange, mais elle surgit naturellement lorsque l'on considère les ensembles de vérité pour des énoncés qui sont toujours faux. Puisqu'un ensemble est complètement déterminé une fois ses éléments spécifiés, il n'existe qu'un seul ensemble qui n'en a pas. On l'appelle l'*ensemble vide*, ou l'*ensemble nul*, et on le note souvent \emptyset . Par exemple, $\{x \in \mathbb{Z} | x = x\} = \emptyset$. Puisque l'ensemble vide n'a pas d'éléments, l'énoncé $x \in \emptyset$ est un exemple d'énoncé toujours faux, quelle que soit la valeur de x .

Une autre notation courante pour l'ensemble vide repose sur le fait que tout ensemble peut être nommé en listant ses éléments entre accolades. Puisque l'ensemble vide ne contient aucun élément, on n'écrit rien entre les accolades, comme ceci : $\emptyset = \{\}$. Notez que $\{\emptyset\}$ n'est pas la notation correcte pour l'ensemble vide. Tout comme nous avons vu précédemment que 2 et {2} sont différents, \emptyset n'est pas identique à $\{\emptyset\}$. Le premier est un ensemble sans élément, tandis que le second est un ensemble avec un seul élément, cet élément étant \emptyset , l'ensemble vide.

Exercices

*1. Analysez les formes logiques des énoncés suivants :

- (a) 3 est un diviseur commun de 6, 9 et 15. (Remarque : vous avez fait cela dans [l'exercice 2](#) de [la section 1.1](#), mais vous devriez être en mesure de donner une meilleure réponse maintenant.)
- (b) x est divisible par 2 et 3 mais pas par 4.
- (c) x et y sont des nombres naturels, et l'un d'entre eux est premier.

2. Analysez les formes logiques des énoncés suivants :

- (a) x et y sont des hommes, et soit x est plus grand que y , soit y est plus grand que x .
- (b) Soit x , soit y a les yeux marrons, et soit x , soit y a les cheveux roux.
- (c) Soit x , soit y a les yeux marrons et les cheveux roux.

*3. Écrivez des définitions en utilisant des tests d'élémentarité pour les ensembles suivants :

- (a) {Mercure, Vénus, Terre, Mars, Jupiter, Saturne, Uranus, Neptune}.
- (b) {Brown, Columbia, Cornell, Dartmouth, Harvard, Princeton, Université de Pennsylvanie, Yale}.
- (c) {Alabama, Alaska, Arizona, ..., Wisconsin, Wyoming}.
- (d) {Alberta, Colombie-Britannique, Manitoba, Nouveau-Brunswick, Terre-Neuve-et-Labrador, Territoires du Nord-Ouest, Nouvelle-Écosse, Nunavut, Ontario, Île-du-Prince-Édouard, Québec, Saskatchewan, Yukon}.

4. Écrivez des définitions en utilisant des tests d'élémentarité pour les ensembles suivants :

- (a) {1, 4, 9, 16, 25, 36, 49, ...}.
- (b) {1, 2, 4, 8, 16, 32, 64, ...}.
- (c) {10, 11, 12, 13, 14, 15, 16, 17, 18, 19}.

*5. Simplifiez les affirmations suivantes. Quelles variables sont libres et lesquelles sont liées ? Si l'affirmation ne contient aucune variable libre, indiquez si elle est vraie ou fausse.

- (a) $-3 \in \{ x \in \mathbb{R} \mid 13 - 2x > 1\}$.
- (b) $4 \in \{ x \in \mathbb{R} \mid 13 - 2x > 1\}$.
- (c) $5 \notin \{ x \in \mathbb{R} \mid 13 - 2x > c\}$.

6. Simplifiez les affirmations suivantes. Quelles variables sont libres et lesquelles sont liées ? Si l'affirmation ne contient aucune variable libre, indiquez si elle est vraie ou fausse.

- (a) $w \in \{ x \in \mathbb{R} \mid 13 - 2x > c\}$.
- (b) $4 \in \{ x \in \mathbb{R} \mid 13 - 2x \in \{ y \mid y \text{ est un nombre premier}\}\}$. (Cette affirmation serait plus lisible si nous posions $P = \{ y \mid y \text{ est un nombre premier}\}$; en utilisant cette notation, nous pourrions la réécrire comme suit : $4 \in \{ x \in \mathbb{R} \mid 13 - 2x \in P\}$.)
- (c) $4 \in \{ x \in \{ y \mid y \text{ est un nombre premier}\} \mid 13 - 2x > 1\}$. (En utilisant la même notation que dans la partie (b), nous pourrions écrire ceci

comme $4 \in \{x \in P \mid 13 - 2x > 1\}.$)

7. Énumérez les éléments des ensembles suivants :

- (a) $\{x \in \mathbb{R} \mid 2x^2 + x - 1 = 0\}.$
- (b) $\{x \in \mathbb{R}^+ \mid 2x^2 + x - 1 = 0\}.$
- (c) $\{x \in \mathbb{Z} \mid 2x^2 + x - 1 = 0\}.$
- (d) $\{x \in \mathbb{N} \mid 2x^2 + x - 1 = 0\}.$

*8. Quels sont les ensembles de vérité des affirmations suivantes ?

Énumérez quelques éléments de cet ensemble de vérité si possible.

- (a) Elizabeth Taylor a été mariée à x .
- (b) x est un connecteur logique étudié dans [la section 1.1](#).
- (c) x est l'auteur de ce livre.

9. Quels sont les ensembles de vérité des affirmations suivantes ? Citez quelques éléments de cet ensemble de vérité si possible.

- (a) x est un nombre réel et $x^2 - 4x + 3 = 0$.
- (b) x est un nombre réel et $x^2 - 2x + 3 = 0$.
- (c) x est un nombre réel et $5 \in \{y \in \mathbb{R} \mid x^2 + y^2 < 50\}$.

1.4 Opérations sur les ensembles

Supposons que A soit l'ensemble de vérité d'une affirmation $P(x)$ et B l'ensemble de vérité de $Q(x)$. Quels sont les ensembles de vérité des affirmations $P(x) \wedge Q(x)$, $P(x) \vee Q(x)$ et $\neg P(x)$? Pour répondre à ces questions, nous introduisons quelques opérations de base sur les ensembles.

Définition 1.4.1. L'*intersection* de deux ensembles A et B est l'ensemble $A \cap B$ défini comme suit :

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

L'*union* de A et B est l'ensemble $A \cup B$ défini comme suit :

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

La *différence* de A et B est l'ensemble $A \setminus B$ défini comme suit :

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$$

Rappelons que les affirmations figurant dans ces définitions sont *des tests d'élémentarité*. Ainsi, par exemple, la définition de $A \cap B$ stipule que pour qu'un objet soit un élément de $A \cap B$, il doit être un élément de A et de B . Autrement dit, $A \cap B$ est l'ensemble constitué des éléments communs à A et B . *Puisque le mot « or » est toujours interprété comme*

« *or* » *inclusif* en mathématiques, Tout élément de A ou B , ou des deux, sera un élément de $A \cup B$. Ainsi, nous pouvons considérer $A \cup B$ comme l'ensemble résultant de la fusion de tous les éléments de A et B en un seul ensemble. $A \setminus B$ est l'ensemble que l'on obtiendrait en partant de l'ensemble A et en enlevant tous les éléments qui étaient également dans B .

Exemple 1.4.2. Supposons que $A = \{1, 2, 3, 4, 5\}$ et $B = \{2, 4, 6, 8, 10\}$. Lister les éléments des ensembles suivants :

1. $A \cap B$.
2. $A \cup B$.
3. $A \setminus B$.
4. $(A \cup B) \setminus (A \cap B)$.
5. $(A \setminus B) \cup (B \setminus A)$.

Solutions

1. $A \cap B = \{2, 4\}$.
2. $A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$.
3. $A \setminus B = \{1, 3, 5\}$.
4. Nous venons de calculer $A \cup B$ et $A \cap B$ dans les solutions 1 et 2, il nous suffit donc de commencer avec l'ensemble $A \cup B$ de la solution 2 et d'en retirer tous les éléments qui sont également dans $A \cap B$. La réponse est $(A \cup B) \setminus (A \cap B) = \{1, 3, 5, 6, 8, 10\}$.
5. Nous avons déjà les éléments de $A \setminus B$ listés dans la solution 3, et $B \setminus A = \{6, 8, 10\}$. Ainsi, leur union est $(A \setminus B) \cup (B \setminus A) = \{1, 3, 5, 6, 8, 10\}$. Est-ce une coïncidence que ce soit la même réponse que la réponse de la partie 4 ?

Exemple 1.4.3. Supposons que $A = \{x \mid x \text{ est un homme}\}$ et $B = \{x \mid x \text{ a les cheveux bruns}\}$. Que sont $A \cap B$, $A \cup B$ et $A \setminus B$?

Solution

Par définition, $A \cap B = \{x \mid x \in A \text{ et } x \in B\}$. Comme nous l'avons vu dans la section précédente, les définitions de A et B indiquent que $x \in A$ signifie la même chose que « x est un homme » et $x \in B$ signifie la même chose que « x a les cheveux bruns ». En intégrant cela à la définition de $A \cap B$, nous obtenons que

$$A \cap B = \{x \mid x \text{ est un homme et } x \text{ a les cheveux bruns}\}.$$

Un raisonnement similaire montre que

$$A \cup B = \{ x \mid \text{soit } x \text{ est un homme, soit } x \text{ a les cheveux bruns}\}$$

et

$$A \setminus B = \{ x \mid x \text{ est un homme et } x \text{ n'a pas les cheveux bruns}\}.$$

Il est parfois utile, lorsqu'on travaille avec des opérations sur des ensembles, de dessiner des images des résultats de ces opérations. Une façon de le faire est d'utiliser des diagrammes comme celui de [la figure 1.7](#). C'est ce qu'on appelle un *diagramme de Venn*. L'intérieur du rectangle entourant le diagramme représente l'univers du discours U , et les intérieurs des deux cercles représentent les deux ensembles A et B . D'autres ensembles formés en combinant ces ensembles seraient représentés par des régions différentes dans le diagramme. Par exemple, la région ombrée de [la figure 1.8](#) est la région commune aux intérieurs des cercles représentant A et B , et représente donc l'ensemble $A \cap B$. [Les figures 1.9](#) et [1.10](#) montrent les régions représentant $A \cup B$ et $A \setminus B$, respectivement.

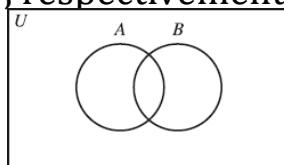


Figure 1.7.

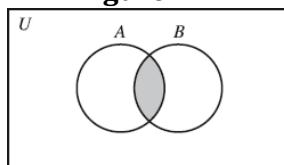


Figure 1.8. $U \cap B$.

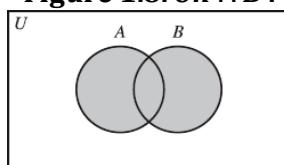


Figure 1.9. $U \cup B$.

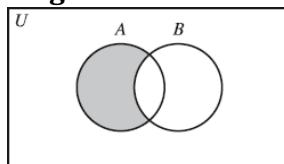


Figure 1.10. $U \setminus B$.

Voici un exemple de la façon dont les diagrammes de Venn peuvent nous aider à comprendre les opérations sur les ensembles. Dans [l'exemple 1.4.2](#), les ensembles $(A \cup B) \setminus (A \cap B)$ et $(A \setminus B) \cup (B \setminus A)$

se sont avérés égaux, pour un choix particulier de A et B . On peut constater en créant des diagrammes de Venn pour les deux ensembles que ce n'était pas une coïncidence. Vous constaterez que les deux diagrammes de Venn ressemblent à [la figure 1.11](#). Ainsi, ces ensembles seront toujours égaux, quels que soient les ensembles A et B , car les deux ensembles seront toujours l'ensemble des objets qui sont des éléments de A ou de B , mais pas des deux. Cet ensemble est appelé *différence symétrique* de A et B et s'écrit $A \Delta B$. Autrement dit, $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Plus loin dans cette section, nous verrons pourquoi ces ensembles sont toujours égaux.

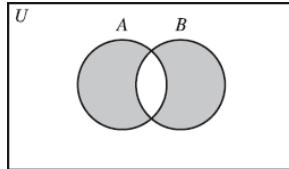


Figure 1.11. $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$.

Revenons maintenant à la question avec laquelle nous avons commencé cette section. Si A est l'ensemble de vérité d'une affirmation $P(x)$ et B est l'ensemble de vérité de $Q(x)$, alors, comme nous l'avons vu dans la section précédente, $x \in A$ signifie la même chose que $P(x)$ et $x \in B$ signifie la même chose que $Q(x)$. Ainsi, l'ensemble de vérité de $P(x) \wedge Q(x)$ est $\{x \mid P(x) \wedge Q(x)\} = \{x \mid x \in A \wedge x \in B\} = A \cap B$. Cela devrait avoir du sens. Cela dit simplement que l'ensemble de vérité de $P(x) \wedge Q(x)$ est constitué des éléments que les ensembles de vérité de $P(x)$ et $Q(x)$ ont en commun – en d'autres termes, les valeurs de x qui font que $P(x)$ et $Q(x)$ sont vrais. Nous en avons déjà vu un exemple. Dans [l'exemple 1.4.3](#), les ensembles A et B étaient les ensembles de vérité des affirmations « x est un homme » et « x a les cheveux bruns », et $A \cap B$ s'est avéré être l'ensemble de vérité de « x est un homme et x a les cheveux bruns ».

Un raisonnement similaire montre que l'ensemble de vérité de $P(x) \vee Q(x)$ est $A \cup B$. Pour trouver l'ensemble de vérité de $\neg P(x)$, nous devons parler de l'univers de discours U . L'ensemble de vérité de $\neg P(x)$ sera constitué des éléments de l'univers pour lesquels $P(x)$ est faux, et nous pouvons trouver cet ensemble en commençant par U et en enlevant les éléments pour lesquels $P(x)$ est vrai. Ainsi, l'ensemble de vérité de $\neg P(x)$ est $U \setminus A$.

Ces observations sur les ensembles de vérité illustrent le fait que les opérations de la théorie des ensembles \cap , \cup et \setminus sont liées aux connecteurs logiques \wedge , \vee et \neg . Cela ne devrait pas être surprenant, car après tout, les mots *et*, *ou*, et *not* apparaissent dans leurs définitions. (Le mot *not* n'apparaît pas explicitement, mais il est là, caché dans le symbole mathématique \notin dans la définition de la différence de deux ensembles.) Il est important de se rappeler, cependant, que bien que les

opérations de la théorie des ensembles et les connecteurs logiques soient liés, ils ne sont pas interchangeables. Les connecteurs logiques ne peuvent être utilisés que pour combiner *des énoncés*, tandis que les opérations de la théorie des ensembles doivent être utilisées pour combiner *des ensembles*. Par exemple, si A est l'ensemble de vérité de $P(x)$ et B est l'ensemble de vérité de $Q(x)$, alors nous pouvons dire que $A \cap B$ est l'ensemble de vérité de $P(x) \wedge Q(x)$, mais des expressions telles que $A \wedge B$ ou $P(x) \cap Q(x)$ n'ont absolument aucun sens et ne doivent jamais être utilisées.

La relation entre les opérations de la théorie des ensembles et les connecteurs logiques devient également apparente lorsque nous analysons les formes logiques des énoncés concernant les intersections, les unions et les différences d'ensembles. Par exemple, selon la définition de l'intersection, dire que $x \in A \cap B$ signifie que $x \in A \wedge x \in B$. De même, dire que $x \in A \cup B$ signifie que $x \in A \vee x \in B$, et $x \in A \setminus B$ signifie $x \in A \wedge x \notin B$, ou en d'autres termes $x \in A \wedge \neg(x \in B)$. Nous pouvons combiner ces règles lors de l'analyse d'énoncés concernant des ensembles plus complexes.

Exemple 1.4.4. Analysez les formes logiques des énoncés suivants :

1. $x \in A \cap (B \cup C)$.
2. $x \in A \setminus (B \cap C)$.
3. $x \in (A \cap B) \cup (A \cap C)$.

Solutions

1. $x \in A \cap (B \cup C)$

is equivalent to $x \in A \wedge x \in (B \cup C)$ (definition of \cap),
which is equivalent to $x \in A \wedge (x \in B \vee x \in C)$ (definition of \cup).

2. $x \in A \setminus (B \cap C)$

is equivalent to $x \in A \wedge \neg(x \in B \cap C)$ (definition of \setminus),
which is equivalent to $x \in A \wedge \neg(x \in B \wedge x \in C)$ (definition of \cap).

3. $x \in (A \cap B) \cup (A \cap C)$

is equivalent to $x \in (A \cap B) \vee x \in (A \cap C)$ (definition of \cup),
which is equivalent to $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$ (definition of \cap).

Regardez à nouveau les solutions des parties 1 et 3 de [l'exemple 1.4.4](#). Vous devriez reconnaître que les énoncés que nous avons obtenus dans ces deux parties sont équivalents. (Si ce n'est pas le cas, revenez aux lois distributives de [la section 1.2](#).) Cette équivalence signifie que les énoncés $x \in A \cap (B \cup C)$ et $x \in (A \cap B) \cup (A \cap C)$ sont équivalents.

En d'autres termes, les objets qui sont des éléments de l'ensemble $A \cap (B \cup C)$ seront exactement les mêmes que les objets qui sont des éléments de $(A \cap B) \cup (A \cap C)$, quels que soient les ensembles A , B et C . Mais rappelons que les ensembles avec les mêmes éléments sont égaux, il s'ensuit que pour tous les ensembles A , B et C , $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Une autre façon de voir cela est avec le Venn Diagramme de [la figure 1.12](#). Nos diagrammes de Venn précédents comportaient deux cercles, car dans les exemples précédents, seuls deux ensembles étaient combinés. Ce diagramme de Venn comporte trois cercles, qui représentent les trois ensembles A , B et C combinés ici. Bien qu'il soit possible de créer des diagrammes de Venn pour plus de trois ensembles, cette méthode est rarement utilisée, car elle est impossible avec des cercles superposés. Pour en savoir plus sur les diagrammes de Venn pour plus de trois ensembles, voir [l'exercice 12](#).

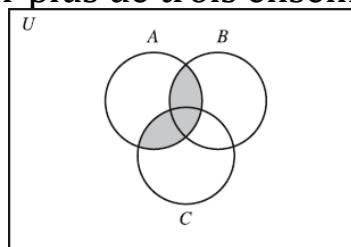


Figure 1.12. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Ainsi, nous voyons qu'une loi distributive pour les connecteurs logiques a conduit à une loi distributive pour les opérations de la théorie des ensembles. On pourrait supposer que, puisqu'il existait *deux* lois distributives pour les connecteurs logiques, \wedge et \vee jouant des rôles opposés dans les deux lois, il pourrait également y avoir deux lois distributives pour les opérations de la théorie des ensembles. La deuxième loi distributive pour les ensembles devrait dire que pour tout ensemble A , B et C , $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Vous pouvez le vérifier par vous-même en écrivant les affirmations $x \in A \cup (B \cap C)$ et $x \in (A \cup B) \cap (A \cup C)$ en utilisant des connecteurs logiques et en vérifiant qu'elles sont équivalentes, en utilisant la deuxième loi distributive pour les connecteurs logiques \wedge et \vee . Une autre façon de le voir est de faire un diagramme de Venn.

Nous pouvons dériver une autre identité de théorie des ensembles en trouvant un énoncé équivalent à l'énoncé avec lequel nous nous sommes retrouvés dans la partie 2 de [l'exemple 1.4.4](#) :

$$x \in A \setminus (B \cap C)$$

est équivalent à $x \in A \neg(x \in B \wedge (Exemple\ 1.4.4))$
 $x \in C)$

ce qui équivaut à $x \in A \wedge (x \notin B \vee x \in C)$ (loi de De Morgan),

$\notin C)$

ce qui équivaut à $(x \in A \wedge x \notin B) \vee (x \in A \wedge x \in C)$ (loi distributive),

$(x \in A \wedge x \notin C)$

ce qui équivaut à $(x \in A \setminus B) \vee (x \in A \setminus C)$ (définition de \setminus),

$\in A \setminus C)$

ce qui équivaut à $x \in (A \setminus B) \cup (A \setminus C)$ (définition de \cup).

$\setminus C)$

Ainsi, nous avons montré que pour tout ensemble A , B et C , nous avons $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. Une fois de plus, vous pouvez également vérifier cela avec un diagramme de Venn.

Nous avons précédemment proposé une méthode alternative pour vérifier l'identité $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$. Voyons maintenant comment procéder. Commençons par écrire les formes logiques des énoncés $x \in (A \cup B) \setminus (A \cap B)$ et $x \in (A \setminus B) \cup (B \setminus A)$:

$$x \in (A \cup B) \setminus (A \cap B) \text{ means } (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B);$$

$$x \in (A \setminus B) \cup (B \setminus A) \text{ means } (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A).$$

Vous pouvez maintenant vérifier, en utilisant les équivalences de [la section 1.2](#), que ces affirmations sont équivalentes. Une autre façon de vérifier l'équivalence est d'utiliser une table de vérité. Pour simplifier la table de vérité, utilisons P et Q comme abréviations pour les affirmations $x \in A$ et $x \in B$. Ensuite, nous devons vérifier que les formules $(P \vee Q) \wedge \neg(P \wedge Q)$ et $(P \wedge \neg Q) \vee (Q \wedge \neg P)$ sont équivalentes. La table de vérité de [la figure 1.13](#) le montre.

P	Q	$(P \vee Q) \wedge \neg(P \wedge Q)$	$(P \wedge \neg Q) \vee (Q \wedge \neg P)$
F	F	F	F
F	T	T	T
T	F	T	T
T	T	F	F

Figure 1.13.

Définition 1.4.5. Supposons que A et B soient des ensembles. On dira que A est un *sous-ensemble* de B si tout élément de A est aussi un élément de B . On écrit $A \subseteq B$ pour signifier que A est un sous-ensemble de B . A et B sont dits *disjoints* s'ils n'ont aucun élément en commun. Notons que cela revient à dire que l'ensemble de leurs éléments communs est l'ensemble vide, autrement dit $A \cap B = \emptyset$.

Exemple 1.4.6. Supposons que $A = \{\text{rouge, vert}\}$, $B = \{\text{rouge, jaune, vert, violet}\}$ et $C = \{\text{bleu, violet}\}$. Alors, les deux éléments de A , rouge et vert,

sont également dans B , et donc $A \subseteq B$. De plus, $A \cap C = \emptyset$, donc A et C sont disjoints.

Si nous savons que $A \subseteq B$, ou que A et B sont disjoints, nous pourrions alors dessiner un diagramme de Venn différent pour A et B afin de refléter ce fait. [Les figures 1.14 et 1.15](#) illustrent ce point.

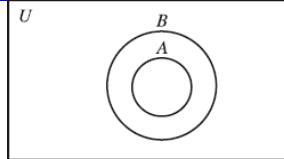


Figure 1.14. $U \subseteq B$.

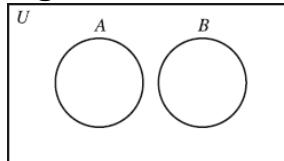


Figure 1.15. $A \cap B = \emptyset$.

Tout comme nous avons précédemment établi des identités montrant que certains ensembles sont toujours égaux, il est parfois possible de montrer que certains ensembles sont toujours disjoints, ou qu'un ensemble est toujours un sous-ensemble d'un autre. Par exemple, un diagramme de Venn montre que les ensembles $A \cap B$ et $A \setminus B$ ne se chevauchent pas et sont donc toujours disjoints pour tous les ensembles A et B . Une autre façon de comprendre cela serait d'écrire ce que signifie $x \in (A \cap B) \cap (A \setminus B)$:

$$x \in (A \cap B) \cap (A \setminus B) \text{ means } (x \in A \wedge x \in B) \wedge (x \in A \wedge x \notin B), \\ \text{which is equivalent to } x \in A \wedge (x \in B \wedge x \notin B).$$

Mais cette dernière affirmation est clairement une contradiction, donc l'affirmation $x \in (A \cap B) \cap (A \setminus B)$ sera toujours fausse, peu importe ce que vaut x . En d'autres termes, rien ne peut être un élément de $(A \cap B) \cap (A \setminus B)$, il doit donc être le cas que $(A \cap B) \cap (A \setminus B) = \emptyset$. Par conséquent, $A \cap B$ et $A \setminus B$ sont disjoints.

Le théorème suivant donne un autre exemple d'un fait général concernant les opérations sur les ensembles. Sa démonstration illustre que les principes du raisonnement déductif que nous avons étudiés sont effectivement utilisés dans les démonstrations mathématiques.

Théorème 1.4.7. Pour tous les ensembles UN et B , $(A \cup B) \setminus B \subseteq A$.

Preuve. Nous devons montrer que si quelque chose est un élément de $(A \cup B) \setminus B$, alors il doit aussi être un élément de A , donc supposons que $x \in (A \cup B) \setminus B$. Cela signifie que $x \in A \cup B$ et $x \notin B$, ou en d'autres termes $x \in A \vee x \in B$ et $x \notin B$. Mais remarquez que ces énoncés ont la

forme logique $P \vee Q$ et $\neg Q$, et c'est précisément la forme des prémisses de notre tout premier exemple d'argument déductif dans [la section 1.1](#) ! Comme nous l'avons vu dans cet exemple, à partir de ces prémisses, nous pouvons conclure que $x \in A$ doit être vrai. Ainsi, tout ce qui est un élément de $(A \cup B) \setminus B$ doit aussi être un élément de A , donc $(A \cup B) \setminus B \subseteq A$.

□

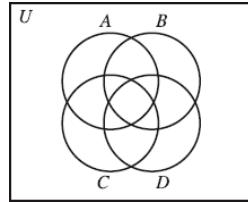
On pourrait penser qu'une application aussi rigoureuse des lois logiques n'est pas nécessaire pour comprendre pourquoi [le théorème 1.4.7](#) est correct. L'ensemble $(A \cup B) \setminus B$ pourrait être considéré comme le résultat de l'ajout, à partir de l'ensemble A , des éléments de B , puis de leur suppression. Le bon sens suggère que le résultat sera soit simplement l'ensemble initial A ; autrement dit, il apparaît que $(A \cup B) \setminus B = A$. Cependant, comme on vous demande de le démontrer dans [l'exercice 10](#), cette conclusion est incorrecte. Cela illustre qu'en mathématiques, il ne faut pas se laisser entraîner par des raisonnements imprécis à des conclusions hâtives. Appliquer soigneusement les lois de la logique, comme nous l'avons fait dans notre démonstration du [théorème 1.4.7](#), peut vous aider à éviter de tirer des conclusions hâtives.

Exercices

- *1. Soit $A = \{1, 3, 12, 35\}$, $B = \{3, 7, 12, 20\}$ et $C = \{x \mid x \text{ est un nombre premier}\}$. Énumérez les éléments des ensembles suivants. Certains de ces ensembles sont-ils disjoints ? Certains de ces ensembles sont-ils des sous-ensembles d'autres ?
 - (a) $A \cap B$.
 - (b) $(A \cup B) \setminus C$.
 - (c) $A \cup (B \setminus C)$.
- 2. Soit $A = \{\text{États-Unis, Allemagne, Chine, Australie}\}$, $B = \{\text{Allemagne, France, Inde, Brésil}\}$ et $C = \{x \mid x \text{ est un pays d'Europe}\}$. Énumérez les éléments des ensembles suivants. Certains de ces ensembles sont-ils disjoints ? Certains de ces ensembles sont-ils des sous-ensembles d'autres ?
 - (a) $A \cup B$.
 - (b) $(A \cap B) \setminus C$.
 - (c) $(B \cap C) \setminus A$.
- 3. Vérifiez que les diagrammes de Venn pour $(A \cup B) \setminus (A \cap B)$ et $(A \setminus B) \cup (B \setminus A)$ ressemblent tous deux à [la figure 1.11](#), comme indiqué dans cette section.
- *4. Utilisez les diagrammes de Venn pour vérifier les identités suivantes :

- (a) $Un \setminus (A \cap B) = A \setminus B$.
 (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

5. Vérifiez les identités de [l'exercice 4](#) en écrivant (en utilisant des symboles logiques) ce que signifie pour un objet x d'être un élément de chaque ensemble, puis en utilisant des équivalences logiques.
6. Utilisez les diagrammes de Venn pour vérifier les identités suivantes :
- (a) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.
 (b) $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$.
7. Vérifiez les identités de [l'exercice 6](#) en écrivant (en utilisant des symboles logiques) ce que signifie pour un objet x d'être un élément de chaque ensemble, puis en utilisant des équivalences logiques.
8. Utilisez la méthode de votre choix pour vérifier les identités suivantes :
- (a) $(A \setminus B) \cap C = (A \cap C) \setminus B$.
 (b) $(A \cap B) \setminus B = \emptyset$.
 (c) $Un \setminus (A \setminus B) = A \cap B$.
- *9. Pour chacun des ensembles suivants, écrivez (à l'aide de symboles logiques) ce que signifie qu'un objet x soit un élément de l'ensemble. Déterminez ensuite lesquels de ces ensembles doivent être égaux en identifiant les affirmations équivalentes.
- (a) $(A \setminus B) \setminus C$.
 (b) $Un \setminus (B \setminus C)$.
 (c) $(A \setminus B) \cup (A \cap C)$.
 (d) $(A \setminus B) \cap (A \setminus C)$.
 (e) $Un \setminus (B \cup C)$.
10. Il a été démontré dans cette section que pour tout ensemble A et B , $(A \cup B) \setminus B \subseteq A$.
- (a) Donnez un exemple de deux ensembles A et B pour lesquels $(A \cup B) \setminus B = A$.
 (b) Montrer que pour tous les ensembles A et B , $(A \cup B) \setminus B = A \setminus B$.
11. Supposons que A et B soient des ensembles. Est-il nécessairement vrai que $(A \setminus B) \cup B = A$? Si non, l'un de ces ensembles est-il nécessairement un sous-ensemble de l'autre? $(A \setminus B) \cup B$ est-il toujours égal à $A \setminus B$ ou à $A \cup B$?
12. Il est affirmé dans cette section que vous ne pouvez pas créer un diagramme de Venn pour quatre ensembles en utilisant des cercles qui se chevauchent.
- (a) Quel est le problème avec le diagramme suivant? (Indice : où se trouve l'ensemble $(A \cap D) \setminus (B \cup C)$?)



(b) Pouvez-vous créer un diagramme de Venn pour quatre ensembles en utilisant des formes autres que des cercles ?

13. (a) Tracez des diagrammes de Venn pour les ensembles $(A \cup B) \setminus C$ et $A \cup (B \setminus C)$. Que pouvez-vous conclure quant à savoir si l'un de ces ensembles est nécessairement un sous-ensemble de l'autre ?

(b) Donnez un exemple d'ensembles A , B et C pour lesquels $(A \cup B) \setminus C \neq A \cup (B \setminus C)$.

14. Utilisez des diagrammes de Venn pour montrer que la loi associative est valable pour les différences symétriques ; c'est-à-dire que pour tous les ensembles A , B et C , $A(B \Delta C) = (A \Delta B)C$.

15. Utilisez la méthode de votre choix pour vérifier les identités suivantes :

$$(un) (A \Delta B) \cup C = (A \cup C) \Delta (B \setminus C).$$

$$(b) (A \Delta B) \cap C = (A \cap C) \Delta (B \cap C).$$

$$(c) (A \Delta B) \setminus C = (A \setminus C) \Delta (B \setminus C).$$

16. Utilisez la méthode de votre choix pour vérifier les identités suivantes :

$$(un) (A \cup B) \Delta C = (A \Delta C) \Delta (B \setminus A).$$

$$(b) (A \cap B) \Delta C = (A \Delta C) \Delta (A \setminus B).$$

$$(c) (A \setminus B) \Delta C = (A \Delta C) \Delta (A \cap B).$$

17. Remplissez les blancs pour créer de véritables identités :

$$(un) (A \Delta B) \cap C = (C \setminus A) \Delta \underline{\hspace{2cm}}.$$

$$(b) C \setminus (A \Delta B) = (A \cap C) \Delta \underline{\hspace{2cm}}.$$

$$(c) (B \setminus A) \Delta C = (A \Delta C) \Delta \underline{\hspace{2cm}}.$$

1.5 Les connecteurs conditionnels et biconditionnels

Il est temps de revenir à une question restée sans réponse dans [la section 1.1](#). Nous avons vu comment le raisonnement des premier et troisième arguments de [l'exemple 1.1.1](#) peut être compris en analysant les connecteurs \vee et \neg . Mais qu'en est-il du raisonnement du deuxième argument ? Rappelons que l'argument était le suivant :

Si c'est dimanche aujourd'hui, je n'ai pas besoin d'aller travailler aujourd'hui.

Aujourd'hui est dimanche.

Je n'ai donc pas besoin d'aller travailler aujourd'hui.

Qu'est-ce qui rend ce raisonnement valable ?

Il apparaît que les mots clés ici sont « *si* » et « *alors* », présents dans la première prémissse. Nous introduisons donc un nouveau connecteur logique, \rightarrow , et écrivons $P \rightarrow Q$ pour représenter l'énoncé « Si P alors Q ». Cet énoncé est parfois appelé « énoncé *conditionnel* », avec P comme *antécédent* et Q comme *conséquent*. Si nous supposons que P représente l'énoncé « Aujourd'hui, c'est dimanche » et Q celui « Je n'ai pas à aller travailler aujourd'hui », la forme logique de l'argument serait :

$$\frac{\begin{array}{c} P \rightarrow Q \\ P \end{array}}{\therefore Q}$$

Notre analyse du nouveau connecteur \rightarrow devrait conduire à la conclusion que cet argument est valable.

Exemple 1.5.1. Analyser les formes logiques des énoncés suivants :

1. S'il pleut et que je n'ai pas mon parapluie, je serai mouillé.
2. Si Marie a fait ses devoirs, le professeur ne les récupérera pas, et si elle ne les a pas fait, il lui demandera de les faire au tableau.

Solutions

1. Soit R pour l'énoncé « Il pleut », U pour « J'ai mon parapluie » et W pour « Je vais être mouillé ». L'énoncé 1 serait alors représenté par la formule $(R \wedge \neg U) \rightarrow W$.
2. Soit H pour « Marie a fait ses devoirs », C pour « Le professeur viendra les chercher » et B pour « Le professeur demandera à Marie de faire les devoirs au tableau ». Alors l'énoncé donné signifie $(H \rightarrow \neg C) \wedge (\neg H \rightarrow B)$.

Pour analyser les arguments contenant le connecteur \rightarrow , nous devons calculer la table de vérité de la formule $P \rightarrow Q$. Puisque $P \rightarrow Q$ est censé signifier que si P est vrai alors Q l'est aussi, nous voulons certainement dire que si P est vrai et Q est faux alors $P \rightarrow Q$ est faux. Si P est vrai et Q est également vrai, alors il semble raisonnable de dire que $P \rightarrow Q$ est vrai. Cela nous donne les deux dernières lignes de la table de vérité de [la figure 1.16](#). Les deux lignes restantes sont plus difficiles à compléter, bien que la plupart des gens diraient probablement que si P et Q sont tous deux faux alors $P \rightarrow Q$ doit être considéré comme vrai. Ainsi, nous pouvons résumer nos conclusions jusqu'à présent avec le tableau de [la figure 1.16](#).

P	Q	$P \rightarrow Q$
F	F	T?
F	T	?
T	F	F
T	T	T

Figure 1.16.

Pour nous aider à compléter les lignes indéterminées de cette table de vérité, prenons un exemple. Prenons l'affirmation « Si $x > 2$ alors $x^2 > 4$ », que nous pourrions représenter par la formule $P(x) \rightarrow Q(x)$, où $P(x)$ représente l'affirmation $x > 2$ et $Q(x)$ représente $x^2 > 4$. Bien sûr, les affirmations $P(x)$ et $Q(x)$ contiennent x comme variable libre, et chacune sera vraie pour certaines valeurs de x et fausse pour d'autres. Mais quelle que soit la valeur de x , nous dirais qu'il est vrai que *si* $x > 2$ alors $x^2 > 4$, donc la condition $P(x) \rightarrow Q(x)$ devrait être vraie. Ainsi, la table de vérité devrait être complétée de telle sorte que, quelle que soit la valeur de x , cette condition soit vraie.

Français Par exemple, supposons $x = 3$. Dans ce cas $x > 2$ et $x^2 = 9 > 4$, donc $P(x)$ et $Q(x)$ sont toutes deux vraies. Cela correspond à la ligne quatre de la table de vérité de [la Figure 1.16](#), et nous avons déjà décidé que l'affirmation $P(x) \rightarrow Q(x)$ devrait être vraie dans ce cas. Mais considérons maintenant le cas $x = 1$. Alors $x < 2$ et $x^2 = 1 < 4$, donc $P(x)$ et $Q(x)$ sont toutes deux fausses, correspondant à la ligne un de la table de vérité. Nous avons provisoirement placé un T dans cette ligne de la table de vérité, et nous voyons maintenant que ce choix provisoire doit être correct. Si nous y mettons un F, alors l'affirmation $P(x) \rightarrow Q(x)$ serait fausse dans le cas $x = 1$, et nous avons déjà décidé qu'elle devrait être vraie pour toutes les valeurs de x .

Enfin, considérons le cas $x = -5$. Alors $x < 2$, donc $P(x)$ est faux, mais $x^2 = 25 > 4$, donc $Q(x)$ est vrai. Ainsi, dans ce cas, nous nous trouvons à la deuxième ligne de la table de vérité, et encore une fois, pour que l'énoncé conditionnel $P(x) \rightarrow Q(x)$ soit vrai dans ce cas, nous devons mettre un T sur cette ligne. Il apparaît donc que toutes les lignes douteuses de la table de vérité de [la figure 1.16](#) doivent être complétées par des T, et la table de vérité complétée pour le connecteur \rightarrow doit être telle que montrée dans [la figure 1.17](#).

P	Q	$P \rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

Figure 1.17.

Bien sûr, il existe de nombreuses autres valeurs de x qui pourraient être intégrées à notre affirmation « Si $x > 2$ alors $x^2 > 4$ » ; mais si vous

les essayez, vous constaterez qu'elles mènent toutes à la ligne un, deux ou quatre de la table de vérité, comme l'ont fait nos exemples $x = 1, -5$ et 3 . Aucune valeur de x ne mènera à la ligne trois, car il ne pourrait jamais y avoir $x > 2$ mais $x^2 \leq 4$. Après tout, c'est pourquoi nous avons dit que l'affirmation « Si $x > 2$ alors $x^2 > 4$ » était toujours vraie, quelle que soit la valeur de x ! Dire que cette affirmation conditionnelle est toujours vraie signifie simplement qu'on ne trouvera jamais de valeur de x telle que $x > 2$ et $x^2 \leq 4$; autrement dit, il n'existe aucune valeur de x pour laquelle $P(x)$ est vraie mais $Q(x)$ est fausse. Il devrait donc être logique que dans la table de vérité pour $P \rightarrow Q$, la seule ligne qui soit fausse soit la ligne dans laquelle P est vrai et Q est faux.

Comme le montre la table de vérité de [la figure 1.18](#), la formule $\neg P \vee Q$ est également vraie dans tous les cas, sauf lorsque P est vrai et Q est faux. Ainsi, si nous acceptons la table de vérité de la [figure 1.17](#) comme la table de vérité correcte pour la formule $P \rightarrow Q$, nous serons alors contraints d'accepter la conclusion que les formules $P \rightarrow Q$ et $\neg P \vee Q$ sont équivalentes. Est-ce cohérent avec l'utilisation courante des mots « *si* » et « *alors* » ? Cela peut sembler faux à première vue, mais, au moins pour certaines utilisations des mots « *si* » et « *alors* », c'est le cas.

P	Q	$\neg P \vee Q$
F	F	T
F	T	T
T	F	F
T	T	T

Figure 1.18.

Par exemple, imaginez un enseignant disant à une classe, d'un ton menaçant : « Vous ne négligerez pas vos devoirs, sinon vous échouerez au cours. » Grammaticalement, cette affirmation a la forme $\neg P \vee Q$, où P est l'affirmation « Vous négligerez vos devoirs » et Q est « Vous échouerez au cours ». Mais quel message l'enseignant essaie-t-il de transmettre avec cette affirmation ? Clairement, le message voulu est « Si vous négligez vos devoirs, alors vous échouerez au cours », ou en d'autres termes $P \rightarrow Q$. Ainsi, dans cet exemple, les formules $\neg P \vee Q$ et $P \rightarrow Q$ semblent signifier la même chose.

Il y a une idée similaire à l'œuvre dans la première affirmation de [l'exemple 1.1.2](#), « Soit John est allé au magasin, soit nous n'avons plus d'œufs. » Dans [la section 1.1](#), nous avons représenté cette affirmation par la formule $P \vee Q$, où P signifie « John est allé au magasin » et Q « Nous n'avons plus d'œufs ». Mais quelqu'un qui ferait cette affirmation essaierait probablement d'exprimer l'idée que si John n'est pas allé au magasin, alors nous n'avons plus d'œufs, ou en d'autres termes $\neg P \rightarrow Q$. Ainsi, cet exemple suggère que $\neg P \rightarrow Q$ signifie la même chose que $P \vee Q$. En fait, nous pouvons déduire cette équivalence de la précédente en substituant $\neg P$ à P . Parce que $P \rightarrow Q$ est équivalent à $\neg P \vee Q$, il s'ensuit

que $\neg P \rightarrow Q$ est équivalent à $\neg\neg P \vee Q$, qui est équivalent à $P \vee Q$ par la loi de double négation.

Nous pouvons déduire une autre équivalence utile comme suit :

$$\begin{array}{ll} \neg P \vee Q \text{ is equivalent to } \neg P \vee \neg\neg Q & (\text{double negation law}), \\ \text{which is equivalent to } \neg(P \wedge \neg Q) & (\text{De Morgan's law}). \end{array}$$

Français Ainsi, $P \rightarrow Q$ est aussi équivalent à $\neg(P \wedge \neg Q)$. En fait, c'est précisément la conclusion à laquelle nous sommes arrivés plus tôt en discutant de l'énoncé « Si $x > 2$ alors $x^2 > 4$ ». Nous avons alors décidé que la raison pour laquelle cet énoncé est vrai pour chaque valeur de x est qu'il n'y a pas de valeur de x pour laquelle $x > 2$ et $x^2 \leq 4$. En d'autres termes, l'énoncé $P(x) \wedge \neg Q(x)$ n'est jamais vrai, alors que comme précédemment $P(x)$ représente $x > 2$ et $Q(x)$ représente $x^2 > 4$. Mais c'est la même chose que de dire que l'énoncé $\neg(P(x) \wedge \neg Q(x))$ est toujours vrai. Ainsi, dire que $P(x) \rightarrow Q(x)$ est toujours vrai signifie la même chose que dire que $\neg(P(x) \wedge \neg Q(x))$ est toujours vrai.

Pour un autre exemple de cette équivalence, considérons l'affirmation « S'il va pleuvoir, alors je prendrai mon parapluie. » Bien sûr, cette affirmation a la forme $P \rightarrow Q$, où P représente l'affirmation « Il va pleuvoir » et Q signifie « Je prendrai mon parapluie. » Mais nous pourrions aussi considérer cette affirmation comme une déclaration selon laquelle je ne serai pas surpris par la pluie sans mon parapluie – en d'autres termes, $\neg(P \wedge \neg Q)$.

Pour résumer, jusqu'à présent, nous avons découvert les équivalences suivantes impliquant des instructions conditionnelles :

Lois conditionnelles

$$\begin{array}{l} P \rightarrow Q \text{ is equivalent to } \neg P \vee Q. \\ P \rightarrow Q \text{ is equivalent to } \neg(P \wedge \neg Q). \end{array}$$

Si vous n'êtes toujours pas convaincu de la validité de la table de vérité de [la figure 1.17](#), nous vous donnons une raison supplémentaire. Nous savons qu'avec cette table de vérité, nous pouvons désormais analyser la validité des arguments déductifs impliquant les mots « si » et « alors ». L'analyse de quelques arguments simples nous permettra de constater que la table de vérité de [la figure 1.17](#) conduit à des conclusions raisonnables sur la validité de ces arguments. Cependant, toute modification de la table de vérité aboutirait à des conclusions clairement erronées. Par exemple, revenons à la forme d'argument avec laquelle nous avons commencé cette section :

$$\frac{\begin{array}{c} P \rightarrow Q \\ P \end{array}}{\therefore Q}$$

Nous avons déjà décidé que ce type d'argumentation était valide, et la table de vérité de [la figure 1.19](#) le confirme. Les prémisses ne sont vraies qu'à la quatrième ligne du tableau, et la conclusion l'est également à cette ligne.

		Premises		Conclusion
P	Q	$P \rightarrow Q$	P	Q
F	F	T	F	F
F	T	T	F	T
T	F	F	T	F
T	T	T	T	T

Figure 1.19.

On peut également constater sur [la figure 1.19](#) que les deux prémisses sont nécessaires pour valider cet argument. Mais si nous modifiions la table de vérité de l'énoncé conditionnel pour rendre $P \rightarrow Q$ faux à la première ligne, la seconde prémissse de cet argument deviendrait inutile. Nous conclurions que, de la seule prémissse $P \rightarrow Q$, nous pourrions inférer que Q doit être vraie, puisque dans les deux lignes de la table de vérité où la prémissse $P \rightarrow Q$ serait toujours vraie, lignes deux et quatre, la conclusion Q est également vraie. Mais cela ne semble pas correct. Le simple fait de savoir que *si P est vrai alors Q est vrai*, mais sans savoir que *P est vraie*, il ne semble pas raisonnable de conclure que *Q est vraie*. Par exemple, supposons que nous sachions que l'affirmation « Si John n'est pas allé au magasin, alors nous n'avons plus d'œufs » est vraie. À moins de savoir également si John est allé au magasin, nous ne pouvons conclure que nous n'avons plus d'œufs. Ainsi, modifier la première ligne de la table de vérité pour $P \rightarrow Q$ conduirait à une conclusion erronée sur la validité d'un argument.

Modifier la deuxième ligne de la table de vérité conduirait également à des conclusions inacceptables quant à la validité des arguments. Pour le comprendre, considérons la forme de l'argument :

$$\frac{P \rightarrow Q \\ Q}{\therefore P}$$

Ceci ne doit *pas* être considéré comme une forme de raisonnement valide. Prenons par exemple l'argument suivant, qui se présente sous cette forme :

Si Jones a été reconnu coupable du meurtre de Smith, il ira en prison.

Jones ira en prison.

Par conséquent, Jones a été reconnu coupable du meurtre de Smith.

Même si les prémisses de cet argument sont vraies, la conclusion selon laquelle Jones a été reconnu coupable du meurtre de Smith ne tient pas. Il ira peut-être en prison pour avoir braqué une banque ou fraudé son impôt sur le revenu. Ainsi, la conclusion de cet argument pourrait être

fausse même si les prémisses étaient vraies, et l'argument n'est donc pas valable.

L'analyse de la table de vérité de [la figure 1.20](#) confirme cette conclusion. À la deuxième ligne du tableau, la conclusion P est fausse, mais les deux prémisses sont vraies ; l'argument est donc invalide. Cependant, si nous modifions la table de vérité pour $P \rightarrow Q$ et la rendons fausse à la deuxième ligne, l'analyse de la table de vérité confirmerait la validité de l'argument. Ainsi, l'analyse de cet argument semble appuyer notre décision d'insérer un T à la deuxième ligne de la table de vérité pour $P \rightarrow Q$.

		Premises		Conclusion
P	Q	$P \rightarrow Q$	Q	P
F	F	T	F	F
F	T	T	T	F
T	F	F	F	T
T	T	T	T	T

Figure 1.20.

Le dernier exemple montre qu'il est incorrect d'inférer P à partir des prémisses $P \rightarrow Q$ et Q . En revanche, il serait certainement correct d'inférer P à partir des prémisses $Q \rightarrow P$ et Q . Cela montre que les formules $P \rightarrow Q$ et $Q \rightarrow P$ n'ont *pas* la même signification. On peut le vérifier en établissant une table de vérité pour les deux et en vérifiant qu'elles ne sont pas équivalentes. Par exemple, une personne pourrait croire que, en général, l'affirmation « Si vous êtes un meurtrier condamné, alors vous n'êtes pas digne de confiance » est vraie, sans croire que l'affirmation « Si vous n'êtes pas digne de confiance, alors vous êtes un meurtrier condamné » est généralement vraie. La formule $Q \rightarrow P$ est appelée la *réciproque* de $P \rightarrow Q$. Il est très important de ne jamais confondre une instruction conditionnelle avec sa réciproque.

La *contraposée* de $P \rightarrow Q$ est la formule $\neg Q \rightarrow \neg P$, et elle est équivalente à $P \rightarrow Q$. Cela peut ne pas sembler évident au premier abord, mais on peut le vérifier à l'aide d'une table de vérité. Par exemple, les affirmations « Si Jean a encaissé le chèque que j'ai émis, alors mon compte bancaire est à découvert » et « Si mon compte bancaire n'est pas à découvert, alors Jean n'a pas encaissé le chèque que j'ai émis » sont équivalentes. Je serais enclin à affirmer les deux dans les mêmes circonstances, à savoir si le chèque que j'ai émis était d'un montant supérieur à celui que j'avais sur mon compte. L'équivalence des énoncés conditionnels et de leurs contraposés est souvent utilisée en raisonnement mathématique. Nous l'ajoutons à notre liste d'équivalences importantes :

Loi contrapositive

$P \rightarrow Q$ est équivalent à $\neg Q \rightarrow \neg P$.

Exemple 1.5.2. Lesquelles des affirmations suivantes sont équivalentes ?

1. S'il pleut ou neige, le match est annulé.
2. Si le match n'a pas été annulé, alors il ne pleut pas et il ne neige pas.
3. Si le match a été annulé, c'est qu'il pleut ou qu'il neige.
4. S'il pleut, le match est annulé, et s'il neige, le match est annulé.
5. S'il ne pleut ni ne neige, le match n'a pas été annulé.

Solution

Nous traduisons toutes les affirmations en notation logique, en utilisant les abréviations suivantes : R signifie « Il pleut », S signifie « Il neige » et C signifie « Le match a été annulé ».

1. $(R \vee S) \rightarrow C$.
2. $\neg C \rightarrow (\neg R \wedge \neg S)$. Selon l'une des lois de De Morgan, cela équivaut à $\neg C \rightarrow \neg(R \vee S)$. C'est la contraposée de l'énoncé 1 ; ils sont donc équivalents.
3. $C \rightarrow (R \vee S)$. C'est la réciproque de l'affirmation 1, qui n'est *pas* équivalente. Vous pouvez le vérifier avec une table de vérité ou simplement réfléchir à la signification de ces affirmations. L'affirmation 1 indique que la pluie ou la neige entraîneraient l'annulation de la partie. L'affirmation 3 indique que ce sont les *seules* circonstances dans lesquelles la partie sera annulée.
4. $(R \rightarrow C) \wedge (S \rightarrow C)$. Ceci est également équivalent à l'énoncé 1, comme le montre le raisonnement suivant :

$$\begin{aligned}
 (R \rightarrow C) \wedge (S \rightarrow C) & \\
 \text{is equivalent to } (\neg R \vee C) \wedge (\neg S \vee C) & \text{(conditional law),} \\
 \text{which is equivalent to } (\neg R \wedge \neg S) \vee C & \text{(distributive law),} \\
 \text{which is equivalent to } \neg(R \vee S) \vee C & \text{(De Morgan's law),} \\
 \text{which is equivalent to } (R \vee S) \rightarrow C & \text{(conditional law).}
 \end{aligned}$$

Vous devriez relire les affirmations 1 et 4 et voir si cela vous semble logique qu'elles soient équivalentes.

5. $\neg(R \vee S) \rightarrow \neg C$. C'est la contraposée de l'énoncé 3 ; ils sont donc équivalents. Ce n'est pas équivalent aux énoncés 1, 2 et 4.

Les énoncés signifiant $P \rightarrow Q$ sont très fréquents en mathématiques, mais ils ne sont pas toujours exprimés sous la forme « Si P alors Q ». Voici quelques autres façons d'exprimer l'idée $P \rightarrow Q$, souvent utilisées en mathématiques :

P implique Q .

Q , si P .

P seulement si Q .

P est une condition suffisante pour Q .

Q est une condition nécessaire pour P .

Certaines de ces affirmations peuvent nécessiter des explications supplémentaires. La deuxième expression, « Q , si P », n'est qu'une légère reformulation de l'énoncé « Si P alors Q », il devrait donc être logique qu'elle signifie $P \rightarrow Q$. À titre d'exemple d'énoncé de la forme « P seulement si Q », considérons la phrase « Vous ne pouvez vous présenter à l'élection présidentielle que si vous êtes citoyen. » Dans ce cas, P signifie « Vous pouvez vous présenter à l'élection présidentielle » et Q « Vous êtes citoyen. » Cela signifie que si vous n'êtes pas citoyen, vous ne pouvez pas vous présenter à l'élection présidentielle, ou en d'autres termes $\neg Q \rightarrow \neg P$. Mais par la loi contraposée, cela équivaut à $P \rightarrow Q$.

Considérez « P est une condition suffisante pour Q » comme signifiant « La vérité de P suffit à garantir la vérité de Q », et il devrait être logique que cela soit représenté par $P \rightarrow Q$. Enfin, « Q est une condition nécessaire pour P » signifie que pour que P soit vraie, il est nécessaire que Q le soit aussi. Cela signifie que si Q n'est pas vraie, alors P ne peut pas l'être non plus, autrement dit, $\neg Q \rightarrow \neg P$. De nouveau, par la loi contraposée, nous obtenons $P \rightarrow Q$.

Exemple 1.5.3. Analysez les formes logiques des énoncés suivants :

1. Si au moins dix personnes sont présentes, alors la conférence aura lieu.
2. La conférence ne sera donnée que si au moins dix personnes sont présentes.
3. La conférence aura lieu si au moins dix personnes sont présentes.
4. La présence d'au moins dix personnes est une condition suffisante pour que la conférence soit donnée.
5. La présence d'au moins dix personnes est une condition nécessaire pour que la conférence soit donnée.

Solutions

Soit T pour l'affirmation « Au moins dix personnes sont présentes » et L pour « La conférence sera donnée ».

1. $T \rightarrow L$.
2. $L \rightarrow T$. L'énoncé donné signifie que s'il n'y a pas au moins dix personnes présentes, alors la conférence n'aura pas lieu, ou en

d'autres termes $\neg T \rightarrow \neg L$. Par la loi contraposée, cela équivaut à $L \rightarrow T$.

3. $T \rightarrow L$. Il s'agit simplement d'une reformulation de l'énoncé 1.
4. $T \rightarrow L$. L'énoncé dit qu'il suffit d'avoir au moins dix personnes présentes pour garantir que la conférence sera donnée, ce qui signifie que s'il y a au moins dix personnes présentes, alors la conférence sera donnée.
5. $L \rightarrow T$. Cette affirmation signifie la même chose que l'affirmation 2 : S'il n'y a pas au moins dix personnes présentes, alors la conférence n'aura pas lieu.

Nous avons déjà vu qu'une instruction conditionnelle $P \rightarrow Q$ et sa réciproque $Q \rightarrow P$ ne sont pas équivalentes. En mathématiques, on veut souvent dire que les deux $P \rightarrow Q$ et $Q \rightarrow P$ sont vraies, et il est donc commode d'introduire un nouveau symbole connecteur, \leftrightarrow , pour exprimer cela. Vous pouvez considérer $P \leftrightarrow Q$ comme une simple abréviation de la formule $(P \rightarrow Q) \wedge (Q \rightarrow P)$. Une instruction de la forme $P \leftrightarrow Q$ est appelée une instruction *biconditionnelle*, car elle représente deux instructions conditionnelles. En créant une table de vérité pour $(P \rightarrow Q) \wedge (Q \rightarrow P)$ vous pouvez vérifier que la table de vérité pour $P \leftrightarrow Q$ est telle que montrée dans [la Figure 1.21](#). Notez que, par la loi contraposée, $P \leftrightarrow Q$ est aussi équivalent à $(P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q)$.

P	Q	$P \leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Figure 1.21.

Puisque $Q \rightarrow P$ peut s'écrire « P si Q » et $P \rightarrow Q$ « P seulement si Q », $P \leftrightarrow Q$ signifie « P si Q et P seulement si Q », et on l'écrit souvent « P si et seulement si Q ». L'expression « *si et seulement si* » est si fréquente en mathématiques qu'il existe une abréviation courante, *ssi*. Ainsi, $P \leftrightarrow Q$ s'écrit souvent « P ssi Q ». Une autre affirmation signifiant que $P \leftrightarrow Q$ est « P est une condition nécessaire et suffisante pour Q ».

Exemple 1.5.4. Analysez les formes logiques des énoncés suivants :

1. Le match sera annulé s'il pleut ou s'il neige.
2. La présence d'au moins dix personnes est une condition nécessaire et suffisante pour que la conférence soit donnée.
3. Si John est allé au magasin, alors nous avons des œufs, et s'il ne l'a pas fait, alors nous n'en avons pas.

Solutions

1. Soit C pour « Le match sera annulé », R pour « Il pleut » et S pour « Il neige ». L'énoncé serait alors représenté par la formule $C \leftrightarrow (R \vee S)$.
2. Soit T pour « Il y a au moins dix personnes présentes » et L pour « La conférence aura lieu ». L'énoncé signifie alors $T \leftrightarrow L$.
3. Soit S pour « Jean est allé au magasin » et E pour « Nous avons des œufs ». La traduction littérale de l'énoncé donné serait alors $(S \rightarrow E) \wedge (\neg S \rightarrow \neg E)$. Ceci équivaut à $S \leftrightarrow E$.

L'une des raisons pour lesquelles il est si facile de confondre une instruction conditionnelle avec sa réciproque est que, dans le langage courant, on utilise parfois une instruction conditionnelle alors que l'on veut transmettre une instruction biconditionnelle. Par exemple, on ne dirait probablement pas « Le cours aura lieu si au moins dix personnes sont présentes », à moins que le nombre de personnes ne soit également inférieur à dix. Après tout, pourquoi mentionner le nombre dix si ce n'est pas le nombre minimum requis ? Ainsi, l'instruction suggère en réalité que le cours aura lieu *si et seulement s'il y a au moins dix personnes présentes*. Prenons un autre exemple : *imaginons qu'un enfant entende ses parents dire* : « *Si tu ne dînes pas*, tu n'auras pas de dessert. » L'enfant s'attend certainement à ce que s'il dîne, il *aura* un dessert, même si ce n'est pas exactement ce que ses parents lui ont dit. Autrement dit, l'enfant interprète l'instruction comme signifiant : « *Dîner est une condition nécessaire et suffisante pour avoir un dessert.* »

Un tel flou entre *si* et *ssi* n'est jamais acceptable en mathématiques. Les mathématiciens utilisent toujours une expression telle que *ssi* ou *nécessaire et condition suffisante* lorsqu'ils souhaitent exprimer une proposition biconditionnelle. Il ne faut jamais interpréter une proposition si-alors en mathématiques comme une proposition biconditionnelle, comme on le ferait dans le langage courant.

Exercices

- *1. Analysez les formes logiques des énoncés suivants :
- (a) Si ce gaz a une odeur désagréable ou n'est pas explosif, alors ce n'est pas de l'hydrogène.
 - (b) Avoir à la fois de la fièvre et un mal de tête est une condition suffisante pour que George aille chez le médecin.
 - (c) Avoir de la fièvre et avoir des maux de tête sont des conditions suffisantes pour que George aille chez le médecin.
 - (d) Si $x \neq 2$, alors une condition nécessaire pour que x soit premier est que x soit impair.
2. Analysez les formes logiques des énoncés suivants :

- (a) Marie vendra sa maison seulement si elle peut obtenir un bon prix et trouver un bel appartement.
- (b) Avoir à la fois un bon historique de crédit et un acompte suffisant est une condition nécessaire pour obtenir un prêt hypothécaire.
- (c) John abandonnera l'école, à moins que quelqu'un ne l'en empêche.
(Indice : essayez d'abord de reformuler cela en utilisant les mots « *si* » et « *alors* » au lieu de « *à moins que* ».)
- (d) Si x est divisible par 4 ou 6, alors il n'est pas premier.

3. Analysez la forme logique de l'énoncé suivant :

- (a) S'il pleut, alors il y a du vent et le soleil ne brille pas. Analysez maintenant les affirmations suivantes. Pour chacune d'elles, déterminez si elle est équivalente à l'affirmation (a) ou à son inverse.
- (b) Il y a du vent et il n'y a pas de soleil seulement s'il pleut.
- (c) La pluie est une condition suffisante pour qu'il y ait du vent sans soleil.
- (d) La pluie est une condition nécessaire au vent sans soleil.
- (e) Il ne pleut pas si le soleil brille ou s'il n'y a pas de vent.
- (f) Le vent est une condition nécessaire pour qu'il pleuve, tout comme le manque de soleil.
- (g) Soit il y a du vent seulement s'il pleut, soit il ne fait pas soleil seulement s'il pleut.

*4. Utilisez les tables de vérité pour déterminer si les arguments suivants sont valides ou non :

- (a) Soit les ventes, soit les dépenses augmenteront. Si les ventes augmentent, le patron sera content. Si les dépenses augmentent, le patron sera mécontent. Par conséquent, les ventes et les dépenses n'augmenteront pas toutes les deux.
- (b) Si le taux d'imposition et le taux de chômage augmentent tous deux, il y aura une récession. Si le PIB augmente, il n'y aura pas de récession. Le PIB et les impôts augmentent tous deux. Par conséquent, le taux de chômage n'augmente pas.
- (c) Le voyant d'avertissement s'allume uniquement si la pression est trop élevée et que la soupape de décharge est obstruée. La soupape de décharge n'est pas obstruée. Par conséquent, le voyant d'avertissement s'allume uniquement si la pression est trop élevée.

5. Utilisez les tables de vérité pour déterminer si les arguments suivants sont valides ou non :

- (a) Si Jones est reconnu coupable, il ira en prison. Jones ne sera condamné que si Smith témoigne contre lui. Par conséquent, Jones n'ira pas en prison si Smith ne témoigne pas contre lui.
- (b) Soit les Démocrates, soit les Républicains auront la majorité au Sénat, mais pas les deux. Avoir une majorité démocrate est une condition nécessaire à l'adoption du projet de loi. Par conséquent,

si les Républicains ont la majorité au Sénat, le projet de loi ne sera pas adopté.

6. (a) Montrer que $P \leftrightarrow Q$ est équivalent à $(P \wedge Q) \vee (\neg P \wedge \neg Q)$.
(b) Montrer que $(P \rightarrow Q) \vee (P \rightarrow R)$ est équivalent à $P \rightarrow (Q \vee R)$.
- *7. (a) Montrer que $(P \rightarrow R) \wedge (Q \rightarrow R)$ est équivalent à $(P \vee Q) \rightarrow R$.
(b) Formuler et vérifier une équivalence similaire impliquant $(P \rightarrow R) \vee (Q \rightarrow R)$.
8. (a) Montrer que $(P \rightarrow Q) \wedge (Q \rightarrow R)$ est équivalent à $(P \rightarrow R) \wedge [(P \leftrightarrow Q) \vee (R \leftrightarrow Q)]$.
(b) Montrer que $(P \rightarrow Q) \vee (Q \rightarrow R)$ est une tautologie.
- *9. Trouvez une formule impliquant uniquement les connecteurs \neg et \rightarrow qui soit équivalente à $P \wedge Q$.
10. Trouvez une formule impliquant uniquement les connecteurs \neg et \rightarrow qui est équivalente à $P \leftrightarrow Q$.
11. (a) Montrez que $(P \vee Q) \leftrightarrow Q$ est équivalent à $P \rightarrow Q$.
(b) Montrer que $(P \wedge Q) \leftrightarrow Q$ est équivalent à $Q \rightarrow P$.
12. Lesquelles des formules suivantes sont équivalentes ?
 - (a) $P \rightarrow (Q \rightarrow R)$.
 - (b) $Q \rightarrow (P \rightarrow R)$.
 - (c) $(P \rightarrow Q) \wedge (P \rightarrow R)$.
 - (d) $(P \wedge Q) \rightarrow R$.
 - (e) $P \rightarrow (Q \wedge R)$.

2

Logique quantificationnelle

2.1 Quantificateurs

Nous avons vu qu'une affirmation $P(x)$ contenant une variable libre x peut être vraie pour certaines valeurs de x et fausse pour d'autres. On souhaite parfois préciser le *nombre* de valeurs de x qui rendent $P(x)$ vraie. En particulier, on souhaite souvent dire que $P(x)$ est vraie pour *toute* valeur de x , ou qu'elle l'est pour *au moins une* valeur de x . Nous introduisons donc deux symboles supplémentaires, appelés *quantificateurs*, pour exprimer ces idées.

Pour dire que $P(x)$ est vrai pour toute valeur de x dans l'univers du discours U , nous écrirons $\forall x P(x)$. Cela se lit « Pour tout x , $P(x)$ ». Imaginez le symbole A à *l'envers* comme représentant le mot *tout*. Le symbole \forall est appelé l'*universel quantificateur*, car l'énoncé $\forall x P(x)$ dit que $P(x)$ est *universellement* vrai. Comme nous l'avons vu dans [la section 1.3](#), dire que $P(x)$ est vrai pour chaque valeur de x dans l'univers signifie que l'ensemble de vérité de $P(x)$ sera l'univers entier U . Ainsi, vous pourriez aussi penser à l'énoncé $\forall x P(x)$ comme disant que l'ensemble de vérité de $P(x)$ est égal à U .

On écrit $\exists x P(x)$ pour dire qu'il existe au moins une valeur de x dans l'univers pour laquelle $P(x)$ est vraie. Cela se lit « Il existe un x tel que $P(x)$ ». Le *E inversé* vient du mot *existe* et est appelé *quantificateur existentiel*. On peut encore interpréter cette affirmation comme une affirmation sur l'ensemble de vérité de $P(x)$. Dire que $P(x)$ est vrai pour au moins une valeur de x signifie qu'il existe au moins un élément dans l'ensemble de vérité de $P(x)$, ou en d'autres termes, que l'ensemble de vérité n'est pas égal à \emptyset .

Par exemple, dans [la section 1.5](#), nous avons discuté de l'énoncé « Si $x > 2$ alors $x^2 > 4$ », où x s'étend sur l'ensemble de tous les nombres réels, et nous avons affirmé que cette affirmation était vraie pour toutes les valeurs de x . Nous pouvons maintenant écrire cette affirmation symboliquement comme $\forall x (x > 2 \rightarrow x^2 > 4)$.

Exemple 2.1.1. Que signifient les formules suivantes ? Sont-elles vraies ou fausses ?

1. $\forall x (x^2 \geq 0)$, où l'univers du discours est \mathbb{R} , l'ensemble de tous les nombres réels.
2. $\exists x (x^2 - 2x + 3 = 0)$, avec à nouveau l'univers \mathbb{R} .
3. $\exists x (M(x) \wedge B(x))$, où l'univers du discours est l'ensemble de toutes les personnes, $M(x)$ représente l'affirmation « x est un homme » et $B(x)$ signifie « x a les cheveux bruns ».
4. $\forall x (M(x) \rightarrow B(x))$, avec le même univers et les mêmes significations pour $M(x)$ et $B(x)$.
5. $\forall x L(x, y)$, où l'univers est l'ensemble de tous les êtres humains, et $L(x, y)$ signifie « x aime y ».

Solutions

1. Cela signifie que pour tout nombre réel x , $x^2 \geq 0$. C'est vrai.
2. Cela signifie qu'il existe au moins un nombre réel x qui rend vraie l'équation $x^2 - 2x + 3 = 0$. Autrement dit, l'équation a au moins une solution réelle. Si vous résolvez l'équation, vous constaterez que cette affirmation est fausse ; l'équation n'a pas de solution réelle. (Essayez de compléter le carré ou d'utiliser la formule quadratique.)
3. Il existe au moins une personne x telle que x est un homme et x a les cheveux bruns. Autrement dit, il existe au moins un homme qui a les cheveux bruns. Bien sûr, c'est vrai.
4. Pour chaque personne x , si x est un homme alors x a les cheveux bruns. Autrement dit, tous les hommes ont les cheveux bruns. Si vous n'êtes pas convaincu de la signification de la formule, il peut être utile de consulter la table de vérité du connecteur conditionnel. D'après cette table, l'affirmation $M(x) \rightarrow B(x)$ ne sera fausse que si $M(x)$ est vraie et $B(x)$ est fausse ; autrement dit, x est un homme et x n'a pas les cheveux bruns. Ainsi, dire que $M(x) \rightarrow B(x)$ est vraie pour chaque personne x signifie que cette situation ne se produit jamais, ou autrement dit, qu'il n'y a pas d'hommes qui n'aient pas les cheveux bruns. Or, c'est exactement ce que signifie dire que tous les hommes ont les cheveux bruns. Bien sûr, cette affirmation est fausse.
5. Pour chaque personne x , x aime y . Autrement dit, tout le monde aime y . On ne peut pas savoir si c'est vrai ou faux sans connaître y .

Notez que dans la cinquième affirmation de cet exemple, nous devons connaître l'identité de y pour déterminer si l'affirmation était

vraie ou fausse, mais pas celle de x . L'affirmation stipule que tout le monde aime y , et cette affirmation concerne y , mais pas x . Cela signifie que y est une variable libre dans cette affirmation, tandis que x est une variable liée.

De même, bien que toutes les autres affirmations contiennent la lettre x , nous n'avons pas besoin de connaître la valeur de x pour déterminer leurs valeurs de vérité ; x est donc une variable liée dans tous les cas. En général, même si x est une variable libre dans une affirmation $P(x)$, elle est une variable liée dans les affirmations $\forall xP(x)$ et $\exists xP(x)$. Pour cette raison, nous disons que les quantificateurs *lient* une variable. Comme dans [la section 1.3](#), cela signifie qu'une variable liée par un quantificateur peut toujours être remplacée par une nouvelle variable sans modifier le sens de l'affirmation, et il est souvent possible de paraphraser l'affirmation sans mentionner la variable liée. Par exemple, l'affirmation $\forall xL(x, y)$ de [l'exemple 2.1.1](#) est équivalente à $\forall wL(w, y)$, car les deux signifient la même chose que « Tout le monde aime y ». Des mots tels que « *everyone* », « *someone* », « *everyone* » ou « *someone* » sont souvent utilisés pour exprimer le sens d'énoncés contenant des quantificateurs. Si vous traduisez une affirmation anglaise en symboles, ces mots vous indiqueront souvent qu'un quantificateur sera nécessaire.

Comme pour le symbole \neg , nous suivons la convention selon laquelle les expressions $\forall x$ et $\exists x$ s'appliquent uniquement aux énoncés qui les suivent immédiatement. Par exemple, $\forall xP(x) \rightarrow Q(x)$ signifie $(\forall xP(x)) \rightarrow Q(x)$, et non $\forall x(P(x) \rightarrow Q(x))$.

Exemple 2.1.2. Analysez les formes logiques des énoncés suivants.

1. Quelqu'un n'a pas fait ses devoirs.
2. Tout dans ce magasin est soit trop cher, soit mal fait.
3. Personne n'est parfait.
4. Susan aime tous ceux qui n'aiment pas Joe.
5. $Un \subseteq B$.
6. $A \cap B \subseteq B \setminus C$.

Solutions

1. Le mot « *quelqu'un* » nous incite à utiliser un quantificateur existentiel. Dans un premier temps, nous écrivons $\exists x(x \text{ n'a pas fait ses devoirs})$. Si nous supposons maintenant que $H(x)$ représente l'affirmation « x a fait ses devoirs », nous pouvons la réécrire sous la forme $\exists x \neg H(x)$.

2. Imaginez cette affirmation comme « Si c'est dans ce magasin, alors c'est soit trop cher, soit mal fait (peu importe ce que c'est). » Ainsi, nous commençons par écrire $\forall x$ (si x est dans ce magasin, alors x est soit trop cher, soit mal fait). Pour écrire symboliquement la partie entre parenthèses, nous supposons que $S(x)$ signifie « x est dans ce magasin », $O(x)$ signifie « x est trop cher » et $P(x)$ signifie « x est mal fait ». Notre réponse finale est donc $\forall x [S(x) \rightarrow (O(x) \vee P(x))]$.

Notez que, comme l'instruction 4 de [l'exemple 2.1.1](#), cette instruction prend la forme d'un quantificateur universel appliqué à une instruction conditionnelle. Cette forme est fréquente, et il est important d'apprendre à la reconnaître. et quand il doit être utilisé. Nous pouvons vérifier notre réponse à ce problème comme nous l'avons fait précédemment, en utilisant la table de vérité pour le connecteur conditionnel. La seule façon pour que l'affirmation $S(x) \rightarrow (O(x) \vee P(x))$ soit fausse est si x est dans ce magasin, mais n'est ni trop cher ni mal fait. Ainsi, dire que l'affirmation est vraie pour toutes les valeurs de x signifie que cela n'arrive jamais, ce qui est exactement ce que signifie dire que tout dans ce magasin est soit trop cher, soit mal fait.

3. Cela signifie $\neg(\text{quelqu'un est parfait})$, ou en d'autres termes $\neg\exists x P(x)$, où $P(x)$ signifie « x est parfait ».
4. Comme dans l'énoncé 2 de cet exemple, on pourrait considérer que cela signifie « Si une personne n'aime pas Joe, alors Susan aime cette personne (peu importe qui elle est). » Ainsi, on peut commencer par réécrire l'énoncé donné sous la forme $\forall x$ (si x n'aime pas Joe, alors Susan aime x). Soit $L(x, y)$ pour « x aime y ». Dans les énoncés qui parlent d'éléments spécifiques du discours, il est parfois pratique d'introduire des lettres pour représenter ces éléments spécifiques. Dans ce cas, nous devons parler de Joe et Susan, donc supposons que j représente Joe et s pour Susan. Ainsi, on peut écrire $L(s, x)$ pour signifier « Susan aime x » et $\neg L(x, j)$ pour « x n'aime pas Joe ». En complétant ces équations, on obtient la réponse $\forall x (\neg L(x, j) \rightarrow L(s, x))$. Notez qu'une fois de plus, nous avons un quantificateur universel appliqué à une instruction conditionnelle. Comme précédemment, vous pouvez vérifier cette réponse à l'aide de la table de vérité du connecteur conditionnel.
5. Selon [la définition 1.4.5](#), dire que A est un sous-ensemble de B signifie que tout ce qui est dans A est dans B . Si vous avez compris le schéma de combinaison des quantificateurs et des conditionnels universels, vous devriez reconnaître que cela s'écrirait symboliquement comme $\forall x (x \in A \rightarrow x \in B)$.

6. Comme dans l'énoncé précédent, nous écrivons d'abord ceci comme $\forall x (x \in A \cap B \rightarrow x \in B \setminus C)$. Maintenant, en utilisant les définitions d'intersection et de différence, nous pouvons développer cela davantage pour obtenir $\forall x [(x \in A \wedge x \in B) \rightarrow (x \in B \wedge x \notin C)]$.

Bien que tous nos exemples jusqu'à présent n'aient contenu qu'un seul quantificateur, il n'y a aucune raison pour qu'une affirmation ne puisse pas en avoir plus d'un. Par exemple, considérons l'affirmation « Certains étudiants sont mariés ». Le mot « *certain*s » indique que cette affirmation doit être écrite à l'aide d'un quantificateur existentiel, nous pouvons donc la considérer comme ayant la forme $\exists x (x \text{ est étudiant et } x \text{ est marié})$. Soit $S(x)$ pour « *x* est étudiant ». Nous pourrions également choisir une lettre pour « *x* est marié », mais une meilleure analyse serait peut-être de reconnaître qu'être marié signifie être marié à *quelqu'un*. Ainsi, si nous posons $M(x, y)$ pour « *x* est marié à *y* », alors nous pouvons écrire « *x* est marié » comme $\exists y M(x, y)$. Nous pouvons donc représenter l'énoncé entier par la formule $\exists x (S(x) \wedge \exists y M(x, y))$, une formule contenant deux quantificateurs existentiels.

Comme autre exemple, analysons l'affirmation « Tous les parents sont mariés ». Nous commençons par l'écrire comme $\forall x (\text{si } x \text{ est un parent alors } x \text{ est marié})$. La parentalité, comme le mariage, est une relation entre deux personnes ; être parent signifie être le parent de *quelqu'un*. Ainsi, il pourrait être préférable de représenter l'affirmation « *x* est un parent » par la formule $\exists y P(x, y)$, où $P(x, y)$ signifie « *x* est le parent de *y* ». Si nous représentons à nouveau « *x* est marié » par la formule $\exists y M(x, y)$, alors notre analyse de l'affirmation originale sera $\forall x (\exists y P(x, y) \rightarrow \exists y M(x, y))$. Bien que ce ne soit pas faux, la double utilisation de la variable *y* pourrait prêter à confusion. Peut-être qu'une meilleure solution serait de remplacer la formule $\exists y M(x, y)$ par la formule équivalente $\exists z M(x, z)$. (Rappelons que ces formules sont équivalentes car une variable liée dans n'importe quelle instruction peut être remplacée par une autre sans changer le sens de l'instruction.) Notre analyse améliorée de l'instruction serait alors $\forall x (\exists y P(x, y) \rightarrow \exists z M(x, z))$.

Une erreur fréquente chez les débutants est d'omettre les quantificateurs. Par exemple, on pourrait être tenté de représenter incorrectement l'affirmation « Tous les parents sont mariés » par la formule $\forall x (P(x, y) \rightarrow M(x, z))$, en omettant $\exists y$ et $\exists z$. Un bon moyen de détecter ce genre d'erreurs est de prêter attention aux variables libres et liées. Dans la formule incorrecte, aucun quantificateur ne lie les variables *y* et *z* ; *y* et *z* sont donc des variables libres. Or, l'affirmation initiale, « Tous les parents sont mariés », ne concerne pas *y* et *z* ; ces variables ne devraient donc pas être libres dans la réponse. C'est un indice que les quantificateurs sur *y* et *z* sont absents. Notez que si nous traduisons la formule incorrecte $\forall x (P(x, y) \rightarrow M(x, z))$

$) \rightarrow M(x, z))$ en anglais, nous obtenons une déclaration sur y et z : « Toute personne qui est parent de y est mariée à z . »

Exemple 2.1.3. Analysez les formes logiques des énoncés suivants.

1. Tout le monde dans le dortoir a un colocataire qu'il ou elle n'aime pas.
2. Personne n'aime les mauvais perdants.
3. Toute personne ayant un ami atteint de la rougeole devra être mise en quarantaine.
4. Si quelqu'un dans le dortoir a un ami qui a la rougeole, alors tout le monde dans le dortoir devra être mis en quarantaine.
5. Si $A \subseteq B$, alors A et $C \setminus B$ sont disjoints.

Solutions

1. Cela signifie $\forall x$ (si x vit dans la résidence universitaire, alors x a un colocataire qu'il ou elle n'aime pas). Pour dire que x a un colocataire qu'il ou elle n'aime pas, nous pourrions écrire $\exists y$ (x et y sont colocataires et x n'aime pas y). Si nous posons $R(x, y)$ pour « x et y sont colocataires » et $L(x, y)$ pour « x aime y », alors cela devient $\exists y (R(x, y) \wedge \neg L(x, y))$. Enfin, si nous posons $D(x)$ pour « x vit dans le dortoir », alors l'analyse complète de l'énoncé original serait $\forall x [D(x) \rightarrow \exists y (R(x, y) \wedge \neg L(x, y))]$.
2. C'est délicat, car l'expression « *mauvais perdant* » ne désigne pas un mauvais perdant *en particulier*, mais *tous* les mauvais perdants. Cette affirmation signifie que tous les mauvais perdants sont détestés, autrement dit $\forall x$ (si x est mauvais perdant, alors personne n'aime x). Pour dire que personne n'aime x , on écrit $\neg(\text{quelqu'un aime } x)$, ce qui signifie $\neg \exists y L(y, x)$, où $L(y, x)$ signifie « y aime x ». Si $S(x)$ signifie « x est mauvais perdant », alors l'énoncé complet s'écrirait $\forall x (S(x) \rightarrow \neg \exists y L(y, x))$.
3. Vous avez probablement déjà compris qu'il est généralement plus facile de traduire de l'anglais en symboles en plusieurs étapes, en traduisant un petit texte à la fois. Voici les étapes que nous pourrions suivre pour traduire cette affirmation :
 - (i) $\forall x$ (si x a un ami qui a la rougeole, alors x devra être mis en quarantaine).
 - (ii) $\forall x [\exists y (y \text{ est un ami de } x \text{ et } y \text{ a la rougeole}) \rightarrow x \text{ devra être mis en quarantaine}]$.

Maintenant, en supposant que $F(y, x)$ signifie « y est un ami de x », $M(y)$ signifie « y a la rougeole » et $Q(x)$ signifie « x devra être mis en quarantaine », nous obtenons :

(iii) $\forall x [\exists y (F(y, x) \wedge M(y)) \rightarrow Q(x)]$.

4. Le mot « *quelqu'un* » est difficile à interpréter, car il signifie des choses différentes selon les énoncés. Dans l'énoncé 3, il signifiait « *tout le monde* », mais dans cet énoncé, il désigne « *quelqu'un* ». Voici les étapes de notre analyse :

(i) (Quelqu'un dans le dortoir a un ami qui a la rougeole) \rightarrow (tout le monde dans le dortoir devra être mis en quarantaine).

(ii) $\exists x (x \text{ vit dans le dortoir et } x \text{ a un ami qui a la rougeole}) \rightarrow \forall z (\text{si } z \text{ vit dans le dortoir, alors } z \text{ devra être mis en quarantaine})$.

En utilisant les mêmes abréviations que dans la dernière affirmation et en laissant $D(x)$ signifier « x vit dans le dortoir », nous obtenons la formule suivante :

(iii) $\exists x [D(x) \wedge \exists y (F(y, x) \wedge M(y))] \rightarrow \forall z (D(z) \rightarrow Q(z))$.

5. De toute évidence, la réponse aura la forme d'une instruction conditionnelle, ($A \subseteq B$) \rightarrow (A et $C \setminus B$ sont disjoints). Nous avons déjà écrit $A \subseteq B$ symboliquement dans [l'exemple 2.1.2](#). Dire que A et $C \setminus B$ sont disjoints signifie qu'ils n'ont aucun élément en commun, ou en d'autres termes $\neg \exists x (x \in A \wedge x \in C \setminus B)$. En mettant tout cela ensemble, et en complétant la définition de $C \setminus B$, nous obtenons $\forall x (x \in A \rightarrow x \in B) \rightarrow \neg \exists x (x \in A \wedge x \in C \setminus B)$.

Lorsqu'une affirmation contient plusieurs quantificateurs, il est parfois difficile d'en déduire la signification et de déterminer si elle est vraie ou fausse. Dans ce cas, il peut être préférable d'envisager les quantificateurs un par un, dans l'ordre. Prenons par exemple l'affirmation $\forall x \exists y (x + y = 5)$, où l'univers du discours est l'ensemble des Tous les nombres réels. En considérant d'abord la première expression du quantificateur $\forall x$, on constate que l'énoncé signifie que pour tout nombre réel x , l'énoncé $\exists y (x + y = 5)$ est vrai. On pourra s'interroger plus tard sur la signification de $\exists y (x + y = 5)$; considérer deux quantificateurs à la fois est trop déroutant.

Si nous voulons déterminer si l'énoncé $\exists y (x + y = 5)$ est vrai pour chaque valeur de x , il peut être utile d'essayer quelques valeurs de x . Par exemple, supposons $x = 2$. *Nous devons alors déterminer si l'énoncé $\exists y (2 + y = 5)$ est vrai* ou non. Il est maintenant temps de penser au quantificateur suivant, $\exists y$. Cet énoncé dit qu'il existe au moins une valeur de y pour laquelle l'équation $2 + y = 5$ est vraie. En d'autres termes, l'équation $2 + y = 5$ a au moins une solution. Bien sûr, c'est vrai, car l'équation a pour solution $y = 5 - 2 = 3$. Ainsi, l'énoncé $\exists y (2 + y = 5)$ est vrai.

Essayons une autre valeur de x . Si $x = 7$, alors nous sommes intéressés par l'affirmation $\exists y (7 + y = 5)$, qui dit que l'équation $7 + y = 5$ a au moins une solution. Encore une fois, c'est vrai, puisque la solution est $y = 5 - 7 = -2$. En fait, vous avez probablement compris

maintenant que quelle que soit la valeur que nous remplaçons par x , l'équation $x + y = 5$ aura toujours pour solution $y = 5 - x$, donc l'affirmation $\exists y (x + y = 5)$ sera vraie. Ainsi, l'affirmation initiale $\forall x \exists y (x + y = 5)$ est vraie.

D'autre part, l'énoncé $\exists y \forall x (x + y = 5)$ signifie quelque chose de complètement différent. Cet énoncé signifie qu'il existe au moins une valeur de y pour laquelle l'énoncé $\forall x (x + y = 5)$ est vrai. Pouvons-nous trouver une telle valeur de y ? Supposons, par exemple, que nous essayions $y = 4$. Nous devons ensuite déterminer si l'énoncé $\forall x (x + 4 = 5)$ est vrai ou non. Cet énoncé dit que quelle que soit la valeur que nous remplaçons par x , l'équation $x + 4 = 5$ est vraie, ce qui est clairement faux. En fait, aucune valeur de x autre que $x = 1$ ne fonctionne dans cette équation. Ainsi, l'énoncé $\forall x (x + 4 = 5)$ est faux.

Nous avons vu que lorsque $y = 4$, l'affirmation $\forall x (x + y = 5)$ est fausse, mais peut-être qu'une autre valeur de y fonctionnera. Rappelez-vous, nous essayons de déterminer s'il existe *au moins une* valeur de y qui fonctionne. Essayons-en une autre, disons, $y = 9$. Nous devons ensuite considérer l'affirmation $\forall x (x + 9 = 5)$, qui dit que quelle que soit la valeur de x , l'équation $x + 9 = 5$ est vraie. Une fois de plus, c'est clairement faux, car seule $x = -4$ fonctionne dans cette équation. En fait, il devrait être clair maintenant que quelle que soit la valeur que nous remplaçons par y , l'équation $x + y = 5$ ne sera vraie que pour une seule valeur de x , à savoir $x = 5 - y$, donc l'affirmation $\forall x (x + y = 5)$ sera fausse. Il n'y a donc *aucune* valeur de y pour laquelle $\forall x (x + y = 5)$ est vrai, donc l'affirmation $\exists y \forall x (x + y = 5)$ est fausse.

Notez que nous avons constaté que l'affirmation $\forall x \exists y (x + y = 5)$ est vraie, mais que $\exists y \forall x (x + y = 5)$ est fausse. Apparemment, l'ordre des quantificateurs joue un rôle ! Qu'est-ce qui explique cette différence ? La première affirmation dit : que pour tout nombre réel x , il existe un nombre réel y tel que $x + y = 5$. Par exemple, lorsque nous avons essayé $x = 2$, nous avons constaté que $y = 3$ fonctionnait dans l'équation $x + y = 5$, et avec $x = 7$, $y = -2$ fonctionnait. Notez que pour différentes valeurs de x , nous avons dû utiliser différentes valeurs de y pour que l'équation soit vraie. Vous pourriez penser à cette affirmation comme disant que pour chaque nombre réel x , il existe un nombre réel *correspondant* y tel que $x + y = 5$. D'un autre côté, lorsque nous avons analysé l'énoncé $\exists y \forall x (x + y = 5)$, nous nous sommes retrouvés à chercher une *seule* valeur de y qui rendait l'équation $x + y = 5$ vraie pour toutes les valeurs de x , et cela s'est avéré impossible. Pour chaque valeur de x , il existe une valeur correspondante de y qui rend l'équation vraie, mais aucune valeur unique de y ne fonctionne pour chaque x .

Pour un autre exemple, considérons l'énoncé $\forall x \exists y L(x, y)$, où l'univers du discours est l'ensemble de toutes les personnes et $L(x, y)$ signifie « x aime y ». Cet énoncé dit que pour chaque personne x ,

l'énoncé $\exists y L(x, y)$ est vrai. Maintenant $\exists y L(x, y)$ pourrait s'écrire « x aime quelqu'un », donc l'énoncé original signifie que pour chaque personne x , x aime quelqu'un. En d'autres termes, tout le monde aime quelqu'un. D'autre part, $\exists y \forall x L(x, y)$ signifie qu'il existe une personne y telle que $\forall x L(x, y)$ est vrai. Comme nous l'avons vu dans [l'exemple 2.1.1](#), $\forall x L(x, y)$ signifie « Tout le monde aime y », donc $\exists y \forall x L(x, y)$ signifie qu'il existe une personne y telle que tout le monde aime y . Autrement dit, il existe une personne universellement appréciée. Ces affirmations ne signifient pas la même chose. Il se peut que tout le monde aime quelqu'un, mais que personne ne soit universellement apprécié.

Exemple 2.1.4. Que signifient les affirmations suivantes ? Sont-elles vraies ou fausses ? Dans chaque cas, l'univers du discours est \mathbb{N} , l'ensemble de tous les nombres naturels.

1. $\forall x \exists y (x < y)$.
2. $\exists y \forall x (x < y)$.
3. $\exists x \forall y (x < y)$.
4. $\forall y \exists x (x < y)$.
5. $\exists x \exists y (x < y)$.
6. $\forall x \forall y (x < y)$.

Solutions

1. Cela signifie que pour tout entier naturel x , l'affirmation $\exists y (x < y)$ est vraie. Autrement dit, pour tout entier naturel x , il existe un entier naturel plus grand que x . C'est vrai. Par exemple, $x + 1$ est toujours plus grand que x .
2. Cela signifie qu'il existe un entier naturel y tel que l'affirmation $\forall x (x < y)$ soit vraie. Autrement dit, il existe un entier naturel y tel que tous les nombres naturels sont inférieurs à y . C'est faux. Quel que soit le nombre naturel y choisi, il existera toujours des nombres naturels plus grands.
3. Cela signifie qu'il existe un entier naturel x tel que l'affirmation $\forall y (x < y)$ soit vraie. On pourrait être tenté de dire que cette affirmation serait vraie si $x = 0$, mais ce n'est pas exact. Puisque 0 est le plus petit entier naturel, l'affirmation $0 < y$ est vraie pour toutes les valeurs de y . *sauf* $y = 0$, mais si $y = 0$, alors l'affirmation $0 < y$ est fausse, et donc $\forall y (0 < y)$ est fausse. Un raisonnement similaire montre que pour toute valeur de x , l'affirmation $\forall y (x < y)$ est fausse, donc $\exists x \forall y (x < y)$ est fausse.

4. Cela signifie que pour tout entier naturel y , il existe un entier naturel plus petit que y . Ceci est vrai pour tout entier naturel y . *sauf* $y = 0$, mais il n'existe pas de nombre naturel inférieur à 0. Par conséquent, cette affirmation est fausse.
5. Cela signifie qu'il existe un entier naturel x tel que $\exists y (x < y)$ soit vraie. Mais comme nous l'avons vu dans la première affirmation, cela est vrai pour *tout* entier naturel x , donc certainement vrai pour au moins un. Ainsi, $\exists x \exists y (x < y)$ est vraie.
6. Cela signifie que pour tout entier naturel x , l'affirmation $\forall y (x < y)$ est vraie. Or, comme nous l'avons vu dans la troisième affirmation, il n'existe aucune *valeur* de x pour laquelle cette affirmation soit vraie. Ainsi, $\forall x \forall y (x < y)$ est fausse.

Exercices

*1. Analysez les formes logiques des énoncés suivants.

- (a) Quiconque a pardonné au moins une personne est un saint.
- (b) Personne dans la classe de calcul n'est plus intelligent que tous ceux dans la classe de mathématiques discrètes.
- (c) Tout le monde aime Marie, sauf Marie elle-même.
- (d) Jane a vu un policier, et Roger en a vu un aussi.
- (e) Jane a vu un policier, et Roger l'a vu aussi.

2. Analysez les formes logiques des énoncés suivants.

- (a) Quiconque a acheté une Rolls Royce en liquide doit avoir un oncle riche.
- (b) Si quelqu'un dans le dortoir a la rougeole, alors tous ceux qui ont un ami dans le dortoir devront être mis en quarantaine.
- (c) Si personne n'a échoué au test, alors tous ceux qui ont eu un A donneront des cours particuliers à quelqu'un qui a eu un D.
- (d) Si quelqu'un peut le faire, c'est Jones.
- (e) Si Jones peut le faire, tout le monde peut le faire.

3. Analysez les formes logiques des énoncés suivants. L'univers du discours est \mathbb{R} . Quelles sont les variables libres de chaque énoncé ?

- (a) Tout nombre supérieur à x est supérieur à y .
- (b) Pour tout nombre a , l'équation $ax^2 + 4x - 2 = 0$ a au moins une solution ssi $a \geq -2$.
- (c) Toutes les solutions de l'inégalité $x^3 - 3x < 3$ sont inférieures à 10.
- (d) S'il existe un nombre x tel que $x^2 + 5x = w$ et qu'il existe un nombre y tel que $4 - y^2 = w$, alors w est strictement compris entre -10 et 10.

*4. Traduisez les affirmations suivantes en anglais idiomatique.

- (a) $\forall x [(H(x) \wedge \neg \exists y M(x , y)) \rightarrow U(x)]$, où $H(x)$ signifie « x est un homme », $M(x , y)$ signifie « x est marié à y », et $U(x)$ signifie « x est malheureux ».
- (b) $\exists z [P(z , x) \wedge S(z , y) \wedge W(y)]$, où $P(z , x)$ signifie « z est un parent de x », $S(z , y)$ signifie « z et y sont frères et sœurs » et $W(y)$ signifie « y est une femme ».

5. Traduisez les affirmations suivantes en anglais mathématique idiomatique.

- (a) $\forall x [(P(x) \wedge \neg (x = 2)) \rightarrow O(x)]$, où $P(x)$ signifie « x est un nombre premier » et $O(x)$ signifie « x est impair ».
- (b) $\exists x [P(x) \wedge \forall y [P(y) \rightarrow y \leq x]]$, où $P(x)$ signifie « x est un nombre parfait ».

6. Traduisez les affirmations suivantes en français mathématique idiomatique. Sont - elles vraies ou fausses ? L'univers du discours est \mathbb{R} .

- (a) $\neg \exists x (x^2 + 2x + 3 = 0 \wedge x^2 + 2x - 3 = 0)$.
- (b) $\neg [\exists x (x^2 + 2x + 3 = 0) \wedge \exists x (x^2 + 2x - 3 = 0)]$.
- (c) $\neg \exists x (x^2 + 2x + 3 = 0) \wedge \neg \exists x (x^2 + 2x - 3 = 0)$.

7. Ces affirmations sont-elles vraies ou fausses ? L'univers du discours est l'ensemble de tous les individus, et $P(x , y)$ signifie « x est un parent de y ».

- (a) $\exists x \forall y P(x , y)$.
- (b) $\forall x \exists y P(x , y)$.
- (c) $\neg \exists x \exists y P(x , y)$.
- (d) $\exists x \neg \exists y P(x , y)$.
- (e) $\exists x \exists y \neg P(x , y)$.

*8. Ces affirmations sont -elles vraies ou fausses ? L'univers du discours est \mathbb{N} .

- (une) $\forall x \exists y (2x - y = 0)$.
- (b) $\exists y \forall x (2x - y = 0)$.
- (c) $\forall x \exists y (x - 2y = 0)$.
- (d) $\forall X (X < 10 \rightarrow \forall y (y < X \rightarrow y < 9))$.
- (e) $\exists y \exists z (y + z = 100)$.
- (f) $\forall x \exists y (y > x \wedge \exists z (y + z = 100))$.

9. Même chose que [l'exercice 8](#) mais avec \mathbb{R} comme univers du discours.

10. Même chose que [l'exercice 8](#) mais avec \mathbb{Z} comme univers du discours.

2.2 Équivalences impliquant des quantificateurs

Dans notre étude des connecteurs logiques au [chapitre 1](#), nous avons jugé utile d'examiner les équivalences entre différentes formules. Dans cette section, nous verrons également qu'il existe un certain nombre d'équivalences importantes impliquant des quantificateurs.

Par exemple, dans [l'exemple 2.1.2](#), nous avons représenté l'affirmation « Personne n'est parfait » par la formule $\neg\exists xP(x)$, où $P(x)$ signifiait « x est parfait ». Mais une autre façon d'exprimer la même idée serait de dire que tout le monde échoue à être parfait, ou en d'autres termes $\forall x \neg P(x)$. Cela suggère que ces deux formules sont équivalentes, et un peu de réflexion devrait montrer qu'elles le sont. Quelle que soit la signification de $P(x)$, la formule $\neg\exists xP(x)$ signifie qu'il n'y a aucune valeur de x dans l'univers du discours pour laquelle $P(x)$ est vraie. Mais cela revient à dire que pour chaque valeur de x dans l'univers, $P(x)$ est faux, ou en d'autres termes $\forall x \neg P(x)$. Ainsi, $\neg\exists xP(x)$ est équivalent à $\forall x \neg P(x)$.

Un raisonnement similaire montre que $\neg\forall xP(x)$ est équivalent à $\exists x \neg P(x)$. Dire que $\neg\forall xP(x)$ signifie que pour toutes les valeurs de x , $P(x)$ n'est pas vrai. Cela revient à dire qu'il existe au moins une valeur de x pour laquelle $P(x)$ est faux, ce qui revient à dire $\exists x \neg P(x)$. Par exemple, dans [l'exemple 2.1.2](#), nous avons traduit « Quelqu'un n'a pas fait ses devoirs » par $\exists x \neg H(x)$, où $H(x)$ signifie « x a fait ses devoirs ». Une affirmation équivalente serait « Tout le monde n'a pas fait ses devoirs », qui serait représentée par la formule $\neg\forall xH(x)$.

Ainsi, nous avons les deux lois suivantes impliquant la négation et les quantificateurs :

Lois de négation des quantificateurs

$$\begin{aligned}\neg\exists x P(x) &\text{ is equivalent to } \forall x \neg P(x). \\ \neg\forall x P(x) &\text{ is equivalent to } \exists x \neg P(x).\end{aligned}$$

En combinant ces lois avec celles de De Morgan et d'autres équivalences impliquant les connecteurs logiques, nous pouvons souvent reformuler une affirmation négative en une affirmation positive équivalente, mais plus facile à comprendre. Cela s'avérera une compétence importante lorsque nous commencerons à travailler avec des affirmations négatives dans les démonstrations.

Exemple 2.2.1. Niez ces affirmations, puis reformulez les résultats sous forme d'affirmations positives équivalentes.

1. $Un \subseteq B$.

2. Tout le monde a un parent qu'il ou elle n'aime pas.

Solutions

1. Nous savons déjà que $A \subseteq B$ signifie $\forall x (x \in A \rightarrow x \in B)$. Pour reformuler la négation de cette affirmation sous forme d'affirmation équivalente, nous raisonnons ainsi :

$$\begin{aligned} & \neg \forall x (x \in A \rightarrow x \in B) \\ & \text{is equivalent to } \exists x \neg(x \in A \rightarrow x \in B) \quad (\text{quantifier negation law}), \\ & \text{which is equivalent to } \exists x \neg(x \notin A \vee x \in B) \quad (\text{conditional law}), \\ & \text{which is equivalent to } \exists x (x \in A \wedge x \notin B) \quad (\text{De Morgan's law}). \end{aligned}$$

Ainsi, $A \not\subseteq B$ signifie la même chose que $\exists x (x \in A \wedge x \notin B)$. Si vous y réfléchissez, cela devrait avoir du sens. Dire que A n'est pas un sous-ensemble de B revient à dire qu'il y a quelque chose dans A qui n'est pas dans B .

2. Tout d'abord, écrivons l'énoncé original symboliquement. Vous devriez pouvoir vérifier que si $R(x, y)$ signifie « x est apparenté à y » et $L(x, y)$ « x aime y », alors l'énoncé original s'écrirait $\forall x \exists y (R(x, y) \wedge \neg L(x, y))$. Maintenant, nous inversons cela et essayons de trouver un énoncé positif équivalent plus simple :

$$\begin{aligned} & \neg \forall x \exists y (R(x, y) \wedge \neg L(x, y)) \\ & \text{is equivalent to } \exists x \neg \exists y (R(x, y) \wedge \neg L(x, y)) \\ & \text{(quantifier negation law),} \\ & \text{which is equivalent to } \exists x \forall y \neg(R(x, y) \wedge \neg L(x, y)) \\ & \text{(quantifier negation law),} \\ & \text{which is equivalent to } \exists x \forall y (\neg R(x, y) \vee L(x, y)) \\ & \text{(De Morgan's law),} \\ & \text{which is equivalent to } \exists x \forall y (R(x, y) \rightarrow L(x, y)) \\ & \text{(conditional law).} \end{aligned}$$

Traduisons cette dernière formule en français courant. Laissons de côté le premier quantificateur pour le moment : la formule $\forall y (R(x, y) \rightarrow L(x, y))$ signifie que pour toute personne y , si x est apparenté à y , alors x aime y . Autrement dit, x aime tous les membres de sa famille. En ajoutant $\exists x$ au début de cette formule, on obtient l'affirmation « Il y a quelqu'un qui aime tous les membres de sa famille. » Prenez un instant pour vous convaincre que cela équivaut bien à la négation de l'affirmation initiale « Tout le monde a un membre de sa famille qu'il n'aime pas. »

Pour un autre exemple de la façon dont les lois de négation des quantificateurs peuvent nous aider à comprendre les affirmations, considérons l'affirmation « Tous ceux que Patricia apprécie, Sue ne les apprécie pas. » Si $L(x, y)$ représente « x aime y », p représente Patricia et s représente Sue, alors cette affirmation serait représentée par la formule $\forall x (L(p, x) \rightarrow \neg L(s, x))$. Nous pouvons maintenant élaborer une formule équivalente à celle-ci :

$$\forall x(L(p,x) \rightarrow \neg L(s,x))$$

is equivalent to $\forall x(\neg L(p,x) \vee \neg L(s,x))$ (conditional law),
 which is equivalent to $\forall x(\neg(L(p,x) \wedge L(s,x)))$ (De Morgan's law),
 which is equivalent to $\neg\exists x(L(p,x) \wedge L(s,x))$ (quantifier negation law).

En traduisant la dernière formule en anglais, nous obtenons l'affirmation « Il n'y a personne que Patricia et Sue aiment à la fois », et cela signifie la même chose que l'affirmation avec laquelle nous avons commencé.

Nous avons vu dans [la section 2.1](#) qu'inverser l'ordre de deux quantificateurs peut parfois modifier le sens d'une formule. Cependant, si les quantificateurs sont du même type (tous deux \forall ou tous deux \exists), il s'avère que l'ordre peut toujours être inversé sans affecter le sens de la formule. Par exemple, considérons l'affirmation « Quelqu'un a un professeur plus jeune que lui ». Pour l'écrire symboliquement, nous écrivons d'abord $\exists x (x \text{ a un professeur plus jeune que } x)$. Maintenant, pour dire « x a un professeur plus jeune que x », nous écrivons $\exists y (T(y, x) \wedge P(y, x))$, où $T(y, x)$ signifie « y est un professeur de x » et $P(y, x)$ signifie « y est plus jeune que x ». En mettant tout cela ensemble, l'énoncé original serait représenté par la formule $\exists x \exists y (T(y, x) \wedge P(y, x))$.

Que se passe-t-il si l'on inverse les quantificateurs ? Autrement dit, que signifie la formule $\exists y \exists x (T(y, x) \wedge P(y, x))$? Vous devriez être capable de vous convaincre que cette formule indique qu'il existe une personne y telle que y est l'enseignant d'une personne plus âgée que y . Autrement dit, une personne a un élève plus âgé que lui. Mais cela serait vrai exactement dans les mêmes circonstances que l'affirmation initiale : « Quelqu'un a un enseignant plus jeune que lui » ! Les deux signifient qu'il existe des personnes x et y telles que y est l'enseignant de x et y est plus jeune que x . En fait, cela suggère qu'une bonne façon d'interpréter la paire de quantificateurs $\exists y \exists x$ ou $\exists x \exists y$ serait « il existe des objets x et y tels que... ».

De même, deux quantificateurs universels consécutifs peuvent toujours être intervertis sans changer le sens d'une formule, car $\forall x \forall y$ et $\forall y \forall x$ peuvent tous deux être considérés comme signifiant « pour tous les objets x et y , ... ». Par exemple, considérons la formule $\forall x \forall y (L(x, y) \rightarrow A(x, y))$, où $L(x, y)$ signifie « x aime y » et $A(x, y)$ signifie « x admire y ». Vous pourriez considérer cette formule comme disant « Pour toutes les personnes x et y , si x aime y alors x admire y ». En d'autres termes, les gens admirent toujours les personnes qu'ils aiment. La formule $\forall y \forall x (L(x, y) \rightarrow A(x, y))$ signifie exactement la même chose.

Il est important de comprendre que lorsque nous disons « il existe des objets x et y » ou « pour tous les objets x et y », nous n'excluons pas la possibilité que x et y soient le même objet. Par exemple, la formule \forall

$\forall x \forall y (L(x, y) \rightarrow A(x, y))$ signifie non seulement qu'une personne qui apprécie une autre personne l'admirer toujours, mais aussi que les personnes qui s'apprécient s'admirent également elles-mêmes. Prenons un autre exemple : supposons que nous voulions écrire une formule signifiant « x est bigame ». (Bien sûr, x sera une variable libre dans cette formule.) On pourrait penser que l'on pourrait exprimer cela par la formule $\exists y \exists z (M(x, y) \wedge M(x, z))$, où $M(x, y)$ signifie « x est marié à y ». Mais pour dire que x est bigame, vous devez dire qu'il y a deux personnes *differentes* avec lesquelles x est marié, et cette formule ne dit pas que y et z sont différents. La bonne réponse est $\exists y \exists z (M(x, y) \wedge M(x, z) \wedge y \neq z)$.

Exemple 2.2.2. Analysez les formes logiques des énoncés suivants.

1. Tous les couples mariés ont des disputes.
2. Tout le monde aime au moins deux personnes.
3. John aime exactement une personne.

Solutions

1. $\forall x \forall y (M(x, y) \rightarrow F(x, y))$, où $M(x, y)$ signifie « x et y sont mariés l'un à l'autre » et $F(x, y)$ signifie « x et y se battent l'un contre l'autre ».
2. $\forall x \exists y \exists z (L(x, y) \wedge L(x, z) \wedge y \neq z)$, où $L(x, y)$ signifie « x aime y ». Notez que l'affirmation signifie que tout le monde aime au moins deux personnes *differentes*, il serait donc incorrect d'omettre le « $y \neq z$ » à la fin.
3. Soit $L(x, y)$ signifiant « x aime y », et j représentant John. Nous traduisons cette affirmation en symboles progressivement :
 - (i) $\exists x (John \text{ aime } x \text{ et } John \text{ n'aime personne d'autre que } x)$.
 - (ii) $\exists x (L(j, x) \wedge \neg \exists y (John \text{ aime } y \text{ et } y \neq x))$.
 - (iii) $\exists x (L(j, x) \wedge \neg \exists y (L(j, y) \wedge y \neq x))$.

Notez que pour la troisième affirmation de cet exemple, nous n'aurions pas pu donner la réponse plus simple $\exists x L(j, x)$, car cela signifierait que John aime *au moins* une personne, et non pas *exactement* une. L'expression « *exactement une* » est si fréquente en mathématiques qu'elle possède une notation spécifique. Nous écrirons $\exists! x P(x)$ pour représenter l'affirmation « Il existe exactement une valeur de x telle que $P(x)$ soit vraie. » On lit parfois aussi « Il existe un unique x tel que $P(x)$. » Par exemple, Par exemple, la troisième affirmation de [l'exemple 2.2.2](#) pourrait s'écrire symboliquement comme $\exists! x L(j, x)$. En fait, nous pourrions considérer cela comme une simple abréviation de la formule donnée dans [l'exemple 2.2.2](#) comme

réponse à l'affirmation 3. De même, en général, nous pouvons considérer $\exists! xP(x)$ comme une abréviation de la formule $\exists x(P(x) \wedge \neg\exists y(P(y) \wedge y \neq x))$.

Français Rappelons que lorsque nous discutons de la théorie des ensembles, nous trouvions parfois utile d'écrire l'ensemble de vérité de $P(x)$ comme $\{x \in U \mid P(x)\}$ plutôt que $\{x \mid P(x)\}$, pour être sûrs qu'il soit clair ce qu'était l'univers du discours. De même, au lieu d'écrire $\forall xP(x)$ pour indiquer que $P(x)$ est vrai pour toute valeur de x dans un univers U , nous pourrions écrire $\forall x \in UP(x)$. Cela se lit « Pour tout x dans U , $P(x)$. » De même, nous pouvons écrire $\exists x \in UP(x)$ pour dire qu'il existe au moins une valeur de x dans l'univers U telle que $P(x)$ soit vraie. Par exemple, l'énoncé $\forall x(x \geq 0)$ serait faux si l'univers du discours était les nombres réels, mais vrai s'il était les nombres naturels. Nous pourrions éviter toute confusion lors de la discussion de cette affirmation en écrivant soit $\forall x \in \mathbb{R}(x \geq 0)$ soit $\forall x \in \mathbb{N}(x \geq 0)$, pour clarifier ce que nous voulons dire.

Comme précédemment, nous utilisons parfois cette notation non pas pour spécifier l'univers du discours, mais pour restreindre l'attention à un sous-ensemble de cet univers. Par exemple, si notre univers de discours est celui des nombres réels et que nous voulons dire qu'un nombre réel x a une racine carrée, nous pourrions écrire $\exists y(y^2 = x)$. Pour dire que tout nombre réel *positif* a une racine carrée, nous dirions $\forall x \in \mathbb{R}^+ \exists y(y^2 = x)$. Nous pourrions dire que tout nombre réel positif a une racine carrée négative en écrivant $\forall x \in \mathbb{R}^+ \exists y \in \mathbb{R}^-(y^2 = x)$. En général, pour tout ensemble A , la formule $\forall x \in AP(x)$ signifie que pour toute valeur de x dans l'ensemble A , $P(x)$ est vraie, et $\exists x \in AP(x)$ signifie qu'il existe au moins une valeur de x dans l'ensemble A tel que $P(x)$ soit vrai. Les quantificateurs de ces formules sont parfois appelés *quantificateurs bornés*, car ils fixent des limites aux valeurs de x à considérer. On peut parfois utiliser des variantes de cette notation pour imposer d'autres types de restrictions aux variables quantifiées. Par exemple, l'affirmation selon laquelle tout nombre réel positif a une racine carrée négative pourrait aussi s'écrire $\forall x > 0 \exists y < 0(y^2 = x)$.

Les formules contenant des quantificateurs bornés peuvent également être considérées comme des abréviations de formules plus complexes contenant uniquement des quantificateurs normaux et non bornés. Dire que $\exists x \in AP(x)$ signifie qu'il existe une valeur de x dans A qui rend également $P(x)$ vraie, et une autre façon d'écrire cela serait $\exists x(x \in A \wedge P(x))$. De même, vous devez vous convaincre que $\forall x \in AP(x)$ signifie la même chose que $\forall x(x \in A \rightarrow P(x))$. Par exemple, la formule $\forall x \in \mathbb{R}^+ \exists y \in \mathbb{R}^-(y^2 = x)$ discutée précédemment signifie la même chose que $\forall x(x \in \mathbb{R}^+ \rightarrow \exists y \in \mathbb{R}^-(y^2 = x))$, qui à son tour peut

être développée comme $\forall x (x \in \mathbb{R}^+ \rightarrow \exists y (y \in \mathbb{R}^- \wedge y^2 = x))$. Par les définitions de \mathbb{R}^+ et \mathbb{R}^- , une manière équivalente de dire cela serait $\forall x (x > 0 \rightarrow \exists y (y < 0 \wedge y^2 = x))$. Vous devez vous assurer que vous êtes convaincu que cette formule, comme la formule originale, signifie que tout nombre réel positif a une racine carrée négative. Pour un autre exemple, notez que l'énoncé $A \subseteq B$, qui par définition signifie $\forall x (x \in A \rightarrow x \in B)$, pourrait également s'écrire $\forall x \in A (x \in B)$.

Il est intéressant de noter que les lois de négation des quantificateurs fonctionnent également pour les quantificateurs bornés. En fait, on peut déduire ces lois de négation des quantificateurs bornés des lois originales en considérant les quantificateurs bornés comme des abréviations, comme décrit précédemment. Par exemple :

$$\begin{aligned} \neg \forall x \in A P(x) \\ \text{is equivalent to } \neg \forall x (x \in A \rightarrow P(x)) \quad (\text{expanding abbreviation}), \\ \text{which is equivalent to } \exists x \neg (x \in A \rightarrow P(x)) \quad (\text{quantifier negation law}), \\ \text{which is equivalent to } \exists x \neg (x \notin A \vee P(x)) \quad (\text{conditional law}), \\ \text{which is equivalent to } \exists x (x \in A \wedge \neg P(x)) \quad (\text{De Morgan's law}), \\ \text{which is equivalent to } \exists x \in A \neg P(x) \quad (\text{abbreviation}). \end{aligned}$$

Ainsi, nous avons montré que $\neg \forall x \in AP(x)$ est équivalent à $\exists x \in A \neg P(x)$. On vous demande dans [l'exercice 5](#) de prouver l'autre loi de négation du quantificateur borné, selon laquelle $\neg \exists x \in AP(x)$ est équivalent à $\forall x \in A \neg P(x)$.

Il est clair que si $A = \emptyset$, alors $\exists x \in AP(x)$ sera faux, quelle que soit l'affirmation $P(x)$. Rien dans A ne peut rendre $P(x)$ vrai, une fois remplacé par x , car A est totalement vide ! La question de savoir si $\forall x \in AP(x)$ doit être considérée comme vraie ou fausse n'est peut-être pas claire, mais on peut trouver la réponse en utilisant les lois de négation des quantificateurs :

$$\begin{aligned} \forall x \in A P(x) \\ \text{is equivalent to } \neg \neg \forall x \in A P(x) \quad (\text{double negation law}), \\ \text{which is equivalent to } \neg \exists x \in A \neg P(x) \quad (\text{quantifier negation law}). \end{aligned}$$

Français Maintenant, si $A = \emptyset$ alors cette dernière formule sera vraie, quelle que soit l'affirmation $P(x)$, car, comme nous l'avons vu, $\exists x \in A \neg P(x)$ doit être faux. Ainsi, $\forall x \in AP(x)$ est toujours vrai si $A = \emptyset$. Les mathématiciens disent parfois qu'une telle affirmation est vraie *par vide*. Une autre façon de voir cela est de réécrire l'affirmation $\forall x \in AP(x)$ sous la forme équivalente $\forall x (x \in A \rightarrow P(x))$. Maintenant, selon la table de vérité pour le connecteur conditionnel, la seule façon dont cela peut être faux est s'il existe une valeur de x telle que $x \in A$ est vrai mais $P(x)$ est faux. Mais il n'existe pas de telle valeur de x , simplement parce qu'il n'existe pas de valeur de x pour laquelle $x \in A$ est vrai.

En application de ce principe, on remarque que l'ensemble vide est un sous-ensemble de tout ensemble. Pour comprendre pourquoi, il suffit de réécrire l'énoncé $A \subseteq B$ sous la forme équivalente $\forall x \in A (x \in B)$. Or, si $A = \emptyset$, alors, comme nous venons de le constater, cet énoncé est vide de sens. Ainsi, quel que soit l'ensemble B , $\emptyset \subseteq B$. Un autre exemple d'énoncé vide de sens est l'énoncé « Toutes les licornes sont violettes ». On pourrait le représenter par la formule $\forall x \in AP (x)$, où A est l'ensemble de toutes les licornes et $P(x)$ signifie « x est violet ». Puisqu'il n'y a pas de licornes, A est l'ensemble vide, donc l'énoncé est vide de sens. (Remarque : l'énoncé « Toutes les licornes sont vertes » est également vrai, ce qui ne contredit pas le fait que toutes les licornes sont violettes !)

Vous avez peut-être remarqué que, bien qu'au [chapitre 1](#) nous ayons toujours pu vérifier les équivalences impliquant des connecteurs logiques en créant des tables de vérité, nous ne disposons pas d'un moyen aussi simple de vérifier les équivalences impliquant des quantificateurs. Jusqu'à présent, nous avons justifié nos équivalences impliquant des quantificateurs en nous basant sur des exemples et en faisant appel au bon sens. À mesure que les formules que nous utilisons se complexifient, cette méthode deviendra peu fiable et difficile à utiliser. Heureusement, au [chapitre 3](#), nous développerons de meilleures méthodes de raisonnement sur des énoncés impliquant des quantificateurs. Pour vous entraîner à réfléchir aux quantificateurs, nous allons résoudre quelques équivalences un peu plus complexes en faisant appel au bon sens. Si vous n'êtes pas entièrement convaincu de la justesse de ces équivalences, vous pourrez les vérifier plus attentivement au [chapitre 3](#).

Considérons l'affirmation « Tout le monde a les yeux brillants et la queue touffue ». Si nous posons $E(x)$ signifiant « x a les yeux brillants » et $T(x)$ signifiant « x a la queue touffue », alors nous pourrions représenter cette affirmation par la formule $\forall x (E(x) \wedge T(x))$. Est-ce équivalent à la formule $\forall x E(x) \wedge \forall x T(x)$? Cette dernière formule signifie « Tout le monde a les yeux brillants et tout le monde a la queue touffue », et intuitivement cela signifie la même chose que l'affirmation originale. Ainsi, il apparaît que $\forall x (E(x) \wedge T(x))$ est équivalent à $\forall x E(x) \wedge \forall x T(x)$. En d'autres termes, nous pourrions dire que le quantificateur universel *distribue sur* la conjonction.

Cependant, la loi distributive correspondante ne fonctionne pas pour le quantificateur existentiel. Considérons les formules $\exists x (E(x) \wedge T(x))$ et $\exists x E(x) \wedge \exists x T(x)$. La première signifie qu'il existe une personne à la fois brillante et à la queue touffue, et la seconde signifie qu'il existe une personne brillante et une personne à la queue touffue. Ces deux affirmations ne signifient pas la même chose. Dans la deuxième affirmation, la personne brillante et la personne à la queue touffue ne

sont pas nécessairement identiques, mais dans la première, elles le sont. Une autre façon de comprendre la différence entre les deux affirmations est de considérer les ensembles de vérité. Soit A l'ensemble de vérité de $E(x)$ et B l'ensemble de vérité de $T(x)$. Autrement dit, A est l'ensemble des personnes brillantes et B l'ensemble des personnes à la queue touffue. Ensuite, la deuxième L'énoncé dit que ni A ni B ne sont l'ensemble vide, mais le premier dit que $A \cap B$ n'est pas l'ensemble vide, ou en d'autres termes que A et B ne sont pas disjoints.

Français En application de la loi distributive pour le quantificateur universel et la conjonction, supposons que A et B soient des ensembles et considérons l'équation $A = B$. Nous savons que deux ensembles sont égaux lorsqu'ils ont exactement les mêmes éléments. Ainsi, l'équation $A = B$ signifie $\forall x (x \in A \leftrightarrow x \in B)$, ce qui est équivalent à $\forall x [(x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)]$. Comme le quantificateur universel distribue sur la conjonction, cela est équivalent à la formule $\forall x (x \in A \rightarrow x \in B) \wedge \forall x (x \in B \rightarrow x \in A)$, et par définition du sous-ensemble cela signifie $A \subseteq B \wedge B \subseteq A$. Ainsi, nous avons montré que l'équation $A = B$ est également équivalente à la formule $A \subseteq B \wedge B \subseteq A$.

Nous avons maintenant introduit sept symboles logiques fondamentaux : les connecteurs \wedge , \vee , \neg , \rightarrow et \leftrightarrow , ainsi que les quantificateurs \forall et \exists . Il est remarquable que la structure de tout énoncé mathématique puisse être comprise grâce à ces symboles, et que tout raisonnement mathématique puisse être analysé à l'aune de leur utilisation appropriée. Pour illustrer la puissance des symboles que nous avons introduits, nous concluons cette section en écrivant quelques énoncés mathématiques supplémentaires en notation logique.

Exemple 2.2.3. Analysez les formes logiques des énoncés suivants.

1. Énoncés sur les nombres naturels. L'univers du discours est \mathbb{N} .
 - (a) x est un carré parfait.
 - (b) x est un multiple de y .
 - (c) x est premier.
 - (d) x est le plus petit nombre positif qui est un multiple de y et de z .

2. Énoncés sur les nombres réels. L'univers du discours est \mathbb{R}

- (a) L'élément d'identité pour l'addition est 0.
- (b) Tout nombre réel a un inverse additif.
- (c) Les nombres négatifs n'ont pas de racines carrées.
- (d) Chaque nombre positif a exactement deux racines carrées.

Solutions

1. (a) Cela signifie que x est le carré d'un nombre naturel, ou en d'autres termes $\exists y (x = y^2)$.

- (b) Cela signifie que x est égal à y fois un nombre naturel, ou en d'autres termes $\exists z (x = yz)$.
- (c) Cela signifie que $x > 1$, et x ne peut pas être écrit comme un produit de deux nombres naturels plus petits. En symboles : $x > 1 \wedge \neg \exists y \exists z (x = yz \wedge y < x \wedge z < x)$.
- (d) Nous traduisons cela en plusieurs étapes :
- x est positif et x est un multiple de y et de z et il n'y a pas de nombre positif plus petit qui soit un multiple de y et de z .
 - $x > 0 \wedge \exists a (x = ya) \wedge \exists b (x = zb) \wedge \neg \exists w (w > 0 \wedge w < x \wedge (w \text{ est un multiple de } y \text{ et de } z))$.
 - $x > 0 \wedge \exists a (x = ya) \wedge \exists b (x = zb) \wedge \neg \exists w (w > 0 \wedge w < x \wedge \exists c (w = yc) \wedge \exists d (w = zd))$.
2. (a) $\forall x (x + 0 = x)$.
- (b) $\forall x \exists y (x + y = 0)$.
- (c) $\forall x (x < 0 \rightarrow \neg \exists y (y^2 = x))$.
- (d) Nous traduisons cela progressivement :
- $\forall x (x > 0 \rightarrow x \text{ a exactement deux racines carrées})$.
 - $\forall x (x > 0 \rightarrow \exists y \exists z (y \text{ et } z \text{ sont des racines carrées de } x \text{ et } y \neq z \text{ et rien d'autre n'est une racine carrée de } x))$.
 - $\forall x (x > 0 \rightarrow \exists y \exists z (y^2 = x \wedge z^2 = x \wedge y \neq z \wedge \neg \exists w (w^2 = x \wedge w \neq y \wedge w \neq z)))$.

Exercices

- *1. Inversez ces affirmations, puis reformulez les résultats sous forme d'affirmations positives équivalentes. (Voir [l'exemple 2.2.1](#).)
- Tous ceux qui se spécialisent en mathématiques ont un ami qui a besoin d'aide pour ses devoirs.
 - Tout le monde a un colocataire qui n'aime personne.
 - $A \cup B \subseteq C \setminus D$.
 - $\exists x \forall y [y > x \rightarrow \exists z (z^2 + 5z = y)]$.
2. Niez ces affirmations, puis reformulez les résultats sous forme d'affirmations positives équivalentes. (Voir [l'exemple 2.2.1](#).)
- Il y a quelqu'un dans la classe de première année qui n'a pas de colocataire.
 - Tout le monde aime quelqu'un, mais personne n'aime tout le monde.
 - $\forall a \in A \exists b \in B (a \in C \leftrightarrow b \in C)$.
 - $\forall y > 0 \exists x (ax^2 + bx + c = y)$.
3. Ces affirmations sont- elles vraies ou fausses ? L'univers du discours est \mathbb{N}_r
- $\forall x (x < 7 \rightarrow \exists a \exists b \exists c (a^2 + b^2 + c^2 = x))$.

- (b) $\exists! x (x^2 + 3 = 4x)$.
- (c) $\exists! x (x^2 = 4x + 5)$.
- (d) $\exists x \exists y (x^2 = 4x + 5 \wedge y^2 = 4y + 5)$.

- *4. Montrer que la deuxième loi de négation des quantificateurs, qui stipule que $\neg\forall x P(x)$ est équivalent à $\exists x \neg P(x)$, peut être dérivée de la première, qui stipule que $\neg\exists x P(x)$ est équivalent à $\forall x \neg P(x)$. (Indice : utiliser la loi de double négation.)
5. Montrer que $\neg\exists x \in AP(x)$ est équivalent à $\forall x \in A \neg P(x)$.
- *6. Montrer que le quantificateur existentiel distribue sur la disjonction. Autrement dit, montrer que $\exists x (P(x) \vee Q(x))$ est équivalent à $\exists x P(x) \vee \exists x Q(x)$. (Indice : Utiliser le fait, discuté dans cette section, que le quantificateur universel distribue sur la conjonction.)
7. Montrer que $\exists x (P(x) \rightarrow Q(x))$ est équivalent à $\forall x P(x) \rightarrow \exists x Q(x)$.
- *8. Montrer que $(\forall x \in AP(x)) \wedge (\forall x \in BP(x))$ est équivalent à $\forall x \in (A \cup B) P(x)$. (Indice : Commencez par écrire la signification des quantificateurs bornés en termes de quantificateurs non bornés.)
9. $\forall x (P(x) \vee Q(x))$ est-il équivalent à $\forall x P(x) \vee \forall x Q(x)$? Expliquez. (Indice : Essayez d'attribuer des significations à $P(x)$ et $Q(x)$.)
10. (a) Montrez que $\exists x \in AP(x) \vee \exists x \in BP(x)$ est équivalent à $\exists x \in (A \cup B) P(x)$.
(b) Est-ce que $\exists x \in AP(x) \wedge \exists x \in BP(x)$ est équivalent à $\exists x \in (A \cap B) P(x)$? Expliquez.
11. Démontrer que les énoncés $A \subseteq B$ et $A \setminus B = \emptyset$ sont équivalents en écrivant chacun d'eux sous forme de symboles logiques, puis en montrant que les formules résultantes sont équivalentes.
12. Démontrez que les énoncés $C \subseteq A \cup B$ et $C \setminus A \subseteq B$ sont équivalents en écrivant chacun d'eux sous forme de symboles logiques, puis en montrant que les formules résultantes sont équivalentes.
13. (a) Démontrer que les énoncés $A \subseteq B$ et $A \cup B = B$ sont équivalents en les écrivant chacun avec des symboles logiques, puis en montrant que les formules résultantes sont équivalentes.
(Indice : [L'exercice 11 de la section 1.5 pourrait vous être utile.](#))
(b) Montrez que les énoncés $A \subseteq B$ et $A \cap B = A$ sont équivalents.
14. Démontrer que les énoncés $A \cap B = \emptyset$ et $A \setminus B = A$ sont équivalents.
15. Soit $T(x, y)$ signifiant « x est un enseignant de y ». Que signifient les affirmations suivantes ? Dans quelles circonstances chacune d'elles serait-elle vraie ? Sont-elles équivalentes ?
(a) $\exists! y T(x, y)$.

- (b) $\exists x \exists! y T(x, y)$.
- (c) $\exists! x \exists y T(x, y)$.
- (d) $\exists y \exists! x T(x, y)$.
- (e) $\exists! x \exists! y T(x, y)$.
- (f) $\exists x \exists y [T(x, y) \wedge \neg \exists u \exists v (T(u, v) \wedge (u \neq x \vee v \neq y))]$.

2.3 Autres opérations sur les ensembles

Maintenant que nous savons comment travailler avec des quantificateurs, nous sommes prêts à discuter de sujets plus avancés en théorie des ensembles.

Jusqu'à présent, la seule façon dont nous disposons pour définir des ensembles, autre que d'énumérer leurs éléments un par un, est d'utiliser la notation de test d'élémentarité $\{x \mid P(x)\}$. Parfois, cette notation est modifiée en permettant de remplacer le *x avant la ligne verticale par une expression plus complexe*. Par exemple, supposons que nous voulions définir S comme l'ensemble de tous les carrés parfaits. La façon la plus simple de décrire cet ensemble est peut-être de dire qu'il est constitué de tous les nombres de la forme n^2 , où n est un entier naturel. Cela s'écrit $S = \{n^2 \mid n \in \mathbb{N}\}$. Notez qu'en utilisant notre solution pour la première affirmation de [l'exemple 2.2.3](#), nous pourrions également définir cet ensemble en écrivant $S = \{x \mid \exists n \in \mathbb{N} (x = n^2)\}$. Ainsi, $\{n^2 \mid n \in \mathbb{N}\} = \{x \mid \exists n \in \mathbb{N} (x = n^2)\}$ et donc $x \in \{n^2 \mid n \in \mathbb{N}\}$ signifie la même chose que $\exists n \in \mathbb{N} (x = n^2)$.

Une notation similaire est souvent utilisée si les éléments d'un ensemble ont été numérotés. Par exemple, supposons que nous voulions former l'ensemble dont les éléments sont les 100 premiers nombres premiers. Nous pourrions commencer par numérotter les nombres premiers, en les appelant p_1, p_2, p_3, \dots . Autrement dit, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, et ainsi de suite. L'ensemble que nous recherchons serait alors l'ensemble $P = \{p_1, p_2, p_3, \dots, p_{100}\}$. Une autre façon de décrire cet ensemble serait de dire qu'il est constitué de tous les nombres p_i , car i est un élément de l'ensemble $I = \{1, 2, 3, \dots, 100\} = \{i \in \mathbb{N} \mid 1 \leq i \leq 100\}$. Cela pourrait s'écrire $P = \{p_i \mid i \in I\}$. Chaque élément p_i de cet ensemble est identifié par un nombre $i \in I$, appelé l'*indice* de l'élément. Un ensemble défini de cette manière est parfois appelé une *famille indexée*, et I est appelé l'*ensemble d'indices*.

Bien que les indices d'une famille indexée soient souvent des nombres, ils ne doivent pas nécessairement l'être. Par exemple, supposons que S soit l'ensemble de tous les élèves de votre école. Si

nous voulions former l'ensemble de toutes les mères des élèves, nous pourrions laisser m_s représenter la mère de s , pour tout élève s . Alors l'ensemble de toutes les mères des élèves pourrait s'écrire $M = \{m_s \mid s \in S\}$. Il s'agit d'une famille indexée dans laquelle l'ensemble d'indices est S , l'ensemble de tous les élèves. Chaque mère de l'ensemble est identifiée en nommant l'élève qui est son enfant. Notez que nous pourrions également définir cet ensemble en utilisant un test d'élémentarité, en écrivant $M = \{m \mid m \text{ est la mère d'un élève}\} = \{m \mid \exists s \in S (m = m_s)\}$. En général, toute famille indexée $A = \{x_i \mid i \in I\}$ peut également être définie comme $A = \{x \mid \exists i \in I (x = x_i)\}$. Il s'ensuit que l'énoncé $x \in \{x_i \mid i \in I\}$ signifie la même chose que $\exists i \in I (x = x_i)$.

Exemple 2.3.1. Analysez les formes logiques des énoncés suivants en écrivant les définitions de la notation de la théorie des ensembles utilisée.

1. $y \in \{\sqrt[3]{x} \mid x \in \mathbb{Q}\}$.
2. $\{x_i \mid i \in I\} \subseteq A$.
3. $\{n^2 \mid n \in \mathbb{N}\}$ et $\{n^3 \mid n \in \mathbb{N}\}$ ne sont pas disjoints.

Solutions

1. $\exists x \in \mathbb{Q} (y = \sqrt[3]{x})$.
2. Par la définition du sous-ensemble, nous devons dire que chaque élément de $\{x_i \mid i \in I\}$ est aussi un élément de A , nous pourrions donc commencer par écrire $\forall x (x \in \{x_i \mid i \in I\} \rightarrow x \in A)$. En complétant la signification de $x \in \{x_i \mid i \in I\}$, que nous avons élaborée précédemment, nous obtiendrions $\forall x (\exists i \in I (x = x_i) \rightarrow x \in A)$. Mais puisque les éléments de $\{x_i \mid i \in I\}$ sont juste les x_i , pour tout $i \in I$, peut-être qu'une manière plus simple de dire que chaque élément de $\{x_i \mid i \in I\}$ est un élément de A serait $\forall i \in I (x_i \in A)$. Les deux réponses que nous avons données sont équivalentes, mais le démontrer nécessiterait les méthodes que nous étudierons au [chapitre 3](#).
3. Nous devons dire que les deux ensembles ont un élément commun, donc une solution est de commencer par écrire $\exists x (x \in \{n^2 \mid n \in \mathbb{N}\} \wedge x \in \{n^3 \mid n \in \mathbb{N}\})$. Cependant, comme dans la dernière affirmation, il existe un moyen plus simple. Un élément commun aux deux ensembles devrait être le carré d'un nombre naturel et aussi le cube

d'un nombre naturel (éventuellement différent). Ainsi, nous pourrions dire qu'il existe un tel élément commun en disant $\exists n \in \mathbb{N} \exists m \in \mathbb{N} (n^2 = m^3)$. Notez qu'il serait erroné d'écrire $\exists n \in \mathbb{N} (n^2 = n^3)$, car cela ne permettrait pas que les deux nombres naturels soient différents. Au fait, cette affirmation est vraie, puisque $64 = 8^2 = 4^3$, donc 64 est un élément des deux ensembles.

N'importe quoi peut être élément d'un ensemble. Des idées intéressantes et utiles surgissent lorsqu'on considère la possibilité qu'un ensemble ait *d'autres ensembles* comme éléments. Par exemple, supposons que $A = \{1, 2, 3\}$, $B = \{4\}$ et $C = \emptyset$. Il n'y a aucune raison pour que nous ne puissions pas former l'ensemble $\mathcal{F} = \{A, B, C\}$, dont les éléments sont les trois ensembles A , B et C . En complétant les définitions de A , B et C , nous pourrions l'écrire autrement : $\mathcal{F} = \{\{1, 2, 3\}, \{4\}, \emptyset\}$. Notons que $1 \in A$ et $A \in \mathcal{F}$ mais $1 \notin \mathcal{F}$. \mathcal{F} n'a que trois éléments, et tous trois sont des ensembles, et non des nombres. Des ensembles comme \mathcal{F} , dont tous les éléments sont des ensembles, sont parfois appelés *familles* d'ensembles.

Il est souvent pratique de définir des familles d'ensembles comme des familles indexées. Par exemple, supposons que S représente l'ensemble de tous les étudiants, et que pour chaque étudiant s , C_s soit l'ensemble des cours suivis par s . L'ensemble de ces ensembles C_s constituerait alors une famille indexée d'ensembles $\mathcal{F} = \{C_s \mid s \in S\}$. Rappelons que les éléments de cette famille ne sont pas des cours, mais *des ensembles* de cours. Si nous laissons t représenter une étudiante particulière, Tina, et si Tina a suivi des cours de calcul, de composition anglaise et d'histoire américaine, alors $C_t = \{\text{Calcul, composition anglaise, histoire américaine}\}$ et $C_t \in \mathcal{F}$, mais $\text{Calcul} \notin \mathcal{F}$.

Un exemple important d'une famille d'ensembles est donné par l'ensemble des puissances d'un ensemble.

Définition 2.3.2. Supposons que A soit un ensemble. L'*ensemble des puissances* de A , noté $\mathcal{P}(A)$, est l'ensemble dont les éléments sont tous les sous-ensembles de A . Autrement dit,

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

Par exemple, l'ensemble $A = \{7, 12\}$ a quatre sous-ensembles : \emptyset , $\{7\}$, $\{12\}$ et $\{7, 12\}$. Ainsi, $\mathcal{P}(A) = \{\emptyset, \{7\}, \{12\}, \{7, 12\}\}$. Qu'en est-il de $\mathcal{P}(\emptyset)$? Bien que \emptyset n'ait aucun élément, il a un sous-ensemble, à savoir \emptyset .

Ainsi, $\mathcal{P}(\emptyset) = \{\emptyset\}$. Notez que, comme nous l'avons vu dans [la section 1.3](#), $\{\emptyset\}$ n'est pas la même chose que \emptyset .

Chaque fois que vous travaillez avec des sous-ensembles d'un ensemble X , il peut être utile de se rappeler que tous ces sous-ensembles de X sont des éléments de $\mathcal{P}(X)$, par définition d'ensemble de puissance. Par exemple, si l'on considère C comme l'ensemble de tous les cours proposés dans votre établissement, alors chacun des ensembles C_s décrits précédemment est un sous-ensemble de C . Ainsi, pour chaque élève s , $C_s \in \mathcal{P}(C)$. Cela signifie que chaque élément de la famille $\mathcal{F} = \{C_s \mid s \in S\}$ est un élément de $\mathcal{P}(C)$, donc $\mathcal{F} \subseteq \mathcal{P}(C)$.

Exemple 2.3.3. Analysez les formes logiques des énoncés suivants.

1. $x \in \mathcal{P}(A)$.
2. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
3. $B \in \{\mathcal{P}(A) \mid A \in \mathcal{F}\}$.
4. $x \in \mathcal{P}(A \cap B)$.
5. $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

Solutions

1. Par définition d'un ensemble entier, les éléments de $\mathcal{P}(A)$ sont les sous-ensembles de A . Ainsi, dire que $x \in \mathcal{P}(A)$ signifie que $x \subseteq A$, dont nous savons déjà qu'il peut s'écrire $\forall y (y \in x \rightarrow y \in A)$.
2. Par définition de sous-ensemble, cela signifie $\forall x (x \in \mathcal{P}(A) \rightarrow x \in \mathcal{P}(B))$. Maintenant, en écrivant $x \in \mathcal{P}(A)$ et $x \in \mathcal{P}(B)$ comme précédemment, nous obtenons $\forall x [\forall y (y \in x \rightarrow y \in A) \rightarrow \forall y (y \in x \rightarrow y \in B)]$.
3. Comme précédemment, cela signifie $\exists A \in \mathcal{F} (B = \mathcal{P}(A))$. Dire que $B = \mathcal{P}(A)$ signifie que les éléments de B sont précisément les sous-ensembles de A , autrement dit $\forall x (x \in B \leftrightarrow x \subseteq A)$. Complétons ceci et écrivons la définition du sous-ensemble, nous obtenons notre réponse finale, $\exists A \in \mathcal{F} \forall x (x \in B \leftrightarrow \forall y (y \in x \rightarrow y \in A))$.
4. Comme dans la première affirmation, nous commençons par écrire ceci comme $\forall y (y \in x \rightarrow y \in A \cap B)$. Maintenant, en complétant la définition de l'intersection, nous obtenons $\forall y (y \in x \rightarrow (y \in A \wedge y \in B))$.

5. Par définition de l'intersection, cela signifie ($x \in \mathcal{P}(A)$) \wedge ($x \in \mathcal{P}(B)$). Maintenant, en écrivant la définition de l'ensemble des puissances comme précédemment, nous obtenons $\forall y (y \in x \rightarrow y \in A) \wedge \forall y (y \in x \rightarrow y \in B)$.

Notez que pour l'énoncé 5 de cet exemple, nous avons d'abord écrit la définition d'intersection, puis utilisé celle d'ensemble de puissances, tandis que pour l'énoncé 4, nous avons commencé par écrire la définition d'ensemble de puissances, puis celle d'intersection. À mesure que vous apprendrez les définitions de termes et de symboles mathématiques, il deviendra plus important de savoir à quelle définition réfléchir en premier pour comprendre un énoncé mathématique complexe. En règle générale, il est conseillé de toujours commencer par le symbole « le plus externe ». Dans l'énoncé 4 de [l'exemple 2.3.3](#), le symbole d'intersection figurait à l'intérieur de la notation d'ensemble de puissances ; nous avons donc d'abord écrit la définition d'ensemble de puissances. Dans l'énoncé 5, la notation d'ensemble de puissances figurait de part et d'autre de la notation d'intersection de deux ensembles ; nous avons donc commencé par la définition d'intersection. Des considérations similaires nous ont conduits à utiliser d'abord la définition de sous-ensemble, plutôt que celle d'ensemble de puissances, dans l'énoncé 2.

Il est intéressant de noter que nos réponses aux affirmations 4 et 5 de [l'exemple 2.3.3](#) sont équivalentes. (Vous êtes invité à vérifier cela dans [l'exercice 11](#).) Comme dans [la section 1.4](#), il s'ensuit que pour tout ensemble A et B , $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$. Dans [l'exercice 12](#), vous êtes invité à montrer que cette équation n'est pas vraie en général si nous changeons \cap en \cup .

Considérons à nouveau la famille d'ensembles $\mathcal{F} = \{C_s \mid s \in S\}$, où S est l'ensemble de tous les étudiants et pour chaque étudiant s , C_s est l'ensemble de tous les cours que s a suivis. Si nous voulions savoir quels cours ont été suivis par tous les étudiants, nous devrions trouver les éléments que tous les ensembles de \mathcal{F} ont en commun. L'ensemble de tous ces éléments communs est appelé l'intersection de la famille \mathcal{F} et s'écrit $\cap \mathcal{F}$. De même, l'union de la famille \mathcal{F} , notée $\cup \mathcal{F}$, est l'ensemble résultant de la réunion de tous les éléments de tous les ensembles de \mathcal{F} en un seul ensemble. Dans ce cas, $\cup \mathcal{F}$ serait l'ensemble de tous les cours qui ont été suivis par un étudiant.

Exemple 2.3.4. Soit $\mathcal{F} = \{\{1, 2, 3, 4\}, \{2, 3, 4, 5\}, \{3, 4, 5, 6\}\}$. Trouver $\cap \mathcal{F}$ et $\cup \mathcal{F}$.

Solution

$$\begin{aligned}\bigcap \mathcal{F} &= \{1, 2, 3, 4\} \cap \{2, 3, 4, 5\} \cap \{3, 4, 5, 6\} = \{3, 4\}, \\ \bigcup \mathcal{F} &= \{1, 2, 3, 4\} \cup \{2, 3, 4, 5\} \cup \{3, 4, 5, 6\} = \{1, 2, 3, 4, 5, 6\}.\end{aligned}$$

Bien que ces exemples puissent clarifier ce que nous entendons par $\bigcap \mathcal{F}$ et $\bigcup \mathcal{F}$, nous n'avons pas encore donné de définition précise de ces ensembles. En général, si \mathcal{F} est une famille d'ensembles, alors nous voulons que $\bigcap \mathcal{F}$ contienne les éléments que tous les ensembles de \mathcal{F} ont en commun. Ainsi, pour être un élément de $\bigcap \mathcal{F}$, un objet devra être un élément de chaque ensemble de \mathcal{F} . D'autre part, tout élément de l'un des ensembles de \mathcal{F} doit être dans $\bigcup \mathcal{F}$, donc pour être dans $\bigcup \mathcal{F} \Leftrightarrow$ un objet n'a besoin que d'être un élément d'au moins un ensemble de \mathcal{F} . Ainsi, nous sommes conduits aux définitions générales suivantes.

Définition 2.3.5. Supposons que \mathcal{F} soit une famille d'ensembles. Alors l'*intersection* et la *réunion* de \mathcal{F} sont les ensembles $\bigcap \mathcal{F}$ et $\bigcup \mathcal{F}$ définis comme suit :

$$\begin{aligned}\bigcap \mathcal{F} &= \{x \mid \forall A \in \mathcal{F} (x \in A)\} = \{x \mid \forall A (A \in \mathcal{F} \rightarrow x \in A)\}. \\ \bigcup \mathcal{F} &= \{x \mid \exists A \in \mathcal{F} (x \in A)\} = \{x \mid \exists A (A \in \mathcal{F} \wedge x \in A)\}.\end{aligned}$$

Certains mathématiciens considèrent que $\bigcap \mathcal{F}$ est indéfini si $\mathcal{F} = \emptyset$. Pour une explication de ce phénomène, voir [l'exercice 15](#). Nous utiliserons la notation $\bigcap \mathcal{F}$ uniquement lorsque $\mathcal{F} \neq \emptyset$.

Notez que si A et B sont deux ensembles quelconques et $\mathcal{F} = \{A, B\}$, alors $\bigcap \mathcal{F} = A \cap B$ et $\bigcup \mathcal{F} = A \cup B$. Ainsi, les définitions de l'intersection et de l'union d'une famille d'ensembles sont en fait des généralisations de nos anciennes définitions de l'intersection et de l'union de deux ensembles.

Exemple 2.3.6. Analysez les formes logiques des énoncés suivants.

1. $x \in \bigcap \mathcal{F}$.
2. $\bigcap \mathcal{F} \not\subseteq \bigcup \mathcal{G}$.
3. $x \in \mathcal{P}(\bigcup \mathcal{F})$.
4. $x \in \bigcup \{\mathcal{P}(A) \mid A \in \mathcal{F}\}$.

Solutions

1. Par définition de l'intersection d'une famille d'ensembles, cela signifie $\forall A \in \mathcal{F} (x \in A)$, ou de manière équivalente, $\forall A (A \in \mathcal{F} \rightarrow x \in A)$.
2. Comme nous l'avons vu dans [l'exemple 2.2.1](#), dire qu'un ensemble n'est pas un sous-ensemble d'un autre signifie qu'il y a quelque chose qui est un élément du premier mais pas du deuxième. Ainsi, nous commençons par écrire $\exists x (x \in \bigcap \mathcal{F} \wedge x \notin \bigcup \mathcal{G})$. Nous avons déjà écrit ce que $x \in \bigcap \mathcal{F}$ signifie dans la solution 1. Par définition de l'union d'une famille d'ensembles, $x \in \bigcup \mathcal{G}$ signifie $\exists A \in \mathcal{G} (x \in A)$, donc $x \notin \bigcup \mathcal{G}$ signifie $\neg \exists A \in \mathcal{G} (x \in A)$. Par les lois de négation des quantificateurs, cela est équivalent à $\forall A \in \mathcal{G} (x \notin A)$. En mettant tout cela ensemble, notre réponse est $\exists x [\forall A \in \mathcal{F} (x \in A) \wedge \forall A \in \mathcal{G} (x \notin A)]$.
3. Puisque le symbole d'union apparaît dans la notation d'ensemble, commençons par définir l'ensemble. Comme dans [l'exemple 2.3.3](#), nous obtenons $x \subseteq \bigcup \mathcal{F}$, autrement dit $\forall y (y \in x \rightarrow y \in \bigcup \mathcal{F})$. Nous utilisons maintenant la définition d'union pour écrire $y \in \bigcup \mathcal{F}$ comme $\exists A \in \mathcal{F} (y \in A)$. La réponse finale est $\forall y (y \in x \rightarrow \exists A \in \mathcal{F} (y \in A))$.
4. Commençons par définir l'union. Selon cette définition, l'énoncé signifie que x est un élément d'au moins un des ensembles $\mathcal{P}(A)$, pour $A \in \mathcal{F}$. Autrement dit, $\exists A \in \mathcal{F} (\exists y (y \in \mathcal{P}(A)))$. En intégrant notre analyse de l'énoncé $x \in \mathcal{P}(A)$ de [l'exemple 2.3.3](#), nous obtenons $\exists A \in \mathcal{F} \forall y (y \in x \rightarrow y \in A)$.

Écrire des énoncés mathématiques complexes en symboles logiques, comme nous l'avons fait dans le dernier exemple, peut parfois vous aider à comprendre leur signification et leur véracité. Par exemple, supposons que nous posions à nouveau C_s l'ensemble de tous les cours suivis par l'étudiant s . Soit M l'ensemble des étudiants en mathématiques et E l'ensemble des étudiants en anglais, et soit $\mathcal{F} = \{C_s | s \in M\}$ et $\mathcal{G} = \{C_s | s \in E\}$. Avec ces définitions, que signifie l'énoncé 2 de [l'exemple 2.3.6](#), et dans quelles circonstances serait-il vrai ? Selon notre solution pour cet exemple, l'énoncé signifie $\exists x [\forall A \in \mathcal{F} (x \in A) \wedge \forall A \in \mathcal{G} (x \notin A)]$.

$\forall A \in \mathcal{G} (x \notin A)$], ou en d'autres termes, il existe un élément qui est un élément de chaque ensemble de \mathcal{F} , et qui n'est pas un élément de chaque ensemble de \mathcal{G} . Compte tenu des définitions de \mathcal{F} et \mathcal{G} que nous utilisons, cela signifie qu'un cours a été suivi par tous les étudiants en mathématiques, mais par aucun étudiant en anglais. Si, par exemple, tous les étudiants en mathématiques ont suivi le calcul, mais aucun étudiant en anglais, alors l'affirmation est vraie.

Prenons un autre exemple : supposons que $\mathcal{F} = \{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}\}$ et $x = \{4, 5, 6\}$. Avec ces définitions, l'affirmation 3 de [l'exemple 2.3.6](#) serait-elle vraie ? On pourrait le déterminer en trouvant $\mathcal{P}(\cap \mathcal{F})$ puis en vérifiant si x en est un élément, mais cela prendrait beaucoup de temps, car il s'avère que $\mathcal{P}(\cap \mathcal{F})$ possède 32 éléments. Il est plus facile d'utiliser la traduction en symboles logiques donnée dans notre solution pour cet exemple. Selon cette traduction, l'affirmation signifie $\forall y (y \in x \rightarrow \exists A \in \mathcal{F} (y \in A))$; autrement dit, chaque élément de x appartient à au moins un ensemble de \mathcal{F} . Revenons à nos définitions de \mathcal{F} et x , il n'est pas difficile de voir que cela est faux, car $6 \in x$, mais 6 n'est dans aucun des ensembles de \mathcal{F} .

Une notation alternative est parfois utilisée pour l'union ou l'intersection d'une famille indexée d'ensembles. Supposons que $\mathcal{F} = \{A_i \mid i \in I\}$, où chaque A_i est un ensemble. Alors $\bigcup \mathcal{F}$ serait l'ensemble de tous les éléments communs à tous les A_i , pour $i \in I$, et cela peut aussi s'écrire ainsi $\cap_{i \in I} A_i$:

$$\bigcap \mathcal{F} = \bigcap_{i \in I} A_i = \{x \mid \forall i \in I (x \in A_i)\}.$$

De même, une notation alternative pour $\bigcup \mathcal{F}$ est $\bigcup_{i \in I} A_i$, donc

$$\bigcup \mathcal{F} = \bigcup_{i \in I} A_i = \{x \mid \exists i \in I (x \in A_i)\}.$$

En revenant à notre exemple de cours suivis par les étudiants, nous pourrions utiliser cette notation pour écrire l'ensemble des cours suivis par tous les étudiants comme $\bigcap_{s \in S} C_s$. Vous pourriez considérer cette notation comme désignant le résultat de l'exécution de tous les éléments s dans S , formant l'ensemble C_s pour chacun d'eux, puis intersectant tous ces ensembles.

Exemple 2.3.7. Soit $I = \{1, 2, 3\}$, et pour tout $i \in I$ soit $A_i = \{i, i+1, i+2, i+3\}$. Trouver $\bigcap_{i \in I} A_i$ and $\bigcup_{i \in I} A_i$.

Solution

Nous listons d'abord les éléments des ensembles A_i , pour $i \in I$:

$$A_1 = \{1, 2, 3, 4\}, \quad A_2 = \{2, 3, 4, 5\}, \quad A_3 = \{3, 4, 5, 6\}.$$

Alors

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 = \{1, 2, 3, 4\} \cap \{2, 3, 4, 5\} \cap \{3, 4, 5, 6\} = \{3, 4\},$$

et de même

$$\bigcup_{i \in I} A_i = \{1, 2, 3, 4\} \cup \{2, 3, 4, 5\} \cup \{3, 4, 5, 6\} = \{1, 2, 3, 4, 5, 6\}.$$

En fait, nous pouvons maintenant voir que la question posée dans cet exemple est exactement la même que celle de [l'exemple 2.3.4](#), mais avec une notation différente.

Exemple 2.3.8. Dans cet exemple, notre univers de discours sera l'ensemble S de tous les élèves. Soit $L(x, y)$ pour « x aime y » et $A(x, y)$ pour « x admire y ». Pour chaque élève s , soit L_s l'ensemble de tous les élèves que s aime. En d'autres termes, mots $L_s = \{t \in S \mid L(s, t)\}$. De même, soit $A_s = \{t \in S \mid A(s, t)\}$ = l'ensemble de tous les étudiants que s admire. Décrivez les ensembles suivants.

- 1. $\bigcap_{s \in S} L_s$.
- 2. $\bigcup_{s \in S} L_s$.
- 3. $\bigcup_{s \in S} L_s \setminus \bigcup_{s \in S} A_s$.
- 4. $\bigcup_{s \in S} (L_s \setminus A_s)$.
- 5. $(\bigcap_{s \in S} L_s) \cap (\bigcap_{s \in S} A_s)$.
- 6. $\bigcap_{s \in S} (L_s \cap A_s)$.
- 7. $\bigcup_{b \in B} L_b$, where $B = \bigcap_{s \in S} A_s$.

Solutions

Tout d'abord, notez qu'en général, $t \in L_s$ signifie la même chose que $L(s, t)$, et de même $t \in A_s$ signifie $A(s, t)$.

- 1. $\bigcap_{s \in S} L_s = \{t \mid \forall s \in S (t \in L_s)\} = \{t \in S \mid \forall s \in S L(s, t)\}$ = l'ensemble de tous les étudiants qui sont appréciés par tous les étudiants.

2. $\bigcup_{s \in S} L_s = \{t \mid \exists s \in S (t \in L_s)\} = \{t \in S \mid \exists s \in S L(s, t)\}$ = l'ensemble de tous les étudiants qui sont appréciés par au moins un étudiant.
3. Comme nous l'avons vu dans la solution 2, $\bigcup_{s \in S} L_s$ = l'ensemble des élèves appréciés par au moins un élève. De même, $\bigcup_{s \in S} A_s$ = l'ensemble de tous les élèves admirés par au moins un élève. Ainsi, $\bigcup_{s \in S} L_s \setminus \bigcup_{s \in S} A_s = \{t \mid t \in \bigcup_{s \in S} L_s \text{ et } t \notin \bigcup_{s \in S} A_s\}$ = l'ensemble de tous les étudiants qui sont appréciés par au moins un étudiant, mais qui ne sont admirés par aucun étudiant.
4. $\bigcup_{s \in S} (L_s \setminus A_s) = \{t \mid \exists s \in S (t \in L_s \setminus A_s)\} = \{t \in S \mid \exists s \in S (L(s, t) \wedge \neg A(s, t))\}$ = l'ensemble de tous les élèves t tels qu'un élève aime t , mais n'admire pas t . Notez que ceci est différent de l'ensemble de la partie 3. Pour qu'un élève t soit dans cet ensemble, il doit y avoir un élève qui aime t mais n'admire pas t , mais il pourrait y avoir d'autres élèves qui admirent t . Pour être dans l'ensemble de la partie 3, t ne doit être admiré par personne.
5. $\bigcap_{s \in S} L_s \cap (\bigcap_{s \in S} A_s) = \{t \mid t \in \bigcap_{s \in S} L_s \text{ and } t \in \bigcap_{s \in S} A_s\} = \{t \mid \forall s \in S (t \in L_s) \wedge \forall s \in S (t \in A_s)\} = \{t \in S \mid \forall s \in S L(s, t) \wedge \forall s \in S A(s, t)\}$ = l'ensemble de tous les étudiants qui sont aimés par tous les étudiants et également admirés par tous les étudiants.
6. $\bigcap_{s \in S} (L_s \cap A_s) = \{t \mid \forall s \in S (t \in L_s \cap A_s)\} = \{t \in S \mid \forall s \in S (L(s, t) \wedge A(s, t))\}$ = L'ensemble de tous les élèves appréciés et admirés par tous. Il s'agit du même ensemble que celui de la partie 5. En fait, on peut utiliser la loi de distribution de quantification universelle et la conjonction pour démontrer l'équivalence des tests d'élémentarité des deux ensembles.
7. $\bigcup_{b \in B} L_b = \{t \mid \exists b \in B (t \in L_b)\} = \{t \in S \mid \exists b (b \in B \wedge L(b, t))\}$. Mais B a été défini comme l'ensemble de tous les étudiants qui sont admirés par tous les étudiants, donc $b \in B$ signifie $b \in S \wedge \forall s \in S A(s, b)$. En insérant ceci, nous obtenons $\bigcup_{b \in B} L_b = \{t \in S \mid \exists b (b \in S \wedge \forall s \in S A(s, b) \wedge L(b, t))\}$ = l'ensemble de tous les étudiants qui sont appréciés par un étudiant qui est admiré par tous les étudiants.

Exercices

- *1. Analysez les formes logiques des affirmations suivantes. Vous pouvez utiliser les symboles \in , \notin , $=$, \neq , \wedge , \vee , \rightarrow , \leftrightarrow , \forall et \exists dans vos réponses, mais pas \subseteq , $\not\subseteq$, \mathcal{P} , \cap , \cup , \setminus , $\{\}$ ni \neg . (Vous devez donc écrire les définitions d'une notation de la théorie des ensembles et utiliser des équivalences pour supprimer toute occurrence de \neg .)
- (a) $\mathcal{F} \subseteq \mathcal{P}(A)$.

(b) $U_n \subseteq \{2n + 1 \mid n \in \mathbb{N}\}$.

(c) $\{n^2 + n + 1 \mid n \in \mathbb{N}\} \subseteq \{2n + 1 \mid n \in \mathbb{N}\}$.

(d) $\mathcal{P}(\bigcup_{i \in I} A_i) \not\subseteq \bigcup_{i \in I} \mathcal{P}(A_i)$.

2. Analysez les formes logiques des affirmations suivantes. Vous pouvez utiliser les symboles \in , \notin , $=$, \neq , \wedge , \vee , \rightarrow , \leftrightarrow , \forall et \exists dans vos réponses, mais pas \subseteq , $\not\subseteq$, \mathcal{P} , \cap , \cup , \setminus , $\{\}$ ni \neg . (Vous devez donc écrire les définitions d'une notation de la théorie des ensembles et utiliser des équivalences pour supprimer toute occurrence de \neg .)

(a) $x \in U \setminus F \cup G$.

(b) $\{x \in B \mid x \notin C\} \in \mathcal{P}(A)$.

(c) $x \in \bigcap_{i \in I} (A_i \cup B_i)$.

(d) $x \in (\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i)$.

3. Nous avons vu que $\mathcal{P}(\emptyset) = \{\emptyset\}$ et $\{\emptyset\} = \emptyset$. Qu'est-ce que $\mathcal{P}(\{\emptyset\})$?

*4. Supposons que $\mathcal{F} = \{\{\text{rouge, vert, bleu}\}, \{\text{orange, rouge, bleu}\}, \{\text{violet, rouge, vert, bleu}\}\}$. Trouvez $\cap \mathcal{F}$ et $\cup \mathcal{F}$.

5. Supposons que $\mathcal{F} = \{\{3, 7, 12\}, \{5, 7, 16\}, \{5, 12, 23\}\}$. Trouvez $\cap \mathcal{F}$ et $\cup \mathcal{F}$.

6. Soit $I = \{2, 3, 4, 5\}$, et pour chaque $i \in I$ soit $A_i = \{i, i+1, i-1, 2i\}$.

(a) Énumérez les éléments de tous les ensembles A_i , pour $i \in I$.

(b) Trouver $\bigcap_{i \in I} A_i$ and $\bigcup_{i \in I} A_i$.

7. Soit $P = \{\text{Jean-Sébastien Bach, Napoléon Bonaparte, Johann Wolfgang von Goethe, David Hume, Wolfgang Amadeus Mozart, Isaac Newton, George Washington}\}$ et soit $Y = \{1750, 1751, 1752, \dots, 1759\}$. Pour chaque $y \in Y$, soit $A_y = \{p \in P \mid \text{la personne } p \text{ était vivante à un moment donné de l'année } y\}$. Trouvez $\bigcup_{y \in Y} A_y$ et $\bigcap_{y \in Y} U_n$.

*8. Soit $I = \{2, 3\}$, et pour chaque $i \in I$ soit $A_i = \{i, 2i\}$ et $B_i = \{i, i+1\}$.

(a) Énumérez les éléments des ensembles A_i et B_i pour $i \in I$.

(b) Trouvez $\bigcap_{i \in I} (A_i \cup B_i)$ et $(\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i)$ sont-ils identiques ?

(c) Dans les parties (c) et (d) de l'exercice 2, vous avez analysé les énoncés $x \in \bigcap_{i \in I} (A_i \cup B_i)$ and $x \in (\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i)$. Que pouvez-vous conclure de votre réponse à la partie (b) quant à savoir si ces énoncés sont équivalents ou non ?

9. (a) Analyser les formes logiques des énoncés $x \in \bigcup_{i \in I} (A_i \setminus B_i)$, $x \in (\bigcup_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$, and $x \in (\bigcup_{i \in I} A_i) \setminus (\bigcap_{i \in I} B_i)$. Pensez-vous que l'une de ces affirmations est équivalente ?

(b) Soient I , A_i et B_i définis comme dans [l'exercice 8](#). Trouver $\bigcup_{i \in I} (A_i \setminus B_i)$,

$(\bigcup_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$, and $(\bigcup_{i \in I} A_i) \setminus (\bigcap_{i \in I} B_i)$. Pensez-vous maintenant que l'une des

affirmations de la partie (a) est équivalente ?

10. Donnez un exemple d'un ensemble d'indices I et de familles d'ensembles indexés $\{ A_i \mid i \in I \}$ et $\{ B_i \mid i \in I \}$ tels que $\bigcup_{i \in I} (A_i \cap B_i) \neq (\bigcup_{i \in I} A_i) \cap (\bigcup_{i \in I} B_i)$.

11. Démontrer que pour tout ensemble A et B , $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$, en montrant que les énoncés $x \in \mathcal{P}(A \cap B)$ et $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$ sont équivalents. (Voir [l'exemple 2.3.3.](#))

12. Donnez des exemples d'ensembles A et B pour lesquels $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

13. Vérifiez les identités suivantes en écrivant (à l'aide de symboles logiques) ce que signifie pour un objet x d'être un élément de chaque ensemble, puis en utilisant des équivalences logiques.

(un) $\bigcup_{i \in I} (A_i \cup B_i) = (\bigcup_{i \in I} A_i) \cup (\bigcup_{i \in I} B_i)$.

(b) $(\bigcap \mathcal{F}) \cap (\bigcap \mathcal{G}) = \bigcap (\mathcal{F} \cup \mathcal{G})$.

(c) $\bigcap_{i \in I} (A_i \setminus B_i) = (\bigcap_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$.

14. Parfois, chaque ensemble d'une famille indexée possède *deux* indices. Pour ce problème, on utilise les définitions suivantes : $I = \{1, 2\}, J = \{3, 4\}$. Pour chaque $i \in I$ et $j \in J$, soit $A_{i,j} = \{i, j, i+j\}$. Ainsi, par exemple, $A_{2,3} = \{2, 3, 5\}$.

- (a) Pour chaque $j \in J$, trouvons $B_j = \bigcup_{i \in I} A_{i,j} = A_{1,j} \cup A_{2,j}$, B_3 et B_4 .

- (b) Trouver $\bigcap_{j \in J} B_j$. (Notez qu'en remplaçant B_j par sa définition, nous pourrions dire que $\bigcap_{j \in J} B_j = \bigcap_{j \in J} (\bigcup_{i \in I} A_{i,j})$.)

- (c) Trouvez $\bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j})$. (Indice : vous pouvez procéder en deux étapes, correspondant aux parties (a) et (b).) Sont $\bigcap_{j \in J} (\bigcup_{i \in I} A_{i,j})$ et $\bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j})$ égaux ?

- (d) Analysez les formes logiques des énoncés $x \in \bigcap_{j \in J} (\bigcup_{i \in I} A_{i,j})$ et $x \in \bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j})$. Sont-elles équivalentes ?

15. (a) Montrez que si $\mathcal{F} = \emptyset$, alors l'affirmation $x \in \bigcup \mathcal{F}$ sera fausse quelle que soit la valeur de x . Il s'ensuit que $\bigcup \emptyset = \emptyset$.

- (b) Montrer que si $\mathcal{F} = \emptyset$, alors l'énoncé $x \in \bigcap \mathcal{F}$ sera vrai quelle que soit la valeur de x . Dans un contexte où l'univers de discours U est clairement défini, on pourrait donc dire que $\bigcap \emptyset = U$. Cependant, cela a pour conséquence regrettable que la notation $\bigcap \emptyset$ aura des significations différentes selon le contexte. De plus, lorsqu'ils travaillent avec des ensembles dont les éléments sont des ensembles, les mathématiciens n'utilisent souvent pas d'univers de discours du tout. (Pour plus d'informations, voir l'exercice suivant.) Pour ces raisons, certains mathématiciens considèrent que la notation $\bigcap \emptyset$ est dénuée de sens. Nous éviterons ce problème dans

ce livre en n'utilisant la notation $\cap \mathcal{F}$ que dans les contextes où nous sommes sûrs que $\mathcal{F} \neq \emptyset$.

16. Dans [la section 2.3](#), nous avons vu qu'un ensemble peut avoir d'autres ensembles comme éléments. Lorsqu'on étudie des ensembles dont les éléments sont des ensembles, il peut sembler plus naturel de considérer l'univers du discours comme l'ensemble de tous les ensembles. Cependant, comme nous le verrons dans ce problème, supposer l'existence d'un tel ensemble conduit à des contradictions.

Supposons que U soit l'ensemble de tous les ensembles. Notons qu'en particulier U est un ensemble, nous aurions donc $U \in U$. Ce n'est pas encore une contradiction ; bien que la plupart des ensembles ne soient pas des éléments d'eux-mêmes, peut-être que certains le sont. Mais cela suggère que les ensembles de l'univers U pourraient être divisés en deux catégories : les ensembles inhabituels qui, comme U lui-même, sont des éléments d'eux-mêmes, et les ensembles plus typiques qui ne le sont pas. Soit R l'ensemble des ensembles de la seconde catégorie. Autrement dit, $R = \{ A \in U \mid A \notin A \}$. Cela signifie que pour tout ensemble A dans l'univers U , A sera un élément de R ssi $A \notin A$. Autrement dit, nous avons $\forall A \in U (A \in R \leftrightarrow A \notin A)$.

- (a) Montrer que l'application de ce dernier fait à l'ensemble R lui-même (autrement dit, remplacer A par R) conduit à une contradiction. Cette contradiction, découverte par Bertrand Russell (1872–1970) en 1901, est connue sous le nom de *paradoxe de Russell*.
(b) Réfléchissez davantage au paradoxe de la partie (a). Que nous apprend-il sur les ensembles, selon vous ?

3

Preuves

3.1 Stratégies de preuve

Les mathématiciens sont des personnes sceptiques. Ils utilisent de nombreuses méthodes, dont l'expérimentation avec des exemples, les essais et erreurs et les conjectures, pour tenter de trouver des réponses aux questions mathématiques. Cependant, ils ne sont généralement pas convaincus de la justesse d'une réponse s'ils ne peuvent la prouver. Vous avez probablement déjà vu des démonstrations mathématiques (des exemples ont été présentés dans l'introduction), mais vous n'avez peut-être pas l'expérience de leur rédaction. Dans ce chapitre, vous découvrirez comment les démonstrations sont construites, afin de pouvoir commencer à écrire les vôtres.

Les épreuves ressemblent beaucoup aux puzzles. Il n'y a pas de règles pour les résoudre. La seule règle concerne le produit final : toutes les pièces doivent s'assembler et l'image doit être correcte. Il en va de même pour les épreuves.

Bien qu'il n'existe aucune règle pour résoudre un puzzle, certaines techniques sont plus efficaces que d'autres. Par exemple, on ne résout jamais un puzzle en remplissant une pièce *sur deux*, puis en revenant en arrière pour combler les trous ! Mais on ne le fait pas non plus en commençant par le haut et en remplissant les pièces dans l'ordre jusqu'en bas. On remplit probablement d'abord le bord, puis on assemble progressivement les autres pièces du puzzle et on détermine leur emplacement. Parfois, on essaie de placer les pièces au mauvais endroit, on se rend compte qu'elles ne s'emboîtent pas et on a l'impression de ne pas progresser. Et de temps en temps, on constate, avec satisfaction, comment deux gros morceaux s'assemblent et on a l'impression d'avoir soudainement beaucoup progressé. À mesure que les pièces du puzzle s'assemblent, une image émerge. On réalise soudain que la tache bleue que l'on a reconstituée est un lac, ou une partie du ciel. Mais ce n'est qu'une fois le puzzle terminé qu'on peut voir l'image dans son ensemble.

On pourrait dire la même chose du processus de démonstration. Et je pense qu'une autre similitude mérite d'être mentionnée : quand on termine un puzzle. Un puzzle, on ne le démonte pas tout de suite, n'est-ce pas ? On le laisse probablement dehors un jour ou deux pour l'admirer. On devrait faire pareil avec une épreuve. On a trouvé comment l'assembler soi-même, et une fois terminé, c'est joli, non ?

Dans ce chapitre, nous aborderons les techniques de démonstration les plus fréquemment utilisées par les mathématiciens et expliquerons comment les utiliser pour commencer à rédiger vos propres démonstrations. Comprendre ces techniques peut également vous aider à lire et à comprendre les démonstrations rédigées par d'autres. Malheureusement, les techniques présentées dans ce chapitre ne proposent pas de procédure étape par étape pour résoudre chaque problème de démonstration. En essayant de rédiger une démonstration, vous risquez de faire quelques faux pas avant de trouver la bonne méthode, et certaines démonstrations peuvent nécessiter une certaine ingéniosité ou perspicacité. Avec la pratique, vos compétences en démonstration devraient s'améliorer et vous serez capable de vous attaquer à des démonstrations de plus en plus complexes.

Les mathématiciens formulent généralement la réponse à une question mathématique sous la forme d'un *théorème* stipulant que si certaines hypothèses, appelées « *hypothèses* du théorème », sont vraies, alors une conclusion doit l'être également. Souvent, les hypothèses et la conclusion contiennent des variables libres ; dans ce cas, il est entendu que ces variables peuvent représenter n'importe quel élément du discours. L'attribution de valeurs particulières à ces variables est appelée une *instance* du théorème ; pour que le théorème soit correct, il faut que pour chaque instance du théorème qui rend les hypothèses vraies, la conclusion le soit également. S'il existe une instance où les hypothèses sont vraies mais la conclusion fausse, alors le théorème est incorrect. Une telle instance est appelée un *contre-exemple* du théorème.

Exemple 3.1.1. Considérons le théorème suivant :

Théorème. Supposer $x > 3$ et $y < 2$. Alors $x^2 - 2y > 5$.

Ce théorème est correct. (On vous demande de le démontrer dans [l'exercice 15.](#)) Les hypothèses du théorème sont $x > 3$ et $y < 2$, et la conclusion est $x^2 - 2y > 5$. À titre d'exemple du théorème, on pourrait remplacer x par 5 et y par 1. Clairement, avec ces valeurs des variables, les hypothèses $x > 3$ et $y < 2$ sont toutes deux vraies, donc le théorème nous dit que la conclusion $x^2 - 2y > 5$ doit aussi être vraie. En fait, en

remplaçant les valeurs de x et y , on trouve que $x^2 - 2y = 25 - 2 = 23$, et certainement $23 > 5$. Notez que ce calcul ne constitue pas une démonstration du théorème. Nous n'avons vérifié qu'une seule instance du théorème, et une démonstration devrait montrer que *toutes* les instances sont correctes.

Si nous abandonnons la deuxième hypothèse, nous obtenons un théorème incorrect :

Théorème incorrect. *Supposer $x > 3$. Alors $x^2 - 2y > 5$.*

On peut constater que ce théorème est incorrect en trouvant un contre-exemple. Supposons par exemple que $x = 4$ et $y = 6$. La seule hypothèse restante, $x > 3$, est alors vraie, mais $x^2 - 2y = 16 - 12 = 4$, donc la conclusion $x^2 - 2y > 5$ est fausse.

Si vous trouvez un contre-exemple à un théorème, vous pouvez être sûr que ce théorème est incorrect, mais la seule façon de savoir avec certitude qu'un théorème est correct est de le prouver. Une démonstration d'un théorème est simplement un argument déductif dont les prémisses sont les hypothèses du théorème et la conclusion est la conclusion du théorème. Tout au long de la démonstration, nous considérons les variables libres des hypothèses et de la conclusion du théorème comme représentant des éléments particuliers, mais non spécifiés, de l'univers du discours. Autrement dit, nous imaginons que nous raisonnons sur une instance du théorème, mais nous ne choisissons pas d'instance particulière ; le raisonnement de la démonstration doit s'appliquer à toutes les instances. Bien sûr, l'argument doit être valide, afin que nous puissions être sûrs que si les hypothèses du théorème sont vraies pour une instance, alors la conclusion le sera également pour cette instance.

La manière dont vous élaborez et rédigez la preuve d'un théorème dépend principalement de la forme logique de la conclusion. Souvent, elle dépend aussi de la forme logique des hypothèses. Les techniques de démonstration abordées dans ce chapitre vous indiqueront les stratégies de démonstration les plus susceptibles de fonctionner pour différentes formes d'hypothèses et de conclusions.

Les techniques de démonstration basées sur les formes logiques des hypothèses suggèrent généralement des moyens d'en tirer des inférences. Lorsque vous tirez une inférence des hypothèses, vous utilisez l'hypothèse de leur véracité pour justifier l'affirmation selon laquelle une autre affirmation est également vraie. Une fois qu'une affirmation est vraie, vous pouvez l'utiliser ultérieurement dans la démonstration, exactement comme s'il s'agissait d'une hypothèse. La règle la plus importante à retenir pour tirer de telles inférences est

peut-être la suivante : *ne jamais rien affirmer . jusqu'à ce que vous puissiez la justifier complètement* à l'aide des hypothèses ou des conclusions tirées de celles-ci plus tôt dans la démonstration. Votre devise devrait être : « Je ne ferai aucune affirmation avant son heure. » Suivre cette règle vous évitera de recourir à un raisonnement circulaire ou de tirer des conclusions hâtives et garantira que, si les hypothèses sont vraies, la conclusion doit l'être également. Et c'est là l'objectif principal de toute démonstration : garantir que la conclusion est vraie si les hypothèses le sont.

Pour vous assurer que vos affirmations sont adéquatement justifiées, vous devez être sceptique quant à chaque inférence de votre preuve. Si vous avez le moindre doute quant à la pertinence de la justification donnée à une affirmation, elle ne l'est pas. Après tout, si votre propre raisonnement ne *vous convainc même pas* , comment pouvez-vous espérer qu'il convainque qui que ce soit ?

Les techniques de correction basées sur la forme logique de la conclusion diffèrent souvent quelque peu de celles basées sur la forme des hypothèses. Elles suggèrent généralement des moyens de transformer le problème en un problème équivalent, mais plus facile à résoudre. L'idée de résoudre un problème en le transformant en un problème plus simple devrait vous être familière. Par exemple, ajouter le même nombre aux deux membres d'une équation transforme celle-ci en une équation équivalente, et l'équation résultante est parfois plus facile à résoudre que l'équation initiale. Les étudiants ayant étudié le calcul différentiel et intégral connaissent peut-être les techniques d'évaluation des intégrales, telles que la substitution ou l'intégration par parties, qui permettent de transformer un problème d'intégration complexe en un problème plus simple.

Les preuves écrites à l'aide de ces stratégies de transformation incluent souvent des étapes où l'on suppose, pour les besoins de l'argumentation, qu'une affirmation est vraie sans fournir de justification pour cette hypothèse. Il peut sembler à première vue qu'un tel raisonnement viole la règle selon laquelle les assertions doivent toujours être justifiées, mais ce n'est pas le cas, car *supposer* quelque chose n'est pas la même chose que l'*affirmer*. Affirmer une affirmation revient à prétendre qu'elle est vraie, et une telle affirmation n'est jamais acceptable dans une preuve, sauf si elle peut être justifiée. Cependant, l'objectif d'émettre une hypothèse dans une preuve n'est pas d'affirmer ce qui *est vrai*, mais plutôt de permettre de découvrir ce qui *serait vrai si l'hypothèse était correcte*. Il faut toujours garder à l'esprit que toute conclusion tirée d'une hypothèse peut se révéler fausse si celle-ci est incorrecte. Chaque fois que vous émettez une affirmation dans une preuve, il est important de savoir s'il s'agit d'une assertion ou d'une hypothèse.

Un exemple pourrait peut-être éclaircir ce point. Supposons qu'au cours d'une démonstration, vous décidiez de supposer qu'une affirmation, appelée P , est vraie, et que vous utilisiez cette hypothèse pour conclure qu'une autre affirmation, *appelée Q* , est vraie. Il serait erroné de qualifier cela de démonstration de la véracité de Q , car vous ne pouvez pas être sûr que votre hypothèse sur la véracité de P était correcte. Tout ce que vous pouvez conclure à ce stade est que *si Si P est vrai, alors vous pouvez être sûr que Q l'est aussi*. Autrement dit, vous savez que l'affirmation $P \rightarrow Q$ est vraie. Si la conclusion du théorème à démontrer est Q , alors la preuve est au mieux incomplète. En revanche, si la conclusion est $P \rightarrow Q$, alors la preuve est complète. Ceci nous amène à notre première stratégie de preuve.

Pour prouver une conclusion de la forme $P \rightarrow Q$:

Supposons que P soit vrai et prouvons ensuite Q .

Voici une autre façon d'envisager cette technique de preuve. Supposer que P est vraie revient à ajouter P à votre liste d'hypothèses. Bien que P n'ait peut-être pas été initialement l'une de vos hypothèses, Hypothèses : une fois posées, vous pouvez les utiliser exactement comme n'importe quelle autre hypothèse. Prouver Q signifie considérer Q comme votre conclusion et oublier la conclusion initiale. Ainsi, cette technique stipule que si la conclusion du théorème que vous essayez de prouver est de la forme $P \rightarrow Q$, vous pouvez *transformer le problème* en ajoutant P à votre liste d'hypothèses et en changeant votre conclusion de $P \rightarrow Q$ à Q . Cela vous donne un nouveau problème de preuve, peut-être plus facile à résoudre. Si vous parvenez à résoudre ce nouveau problème, vous aurez démontré que *si Si P est vrai, alors Q est également vrai*, résolvant ainsi le problème initial de prouver $P \rightarrow Q$. La manière dont vous résolvez ce nouveau problème sera désormais guidée par la forme logique de la nouvelle conclusion Q (qui pourrait elle-même être une déclaration complexe), et peut-être aussi par la forme logique de la nouvelle hypothèse P .

Notez que cette technique ne vous explique pas comment réaliser la preuve dans son intégralité ; elle vous propose simplement une étape, vous laissant avec un nouveau problème à résoudre pour terminer la preuve. Les preuves ne sont généralement pas écrites d'un coup, mais créées progressivement en appliquant successivement plusieurs techniques de preuve. L'utilisation de ces techniques conduit souvent à transformer le problème plusieurs fois. Pour aborder ce processus, il est utile de disposer d'un moyen de suivre les résultats de cette séquence de transformations. Nous introduisons donc la terminologie suivante. Nous appellerons les affirmations connues ou supposées vraies à un moment donné de la démonstration une *donnée*, et l'affirmation restant à prouver à ce stade l'*objectif*. Lorsque vous

commencez à développer une preuve, les données seront simplement les hypothèses du théorème à démontrer, mais elles pourront ultérieurement inclure d'autres affirmations déduites de ces hypothèses ou ajoutées comme nouvelles hypothèses suite à une transformation du problème. L'objectif sera initialement la conclusion du théorème, mais il pourra être modifié plusieurs fois au cours de l'élaboration d'une preuve.

Afin de garder à l'esprit que toutes nos stratégies de preuve s'appliquent non seulement au problème initial, mais aussi aux résultats de toute transformation du problème, nous parlerons désormais uniquement de données et d'objectifs, plutôt que d'hypothèses et de conclusions, lorsque nous aborderons les stratégies de démonstration. Par exemple, la stratégie énoncée précédemment devrait plutôt être qualifiée de stratégie de démonstration d'un *objectif* de la forme $P \rightarrow Q$, plutôt que de conclusion de cette forme. Même si la conclusion du théorème démontré n'est pas une proposition conditionnelle, si vous transformez le problème de telle sorte qu'une proposition conditionnelle devienne l'objectif, vous pouvez appliquer cette stratégie comme étape suivante de la démonstration.

Exemple 3.1.2. Supposons que a et b soient des nombres réels. Démontrer que si $0 < a < b$ alors $a^2 < b^2$.

Travail à partir de zéro

On nous pose comme hypothèse que a et b sont des nombres réels. Notre conclusion est de la forme $P \rightarrow Q$, où P est l'énoncé $0 < a < b$ et Q est l'énoncé $a^2 < b^2$. Nous commençons donc avec ces énoncés comme donnés et objectif :

<i>Givens</i>	<i>Goal</i>
a and b are real numbers	$(0 < a < b) \rightarrow (a^2 < b^2)$

Selon notre technique de preuve, nous devrions supposer que $0 < a < b$ et essayer d'utiliser cette hypothèse pour prouver que $a^2 < b^2$. En d'autres termes, nous transformons le problème en ajoutant $0 < a < b$ à la liste des données et en faisant $a^2 < b^2$ notre objectif :

<i>Givens</i>	<i>Goal</i>
a and b are real numbers $0 < a < b$	$a^2 < b^2$

Comparaison des inégalités $a < b$ et $a^2 < b^2$ suggère que multiplier les deux côtés de l'inégalité donnée $a < b$ par a ou b pourrait nous rapprocher de notre objectif. Puisque a et b sont positifs, il n'est pas nécessaire d'inverser le sens de l'inégalité. Multiplier $a < b$ par a nous

donne $a^2 < ab$, et en le multipliant par b nous donne $ab < b^2$. Ainsi $a^2 < ab < b^2$, donc $a^2 < b^2$.

Solution

Théorème. *Supposer un et b sont des nombres réels. Si $0 < a < b$ alors $a^2 < b^2$.*

Preuve. Supposons que $0 < a < b$. En multipliant l'inégalité $a < b$ par le nombre positif a , nous pouvons conclure que $a^2 < ab$, et de même en multipliant par b on obtient $ab < b^2$. Par conséquent $a^2 < ab < b^2$, donc $a^2 < b^2$, comme requis. Ainsi, si $0 < a < b$ alors $a^2 < b^2$.

□

Comme le montre l'exemple précédent, il existe une différence entre le raisonnement utilisé pour établir une preuve et les étapes décrites dans la version finale. En particulier, bien que nous parlions souvent de données et d'objectifs lors de la conception d'une preuve, la version finale n'y fera généralement pas référence. Tout au long de ce chapitre, et parfois dans les chapitres suivants, nous ferons précéder nos preuves du travail préparatoire nécessaire à leur élaboration, mais ceci vise simplement à vous aider à comprendre comment les preuves sont construites. Lorsque les mathématiciens écrivent des preuves, ils se contentent généralement d'écrire les étapes nécessaires à la justification de leurs conclusions, sans aucune explication. Comment ils les ont conçues. Certaines de ces étapes seront des phrases indiquant que le problème a été transformé (généralement selon une stratégie de preuve basée sur la forme logique de l'objectif) ; d'autres seront des affirmations justifiées par des inférences à partir des données (souvent en utilisant une stratégie de preuve basée sur la forme logique d'une donnée). Cependant, il n'y aura généralement aucune explication sur la façon dont le mathématicien a pensé ces transformations et inférences. Par exemple, la preuve de [l'exemple 3.1.2](#) commence par la phrase « Supposons que $0 < a < b$ », indiquant que le problème a été transformé selon notre stratégie, puis se poursuit par une séquence d'inférences menant à la conclusion que $a^2 < b^2$. Aucune autre explication n'était nécessaire pour justifier la conclusion finale, dans la dernière phrase, que si $0 < a < b$ alors $a^2 < b^2$.

Bien que ce manque d'explication rende parfois les preuves difficiles à lire, il sert à garder deux objectifs distincts séparés : *expliquer votre Processus de pensée et justification des conclusions*. La première relève de la psychologie ; la seconde des mathématiques. L'objectif principal

d'une preuve est de justifier l'affirmation selon laquelle la conclusion découle des hypothèses, et aucune explication des processus de pensée ne saurait se substituer à une justification adéquate de cette affirmation. Limiter au minimum la discussion des processus de pensée dans une preuve permet de clarifier cette distinction. Il arrive parfois, dans une preuve très complexe, qu'un mathématicien aborde la stratégie de la preuve afin d'en faciliter la lecture. Cependant, il appartient généralement au lecteur de la comprendre par lui-même. Ne vous inquiétez pas si vous ne comprenez pas immédiatement la stratégie derrière une preuve que vous lisez. Essayez simplement de suivre les justifications des étapes, et la stratégie finira par devenir claire. Dans le cas contraire, une relecture de la preuve pourrait vous aider.

Afin de bien distinguer la preuve de la stratégie qui la sous-tend, à l'avenir, lorsque nous présenterons une stratégie de preuve, nous décrirons souvent à la fois le travail préliminaire nécessaire pour élaborer la preuve et la forme que devrait prendre la rédaction finale de la preuve. Par exemple, voici une reformulation de la stratégie de preuve évoquée précédemment, sous la forme que nous utiliserons désormais pour présenter les stratégies de preuve.

Pour prouver un but de la forme $P \rightarrow Q$:

Supposons que P soit vrai et prouvons ensuite Q .

Travail à partir de zéro

Avant d'utiliser la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$P \rightarrow Q$
—	

Après avoir utilisé la stratégie :

<i>Givens</i>	<i>Goal</i>
—	Q
—	
P	

Forme de l'épreuve finale :

Supposons que P .

[La preuve de Q va ici.]

Par conséquent $P \rightarrow Q$.

Notez que la forme suggérée pour la preuve finale indique le déroulement du début et de la fin de la preuve, mais des étapes supplémentaires devront être ajoutées au milieu. La liste des données et des objectifs, sous la rubrique « Après l'utilisation de la stratégie », indique ce qui est connu ou supposé et ce qui doit être prouvé pour

combler cette lacune dans la preuve. Nombre de nos stratégies de preuve vous indiqueront comment rédiger le début ou la fin de votre preuve, laissant une lacune à combler par un raisonnement plus approfondi.

Il existe une deuxième méthode, parfois utilisée pour prouver des objectifs de la forme $P \rightarrow Q$. Puisque toute condition $P \rightarrow Q$ est équivalente à sa contraposée $\neg Q \rightarrow \neg P$, on peut prouver $P \rightarrow Q$ en prouvant $\neg Q \rightarrow \neg P$, en utilisant la stratégie décrite précédemment. Autrement dit :

Pour prouver un but de la forme $P \rightarrow Q$:

Supposons que Q soit faux et prouvons que P est faux.

Travail à partir de zéro

Avant d'utiliser la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$P \rightarrow Q$
—	

Après avoir utilisé la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$\neg P$
—	
$\neg Q$	

Forme de l'épreuve finale :

Supposons que Q soit faux.

[La preuve de $\neg P$ va ici.]

Par conséquent $P \rightarrow Q$.

Exemple 3.1.3. Supposons que a , b et c soient des nombres réels et que $a > b$. Démontrer que si $ac \leq bc$ alors $c \leq 0$.

Travail à partir de zéro

<i>Givens</i>	<i>Goal</i>
a, b , and c are real numbers	$(ac \leq bc) \rightarrow (c \leq 0)$
$a > b$	

La contraposée du but est $\neg(c \leq 0) \rightarrow \neg(ac \leq bc)$, ou en d'autres termes $(c > 0) \rightarrow (ac > bc)$, nous pouvons donc le prouver en ajoutant $c > 0$ à la liste des données et en faisant $ac > bc$ notre nouveau but :

<i>Givens</i>	<i>Goal</i>
a, b , and c are real numbers	
$a > b$	
$c > 0$	$ac > bc$

Nous pouvons maintenant écrire les première et dernière phrases de la preuve. Selon la stratégie, la preuve finale devrait se présenter sous la

forme suivante :

Supposons que $c > 0$.

[La preuve de $ac > bc$ va ici.]

Par conséquent, si $ac \leq bc$ alors $c \leq 0$.

En utilisant la nouvelle donnée $c > 0$, nous voyons que l'objectif $ac > bc$ découle immédiatement de la donnée $a > b$ en multipliant les deux côtés par le nombre positif c . L'insertion de cette étape entre la première et la dernière phrase complète la preuve.

Solution

Théorème. Supposer un, groupe c sont des nombres réels et $a > b$. Si $ac \leq bc$ alors $c \leq 0$.

Preuve. Nous allons démontrer la contraposée. Supposons que $c > 0$. On peut alors multiplier les deux côtés de l'inégalité donnée $a > b$ par c et conclure que $ac > bc$. Par conséquent, si $ac \leq bc$ alors $c \leq 0$. □

Notez que, bien que nous ayons utilisé librement les symboles logiques dans le travail préliminaire, nous ne les avons pas utilisés dans la version finale de la démonstration. Bien qu'il ne soit pas incorrect d'utiliser des symboles logiques dans une démonstration, les mathématiciens cherchent généralement à l'éviter. L'utilisation de la notation et des règles logiques peut être très utile pour déterminer la stratégie d'une démonstration, mais dans la version finale, il est conseillé de s'en tenir autant que possible à un langage courant.

Vous vous demandez peut-être comment nous avons su, dans [l'exemple 3.1.3](#), qu'il fallait utiliser la deuxième méthode pour prouver un objectif de la forme $P \rightarrow Q$ plutôt que la première. La réponse est simple : nous avons essayé les deux méthodes, et la seconde a fonctionné. Lorsqu'il existe plusieurs stratégies pour prouver un objectif d'une forme particulière, il peut être nécessaire d'en essayer plusieurs avant d'en trouver une qui fonctionne. Avec la pratique, vous deviendrez plus apte à deviner quelle stratégie est la plus susceptible de fonctionner pour une preuve donnée.

Notez que dans chacun des exemples donnés, notre stratégie consistait à modifier nos données et notre objectif afin de simplifier le problème. Le début et la fin de la preuve, fournis dans l'énoncé de la technique de preuve, servent à informer le lecteur de la preuve que ces modifications ont été apportées et que la solution à ce problème révisé résout le problème initial. Le reste de la preuve contient la solution à ce problème révisé, plus simple.

La plupart des autres techniques de preuve présentées dans ce chapitre suggèrent également de réviser vos données et votre objectif. Ces révisions donnent lieu à un nouveau problème de preuve, et dans tous les cas, elles ont été conçues de manière à ce que la solution de ce nouveau problème, combinée à des phrases initiales ou finales expliquant ces révisions, résolve également le problème initial. Ainsi, chaque fois que vous utilisez l'une de ces stratégies, vous pouvez écrire une ou deux phrases au début ou à la fin de la preuve, puis oublier le problème initial et vous concentrer sur le nouveau problème, ce qui sera généralement plus facile. Vous parviendrez souvent à établir une preuve en utilisant les techniques présentées dans ce chapitre pour réviser vos données et votre objectif à plusieurs reprises, ce qui rendra le problème restant de plus en plus facile jusqu'à ce qu'il devienne évident que l'objectif découle des données.

Exercices

- *1. Considérons le théorème suivant. (Ce théorème a été démontré dans l'introduction.)

Théorème. *Supposer n est un entier supérieur à 1 et n n'est pas premier. Alors $2^n - 1$ n'est pas premier .*

- (a) Identifiez les hypothèses et la conclusion du théorème. Les hypothèses sont-elles vraies lorsque $n = 6$? Que dit le théorème dans ce cas ? Est-il correct ?
 - (b) Que pouvez-vous conclure du théorème dans le cas $n = 15$? Vérifiez directement que cette conclusion est correcte.
 - (c) Que pouvez-vous conclure du théorème dans le cas $n = 11$?
2. Considérez le théorème suivant. (Ce théorème est correct, mais nous ne vous demanderons pas de le prouver ici.)

Théorème. *Supposons que $b^2 > 4ac$. Alors l'équation quadratique $ax^2 + bx + c = 0$ a exactement deux solutions réelles .*

- (a) Identifiez les hypothèses et la conclusion du théorème.
- (b) Pour donner un exemple du théorème, vous devez spécifier des valeurs pour a , b et c , mais pas x . Pourquoi ?
- (c) Que peut-on conclure du théorème dans le cas où $a = 2$, $b = -5$, $c = 3$? Vérifiez directement que cette conclusion est correcte.
- (d) Que pouvez-vous conclure du théorème dans le cas $a = 2$, $b = 4$, $c = 3$?

3. Considérez le théorème incorrect suivant :

Théorème incorrect. Supposer n est un nombre naturel supérieur à 2, et n n'est pas un nombre premier. Alors $2n + 13$ n'est pas un nombre premier.

Quelles sont les hypothèses et la conclusion de ce théorème ? Démontrer que le théorème est incorrect en trouvant un contre-exemple.

- *4. Complétez la preuve alternative suivante du théorème de [l'exemple 3.1.2](#).

Preuve. Supposons que $0 < a < b$. Alors $b - a > 0$.

[Remplissez une preuve de $b^2 - a^2 > 0$ ici.]

Puisque $b^2 - a^2 > 0$, il s'ensuit qu'un $a^2 < b^2$. Par conséquent, si $0 < a < b$ alors $a^2 < b^2$.

□

5. Supposons que a et b soient des nombres réels. Démontrer que si $a < b < 0$ alors $a^2 > b^2$.
6. Supposons que a et b soient des nombres réels. Démontrer que si $0 < a < b$ alors $1/b < 1/a$.
7. Supposons que a soit un nombre réel. Démontrer que si $a^3 > un$ puis $un^5 > a$. (Indice : une approche consiste à commencer par compléter l'équation suivante : $a^5 - a = (a^3 - a) \cdot ?$.)
- *8. Supposons que $A \setminus B \subseteq C \cap D$ et $x \in A$. Démontrer que si $x \notin D$ alors $x \in B$.
9. Supposons que $A \cap B \subseteq C \setminus D$. Démontrer que si $x \in A$, alors si $x \in D$ alors $x \notin B$.
10. Supposons que a et b soient des nombres réels. Démontrer que si $a < b$ alors $(a + b)/2 < b$.
11. Supposons que x soit un nombre réel et que $x \neq 0$. Démontrer que si $\sqrt[3]{x+5}/(x^2+6) = 1/x$ alors $x \neq 8$.
12. Supposons que a, b, c et d soient des nombres réels, $0 < a < b$ et $d > 0$. Démontrer que si $ac \geq bd$ alors $c > d$.
13. Supposons que x et y soient des nombres réels et que $3x + 2y \leq 5$. Démontrer que si $x > 1$ alors $y < 1$.
14. Supposons que x et y soient des nombres réels. Démontrer que si $x^2 + y = -3$ et $2x - y = 2$, alors $x = -1$.
15. Démontrer le premier théorème de [l'exemple 3.1.1](#). (Indice : il pourrait être utile d'appliquer le théorème de [l'exemple 3.1.2](#).)
16. Considérez le théorème suivant.

Théorème. Supposer x est un nombre réel et $x \neq 4$. Si $(2x - 5)/(x - 4) = 3$ alors $x = 7$.

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve. Supposons que $x = 7$. Alors $(2x - 5)/(x - 4) = (2(7) - 5)/(7 - 4) = 9/3 = 3$. Par conséquent, si $(2x - 5)/(x - 4) = 3$ alors $x = 7$. \square

(b) Donnez une preuve correcte du théorème.

17. Considérez le théorème incorrect suivant :

Théorème incorrect. Supposons que x et y sont des nombres réels et $x \neq 3$. Si $x^2y = 9y$ alors $y = 0$.

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve. Supposons que $x^2y = 9y$. Alors $(x^2 - 9)y = 0$. Puisque $x \neq 3$, $x^2 \neq 9$, donc $x^2 - 9 = 0$. Par conséquent, nous pouvons diviser les deux côtés de l'équation $(x^2 - 9)y = 0$ par $x^2 - 9$, ce qui conduit à la conclusion que $y = 0$. Ainsi, si $x^2y = 9y$ alors $y = 0$. \square

(b) Montrez que le théorème est incorrect en trouvant un contre-exemple.

3.2 Preuves impliquant des négations et des conditionnels

Nous nous tournons maintenant vers les preuves dont le but est de la forme $\neg P$. Il est généralement plus facile de prouver une affirmation positive qu'une affirmation négative ; il est donc souvent utile de réexprimer un but de la forme $\neg P$ avant de le prouver. Au lieu d'essayer de prouver Si vous cherchez un objectif qui énonce ce qui *ne devrait pas* être vrai, essayez de le reformuler en un objectif qui énonce ce qui *devrait* être vrai. Heureusement, nous avons déjà étudié plusieurs équivalences qui faciliteront cette reformulation. Ainsi, notre première stratégie pour prouver les affirmations négatives est la suivante :

Pour prouver un but de la forme $\neg P$:

Si possible, réexprimez l'objectif sous une autre forme, puis utilisez l'une des stratégies de preuve pour cette autre forme d'objectif.

Exemple 3.2.1. Supposons que $A \cap C \subseteq B$ et $a \in C$. Démontrer que $a \notin A \setminus B$.

Travail à partir de zéro

<i>Givens</i>	<i>Goal</i>
$A \cap C \subseteq B$	
$a \in C$	$a \notin A \setminus B$

Pour prouver l'objectif, nous devons montrer qu'il ne peut pas être le cas *qu'un* $\in A$ et $a \notin B$. Puisqu'il s'agit d'un objectif négatif, nous essayons de le reformuler sous forme d'énoncé positif :

$$\begin{aligned} a \notin A \setminus B &\text{ is equivalent to } \neg(a \in A \wedge a \notin B) && (\text{definition of } A \setminus B), \\ &\text{which is equivalent to } a \notin A \vee a \in B && (\text{De Morgan's law}), \\ &\text{which is equivalent to } a \in A \rightarrow a \in B && (\text{conditional law}). \end{aligned}$$

Réécrire l'objectif de cette manière nous donne :

<i>Givens</i>	<i>Goal</i>
$A \cap C \subseteq B$	
$a \in C$	$a \in A \rightarrow a \in B$

Nous prouvons maintenant l'objectif sous cette nouvelle forme, en utilisant la première stratégie de [la section 3.1](#). Ainsi, nous ajoutons *un* $\in B$ à notre liste de données et faisons *un* $\in B$ notre objectif :

<i>Givens</i>	<i>Goal</i>
$A \cap C \subseteq B$	
$a \in C$	$a \in B$
$a \in A$	

La preuve est désormais simple : à partir des données $a \in A$ et $un \in C$ nous pouvons conclure qu' $un \in A \cap C$, et alors, puisque $A \cap C \subseteq B$, il s'ensuit que $a \in B$.

Solution

Théorème. Supposer $A \cap C \subseteq B$ et $un \in C$. Alors $un \notin A \setminus B$.

Preuve. Supposons qu' $un \in A$. Puis depuis $un \in C$, $un \in A \cap C$. Mais alors puisque $A \cap C \subseteq B$ il s'ensuit que $a \in B$. Ainsi, il ne peut pas être le cas que a soit un élément de A mais pas de B , donc $a \notin A \setminus B$.

□

Parfois, un objectif de la forme $\neg P$ ne peut être réexprimé sous forme d'énoncé positif, et cette stratégie est donc inapplicable. Dans ce cas, il est généralement préférable d'effectuer une *preuve par contradiction*. Commencez par supposer que P est vrai et essayez d'utiliser cette hypothèse pour prouver quelque chose que vous savez être faux. Cela se fait souvent en prouvant une affirmation qui contredit l'une des données. Puisque vous savez que l'affirmation que vous avez prouvée est fausse, l'hypothèse selon laquelle P était vrai devait être incorrecte. La seule possibilité restante est alors que P soit faux.

Pour prouver un but de la forme $\neg P$:

Supposons que P soit vrai et cherchons une contradiction. Une fois cette contradiction trouvée, nous pouvons conclure que P doit être faux.

Travail à partir de zéro

Avant d'utiliser la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$\neg P$
—	

Après avoir utilisé la stratégie :

<i>Givens</i>	<i>Goal</i>
—	Contradiction
—	
P	

Forme de l'épreuve finale :

Supposons que P soit vrai.

[La preuve de contradiction va ici.]

Ainsi, P est faux.

Exemple 3.2.2. Démontrer que si $x^2 + y = 13$ et $y \neq 4$, alors $x \neq 3$.

Travail à partir de zéro

L'objectif est une instruction conditionnelle, donc selon la première stratégie de preuve de [la section 3.1](#), nous pouvons traiter l'antécédent comme donné et faire du conséquent notre nouvel objectif :

<i>Givens</i>	<i>Goal</i>
$x^2 + y = 13$	
$y \neq 4$	$x \neq 3$

Cette stratégie de preuve suggère également la forme que devrait prendre la preuve finale. Selon cette stratégie, la preuve devrait ressembler à ceci :

Supposons que $x^2 + y = 13$ et $y \neq 4$.

[La preuve que $x \neq 3$ va ici.]

Ainsi, si $x^2 + y = 13$ et $y \neq 4$ alors $x \neq 3$.

Autrement dit, les première et dernière phrases de la preuve finale ont déjà été écrites, et le problème restant à résoudre est de compléter la preuve de $x \neq 3$ entre ces deux phrases. La liste des données et des objectifs résume ce que nous savons et ce que nous devons prouver pour résoudre ce problème.

L'objectif $x \neq 3$ signifie $\neg(x = 3)$, mais comme $x = 3$ ne contient aucun connecteur logique, aucune des équivalences connues ne peut être utilisée pour réexprimer cet objectif sous une forme positive. Nous tentons donc une preuve par contradiction et transformons le problème comme suit :

<i>Givens</i>	<i>Goal</i>
$x^2 + y = 13$	
$y \neq 4$	Contradiction
$x = 3$	

Une fois de plus, la stratégie de preuve qui a suggéré cette transformation nous indique également comment compléter quelques phrases supplémentaires de la preuve finale. Comme indiqué précédemment, ces phrases se situent entre la première et la dernière phrase de la preuve, écrites auparavant.

Supposons que $x^2 + y = 13$ et $y \neq 4$.

Supposons que $x \neq 3$.

[La preuve de contradiction va ici.]

Par conséquent $x \neq 3$.

Ainsi, si $x^2 + y = 13$ et $y \neq 4$ alors $x \neq 3$.

L'indentation dans ce plan de démonstration ne fera pas partie de la démonstration finale. Elle vise à clarifier la structure sous-jacente de la démonstration. Les première et dernière lignes sont jointes et indiquent que nous démontrons une démonstration conditionnelle. Énoncé en supposant l'antécédent et en prouvant le conséquent. Entre

ces lignes se trouve une preuve du conséquent, $x \neq 3$, que nous avons séparée des première et dernière lignes par un retrait. Cette preuve interne a la forme d'une preuve par contradiction, comme l'indiquent ses première et dernière lignes. Entre ces lignes, il nous reste à compléter une preuve par contradiction.

À ce stade, nous n'avons pas d'énoncé particulier comme objectif ; toute conclusion impossible fera l'affaire. Il nous faut donc examiner de plus près les données pour voir si certaines d'entre elles se contredisent. Dans ce cas, la première et la troisième ensemble impliquent que $y = 4$, ce qui contredit la seconde.

Solution

Théorème. *Si $x^2 + y = 13$ et $y \neq 4$ alors $x \neq 3$.*

Preuve. Supposons que $x^2 + y = 13$ et $y \neq 4$. Supposons que $x = 3$. En substituant cela dans l'équation $x^2 + y = 13$, nous obtenons $9 + y = 13$, donc $y = 4$. Mais cela contredit le fait que $y \neq 4$. Par conséquent $x \neq 3$. Ainsi, si $x^2 + y = 13$ et $y \neq 4$ alors $x \neq 3$.

□

Vous vous demandez peut-être à ce stade pourquoi nous étions fondés à conclure, face à une contradiction dans la preuve, que $x \neq 3$. Après tout, la deuxième liste de données de notre travail préliminaire en contenait trois. Comment pouvions-nous être sûrs, face à une contradiction, que le coupable était la troisième donnée, $x = 3$? Pour répondre à cette question, revenons à la première analyse des données et des objectifs de cet exemple. Selon cette analyse, il y avait deux données, $x^2 + y = 13$ et $y \neq 4$, desquelles nous devions déduire l'objectif $x \neq 3$. Ces données ont été introduites comme hypothèses dans la première phrase de la preuve. Notre preuve que $x \neq 3$ a été réalisée dans un contexte où ces hypothèses étaient en vigueur, comme l'indique l'indentation dans le plan de la preuve de notre travail préliminaire. Ainsi, il nous suffisait de démontrer que $x \neq 3$ *en supposant que* $x^2 + y = 13$ *et* $y \neq 4$. Lorsque nous avons rencontré une contradiction, nous n'avions pas besoin de déterminer laquelle des trois affirmations de la deuxième liste de données était fausse. Nous étions tout à fait fondés à conclure que *si* aucune des deux premières n'était en cause, alors c'était la troisième, et c'était tout ce qui était nécessaire pourachever la preuve.

Prouver un objectif par contradiction présente l'avantage de permettre de supposer que la conclusion est fausse, ce qui fournit une autre donnée de travail. Cependant, cela présente l'inconvénient de

laisser un objectif assez vague : produire une contradiction en prouvant quelque chose que l'on sait faux. Puisque toutes les stratégies de preuve présentées jusqu'à présent reposent sur l'analyse de la forme logique de l'objectif, il semble qu'aucune d'entre elles ne vous aidera à... Atteindre l'objectif de produire une contradiction. Dans la démonstration précédente, nous avons dû examiner nos données plus en détail pour trouver une contradiction. Dans ce cas, nous y sommes parvenus en prouvant que $y = 4$, ce qui contredit la donnée $y \neq 4$. Ceci illustre un schéma fréquent dans les démonstrations par contradiction : si l'une des données est de la forme $\neg P$, alors on peut produire une contradiction en prouvant P . Il s'agit de notre première stratégie basée sur la forme logique d'une *donnée*.

Pour utiliser une donnée de la forme $\neg P$:

Si vous effectuez une preuve par contradiction, essayez de faire *de P* votre objectif. Si vous pouvez prouver P , alors la preuve sera complète, car P contredit le $\neg P$ donné.

Travail à partir de zéro

Avant d'utiliser la stratégie :

<i>Givens</i>	<i>Goal</i>
$\neg P$	
—	
—	

Après avoir utilisé la stratégie :

<i>Givens</i>	<i>Goal</i>
$\neg P$	P
—	
—	

Forme de l'épreuve finale :

[La preuve de P va ici.]

Puisque nous connaissons déjà $\neg P$, c'est une contradiction.

Bien que nous ayons recommandé la preuve par contradiction pour prouver des buts de la forme $\neg P$, elle peut être utilisée pour n'importe quel but. Il est généralement préférable d'essayer d'abord les autres stratégies si l'une d'elles s'applique ; mais en cas de blocage, vous pouvez essayer la preuve par contradiction pour n'importe quelle preuve.

L'exemple suivant illustre cela, ainsi qu'une autre règle importante de la démonstration : dans de nombreux cas, la forme logique d'un énoncé peut être déterminée en *écrivant la définition* d'un mot ou d'un symbole mathématique qui y apparaît. C'est pourquoi il est essentiel de

connaître précisément les définitions de tous les termes mathématiques lors de la rédaction d'une démonstration.

Exemple 3.2.3. Supposons que A , B et C soient des ensembles, $A \setminus B \subseteq C$ et x soit quelconque. Démontrer que si $x \in A \setminus C$ puis $x \in B$.

Travail à partir de zéro

On nous donne que $A \setminus B \subseteq C$, et notre objectif est $x \in A \setminus C \rightarrow x \in B$. Parce que l'objectif est une instruction conditionnelle, notre première étape consiste à transformer le problème en ajoutant $x \in A \setminus C$ comme une seconde donnée et faisant $x \in B$ notre objectif :

<i>Givens</i>	<i>Goal</i>
$A \setminus B \subseteq C$	
$x \in A \setminus C$	$x \in B$

La forme de l'épreuve finale sera donc la suivante :

Supposons que $x \in Un \setminus C$.

[Preuve de $x \in B$ va ici.]

Ainsi, si $x \in A \setminus C$ puis $x \in B$.

Le but $x \in B$ ne contient aucun connecteur logique ; aucune des techniques étudiées jusqu'à présent ne s'applique donc, et la raison pour laquelle le but découle des données n'est pas évidente. Faute d'autre solution, nous tentons une preuve par contradiction :

<i>Givens</i>	<i>Goal</i>
$A \setminus B \subseteq C$	
$x \in A \setminus C$	Contradiction
$x \notin B$	

Comme précédemment, cette transformation du problème nous permet également de compléter quelques phrases supplémentaires de la preuve :

Supposons que $x \in Un \setminus C$.

Supposons que $x \notin B$.

[La preuve de contradiction va ici.]

Par conséquent $x \in B$.

Ainsi, si $x \in A \setminus C$ puis $x \in B$.

Puisque nous faisons une preuve par contradiction et que notre dernière donnée est maintenant une déclaration niée, nous pourrions essayer d'utiliser notre stratégie pour utiliser des données de la forme $\neg P$. Malheureusement, cette stratégie suggère de faire $x \in B$ notre objectif, qui nous ramène simplement au point de départ. Nous devons examiner les autres données pour tenter de trouver la contradiction.

Dans ce cas, l'écriture de la définition de la seconde donnée est la clé de la preuve, car cette définition contient également une négation. Par définition, $x \in A \setminus C$ signifie $x \in A$ et $x \notin C$. En remplaçant cette donnée par sa définition, on obtient :

<i>Givens</i>	<i>Goal</i>
$A \setminus B \subseteq C$	
$x \in A$	
$x \notin C$	
$x \notin B$	Contradiction

Maintenant, la troisième donnée a également la forme $\neg P$, où P est l'énoncé $x \in C$, nous pouvons donc appliquer la stratégie d'utilisation des données de la forme $\neg P$ et faire $x \in C$ notre objectif. Montrant que $x \in C$ compléterait la preuve car il contredirait le $x \notin C$ donné.

<i>Givens</i>	<i>Goal</i>
$A \setminus B \subseteq C$	
$x \in A$	
$x \notin C$	
$x \notin B$	$x \in C$

Encore une fois, nous pouvons ajouter un peu plus à la preuve que nous écrivons progressivement en complétant le fait que nous prévoyons de dériver notre contradiction en prouvant $x \in C$. Nous ajoutons également la définition de $x \in A \setminus C$ à la preuve, en l'insérant dans ce qui semble être l'endroit le plus logique, juste après avoir déclaré que $x \in A \setminus C$:

Supposons que $x \in A \setminus C$. Cela signifie que $x \in A$ et $x \notin C$.

Supposons que $x \notin B$.

[Preuve de $x \in C$ va ici.]

Cela contredit le fait que $x \notin C$.

Par conséquent $x \in B$.

Ainsi, si $x \in A \setminus C$ puis $x \in B$.

Nous avons enfin atteint un point où l'objectif découle facilement des données. De $x \in A$ et $x \notin B$ nous concluons que $x \in A \setminus B$. Puisque $A \setminus B \subseteq C$, il s'ensuit que $x \in C$.

Solution

Théorème. Supposer UN, Groupe C sont des ensembles, $A \setminus B \subseteq C$, et x est-ce que quelque chose à tous. Si $x \in A \setminus C$ puis $x \in B$.

Preuve. Supposons que $x \in A \setminus C$. Cela signifie que $x \in A$ et $x \notin C$. Supposons que $x \notin B$. Alors $x \in A \setminus B$, donc puisque $A \setminus B \subseteq C$, $x \in C$. Mais cela contredit le fait que $x \notin C$. Par conséquent $x \in B$. Ainsi, si $x \in A \setminus C$ puis $x \in B$.

□

La stratégie que nous avons recommandée pour utiliser des données de la forme $\neg P$ ne s'applique qu'aux démonstrations par contradiction. Pour les autres types de démonstrations, la stratégie suivante peut être utilisée. Cette stratégie repose sur le fait que les données de la forme $\neg P$, comme les buts de cette forme, peuvent être plus faciles à exploiter si elles sont exprimées sous forme d'énoncés positifs.

Pour utiliser une donnée de la forme $\neg P$:

Si possible, réexprimez cette information sous une autre forme.

Nous avons discuté des stratégies pour travailler avec des données et des objectifs de la forme $\neg P$, mais seulement des stratégies pour les objectifs de la forme $P \rightarrow Q$. Nous comblons maintenant cette lacune en donnant deux stratégies pour utiliser des données de la forme $P \rightarrow Q$. Nous avons dit précédemment que de nombreuses stratégies d'utilisation des données suggèrent des façons de tirer des inférences à partir de ces données. De telles stratégies sont appelées *règles d'inférence*. Nos deux stratégies d'utilisation des données de la forme $P \rightarrow Q$ sont des exemples de règles d'inférence.

Pour utiliser une donnée de la forme $P \rightarrow Q$:

Si l'on vous donne également P , ou si vous pouvez prouver que P est vrai, alors vous pouvez utiliser cette donnée pour conclure que Q est vrai. Puisqu'elle est équivalente à $\neg Q \rightarrow \neg P$, si vous pouvez prouver que Q est faux, vous pouvez utiliser cette donnée pour conclure que P est faux.

La première de ces règles d'inférence stipule que si l'on sait que P et $P \rightarrow Q$ sont tous deux vrais, on peut conclure que Q doit également l'être. Les logiciens appellent cette règle *modus ponens*. Nous avons vu cette règle utilisée dans l'un de nos premiers exemples de raisonnement déductif valide au [chapitre 1](#), argument 2 de [l'exemple 1.1.1](#). La validité de ce raisonnement a été vérifiée à l'aide de la table de vérité du connecteur conditionnel de [la section 1.5](#).

La deuxième règle, appelée *modus tollens*, stipule que si vous savez que $P \rightarrow Q$ est vrai et Q est faux, vous pouvez conclure que P doit également être faux. La validité de cette règle peut également être vérifiée à l'aide de tables de vérité, comme on vous demande de le démontrer dans [l'exercice 14](#). En général, vous ne trouverez pas d'utilité à une donnée de la forme $P \rightarrow Q$ tant que vous ne serez pas capable de prouver P ou $\neg Q$. Cependant, si jamais vous atteignez un point dans votre preuve où vous avez déterminé que P est vrai, vous devriez probablement utiliser cette donnée immédiatement pour conclure que Q est vrai. De même, si jamais vous établissez $\neg Q$, utilisez immédiatement cette donnée pour conclure $\neg P$.

Bien que la plupart de nos exemples portent sur des énoncés mathématiques précis, nous utiliserons occasionnellement des exemples de preuves contenant des lettres représentant des énoncés non spécifiés. Plus tard dans ce chapitre, nous pourrons utiliser cette méthode. Méthode permettant de vérifier certaines équivalences du [chapitre 2](#), auparavant justifiées uniquement par des raisons intuitives. Voici un exemple de ce type, illustrant l'utilisation du modus ponens et du modus tollens.

Exemple 3.2.4. Supposons $P \rightarrow (Q \rightarrow R)$. Démontrer que $\neg R \rightarrow (P \rightarrow \neg Q)$.

Travail à partir de zéro

Cela pourrait être réalisé avec une table de vérité, comme on vous le demande dans [l'exercice 15](#), mais utilisons les stratégies de preuve présentées précédemment. Commençons par la situation suivante :

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ P \rightarrow (Q \rightarrow R) & & \neg R \rightarrow (P \rightarrow \neg Q) \end{array}$$

Notre seule donnée est une instruction conditionnelle. D'après les règles d'inférence précédemment exposées, si nous connaissons P , nous pourrions utiliser le modus ponens pour conclure $Q \rightarrow R$, et si nous connaissons $\neg(Q \rightarrow R)$, nous pourrions utiliser le modus tollens pour conclure $\neg P$. Comme nous ne connaissons actuellement ni l'une ni l'autre de ces données, nous ne pouvons encore rien faire avec cette donnée. Si P ou $\neg(Q \rightarrow R)$ venait à s'ajouter à la liste des données, nous devrions envisager d'utiliser le modus ponens ou le modus tollens. Pour l'instant, concentrons-nous sur l'objectif.

L'objectif est également une instruction conditionnelle, nous supposons donc l'antécédent et définissons le conséquent comme notre nouvel objectif :

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ P \rightarrow (Q \rightarrow R) & & P \rightarrow \neg Q \\ \neg R & & \end{array}$$

Nous pouvons également maintenant écrire un peu de la preuve :

Supposons que $\neg R$.

[La preuve de $P \rightarrow \neg Q$ va ici.]

Par conséquent $\neg R \rightarrow (P \rightarrow \neg Q)$.

Nous ne pouvons toujours rien faire avec les données, mais le but est une autre condition, nous utilisons donc à nouveau la même stratégie :

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ P \rightarrow (Q \rightarrow R) & & \neg Q \\ \neg R & & \\ P & & \end{array}$$

Maintenant, la preuve ressemble à ceci :

Supposons que $\neg R$.

Supposons que P .

[La preuve de $\neg Q$ va ici.]

Par conséquent $P \rightarrow \neg Q$.

Par conséquent $\neg R \rightarrow (P \rightarrow \neg Q)$.

Nous avons cherché l'occasion d'utiliser notre première donnée en appliquant le modus ponens ou le modus tollens, et maintenant nous pouvons le faire. Puisque nous connaissons $P \rightarrow (Q \rightarrow R)$ et P , le modus ponens nous permet d'inférer $Q \rightarrow R$. Toute conclusion déduite des données peut être ajoutée à la colonne des données :

<i>Givens</i>	<i>Goal</i>
$P \rightarrow (Q \rightarrow R)$	
$\neg R$	
P	
$Q \rightarrow R$	
	$\neg Q$

Nous ajoutons également une ligne supplémentaire à la preuve :

Supposons que $\neg R$.

Supposons que P .

Puisque P et $P \rightarrow (Q \rightarrow R)$, il s'ensuit que $Q \rightarrow R$.

[La preuve de $\neg Q$ va ici.]

Par conséquent $P \rightarrow \neg Q$.

Par conséquent $\neg R \rightarrow (P \rightarrow \neg Q)$.

Enfin, notre dernière étape consiste à utiliser le modus tollens. Nous connaissons maintenant $Q \rightarrow R$ et $\neg R$, donc par modus tollens nous pouvons conclure $\neg Q$. C'est notre objectif, la preuve est donc faite.

Solution

Théorème. Supposer $P \rightarrow (Q \rightarrow R)$. Alors $\neg R \rightarrow (P \rightarrow \neg Q)$.

Preuve. Supposons $\neg R$. Supposons P . Puisque P et $P \rightarrow (Q \rightarrow R)$, il s'ensuit que $Q \rightarrow R$. Mais alors, puisque $\neg R$, nous pouvons conclure $\neg Q$. Ainsi, $P \rightarrow \neg Q$. Par conséquent $\neg R \rightarrow (P \rightarrow \neg Q)$.

□

Parfois, si vous êtes bloqué, vous pouvez utiliser des règles d'inférence pour travailler à rebours. Par exemple, supposons que l'une de vos données soit de la forme $P \rightarrow Q$ et que votre objectif soit Q . Si seulement vous pouviez prouver P , vous pourriez utiliser le modus ponens pour atteindre votre objectif. Cela suggère de considérer P comme votre objectif plutôt que Q . Si vous pouvez prouver P , alors il

vous suffira d'ajouter une étape supplémentaire à la preuve pour atteindre votre objectif initial Q .

Exemple 3.2.5. Supposons que $A \subseteq B$, $a \in A$, et $a \notin B \setminus C$. Démontrer que $a \in C$.

Travail à partir de zéro

<i>Givens</i>	<i>Goal</i>
$A \subseteq B$	
$a \in A$	
$a \notin B \setminus C$	

Notre troisième donnée est une affirmation négative ; nous commençons donc par la reformuler sous la forme d'une affirmation positive équivalente. Selon la définition de la différence de deux ensembles, cette donnée signifie $\neg(a \in B \wedge a \notin C)$, et selon l'une des lois de De Morgan, cela équivaut à $a \notin B \vee a \in C$. Parce que notre objectif est $un \in C$, il est probablement plus utile de réécrire ceci sous la forme équivalente $a \in B \rightarrow a \in C$:

<i>Givens</i>	<i>Goal</i>
$A \subseteq B$	
$a \in A$	
$a \in B \rightarrow a \in C$	

Nous pouvons maintenant utiliser notre stratégie pour utiliser des données de la forme $P \rightarrow Q$. Notre objectif est $un \in C$, et on nous donne *qu'un* $\in B \rightarrow a \in C$. Si nous pouvions prouver *qu'un* $\in B$, alors nous pourrions utiliser le modus ponens pour atteindre notre objectif. Essayons donc de traiter $un \in B$ comme objectif et voyons si cela rend le problème plus facile :

<i>Givens</i>	<i>Goal</i>
$A \subseteq B$	
$a \in A$	
$a \in B \rightarrow a \in C$	

Maintenant, on sait comment atteindre l'objectif. *Puisqu'un* $\in A$ et $A \subseteq B$, *un* $\in B$.

Solution

Théorème. *Supposons que $A \subseteq B$, $un \in A$, et $a \notin B \setminus C$. Alors $un \in C$.*

Preuve. Depuis $un \in A$ et $A \subseteq B$, nous pouvons conclure *qu'un* $\in B$. Mais $a \notin B \setminus C$, il s'ensuit donc que $a \in C$.

□

Exercices

- *1. Ce problème pourrait être résolu en utilisant des tables de vérité, mais ne procédez pas ainsi. Utilisez plutôt les méthodes d'écriture de preuves décrites jusqu'à présent dans ce chapitre. (Voir [l'exemple 3.2.4](#).)
- (a) Supposons que $P \rightarrow Q$ et $Q \rightarrow R$ soient tous deux vrais. Démontrer que $P \rightarrow R$ est vrai.
- (b) Supposons que $\neg R \rightarrow (P \rightarrow \neg Q)$ soit vrai. Démontrer que $P \rightarrow (Q \rightarrow R)$ est vrai.
2. Ce problème pourrait être résolu en utilisant des tables de vérité, mais ne procédez pas ainsi. Utilisez plutôt les méthodes d'écriture de preuves décrites jusqu'à présent dans ce chapitre. (Voir [l'exemple 3.2.4](#).)
- (a) Supposons que $P \rightarrow Q$ et $R \rightarrow \neg Q$ soient tous deux vrais. Démontrer que $P \rightarrow \neg R$ est vrai.
- (b) Supposons que P soit vrai. Démontrer que $Q \rightarrow \neg(Q \rightarrow \neg P)$ est vrai.
3. Supposons que $A \subseteq C$ et que B et C soient disjoints. Démontrer que si $x \in A$ alors $x \notin B$.
4. Supposons que $A \setminus B$ soit disjoint de C et $x \in A$. Démontrer que si $x \in C$ puis $x \in B$.
- *5. Démontrer qu'il ne peut pas être le cas que $x \in A \setminus B$ et $x \in B \setminus C$.
- *6. Utilisez la méthode de la preuve par contradiction pour prouver le théorème de [l'exemple 3.2.1](#).
7. Utilisez la méthode de la preuve par contradiction pour prouver le théorème de [l'exemple 3.2.5](#).
8. Supposons que $y + x = 2y - x$ et que x et y ne soient pas tous deux nuls. Démontrer que $y \neq 0$.
- *9. Supposons que a et b soient des nombres réels non nuls. Démontrer que si $a < 1/a < b < 1/b$ alors $a < -1$.
10. Supposons que x et y soient des nombres réels. Démontrer que si $x - y = 2x + y$, alors si $y \neq 0$, alors $x \neq 0$.
11. Supposons que x et y soient des nombres réels. Démontrer que si $x \neq 0$, alors si $y = (3x^2 + 2y)/(x^2 + 2)$ alors $y = 3$.
12. Considérez le théorème incorrect suivant :

Théorème incorrect. *Supposer x et y sont des nombres réels et $x + y = 10$. Alors $x \neq 3$ et $y \neq 8$.*

- (a) Quel est le problème avec la preuve suivante du théorème ?

Preuve . Supposons que la conclusion du théorème soit fausse. Alors $x = 3$ et $y = 8$. Mais alors $x + y = 11$, ce qui contredit la donnée information selon laquelle $x + y = 10$. Par conséquent, la conclusion doit être vraie.

□

(b) Montrez que le théorème est incorrect en trouvant un contre-exemple.

13. Considérez le théorème incorrect suivant :

Théorème incorrect. *Supposons que $A \subseteq C$, $B \subseteq C$, et $x \in A$. Alors $x \in B$.*

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve . Supposons que $x \notin B$. Puisque $x \in A$ et $A \subseteq C$, $x \in C$. Puisque $x \notin B$ et $B \subseteq C$, $x \notin C$. Mais maintenant nous avons prouvé que $x \in C$ et $x \notin C$, nous sommes donc arrivés à une contradiction. Par conséquent, $x \in B$. □

(b) Montrez que le théorème est incorrect en trouvant un contre-exemple.

14. Utilisez des tables de vérité pour montrer que le modus tollens est une règle d'inférence valide.

15. Utilisez les tables de vérité pour vérifier l'exactitude du théorème de [l'exemple 3.2.4](#).

16. Utilisez les tables de vérité pour vérifier l'exactitude des affirmations de [l'exercice 1](#).

17. Utilisez les tables de vérité pour vérifier l'exactitude des affirmations de [l'exercice 2](#).

18. La preuve de [l'exemple 3.2.2 peut-elle](#) être modifiée pour prouver que si $x^2 + y = 13$ et $x \neq 3$ alors $y \neq 4$? Expliquez.

3.3 Preuves impliquant des quantificateurs

Reprenez [l'exemple 3.2.3](#) . Dans cet exemple, nous avons dit que x pouvait être n'importe quoi, et nous avons prouvé l'affirmation $x \in A \setminus C \rightarrow x \in B$. Étant donné que le raisonnement que nous avons utilisé s'appliquerait quelle que soit la valeur *de* x , notre preuve montre en fait que $x \in A \setminus C \rightarrow x \in B$ est vrai pour toutes les valeurs de x . En d'autres termes, nous pouvons conclure $\forall x (x \in A \setminus C \rightarrow x \in B)$.

Ceci illustre la manière la plus simple et la plus directe de prouver un objectif de la forme $\forall xP(x)$. Si vous pouvez fournir une preuve de l'objectif $P(x)$ qui fonctionnerait quelle que soit la valeur *de* x , alors vous pouvez conclure que $\forall xP(x)$ doit être vraie. Pour garantir que votre preuve fonctionne quelle que soit la valeur de x , il est important de commencer votre preuve sans faire d'hypothèses sur x . Les mathématiciens expriment cela en disant que x doit être *arbitraire* . En particulier, vous ne devez pas supposer que x est égal à un autre objet déjà traité dans la preuve. Ainsi, si la lettre x est déjà utilisée dans la

preuve pour représenter un objet particulier, elle ne peut pas être utilisée pour représenter un objet arbitraire. Dans ce cas, vous devez choisir une variable différente qui n'est pas déjà utilisée dans la preuve, par exemple y . et remplacez l'objectif $\forall x P(x)$ par l'énoncé équivalent $\forall y P(y)$. Vous pouvez maintenant procéder en posant y pour un objet arbitraire et en prouvant $P(y)$.

Pour prouver un but de la forme $\forall x P(x)$:

Soit x pour un objet quelconque et démontrons $P(x)$. La lettre x doit être une nouvelle variable dans la démonstration. Si x est déjà utilisé dans la démonstration pour représenter quelque chose, il faut choisir une variable inutilisée, par exemple y , pour représenter l'objet quelconque et démontrons $P(y)$.

Travail à partir de zéro

Avant d'utiliser la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$\forall x P(x)$
—	

Après avoir utilisé la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$P(x)$
—	

Forme de l'épreuve finale :

Soit x arbitraire.

[La preuve de $P(x)$ va ici.]

Puisque x est arbitraire, nous pouvons conclure que $\forall x P(x)$.

Exemple 3.3.1. Supposons que A , B et C sont des ensembles, et $A \setminus B \subseteq C$. Démontrer que $A \setminus C \subseteq B$.

Travail à partir de zéro

<i>Givens</i>	<i>Goal</i>
$A \setminus B \subseteq C$	$A \setminus C \subseteq B$
—	

Comme d'habitude, nous examinons d'abord la forme logique de l'objectif pour planifier notre stratégie. Dans ce cas, nous devons définir \subseteq pour déterminer la forme logique de l'objectif.

<i>Givens</i>	<i>Goal</i>
$A \setminus B \subseteq C$	$\forall x (x \in A \setminus C \rightarrow x \in B)$
—	

Parce que l'objectif a la forme $\forall x P(x)$, où $P(x)$ est l'énoncé $x \in A \setminus C \rightarrow x \in B$, nous allons introduire une nouvelle variable x dans la preuve pour représenter un objet arbitraire et ensuite essayer de prouver $x \in A \setminus C \rightarrow x \in B$. Notez que x est une nouvelle variable dans la preuve. Elle apparaît

sous la forme logique de l'objectif comme variable liée, mais rappelons que les variables liées ne représentent rien de particulier. Nous n'avons pas encore utilisé x comme variable libre dans aucune instruction ; elle n'a donc pas été utilisée pour représenter un objet particulier. Pour garantir l'arbitraire de x , nous devons veiller à ne pas ajouter d'hypothèses sur x à la colonne des données. Cependant, nous modifions notre objectif :

$$\begin{array}{c} \text{Given} \\ A \setminus B \subseteq C \\ \hline \text{Goal} \\ x \in A \setminus C \rightarrow x \in B \end{array}$$

Selon notre stratégie, la preuve finale devrait ressembler à ceci :

Soit x arbitraire.

[Preuve de $x \in A \setminus C \rightarrow x \in B$ va ici.]

Puisque x est arbitraire, nous pouvons conclure que $\forall x (x \in A \setminus C \rightarrow x \in B)$, donc $A \setminus C \subseteq B$.

Le problème est maintenant identique à celui de [l'exemple 3.2.3](#) ; le reste de la solution est donc identique. Autrement dit, nous pouvons simplement insérer la preuve de [l'exemple 3.2.3](#) entre la première et la dernière phrase de la preuve présentée ici.

Solution

Théorème. Supposer UN , Groupe C sont des ensembles, et $A \setminus B \subseteq C$. Alors $UN \setminus C \subseteq B$.

Preuve. Soit x arbitraire. Supposons que $x \in A \setminus C$. Cela signifie que $x \in A$ et $x \notin C$. Supposons que $x \notin B$. Alors $x \in A \setminus B$, donc puisque $A \setminus B \subseteq C$, $x \in C$. Mais cela contredit le fait que $x \notin C$. Par conséquent $x \in B$. Ainsi, si $x \in A \setminus C$ puis $x \in B$. Puisque x était arbitraire, nous pouvons conclure que $\forall x (x \in A \setminus C \rightarrow x \in B)$, donc $A \setminus C \subseteq B$.

□

Notez que, bien que cette preuve montre que chaque élément de $A \setminus C$ est aussi un élément de B , elle ne contient pas d'expressions telles que « chaque élément de $A \setminus C$ » ou « tous les éléments de $A \setminus C$ ». Pour la majeure partie de la preuve, nous raisonnons simplement sur x , qui est traité comme un élément unique et fixe de $A \setminus C$. Nous supposons que x représente un élément particulier de $A \setminus C$, en prenant soin de ne faire aucune hypothèse sur l'élément qu'il représente. Ce n'est qu'à la fin de la preuve que nous observons que, puisque x est arbitraire, nos conclusions sur x seraient vraies quelle que soit x . C'est le principal avantage de cette stratégie pour prouver un but de la forme $\forall xP(x)$. Elle permet de prouver un but sur *tous* les objets en raisonnant sur *un seul* objet, pourvu que cet objet soit arbitraire. Si vous prouvez un objectif de la forme $\forall xP(x)$ et que vous vous retrouvez à dire

beaucoup de choses sur « tous *les* x » ou « chaque x », vous compliquez probablement inutilement votre preuve en n'utilisant pas cette stratégie.

Comme nous l'avons vu au [chapitre 2](#), les énoncés de la forme $\forall x (P(x) \rightarrow Q(x))$ sont assez courants en mathématiques. Il pourrait donc être utile d'examiner comment les stratégies que nous avons discutées peuvent être combinées pour prouver un objectif de cette forme. Puisque l'objectif commence par $\forall x$, la première étape est de poser x arbitraire et d'essayer de prouver $P(x) \rightarrow Q(x)$. Pour prouver cet objectif, vous voudrez probablement supposer que $P(x)$ est vrai et prouver $Q(x)$. Ainsi, la preuve commencera probablement ainsi : « Soit x arbitraire. Supposons $P(x)$. » Elle poursuivra ensuite avec les étapes nécessaires pour atteindre l'objectif $Q(x)$. Souvent, dans ce type de preuve, l'affirmation que x est arbitraire est omise, et la preuve commence simplement par « Supposons $P(x)$. » Lorsqu'une nouvelle variable x est introduite dans une preuve de cette manière, il est généralement compris que x est arbitraire. En d'autres termes, aucune hypothèse n'est faite sur x autre que celle énoncée selon laquelle $P(x)$ est vrai.

Un exemple important de ce type de preuve est une preuve dans laquelle le but a la forme $\forall x \in AP(x)$. Rappelons que $\forall x \in AP(x)$ signifie la même chose que $\forall x (x \in A \rightarrow P(x))$, donc selon notre stratégie, la preuve devrait commencer par « Supposons que $x \in A$ » et ensuite suivre les étapes nécessaires pour conclure que $P(x)$ est vraie. Encore une fois, il est entendu qu'aucune hypothèse n'est formulée sur x autre que l'hypothèse énoncée selon laquelle $x \in A$, donc x représente un élément arbitraire de A .

Les mathématiciens sautent parfois d'autres étapes dans leurs démonstrations, si l'on peut s'attendre à ce que des lecteurs avertis les complètent eux-mêmes. En particulier, nombre de nos stratégies de démonstration suggèrent que la démonstration se termine par une phrase résumant pourquoi le raisonnement avancé mène à la conclusion souhaitée. Dans une démonstration combinant plusieurs de ces stratégies, plusieurs phrases résumant ces étapes peuvent se succéder à la fin de la démonstration. Les mathématiciens condensent souvent cette synthèse en une seule phrase, voire la sautent complètement. Lorsque vous lisez une démonstration rédigée par quelqu'un d'autre, il peut être utile de compléter ces étapes omises.

Exemple 3.3.2. Supposons que A et B soient des ensembles. Démontrer que si $A \cap B = A$ alors $A \subseteq B$.

Travail à partir de zéro

Notre objectif est $A \cap B = A \rightarrow A \subseteq B$. Comme l'objectif est une instruction conditionnelle, nous ajoutons l'antécédent à la liste des données et faisons du conséquent l'objectif. Nous allons également écrire la définition de \subseteq dans le nouvel objectif pour montrer sa forme logique.

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ A \cap B = A & & \forall x(x \in A \rightarrow x \in B) \end{array}$$

Maintenant, l'objectif a la forme $\forall x(P(x) \rightarrow Q(x))$, où $P(x)$ est l'énoncé $x \in A$ et $Q(x)$ est l'énoncé $x \in B$. Nous laissons donc x arbitraire, supposons $x \in A$, et prouver $x \in B$:

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ A \cap B = A & & x \in B \\ x \in A & & \end{array}$$

En combinant les stratégies de preuve que nous avons utilisées, nous voyons que la preuve finale aura cette forme :

Supposons que $A \cap B = A$.

Soit x arbitraire.

Supposons que $x \in UN$.

[Preuve de $x \in B$ va ici.]

Par conséquent $x \in A \rightarrow x \in B$.

Puisque x est arbitraire, nous pouvons conclure que $\forall x(x \in A \rightarrow x \in B)$, donc $A \subseteq B$.

Par conséquent, si $A \cap B = A$ alors $A \subseteq B$.

Comme indiqué précédemment, lorsque nous rédigeons la preuve finale, nous pouvons ignorer la phrase « Soit x arbitraire », et nous pouvons également ignorer certaines ou la totalité des trois dernières phrases.

Nous avons maintenant atteint le point où nous ne pouvons plus analyser la forme logique de l'objectif. Heureusement, en examinant les données, nous découvrons que l'objectif suit facilement. Puisque $x \in A$ et $A \cap B = A$, il s'ensuit que $x \in A \cap B$, donc $x \in B$. (Dans cette dernière étape, nous utilisons la définition de \cap : $x \in A \cap B$ signifie $x \in A$ et $x \in B$.)

Solution

Théorème. Supposer UN et B sont des ensembles. Si $A \cap B = A$ alors $UN \subseteq B$.

Preuve. Supposons que $A \cap B = A$, et supposons que $x \in A$. Alors puisque $A \cap B = A$, $x \in A \cap B$, donc $x \in B$. Puisque x est un élément arbitraire de A , nous pouvons conclure que $A \subseteq B$.

□

Prouver un objectif de la forme $\exists xP(x)$ implique également d'introduire une nouvelle variable x dans la preuve et de prouver $P(x)$, mais dans ce cas x ne sera pas arbitraire. Car il suffit de prouver que $P(x)$ est vrai pour *au moins une* x , il suffit d'assigner une valeur particulière à x et de prouver $P(x)$ pour cette valeur de x .

Pour prouver un but de la forme $\exists xP(x)$:

Essayez de trouver une valeur de x pour laquelle vous pensez que $P(x)$ sera vraie. Commencez ensuite votre preuve par « Soit $x =$ (la valeur que vous avez choisie) » et prouvez $P(x)$ pour cette valeur de x . Là encore, x doit être une nouvelle variable. Si la lettre x est déjà utilisée dans la preuve à d'autres fins, vous devez choisir une variable inutilisée, par exemple y , et réécrire l'objectif sous la forme équivalente $\exists yP(y)$. Procédez maintenant comme précédemment en commençant votre preuve par « Soit $y =$ (la valeur que vous avez choisie) » et prouvez $P(y)$.

Travail à partir de zéro

Avant d'utiliser la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$\exists x P(x)$

Après avoir utilisé la stratégie :

<i>Givens</i>	<i>Goal</i>
—	$P(x)$

x = (the value you decided on)

Forme de l'épreuve finale :

Soit $x =$ (la valeur que vous avez choisie).

[La preuve de $P(x)$ va ici.]

Ainsi, $\exists xP(x)$.

Trouver la bonne valeur pour x peut parfois s'avérer difficile. Une méthode parfois utile consiste à supposer que $P(x)$ est vraie, puis à déterminer la valeur de x à partir de cette hypothèse. Si $P(x)$ est une équation impliquant x , cela revient à résoudre l'équation pour x . Cependant, si cela ne fonctionne pas, vous pouvez utiliser toute autre méthode pour essayer de trouver une valeur pour x , y compris les essais-erreurs et les suppositions. La raison pour laquelle vous avez une telle liberté avec cette étape est que *le raisonnement que vous utilisez pour trouver une valeur pour x n'apparaîtra pas dans la preuve finale*. Ceci est dû à notre règle selon laquelle une preuve ne doit contenir que le raisonnement nécessaire pour justifier sa conclusion, et

non une explication de votre raisonnement. Pour justifier la conclusion selon laquelle $\exists x P(x)$ est vraie, il suffit de vérifier que $P(x)$ est vraie lorsqu'une valeur particulière est attribuée à x . La manière dont vous avez pensé à cette valeur ne concerne que vous et ne fait pas partie de la justification de la conclusion.

Exemple 3.3.3. Démontrer que pour tout nombre réel x , si $x > 0$ alors il existe un nombre réel y tel que $y(y + 1) = x$.

Travail à partir de zéro

En symboles, notre objectif est $\forall x (x > 0 \rightarrow \exists y [y(y + 1) = x])$, où les variables x et y dans cette instruction sont comprises comme s'étendant sur \mathbb{R} . Nous commençons donc par poser x comme un nombre réel arbitraire, puis nous supposons que $x > 0$ et essayons de prouver que $\exists y [y(y + 1) = x]$. Ainsi, nous avons maintenant la donnée et l'objectif suivants :

$$\begin{array}{ll} \text{Givens} & \text{Goal} \\ x > 0 & \exists y [y(y + 1) = x] \end{array}$$

Puisque notre objectif est de la forme $\exists y P(y)$, où $P(y)$ est l'énoncé $y(y + 1) = x$, notre stratégie consiste à trouver une valeur de y pour laquelle $P(y)$ est vraie. Dans ce cas, nous pouvons résoudre l'équation $y(y + 1) = x$ pour y . Il s'agit d'une équation quadratique, dont la résolution est assurée par la formule :

$$y(y + 1) = x \Leftrightarrow y^2 + y - x = 0 \Leftrightarrow y = \frac{-1 \pm \sqrt{1 + 4x}}{2}.$$

Notez que $\sqrt{1 + 4x}$ est défini, puisque $x > 0$ est une donnée. Nous avons en fait trouvé deux solutions pour y , mais pour prouver que $\exists y [y(y + 1) = x]$, il suffit de montrer une valeur de y qui rend l'équation $y(y + 1) = x$ vraie. L'une ou l'autre des deux solutions pourrait être utilisée dans la preuve. Nous utiliserons la solution suivante. $y = (-1 + \sqrt{1 + 4x})/2$.

Les étapes utilisées pour résoudre y ne devraient pas apparaître dans la preuve finale. Dans cette dernière, nous dirons simplement : « Soit $y = (-1 + \sqrt{1 + 4x})/2$ et démontrons que $y(y + 1) = x$. » Autrement dit, la preuve finale aura la forme suivante :

Soit x un nombre réel arbitraire.

Supposons que $x > 0$.

Laisser $y = (-1 + \sqrt{1 + 4x})/2$.

[Preuve de $y(y + 1) = x$ va ici.]

Ainsi, $\exists y [y(y + 1) = x]$.

Par conséquent $x > 0 \rightarrow \exists y [y(y + 1) = x]$.

Puisque x est arbitraire, nous pouvons conclure que $\forall x (x > 0 \rightarrow \exists y [y(y+1) = x])$.

Pour voir ce qui doit être fait pour combler le vide restant dans la preuve, nous ajoutons $y = (-1 + \sqrt{1+4x})/2$ à la liste des données et faisons de $y(y+1) = x$ l'objectif :

$$\begin{array}{ccc} & \text{Given} & \text{Goal} \\ x > 0 & & y(y+1) = x \\ y = (-1 + \sqrt{1+4x})/2 & & \end{array}$$

Nous pouvons maintenant prouver que l'équation $y(y+1) = x$ est vraie en remplaçant simplement $y = (-1 + \sqrt{1+4x})/2$ et en vérifiant que l'équation résultante est vraie.

Solution

Théorème. Pour chaque nombre réel x , si $x > 0$ alors il existe un nombre réel et tel que $y(y+1) = x$.

Preuve. Soit x un nombre réel arbitraire, et supposons $x > 0$. Soit

$$y = \frac{-1 + \sqrt{1+4x}}{2},$$

qui est défini puisque $x > 0$. Alors

$$\begin{aligned} y(y+1) &= \left(\frac{-1 + \sqrt{1+4x}}{2}\right) \cdot \left(\frac{-1 + \sqrt{1+4x}}{2} + 1\right) \\ &= \left(\frac{\sqrt{1+4x} - 1}{2}\right) \cdot \left(\frac{\sqrt{1+4x} + 1}{2}\right) \\ &= \frac{1+4x-1}{4} = \frac{4x}{4} = x. \end{aligned}$$

□

Parfois, lorsque vous démontrez un objectif de la forme $\exists y Q(y)$, vous ne pourrez pas déterminer, en regardant simplement l'énoncé $Q(y)$, la valeur à remplacer par y . Dans ce cas, il peut être judicieux d'examiner de plus près les données pour voir si elles suggèrent une valeur à utiliser pour y . En particulier, une donnée de la forme $\exists x P(x)$ peut être utile dans cette situation. Cette donnée indique l'existence d'un objet possédant une certaine propriété. Il est probablement judicieux d'imaginer qu'un objet particulier possédant cette propriété a été choisi et d'introduire une nouvelle variable, par exemple x_0 , dans la preuve pour le représenter. Ainsi, pour le reste de la preuve, vous utiliserez x_0 pour représenter un objet particulier, et vous pouvez supposer qu'avec x_0 représentant cet objet, $P(x_0)$ est vraie. Autrement dit, vous pouvez ajouter $P(x_0)$ à votre liste de données. Cet objet x_0 , ou

quelque chose qui lui est lié, pourrait s'avérer être la bonne chose à brancher pour que y fasse que $Q(y)$ soit vrai.

Pour utiliser une donnée de la forme $\exists xP(x)$:

Introduisez une nouvelle variable x_0 dans la preuve pour représenter un objet pour lequel $P(x_0)$ est vrai. Cela signifie que vous pouvez désormais supposer que $P(x_0)$ est vrai. Les logiciens appellent cette règle d'inférence *l'instanciation existentielle*.

Notez que l'utilisation d'une donnée de la forme $\exists xP(x)$ est très différente de la preuve d'un objectif de la forme $\exists xP(x)$, car lorsque vous utilisez une donnée de la forme $\exists xP(x)$, vous *On ne peut pas choisir une valeur particulière à insérer pour x*. On peut supposer que x_0 représente un objet pour lequel $P(x_0)$ est vrai, mais on ne peut rien supposer d'autre à propos de x_0 . D'autre part, une donnée de la forme $\forall xP(x)$ indique que $P(x)$ serait vrai *quelle que soit* la valeur attribuée à x . On peut donc *choisir toute valeur que vous souhaitez* insérer pour x et utiliser celle-ci pour conclure que $P(x)$ est vrai.

Pour utiliser une donnée de la forme $\forall xP(x)$:

Vous pouvez insérer n'importe quelle valeur, par exemple a , pour x et utiliser cette valeur pour conclure que $P(a)$ est vrai. Cette règle est appelée *instanciation universelle*.

Habituellement, si vous avez une donnée de la forme $\exists xP(x)$, vous devez lui appliquer immédiatement l'instanciation existentielle. Une bonne règle est la suivante : si vous savez que quelque chose existe, vous devez lui donner un nom. D'un autre côté, vous ne pourrez pas appliquer l'instanciation universelle à une donnée de la forme $\forall xP(x)$ à moins d'avoir une valeur particulière a à remplacer par x ; vous souhaiterez donc peut-être attendre qu'un choix probable pour a apparaisse dans la preuve. Par exemple, considérons une donnée de la forme $\forall x(P(x) \rightarrow Q(x))$. Vous pouvez utiliser cette donnée pour conclure que $P(a) \rightarrow Q(a)$ pour tout a , mais selon notre règle d'utilisation des données qui sont des instructions conditionnelles, cette conclusion ne sera probablement pas très utile à moins que vous ne connaissiez $P(a)$ ou $\neg Q(a)$. Vous devriez probablement attendre qu'un objet a apparaisse dans la preuve pour lequel vous connaissez soit $P(a)$ soit $\neg Q(a)$, et remplacer ce a par x lorsqu'il apparaît.

Nous avons déjà utilisé cette technique dans certaines de nos preuves précédentes en traitant des données de la forme $A \subseteq B$. Par exemple, dans [l'exemple 3.2.5](#), nous avons utilisé les données $A \subseteq B$ et $a \in A$ pour conclure *qu'un ϵB* . La justification de ce raisonnement est que $A \subseteq B$

signifie $\forall x (x \in A \rightarrow x \in B)$, donc par instantiation universelle, nous pouvons brancher *un* pour x et conclure que $a \in A \rightarrow un \in B$. Puisque nous savons aussi *qu'un* $\in A$, il s'ensuit par modus ponens *qu'un* $\in B$.

Exemple 3.3.4. Supposons que \mathcal{F} et \mathcal{G} sont des familles d'ensembles et que $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Démontrer que $\bigcap \mathcal{F} \subseteq \bigcup \mathcal{G}$.

Travail à partir de zéro

Notre première étape dans l'analyse de la forme logique de l'objectif est d'écrire la signification du symbole du sous-ensemble, ce qui nous donne l'énoncé $\forall x (x \in \bigcap \mathcal{F} \rightarrow x \in \bigcup \mathcal{G})$. Nous pourrions aller plus loin dans cette analyse en écrivant les définitions d'union et d'intersection, mais la partie de l'analyse que nous avons déjà faite sera suffisant pour nous permettre de décider comment commencer la preuve. Les définitions d'union et d'intersection seront nécessaires plus tard dans la preuve, mais nous attendrons qu'elles soient nécessaires avant de les compléter. Lors de l'analyse des formes logiques des données et des buts afin de déterminer une preuve, il est généralement préférable de ne faire que ce qui est nécessaire pour déterminer l'étape suivante. Aller plus loin dans l'analyse logique ne fait généralement qu'ajouter des complications inutiles, sans apporter aucun bénéfice.

Parce que le but signifie $\forall x (x \in \bigcap \mathcal{F} \rightarrow x \in \bigcup \mathcal{G})$, nous laissons x arbitraire, supposons $x \in \bigcap \mathcal{F}$ et essayez de prouver $x \in \bigcup \mathcal{G}$.

$$\begin{array}{ll} \text{Given} & \text{Goal} \\ \mathcal{F} \cap \mathcal{G} \neq \emptyset & x \in \bigcup \mathcal{G} \\ x \in \bigcap \mathcal{F} & \end{array}$$

Le nouvel objectif signifie $\exists A \in \mathcal{G}(x \in A)$, donc pour le prouver, nous devons essayer de trouver une valeur qui « fonctionne » pour A . Se contenter d'examiner l'objectif ne permet pas de savoir clairement comment choisir A ; nous examinons donc de plus près les données. Nous commençons par les écrire sous forme de symboles logiques :

$$\begin{array}{ll} \text{Given} & \text{Goal} \\ \exists A(A \in \mathcal{F} \cap \mathcal{G}) & \exists A \in \mathcal{G}(x \in A) \\ \forall A \in \mathcal{F}(x \in A) & \end{array}$$

La seconde donnée commence par $\forall A$; nous ne pourrions donc peut-être pas l'utiliser tant qu'une valeur appropriée pour remplacer A n'apparaîtra pas au cours de la preuve. En particulier, il faut garder à l'esprit que si nous rencontrons un élément de \mathcal{F} lors de la démonstration, nous pouvons le remplacer par A dans la seconde donnée et conclure qu'il contient x comme élément. La première

donnée, en revanche, commence par $\exists A$; nous devons donc l'utiliser immédiatement. Elle indique qu'il existe un objet qui est un élément de $\mathcal{F} \cap \mathcal{G}$. Par instantiation existentielle, nous pouvons introduire un nom, par exemple A_0 , pour cet objet. Ainsi, nous pouvons traiter $A_0 \in \mathcal{F} \cap \mathcal{G}$ comme une donnée à partir de maintenant. Puisque nous avons maintenant un nom, A_0 , pour un élément particulier de $\mathcal{F} \cap \mathcal{G}$, il serait redondant de continuer à discuter de l'énoncé donné $\exists A (A \in \mathcal{F} \cap \mathcal{G})$, nous allons donc le supprimer de notre liste de données. Puisque notre nouvelle donnée $A_0 \in \mathcal{F} \cap \mathcal{G}$ signifie $A_0 \in \mathcal{F}$ et $A_0 \in \mathcal{G}$, nous avons maintenant la situation suivante :

<i>Givens</i>	<i>Goal</i>
$A_0 \in \mathcal{F}$	
$A_0 \in \mathcal{G}$	
$\forall A \in \mathcal{F}(x \in A)$	

Si vous avez été attentif, vous devriez savoir quelle est la prochaine étape. Nous avions déjà décidé de rester attentifs à tout élément de \mathcal{F} qui pourrait survenir pendant la démonstration, car nous pourrions vouloir les remplacer par A dans la dernière donnée. Un élément de \mathcal{F} est apparu : A_0 ! En remplaçant A_0 par A dans la dernière donnée, nous pouvons conclure que $x \in A_0$. Toutes les conclusions peuvent être traitées à l'avenir comme des données acquises, vous pouvez donc ajouter cette déclaration à la colonne des données acquises si vous le souhaitez.

Rappelons que nous avons décidé d'examiner les données car nous ne savions pas quelle valeur attribuer à A dans l'objectif. Il nous faut une valeur pour A qui soit dans \mathcal{G} et qui rende l'énoncé $x \in A$ s'avère vrai. Cette considération des données suggère-t-elle une valeur à utiliser pour A ? Oui ! Utilisez $A = A_0$.

Bien que nous ayons traduit les déclarations données $x \in \mathcal{F}$, $x \in \mathcal{G}$ et $\mathcal{F} \cap \mathcal{G} \neq \emptyset$ en symboles logiques afin de comprendre leur utilisation dans la preuve. Ces traductions ne sont généralement pas écrites lors de la rédaction de la preuve finale. Dans la preuve finale, nous écrivons simplement ces énoncés dans leur forme originale et laissons le lecteur de la preuve en déduire leurs formes logiques afin de suivre notre raisonnement.

Solution

Théorème. Supposer \mathcal{F} et \mathcal{G} sont des familles d'ensembles, et $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Alors $\bigcap \mathcal{F} \subseteq \bigcup \mathcal{G}$.

Preuve . Supposons que $x \in \bigcap \mathcal{F}$. Puisque $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, on peut laisser A_0 être un élément de $\mathcal{F} \cap \mathcal{G}$. Ainsi, $A_0 \in \mathcal{F}$ et $A_0 \in \mathcal{G}$. Puisque $x \in \bigcap \mathcal{F}$ et $A_0 \in \mathcal{F}$, il s'ensuit que $x \in A_0$. Mais nous savons aussi que $A_0 \in \mathcal{G}$, nous pouvons donc conclure que $x \in \bigcup \mathcal{G}$.

□

Les preuves impliquant les quantificateurs *pour tous* et *il existe* sont souvent difficiles pour eux.

Cette dernière phrase vous a embrouillé, n'est-ce pas ? Vous vous demandez probablement : « Qui sont-ils ? » Les lecteurs de vos preuves éprouveront la même confusion si vous utilisez des variables sans expliquer leur signification. Les débutants en preuve sont parfois négligents à ce sujet, et c'est pourquoi les preuves impliquant les quantificateurs *pour tout* et *il existe* sont souvent difficiles pour eux. (C'était plus logique cette fois-ci, non ?) En utilisant les stratégies présentées dans cette section, vous introduisez de nouvelles variables dans votre preuve, et ce faisant, veillez à toujours bien expliquer au lecteur leur signification.

Par exemple, si vous prouvez un objectif de la forme $\forall x \in AP(x)$, vous commenceriez probablement par introduire une variable x pour représenter un élément arbitraire de A . Votre lecteur ne saura pas ce que signifie x , cependant, à moins que vous ne commenciez votre démonstration par « Soit x un élément arbitraire de A » ou « Supposons que $x \in A$ ». Ces phrases indiquent au lecteur qu'à partir de maintenant, il ou elle doit penser à x comme représentant un élément particulier de A , bien que l'élément qu'il représente ne soit pas précisé. Bien sûr, vous devez être clair sur la signification de x . En particulier, x étant arbitraire, vous devez veiller à ne rien supposer à propos de x autre que le fait que $x \in A$. Il peut être utile de considérer la valeur de x comme étant choisie par *quelqu'un d'autre* ; vous n'avez aucun contrôle sur l'élément de A qu'il choisira. Utiliser une donnée de la forme $\exists xP(x)$ est similaire. Cette donnée vous indique que vous pouvez introduire une nouvelle variable x_0 dans la preuve pour représenter un objet pour lequel $P(x_0)$ est vrai, mais vous ne pouvez rien supposer d'autre à propos de x_0 . D'un autre côté, si vous *prouvez* $\exists xP(x)$, votre preuve commencera probablement par « Soit $x = \dots$ ». Cette fois, vous pouvez

choisir la valeur de x , et vous devez indiquer explicitement au lecteur que vous choisissez la valeur de x et quelle valeur vous avez choisie.

Il est également important, lorsque vous introduisez une nouvelle variable x , de bien comprendre à quel *type* d'objet x correspond. S'agit-il d'un nombre ? D'un ensemble ? D'une fonction ? D'une matrice ? Mieux vaut éviter d'écrire $un \in X$, sauf si X est un ensemble, par exemple. Si vous n'y prêtez pas attention, vous risquez d'écrire n'importe quoi. Il est également parfois nécessaire de savoir à quel type d'objet correspond une variable pour déterminer la forme logique d'une instruction impliquant cette variable. Par exemple, $A = B$ signifie $\forall x (x \in A \leftrightarrow x \in B)$ si A et B sont des ensembles, mais pas s'ils sont des nombres.

Le point le plus important à retenir concernant l'introduction de variables dans une preuve est simplement le fait que les variables doivent toujours être introduites avant leur utilisation. Si vous formulez une affirmation concernant x (c'est-à-dire une affirmation où x apparaît comme une variable libre) sans expliquer au préalable *sa* signification, le lecteur de votre preuve ne comprendra pas de quoi vous parlez – et il y a de fortes chances que vous ne compreniez pas non plus !

Étant donné que les preuves impliquant des quantificateurs peuvent nécessiter plus de pratique que les autres preuves que nous avons abordées jusqu'à présent, nous terminons cette section avec deux exemples supplémentaires.

Exemple 3.3.5. Supposons que B soit un ensemble et \mathcal{F} une famille d'ensembles. Démontrer que si $\bigcup \mathcal{F} \subseteq B$ alors $\mathcal{F} \subseteq \mathcal{P}(B)$.

Travail à partir de zéro

Nous supposons $\bigcup \mathcal{F} \subseteq B$ et essayons de prouver $\mathcal{F} \subseteq \mathcal{P}(B)$. Parce que cet objectif signifie $\forall x (x \in \mathcal{F} \rightarrow x \in \mathcal{P}(B))$, nous laissons x arbitraire, supposons $x \in \mathcal{F}$, et définir $x \in \mathcal{P}(B)$ comme objectif. Rappelons que \mathcal{F} est une famille d'ensembles, donc puisque $x \in \mathcal{F}$, x est un ensemble. Ainsi, nous avons maintenant les données et l'objectif suivants :

$$\begin{array}{ll} \textit{Givens} & \textit{Goal} \\ \bigcup \mathcal{F} \subseteq B & x \in \mathcal{P}(B) \\ x \in \mathcal{F} & \end{array}$$

Pour comprendre comment prouver cet objectif, nous devons utiliser la définition d'un ensemble de puissances. L'énoncé $x \in \mathcal{P}(B)$ signifie $x \subseteq B$, ou en d'autres termes $\forall y (y \in x \rightarrow y \in B)$. Il faut donc introduire

un autre objet arbitraire dans la preuve. Soit y arbitraire, supposons $y \in x$, et essayez de prouver $y \in B$.

<i>Givens</i>	<i>Goal</i>
$\bigcup \mathcal{F} \subseteq B$	
$x \in \mathcal{F}$	
$y \in x$	

donc examiner de plus près les données. Notre objectif est $y \in B$, et la seule donnée qui mentionne B est la première. En fait, la première donnée nous permettrait d'atteindre cet objectif, si seulement nous savions que $y \in \bigcup \mathcal{F}$. Cela suggère que nous pourrions essayer de traiter $y \in \bigcup \mathcal{F}$ comme objectif. Si nous pouvons atteindre cet objectif, il nous suffit d'ajouter une étape supplémentaire, en appliquant la première donnée, et la preuve sera faite.

<i>Givens</i>	<i>Goal</i>
$\bigcup \mathcal{F} \subseteq B$	
$x \in \mathcal{F}$	
$y \in x$	

Encore une fois, nous disposons d'un objectif dont la forme logique peut être analysée ; nous utilisons donc cette forme pour guider notre stratégie. L'objectif signifie $\exists A. \in \mathcal{F}(y \in A)$, donc pour le prouver il faut trouver un ensemble A tel que $A \in \mathcal{F}$ et $y \in A$. En regardant les données, nous voyons que x est un tel ensemble, donc la preuve est faite.

Solution

Théorème. *Supposer B est un ensemble et \mathcal{F} est une famille d'ensembles. Si $\bigcup \mathcal{F} \subseteq B$ alors $\mathcal{F} \subseteq \mathcal{P}(B)$.*

Preuve. Supposons $\bigcup \mathcal{F} \subseteq B$. Soit x un élément arbitraire de \mathcal{F} . Soit y un élément arbitraire de x . Puisque $y \in x$ et $x \in \mathcal{F}$, par la définition de $\bigcup \mathcal{F}$, $y \in \bigcup \mathcal{F}$. Mais alors puisque $\bigcup \mathcal{F} \subseteq B$, $y \in B$. Puisque y était un élément arbitraire de x , nous pouvons conclure que $x \subseteq B$, donc $x \in \mathcal{P}(B)$. Mais x était un élément arbitraire de \mathcal{F} , donc cela montre que $\mathcal{F} \subseteq \mathcal{P}(B)$, comme requis. □

Le diagramme de Venn de [la figure 3.1](#) peut vous aider à comprendre pourquoi le théorème de [l'exemple 3.3.5](#) est vrai, et vous pourriez trouver utile de vous référer à l'image lors de la relecture de la démonstration. Notez cependant que nous n'avons pas prouvé le théorème en expliquant simplement cette image ; la démonstration a

été construite en suivant les stratégies de démonstration décrites précédemment. De nombreuses méthodes, comme dessiner des images ou travailler sur des exemples, peuvent vous aider à comprendre pourquoi un théorème est vrai. Cependant, expliquer cette compréhension ne constitue pas une démonstration. Pour démontrer un théorème, vous devez suivre les stratégies de ce chapitre.

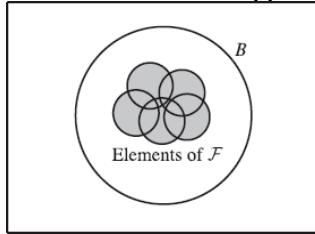


Figure 3.1. Les petits cercles représentent les éléments de \mathcal{F} , et la région ombrée est $\bigcup \mathcal{F}$.

Le grand cercle représente B .

La preuve de [l'exemple 3.3.5](#) est probablement la plus complexe que nous ayons réalisée jusqu'à présent. Relisez-la et assurez-vous d'en comprendre la structure et le but de chaque phrase. N'est-il pas remarquable de constater à quel point cette complexité logique est concentrée en quelques lignes ?

Il n'est pas rare qu'une preuve courte présente une structure logique aussi riche. Cette efficacité d'exposition est l'un des atouts majeurs des preuves, mais elle les rend souvent difficiles à lire. Bien que nous nous soyons concentrés jusqu'ici sur *l'écriture* de preuves, il est également important d'apprendre à *lire* des preuves rédigées par d'autres. Pour vous entraîner, nous présentons notre dernière preuve de cette section, sans le travail de base. Essayez de suivre la structure de la preuve au fur et à mesure de votre lecture. Un commentaire vous sera fourni après la preuve pour vous aider à la comprendre.

Pour cette preuve, nous avons besoin de la définition suivante :

Définition 3.3.6. Pour tout entier x et y , on dira que x *divise* y (ou y est divisible par x) si $\exists k \in \mathbb{Z}$ ($kx = y$). On utilise la notation $x | y$ pour signifier « x divise y » et $x \nmid y$ signifie « x ne divise pas y ».

Par exemple, $4 | 20$, puisque $5 \cdot 4 = 20$, mais $4 \nmid 21$.

Théorème 3.3.7. Pour tous les entiers un, groupe c , si $un | b$ et $b | c$ alors $un | c$.

Preuve. Soient a , b et c des entiers arbitraires et supposons $a | b$ et $b | c$. Puisque $a | b$, on peut choisir un entier m tel que $ma = b$. De même, puisque $b | c$, on peut choisir un entier n tel que $nb = c$. Par conséquent $c = nb = nma$, donc puisque nm est un entier, $a | c$.

□

Commentaire. Le théorème dit $\forall a \in \mathbb{Z} \forall b \in \mathbb{Z} \forall c \in \mathbb{Z} (a | b \wedge b | c \rightarrow a | c)$, la méthode la plus naturelle consiste donc à poser a , b et c comme entiers arbitraires, à supposer $a | b$ et $b | c$, puis à prouver $a | c$. La première phrase de la preuve indique que cette stratégie est utilisée ; l'objectif de la suite de la preuve doit donc être de prouver que $a | c$. Ce n'est pas explicitement mentionné. Vous êtes censé le découvrir par vous-même en utilisant vos connaissances en stratégies de preuve. Vous pourriez même dresser une liste de données et d'objectifs pour vous aider à suivre ce qui est connu et ce qui reste à prouver au fil de la lecture de la preuve. À ce stade de la preuve, la liste se présente comme suit :

<i>Givens</i>	<i>Goal</i>
$a, b, \text{ and } c \text{ are integers}$	
$a b$	
$b c$	$a c$

Parce que le nouvel objectif signifie $\exists k \in \mathbb{Z} (ka = c)$, la preuve se poursuivra probablement en trouvant un entier k tel que $ka = c$. Comme pour de nombreuses démonstrations d'énoncés existentiels, la première étape pour trouver un tel k consiste à examiner de plus près les données. La phrase suivante de la démonstration utilise la donnée $a | b$ pour conclure que nous pouvons choisir un entier m tel que $ma = b$. La démonstration ne précise pas quelle règle d'inférence justifie cela. Il vous appartient de la déterminer en élaborant la forme logique de l'énoncé $a | b$, en utilisant la définition de *divide*. Car cette donnée signifie $\exists k \in \mathbb{Z} (ka = b)$, il faut comprendre que la règle d'inférence utilisée est l'instanciation existentielle. Cette instanciation est également utilisée dans la phrase suivante de la preuve pour justifier le choix d'un entier n tel que $nb = c$. Les équations $ma = b$ et $nb = c$ peuvent maintenant être ajoutées à la liste des données.

Certaines étapes ont également été omises dans la dernière phrase de la preuve. Nous nous attendions à ce que l'objectif $a | c$ soit démontré en trouvant un entier k tel que $ka = c$. De l'équation $c = nma$ et du fait que nm est un entier, il s'ensuit que $k = nm$ fonctionnera, mais la preuve n'indique pas explicitement que cette valeur de k est utilisée ; en fait, la variable k n'apparaît pas du tout dans la preuve. Bien sûr, la variable k n'apparaît pas non plus dans l'énoncé du théorème. Un lecteur de la preuve s'attendrait à ce que nous prouvions que $a | c$ en trouvant un entier qui, multiplié par a , donne la valeur c , mais à la lecture de l'énoncé du théorème, le lecteur n'aurait aucune raison de s'attendre à ce que cet entier soit nommé k . Attribuer ce nom à l'entier nm n'aurait donc pas facilité la compréhension de la preuve, nous ne l'avons donc pas fait.

Exercices

Remarque : Les exercices marqués du symbole ^PD peuvent être réalisés avec Proof Designer, un logiciel informatique disponible gratuitement sur Internet.

*1. Dans [l'exercice 7 de la section 2.2](#), vous avez utilisé des équivalences logiques pour montrer que $\exists x (P(x) \rightarrow Q(x))$ est équivalent à $\forall x P(x) \rightarrow \exists x Q(x)$. Utilisez maintenant les méthodes de cette section pour prouver que si $\exists x (P(x) \rightarrow Q(x))$ est vraie, alors $\forall x P(x) \rightarrow \exists x Q(x)$ est vraie. (Remarque : l'inverse de l'équivalence est beaucoup plus difficile à prouver. Voir [l'exercice 30 de la section 3.5](#).)

2. Démontrer que si A et $B \setminus C$ sont disjoints, alors $A \cap B \subseteq C$.

*3. Démontrer que si $A \subseteq B \setminus C$ alors A et C sont disjoints.

_D 4. Supposons que $A \subseteq \mathcal{P}(A)$. Démontrer que $\mathcal{P}(A) \subseteq \mathcal{P}(\mathcal{P}(A))$.

5. L'hypothèse du théorème démontré dans [l'exercice 4](#) est $A \subseteq \mathcal{P}(A)$.

(a) Pouvez-vous penser à un ensemble A pour lequel cette hypothèse est vraie ?

(b) Pouvez-vous en penser à un autre ?

6. Supposons que x soit un nombre réel.

(a) Démontrer que si $x \neq 1$ alors il existe un nombre réel y tel que $\frac{y+1}{y-2} = x$.

(b) Démontrer que s'il existe un nombre réel y tel que $\frac{y+1}{y-2} = x$ alors $x \neq 1$.

*7. Démontrer que pour tout nombre réel x , si $x > 2$ alors il existe un nombre réel y tel que $y + 1/y = x$.

_D 8. Démontrer que si \mathcal{F} est une famille d'ensembles et $A \in \mathcal{F}$, alors $A \subseteq \bigcup \mathcal{F}$.

*9. Démontrer que si \mathcal{F} est une famille d'ensembles et $A \in \mathcal{F}$, alors $\bigcap \mathcal{F} \subseteq A$.

10. Supposons que \mathcal{F} est une famille d'ensembles non vide, B est un ensemble et $\forall A \in \mathcal{F} (B \subseteq A)$. Démontrer que $B \subseteq \bigcap \mathcal{F}$.

11. Supposons que \mathcal{F} soit une famille d'ensembles. Démontrer que si $\emptyset \in \mathcal{F}$ alors $\bigcap \mathcal{F} = \emptyset$.

_D *12. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles. Démontrer que si $\mathcal{F} \subseteq \mathcal{G}$ alors $\bigcup \mathcal{F} \subseteq \bigcup \mathcal{G}$.

13. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles non vides. Démontrer que si $\mathcal{F} \subseteq \mathcal{G}$ alors $\bigcap \mathcal{G} \subseteq \bigcap \mathcal{F}$.

14. Supposons que $\{A_i \mid i \in I\}$ est une famille d'ensembles indexés.
Démontrer que $\bigcup_{i \in I} \mathcal{P}(A_i) \subseteq \mathcal{P}(\bigcup_{i \in I} A_i)$. (Indice : assurez-vous d'abord de bien comprendre la signification de toutes les notations !)

15. Supposons que $\{A_i \mid i \in I\}$ est une famille indexée d'ensembles et $I = \emptyset$. Démontrer que $\bigcap_{i \in I} A_i \in \bigcap_{i \in I} \mathcal{P}(A_i)$.

16. Démontrer la réciproque de l'énoncé démontré dans [l'exemple 3.3.5](#). Autrement dit, démontrer que si $\mathcal{F} \subseteq \mathcal{P}(B)$ alors $\bigcup \mathcal{F} \subseteq B$.

17. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles non vides, et que chaque élément de \mathcal{F} soit un sous-ensemble de chaque élément de \mathcal{G} . Démontrer que $\bigcup \mathcal{F} \subseteq \bigcap \mathcal{G}$.

18. Dans ce problème, toutes les variables sont comprises dans \mathbb{Z} , l'ensemble de tous les entiers.

- (a) Démontrer que si $a \mid b$ et $a \mid c$, alors $a \mid (b + c)$.
(b) Démontrer que si $ac \mid bc$ et $c \neq 0$, alors $a \mid b$.

19. (a) Démontrer que pour tous les nombres réels x et y , il existe un nombre réel z tel que $x + z = y - z$.

(b) L'affirmation de la partie (a) serait-elle correcte si « nombre réel » était remplacé par « entier » ? Justifiez votre réponse.

20. Considérons le théorème suivant :

Théorème. Pour chaque nombre réel x , $x^2 \geq 0$.

Quel est le problème avec la preuve suivante du théorème ?

Preuve . Supposons que non. Alors pour tout nombre réel x , $x^2 < 0$. En particulier, en remplaçant $x = 3$, on obtiendrait $9 < 0$, ce qui est clairement faux. Cette contradiction montre que pour tout nombre x , $x^2 \geq 0$.

□

21. Considérez le théorème incorrect suivant :

Théorème incorrect. Si $\forall x \in A (x \neq 0)$ et $A \subseteq B$ alors $\forall x \in B (x \neq 0)$.

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve . Supposons que $\forall x \in A (x \neq 0)$ et $A \subseteq B$. Soit x un élément arbitraire de A . Puisque $\forall x \in A (x \neq 0)$, nous pouvons conclure que $x \neq 0$. De plus, puisque $A \subseteq B$, $x \in B$. Puisque $x \in B$, $x \neq 0$, et x était arbitraire, nous pouvons conclure que $\forall x \in B (x \neq 0)$. □

(b) Trouver un contre-exemple au théorème. Autrement dit, trouver un exemple d'ensembles A et B pour lesquels les hypothèses du théorème sont vraies, mais la conclusion est fausse.

22. Considérez le théorème incorrect suivant :

Théorème incorrect. $\exists x \in \mathbb{R} \forall y \in \mathbb{R} (xy^2 = y - x)$.

Quel est le problème avec la preuve suivante du théorème ?

Preuve. Soit $x = y / (y^2 + 1)$. Alors

$$y - x = y - \frac{y}{y^2 + 1} = \frac{y^3}{y^2 + 1} = \frac{y}{y^2 + 1} \cdot y^2 = xy^2.$$

□

23. Considérez le théorème incorrect suivant :

Théorème incorrect. Supposer \mathcal{F} et \mathcal{G} sont des familles d'ensembles.

Si $\bigcup \mathcal{F}$ et $\bigcup \mathcal{G}$ sont disjoints, alors \mathcal{F} et \mathcal{G} sont disjoints.

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve. Supposons que $\bigcup \mathcal{F}$ et $\bigcup \mathcal{G}$ soient disjoints. Supposons que \mathcal{F} et \mathcal{G} ne soient pas disjoints. Alors, nous pouvons choisir un ensemble A tel que $A \in \mathcal{F}$ et $A \in \mathcal{G}$. Depuis $A \in \mathcal{F}$, par l'[exercice 8](#), $A \subseteq \bigcup \mathcal{F}$, donc tout élément de A est dans $\bigcup \mathcal{F}$. De même, puisque $A \in \mathcal{G}$, tout élément de A est dans $\bigcup \mathcal{G}$. Mais alors tout élément de A est à la fois dans $\bigcup \mathcal{F}$ et $\bigcup \mathcal{G}$, ce qui est impossible puisque $\bigcup \mathcal{F}$ et $\bigcup \mathcal{G}$ sont disjoints. Ainsi, nous avons atteint une contradiction, donc \mathcal{F} et \mathcal{G} doivent être disjoints .

□

(b) Trouvez un contre-exemple au théorème.

24. Considérons le théorème putatif suivant :

Théorème? Pour tous les nombres réels x et y , $x^2 + xy - 2y^2 = 0$.

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve. Soit x et y égaux à un nombre réel arbitraire r . Alors

$$x^2 + xy - 2y^2 = r^2 + r \cdot r - 2r^2 = 0.$$

Étant donné que x et y sont tous deux arbitraires, cela montre que pour tous les nombres réels x et y , $x^2 + xy - 2y^2 = 0$.

□

(b) Le théorème est-il correct ? Justifiez votre réponse par une preuve ou un contre-exemple.

25. Démontrer que pour tout nombre réel x , il existe un nombre réel y tel que pour tout nombre réel z , $yz = (x + z)^2 - (x^2 + z^2)$.

26. (a) En comparant les différentes règles de traitement des quantificateurs dans les preuves, vous devriez observer une similitude entre les règles pour les buts de la forme $\forall x P(x)$ et les données de la forme $\exists x P(x)$. Quelle est cette similitude ? Qu'en

est-il des règles pour les buts de la forme $\exists xP(x)$ et les données de la forme $\forall xP(x)$?

- (b) Pouvez-vous penser à une raison pour laquelle ces similitudes pourraient être attendues ? (Indice : réfléchissez au fonctionnement de la preuve par contradiction lorsque l'objectif commence par un quantificateur.)

3.4 Preuves impliquant des conjonctions et des biconditions

La méthode pour prouver un objectif de la forme $P \wedge Q$ est très simple :

Pour prouver un but de la forme $P \wedge Q$:

Prouver P et Q séparément.

En d'autres termes, un objectif de la forme $P \wedge Q$ est traité comme deux objectifs distincts : P , et Q . Il en va de même pour les données de la forme $P \wedge Q$:

Pour utiliser une donnée de la forme $P \wedge Q$:

Traitez ces données comme deux données distinctes : P et Q .

Nous avons déjà utilisé ces idées, sans les mentionner, dans certains de nos exemples précédents. Par exemple, la définition de x donné. $\epsilon A \setminus C$ dans [l'exemple 3.2.3](#) était $x \in A \wedge x \notin C$, mais nous l'avons traité comme deux données distinctes : $x \in A$, et $x \notin C$.

Exemple 3.4.1. Supposons que $A \subseteq B$, et que A et C soient disjoints. Démontrer que $A \subseteq B \setminus C$.

Travail à partir de zéro

<i>Givens</i>	<i>Goal</i>
$A \subseteq B$	$A \subseteq B \setminus C$
$A \cap C = \emptyset$	

En analysant la forme logique du but, nous voyons qu'il a la forme $\forall x (x \in A \rightarrow x \in B \setminus C)$, donc nous laissons x arbitraire, supposons $x \in A$, et essayez de prouver que $x \in B \setminus C$. Le nouvel objectif $x \in B \setminus C$ signifie $x \in B \wedge x \notin C$, donc selon notre stratégie, nous devrions diviser cela en deux objectifs, $x \in B$ et $x \notin C$, et les prouver séparément.

<i>Givens</i>	<i>Goals</i>
$A \subseteq B$	$x \in B$
$A \cap C = \emptyset$	$x \notin C$
$x \in A$	

La preuve finale aura cette forme :

Soit x arbitraire.

Supposons que $x \in UN$.

[Preuve de $x \in B$ va ici.]

[La preuve de $x \notin C$ va ici.]

Ainsi, $x \in B \wedge x \notin C$, donc $x \in B \setminus C$.

Par conséquent $x \in A \rightarrow x \in B \setminus C$.

Puisque x était arbitraire, $\forall x (x \in A \rightarrow x \in B \setminus C)$, donc $A \subseteq B \setminus C$.

Le premier but, $x \in B$, découle clairement du fait que $x \in A$ et $A \subseteq B$. Le deuxième objectif, $x \notin C$, découle de $x \in A$ et $A \cap C = \emptyset$. Vous pouvez voir Ceci en analysant la forme logique de l'énoncé $A \cap C = \emptyset$. C'est un énoncé négatif, mais on peut le reformuler comme un énoncé positif équivalent :

$A \cap C = \emptyset$ is equivalent to $\neg \exists y(y \in A \wedge y \in C)$ (definitions of \cap and \emptyset),
which is equivalent to $\forall y \neg(y \in A \wedge y \in C)$ (quantifier negation law),
which is equivalent to $\forall y(y \notin A \vee y \notin C)$ (De Morgan's law),
which is equivalent to $\forall y(y \in A \rightarrow y \notin C)$ (conditional law).

En remplaçant x par y dans cette dernière instruction, nous voyons que $x \in A \rightarrow x \notin C$, et puisque nous connaissons déjà $x \in A$, nous pouvons conclure que $x \notin C$.

Solution

Théorème. Supposer $A \subseteq B$, et UN et C sont disjoints. Alors $UN \subseteq B \setminus C$.

Preuve. Supposons que $x \in A$. Puisque $A \subseteq B$, il s'ensuit que $x \in B$, et puisque A et C sont disjoints, nous devons avoir $x \notin C$. Ainsi, $x \in B \setminus C$. Puisque x est un élément arbitraire de A , nous pouvons conclure que $A \subseteq B \setminus C$.

□

Grâce à nos stratégies de travail avec les conjonctions, nous pouvons maintenant déterminer la manière appropriée de traiter les énoncés de la forme $P \leftrightarrow Q$ dans les preuves. Puisque $P \leftrightarrow Q$ est équivalent à $(P \rightarrow Q) \wedge (Q \rightarrow P)$, selon nos stratégies, une donnée ou un objectif de la forme $P \leftrightarrow Q$ doit être traité comme deux données ou objectifs distincts : $P \rightarrow Q$ et $Q \rightarrow P$.

Pour prouver un but de la forme $P \leftrightarrow Q$:

Démontrer que $P \rightarrow Q$ et $Q \rightarrow P$ séparément.

Pour utiliser une donnée de la forme $P \leftrightarrow Q$:

Traitez cela comme deux données distinctes : $P \rightarrow Q$ et $Q \rightarrow P$.

Ceci est illustré dans l'exemple suivant, dans lequel nous utilisons les définitions suivantes.

Définition 3.4.2. Un entier x est *pair* si $\exists k \in \mathbb{Z}$ ($x = 2k$), et x est *impair* si $\exists k \in \mathbb{Z}$ ($x = 2k + 1$).

Nous utilisons également le fait que tout entier est pair ou impair, mais pas les deux. Pour une démonstration de ce fait, voir [l'exercice 16](#) de la [section 6.1](#).

Exemple 3.4.3. Supposons que x soit un entier. Démontrer que x est pair ssi x^2 est pair.

Travail à partir de zéro

L'objectif est $(x \text{ est pair}) \leftrightarrow (x^2 \text{ est pair})$. Nous prouvons donc les deux objectifs $(x \text{ est pair}) \rightarrow (x^2 \text{ est pair})$ et $(x^2 \text{ est pair}) \rightarrow (x \text{ est pair})$ séparément. Pour le premier, nous supposons que x est pair et prouvons que x^2 est pair :

<i>Givens</i>	<i>Goal</i>
$x \in \mathbb{Z}$ x is even	x^2 is even

Écrire la définition de *même* dans le donné et dans le but révélera leurs formes logiques :

<i>Givens</i>	<i>Goal</i>
$x \in \mathbb{Z}$ $\exists k \in \mathbb{Z}(x = 2k)$	$\exists k \in \mathbb{Z}(x^2 = 2k)$

Puisque la seconde donnée commence par $\exists k$, nous l'utilisons immédiatement et posons k comme un entier particulier pour lequel l'affirmation $x = 2k$ est vraie. Nous avons ainsi deux nouvelles données : $k \in \mathbb{Z}$ et $x = 2k$.

<i>Givens</i>	<i>Goal</i>
$x \in \mathbb{Z}$	
$k \in \mathbb{Z}$	
$x = 2k$	

L'objectif commence par $\exists k$, mais comme k représente déjà un nombre particulier, on ne peut pas *lui attribuer une nouvelle valeur* pour prouver l'objectif. Il faut donc utiliser une autre lettre, par exemple j . Une façon de comprendre cela est de réécrire l'objectif sous la forme équivalente $\exists j \in \mathbb{Z} (x^2 = 2j)$. Pour prouver cet objectif, nous devons trouver une valeur à remplacer par j . Il doit s'agir d'un entier et satisfaire l'équation $x^2 = 2j$. En utilisant l'équation donnée $x = 2k$, nous voyons que $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$, il semble donc que la bonne valeur à choisir pour j soit $j = 2k^2$. De toute évidence, $2k^2$ est un entier, donc ce choix pour j fonctionnera pour compléter la preuve de notre premier objectif.

Pour démontrer le deuxième objectif $(x^2 \text{ est pair}) \rightarrow (x \text{ est pair})$, nous démontrerons la contraposée $(x \text{ n'est pas pair}) \rightarrow (x^2 \text{ n'est pas pair})$. Puisque tout entier est pair ou impair, mais pas les deux, cela équivaut à $(x \text{ est impair}) \rightarrow (x^2 \text{ est impair})$.

<i>Givens</i>	<i>Goal</i>
$x \in \mathbb{Z}$ x is odd	x^2 is odd

Les étapes sont maintenant assez similaires à la première partie de la preuve. Comme précédemment, nous commençons par écrire la définition d'*impair* dans la seconde donnée et dans l'Objectif. Cette fois, pour éviter le conflit de noms de variables rencontré dans la première partie de la preuve, nous utilisons des noms différents pour les variables liées dans les deux instructions.

$$\begin{array}{ccc} \text{Givens} & & \text{Goal} \\ x \in \mathbb{Z} & & \exists j \in \mathbb{Z}(x^2 = 2j + 1) \\ \exists k \in \mathbb{Z}(x = 2k + 1) & & \end{array}$$

Ensuite, nous utilisons la deuxième donnée et laissons k représenter un entier particulier pour lequel $x = 2k + 1$.

$$\begin{array}{ccc} \text{Givens} & & \text{Goal} \\ x \in \mathbb{Z} & & \exists j \in \mathbb{Z}(x^2 = 2j + 1) \\ k \in \mathbb{Z} & & \\ x = 2k + 1 & & \end{array}$$

Nous devons maintenant trouver un entier j tel que $x^2 = 2j + 1$. En remplaçant x par $2k + 1$, nous obtenons $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, donc $j = 2k^2 + 2k$ semble être le bon choix.

Avant de rédiger la preuve finale, quelques remarques explicatives s'imposent. Les deux énoncés conditionnels que nous avons prouvés peuvent être considérés comme représentant les deux directions \rightarrow et \leftarrow du symbole biconditionnel \leftrightarrow dans l'objectif initial. Ces deux parties de la preuve sont parfois désignées par les symboles \rightarrow et \leftarrow . Dans chaque partie, nous prouvons un énoncé affirmant l'existence d'un nombre possédant certaines propriétés. Nous avons appelé ce nombre j dans le travail préliminaire, mais notez que j n'était pas mentionné explicitement dans l'énoncé du problème. Comme dans la preuve du [théorème 3.3.7](#), nous avons choisi de ne pas mentionner j explicitement dans la preuve finale.

Solution

Théorème. *Supposer x est un entier. Alors x est pair si et seulement si x^2 est pair .*

Preuve. (\rightarrow) Supposons que x soit pair. Alors, pour un entier k , $x = 2k$. Par conséquent, $x^2 = 4k^2 = 2(2k^2)$, donc puisque $2k^2$ est un entier, x^2 est pair. Ainsi, si x est pair, alors x^2 est pair.

(\leftarrow) Supposons que x soit impair. Alors $x = 2k + 1$ pour un entier k . Par conséquent, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, donc puisque $2k^2 + 2k$ est un entier, x^2 est impair. Ainsi, si x^2 est pair alors x est pair.

□

Grâce aux techniques de preuve que nous avons développées, nous pouvons maintenant vérifier certaines des équivalences que nous n'avons pu justifier que par des raisons intuitives au [chapitre 2](#). À titre d'exemple, prouvons que les formules $\forall x \neg P(x)$ et $\neg \exists x P(x)$ sont équivalentes. Dire que ces formules sont équivalentes signifie qu'elles auront toujours la même valeur de vérité. Autrement dit, quelle que soit la signification de $P(x)$, l'énoncé $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$ sera vrai. Nous pouvons le démontrer grâce à notre technique de démonstration des énoncés biconditionnels.

Exemple 3.4.4. Démontrer que $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$.

Travail à partir de zéro

(\rightarrow) Il faut prouver $\forall x \neg P(x) \rightarrow \neg \exists x P(x)$. On suppose donc $\forall x \neg P(x)$ et on essaie de prouver $\neg \exists x P(x)$. Notre objectif est maintenant une proposition négative, et sa réexpression nécessiterait l'utilisation de l'équivalence même que nous cherchons à prouver ! Nous avons donc recours à notre seule autre stratégie pour traiter les objectifs négatifs : la preuve par contradiction. Nous nous trouvons alors dans la situation suivante :

<i>Givens</i>	<i>Goal</i>
$\forall x \neg P(x)$	
$\exists x P(x)$	Contradiction

La seconde donnée commence par un quantificateur existentiel ; nous l'utilisons donc immédiatement et posons x_0 comme objet pour lequel l'énoncé $P(x_0)$ est vrai. Mais en remplaçant x_0 par x dans la première donnée, nous pouvons conclure que $\neg P(x_0)$, ce qui nous donne la contradiction recherchée.

(\leftarrow) Pour cette direction de la biconditionnelle, on suppose $\neg \exists x P(x)$ et on essaie de prouver $\forall x \neg P(x)$. Puisque cet objectif part d'un quantificateur universel, on pose x comme arbitraire et on essaie de prouver $\neg P(x)$. De nouveau, on a un objectif négatif qui ne peut être réexprimé, on utilise donc la preuve par contradiction :

<i>Givens</i>	<i>Goal</i>
$\neg \exists x P(x)$	
$P(x)$	Contradiction

Notre première donnée est également une affirmation négative, ce qui suggère que nous pourrions obtenir la contradiction dont nous avons besoin en prouvant $\exists x P(x)$. Nous nous fixons donc cet objectif.

<i>Givens</i>	<i>Goal</i>
$\neg \exists x P(x)$	
$P(x)$	$\exists x P(x)$

Pour éviter de confondre x , variable libre dans la seconde donnée (x arbitraire introduit plus tôt dans la preuve), avec x , variable liée dans l'objectif, il serait judicieux de réécrire l'objectif sous la forme équivalente $\exists y P(y)$. Pour prouver cet objectif, il faut trouver une valeur de y qui rend $P(y)$ vrai. Mais c'est facile ! Notre deuxième donnée, $P(x)$, nous indique que notre x arbitraire est la valeur dont nous avons besoin.

Solution

Théorème. $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$.

Preuve. (\rightarrow) Supposons $\forall x \neg P(x)$, et supposons $\exists x P(x)$. Alors on peut choisir un x_0 tel que $P(x_0)$ soit vrai. Mais puisque $\forall x \neg P(x)$, on peut conclure que $\neg P(x_0)$, et c'est une contradiction. Donc $\forall x \neg P(x) \rightarrow \neg \exists x P(x)$.

(\leftarrow) Supposons $\neg \exists x P(x)$. Soit x arbitraire, et supposons $P(x)$. Puisque nous avons un x spécifique pour lequel $P(x)$ est vrai, il s'ensuit que $\exists x P(x)$, ce qui est une contradiction. Par conséquent, $\neg P(x)$. Puisque x était arbitraire, nous pouvons conclure que $\forall x \neg P(x)$, donc $\neg \exists x P(x) \rightarrow \forall x \neg P(x)$.

□

Parfois, dans une preuve d'un objectif de la forme $P \leftrightarrow Q$, les étapes de la preuve de $Q \rightarrow P$ sont les mêmes que celles utilisées pour prouver $P \rightarrow Q$, mais dans l'ordre inverse. Dans ce cas, vous pouvez simplifier la preuve en l'écrivant sous la forme d'une chaîne d'équivalences, commençant par P et terminant par Q . Par exemple, supposons que vous trouviez que vous pouvez prouver $P \rightarrow Q$ en supposant d'abord P , puis en utilisant P pour inférer une autre affirmation R , puis en utilisant R pour déduire Q ; et supposons que les mêmes étapes puissent être utilisées, dans l'ordre inverse, pour prouver que $Q \rightarrow P$. En d'autres termes, vous pourriez supposer Q , utiliser cette hypothèse pour conclure que R est vraie, puis utiliser R pour prouver P . Puisque vous affirmeriez à la fois $P \rightarrow R$ et $R \rightarrow P$, vous pourriez résumer ces deux étapes en disant $P \leftrightarrow R$. De même, les deux autres étapes de la preuve vous indiquent que $R \leftrightarrow Q$. Ces deux affirmations impliquent l'objectif $P \leftrightarrow Q$. Les mathématiciens présentent parfois ce type de preuve en écrivant simplement la chaîne d'équivalences

P si et seulement R si et seulement Q .

Vous pouvez considérer cela comme une abréviation de « P ssi R et R ssi Q (et donc P ssi Q) ». Ceci est illustré dans l'exemple suivant.

Exemple 3.4.5. Supposons que A , B et C sont des ensembles. Démontrer que $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Travail à partir de zéro

Comme nous l'avons vu au [chapitre 2](#), l'équation $A \cap (B \setminus C) = (A \cap B) \setminus C$ signifie $\forall x (x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, mais elle est également équivalente à l'énoncé $[A \cap (B \setminus C) \subseteq (A \cap B) \setminus C] \wedge [(A \cap B) \setminus C \subseteq A \cap (B \setminus C)]$. Ceci suggère deux approches pour la preuve. On pourrait poser x comme arbitraire, puis prouver $x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C$, ou nous pourrions prouver les deux affirmations $A \cap (B \setminus C) \subseteq (A \cap B) \setminus C$ et $(A \cap B) \setminus C \subseteq A \cap (B \setminus C)$. En fait, presque toutes les preuves que deux ensembles sont égaux impliqueront l'une de ces deux approches. Dans ce cas, nous utiliserons la première approche, donc une fois que nous aurons introduit notre x *arbitraire*, nous aurons un objectif ssi.

Pour la moitié (\rightarrow) de la preuve, nous supposons $x \in A \cap (B \setminus C)$ et essayez de prouver $x \in (A \cap B) \setminus C$:

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ x \in A \cap (B \setminus C) & & x \in (A \cap B) \setminus C \end{array}$$

Pour voir les formes logiques du donné et du but, nous écrivons leurs définitions comme suit :

$$\begin{aligned} x \in A \cap (B \setminus C) \text{ iff } & x \in A \wedge x \in B \setminus C \text{ iff } x \in A \wedge x \in B \wedge x \notin C; \\ x \in (A \cap B) \setminus C \text{ iff } & x \in A \cap B \wedge x \notin C \text{ iff } x \in A \wedge x \in B \wedge x \notin C. \end{aligned}$$

À ce stade, il est clair que la donnée implique le but, puisque les dernières étapes des deux chaînes d'équivalences se sont avérées identiques. De plus, il est clair que le raisonnement dans le sens (\leftarrow) de la preuve sera exactement le même, mais avec les colonnes donnée et but inversées. Ainsi, nous pourrions essayer de raccourcir la preuve en l'écrivant sous la forme d'une chaîne d'équivalences commençant par $x \in A \cap (B \setminus C)$ et se terminant par $x \in (A \cap B) \setminus C$. Dans ce cas, si nous commençons par $x \in$ En suivant la première chaîne d' *équivalences affichée ci-dessus*, on obtient une affirmation identique à la dernière affirmation de la deuxième chaîne. On peut ensuite poursuivre en suivant la deuxième chaîne d'équivalences *à l'envers*, en terminant par $x \in (A \cap B) \setminus C$.

Solution

Théorème. Supposer UN , Groupe C sont des ensembles. Alors $UN \cap (B \setminus C) = (UN \cap B) \setminus C$.

Preuve. Soit x arbitraire. Alors

$$\begin{aligned}
x \in A \cap (B \setminus C) &\iff x \in A \wedge x \in B \setminus C \\
&\iff x \in A \wedge x \in B \wedge x \notin C \\
&\iff x \in (A \cap B) \wedge x \notin C \\
&\iff x \in (A \cap B) \setminus C.
\end{aligned}$$

Ainsi, $\forall x (x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, donc $A \cap (B \setminus C) = (A \cap B) \setminus C$.

□

La technique consistant à déterminer une suite d'équivalences dans un ordre, puis à l'écrire dans l'ordre inverse, est fréquemment utilisée dans les démonstrations. L'ordre des étapes de la démonstration finale est déterminé par notre règle selon laquelle une assertion ne doit jamais être formulée tant qu'elle n'est pas justifiée. En particulier, si vous essayez de prouver $P \leftrightarrow Q$, il est erroné de commencer la démonstration par l'affirmation non justifiée $P \leftrightarrow Q$, puis de déterminer la signification des deux membres P et Q , en montrant qu'ils sont identiques. Il est préférable de commencer par les équivalences justifiables et de les enchaîner pour justifier l'objectif $P \leftrightarrow Q$ avant d'affirmer cet objectif. Une technique similaire peut parfois être utilisée pour déterminer les démonstrations d'équations, comme le montre l'exemple suivant.

Exemple 3.4.6. Démontrer que pour tout nombre réel a et b ,

$$(a + b)^2 - 4(a - b)^2 = (3b - a)(3a - b).$$

Travail à partir de zéro

L'objectif est de la forme $\forall a \forall b ((a + b)^2 - 4(a - b)^2 = (3b - a)(3a - b))$, donc on commence par poser a et b comme nombres réels arbitraires et on essaie de prouver l'équation. La multiplication des deux côtés donne :

$$\begin{aligned}
(a + b)^2 - 4(a - b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2) \\
&= -3a^2 + 10ab - 3b^2; \\
(3b - a)(3a - b) &= 9ab - 3a^2 - 3b^2 + ab = -3a^2 + 10ab - 3b^2.
\end{aligned}$$

Il est clair que les deux côtés sont égaux. La façon la plus simple d'en faire la preuve est d'écrire une chaîne d'égalités commençant par $(a + b)^2 - 4(a - b)^2$ et se terminant par $(3b - a)(3a - b)$. Pour ce faire, nous pouvons recopier la première chaîne d'égalités affichée ci-dessus, puis la suivre de la dernière ligne, écrite à l'envers.

Solution

Théorème. Pour tout nombre réel a et b ,

$$(a + b)^2 - 4(a - b)^2 = (3b - a)(3a - b).$$

Preuve. Soient a et b des nombres réels arbitraires. Alors

$$\begin{aligned}(a+b)^2 - 4(a-b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2) \\&= -3a^2 + 10ab - 3b^2 \\&= 9ab - 3a^2 - 3b^2 + ab = (3b-a)(3a-b).\end{aligned}$$

□

Nous terminons cette section en présentant une autre preuve sans travail préliminaire, mais avec un commentaire pour vous aider à lire la preuve.

Théorème 3.4.7. Pour chaque entier n , $6 \mid n$ ssi $2 \mid n$ et $3 \mid n$.

Preuve. Soit n un entier arbitraire.

(→) Supposons $6 \mid n$. On peut alors choisir un entier k tel que $6k = n$. Par conséquent $n = 6k = 2(3k)$, donc $2 \mid n$, et de même $n = 6k = 3(2k)$, donc $3 \mid n$.

(←) Supposons $2 \mid n$ et $3 \mid n$. On peut alors choisir des entiers j et k tels que $n = 2j$ et $n = 3k$. Par conséquent $6(j-k) = 6j - 6k = 3(2j) - 2(3k) = 3n - 2n = n$, donc $6 \mid n$.

□

Commentaire. L'énoncé à prouver est $\forall n \in \mathbb{Z} [6 \mid n \leftrightarrow ((2 \mid n) \wedge (3 \mid n))]$, et la stratégie la plus naturelle pour prouver un objectif de cette forme est de poser n comme arbitraire, puis de prouver séparément les deux directions de la biconditionnelle. Il devrait être clair que c'est la stratégie utilisée dans la preuve.

Pour la direction gauche-droite de la biconditionnelle, nous supposons $6 \mid n$, puis prouvons $2 \mid n$ et $3 \mid n$, en considérant ces deux objectifs comme distincts. L'introduction de l'entier k se justifie par l'instanciation existentielle, puisque l'hypothèse $6 \mid n$ signifie $\exists k \in \mathbb{Z} (6k = n)$. À ce stade de la preuve, nous avons les données et objectifs suivants :

Givens	Goals
$n \in \mathbb{Z}$	$2 \mid n$
$k \in \mathbb{Z}$	$3 \mid n$
$6k = n$	

Le premier objectif, $2 \mid n$, signifie $\exists j \in \mathbb{Z} (2j = n)$, nous devons donc trouver un entier j tel que $2j = n$. Bien que la preuve ne le dise pas explicitement, l'équation $n = 2(3k)$, qui en est dérivée, suggère que la valeur utilisée pour j est $j = 3k$. Clairement, $3k$ est un entier (une autre étape sautée dans la preuve), donc ce choix pour j fonctionne. La preuve de $3 \mid n$ est similaire.

Français Pour le sens de droite à gauche, nous supposons $2 \mid n$ et $3 \mid n$ et prouvons $6 \mid n$. Une fois de plus, l'introduction de j et k est justifiée

par l'instanciation existentielle. Aucune explication n'est donnée quant à la raison pour laquelle nous devrions calculer $6(j - k)$, mais une preuve n'a pas besoin de fournir de telles explications. La raison du calcul devrait devenir claire lorsque, de manière surprenante, il s'avère que $6(j - k) = n$. De telles surprises font partie du plaisir de travailler avec des preuves. Comme dans la première moitié de la preuve, puisque $j - k$ est un entier, cela montre que $6 \mid n$.

Exercices

- *1. Utilisez les méthodes de ce chapitre pour prouver que $\forall x (P(x) \wedge Q(x))$ est équivalent à $\forall x P(x) \wedge \forall x Q(x)$.
- \exists 2. Démontrer que si $A \subseteq B$ et $A \subseteq C$ alors $A \subseteq B \cap C$.
- \exists 3. Supposons que $A \subseteq B$. Démontrer que pour tout ensemble C , $C \setminus B \subseteq C \setminus A$.
- \exists *4. Démontrer que si $A \subseteq B$ et $A \not\subseteq C$ alors $B \not\subseteq C$.
- \exists 5. Démontrer que si $A \subseteq B \setminus C$ et $A \neq \emptyset$ alors $B \not\subseteq C$.
- 6. Démontrer que pour tout ensemble A , B et C , $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$, en trouvant une chaîne d'équivalences commençant par $x \in A \setminus (B \cap C)$ et se terminant par $x \in (A \setminus B) \cup (A \setminus C)$. (Voir [l'exemple 3.4.5](#).)
- \exists *7. Utilisez les méthodes de ce chapitre pour prouver que pour tous les ensembles A et B , $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
- \exists 8. Démontrer que $A \subseteq B$ ssi $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- *9. Démontrer que si x et y sont des entiers impairs, alors xy est impair.
- 10. Démontrer que si x et y sont des entiers impairs, alors $x - y$ est pair.
- 11. Démontrer que pour tout entier n , n^3 est pair ssi n est pair.
- 12. Considérons le théorème putatif suivant :

Théorème? *Supposer m est un entier pair et n est un entier impair. Alors $n^2 - m^2 = n + m$.*

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve. Puisque m est pair, on peut choisir un entier k tel que $m = 2k$. De même, puisque n est impair, on a $n = 2k + 1$. Par conséquent

$$\begin{aligned} n^2 - m^2 &= (2k+1)^2 - (2k)^2 = 4k^2 + 4k + 1 - 4k^2 = 4k + 1 \\ &= (2k+1) + (2k) = n + m. \end{aligned}$$

(b) Le théorème est-il correct ? Justifiez votre réponse par une preuve ou un contre-exemple.

13. Démontrer que $\forall x \in \mathbb{R} [\exists y \in \mathbb{R} (x + y = xy) \leftrightarrow x = 1]$.

14. Démontrer que $\exists z \in \mathbb{R} \forall x \in \mathbb{R}^+ [\exists y \in \mathbb{R} (y - x = y/x) \leftrightarrow x = z]$.

D 15. Supposons que B soit un ensemble et \mathcal{F} une famille d'ensembles.

Démontrer que $\bigcup \{A \setminus B \mid A \in \mathcal{F}\} \subseteq \bigcup (F \setminus \mathcal{P}(B))$.

16. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles non vides et que tout élément de \mathcal{F} soit disjoint d'un élément de \mathcal{G} . Démontrer que $\bigcup \mathcal{F}$ et $\bigcup \mathcal{G}$ sont disjoints.

D 17. Démontrer que pour tout ensemble A , $A = \bigcup \mathcal{P}(A)$.

*18. Supposons que \mathcal{F} et \mathcal{G} sont des familles d'ensembles.

(a) Démontrer que $\bigcup (\mathcal{F} \cap \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$.

(b) Quel est le problème avec la preuve suivante selon laquelle $(\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G}) \subseteq \bigcup (\mathcal{F} \cap \mathcal{G})$?

Preuve. Supposons que $x \in (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$. Cela signifie que $x \in \bigcup \mathcal{F}$ et $x \in \bigcup \mathcal{G}$, donc $\exists A \in \mathcal{F} (x \in A)$ et $\exists B \in \mathcal{G} (x \in B)$. Ainsi, nous pouvons choisir un ensemble A tel que $A \in \mathcal{F}, A \in \mathcal{G}$ et $x \in A$. Depuis $A \in \mathcal{F}$ et $A \in \mathcal{G}$, $A \in \mathcal{F} \cap \mathcal{G}$. Par conséquent $\exists A \in \mathcal{F} \cap \mathcal{G} (x \in A)$, donc $x \in \bigcup (\mathcal{F} \cap \mathcal{G})$. Puisque x est arbitraire, nous pouvons conclure que $(\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G}) \subseteq \bigcup (\mathcal{F} \cap \mathcal{G})$. \square

(c) Trouvez un exemple de familles d'ensembles \mathcal{F} et \mathcal{G} pour lesquels $\bigcup (\mathcal{F} \cap \mathcal{G}) \neq (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$.

D 19. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles. Démontrer que $(\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G}) \subseteq \bigcup (\mathcal{F} \cap \mathcal{G})$ ssi $\forall A \in \mathcal{F} \forall B \in \mathcal{G} (A \cap B \subseteq \bigcup (\mathcal{F} \cap \mathcal{G}))$.

D 20. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles. Démontrer que $\bigcup \mathcal{F}$ et $\bigcup \mathcal{G}$ sont disjoints ssi pour tout $A \in \mathcal{F}$ et $B \in \mathcal{G}$, A et B sont disjoints.

D 21. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles.

(a) Démontrer que $(\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G}) \subseteq \bigcup (\mathcal{F} \setminus \mathcal{G})$.

(b) Quel est le problème avec la preuve suivante selon laquelle $\bigcup (\mathcal{F} \setminus \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$?

Preuve. Supposons que $x \in \bigcup(\mathcal{F} \setminus \mathcal{G})$. Alors nous pouvons choisir un $A \in \mathcal{F}$ tel que $x \in A$. Depuis $A \in \mathcal{F}, A \in \mathcal{G}$ et $A \not\in \mathcal{G}$. Puisque $x \in A$ et $A \in \mathcal{F}$, $x \in \bigcup \mathcal{F}$. Puisque $x \in A$ et $A \notin \mathcal{G}$, $x \notin \bigcup \mathcal{G}$. Par conséquent $x \in (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$.

(c) Démontrer que $\bigcup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$ ssi $\forall A \in (\mathcal{F} \setminus \mathcal{G}) \forall B \in \mathcal{G}(A \cap B = \emptyset)$. \square

(d) Trouvez un exemple de familles d'ensembles \mathcal{F} et \mathcal{G} pour lesquels $\bigcup(\mathcal{F} \setminus \mathcal{G}) \neq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$.

*22. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles. Démontrer que si $\bigcup \mathcal{F} \cup \bigcup \mathcal{G}$, alors il existe un $A \in \mathcal{F}$ tel que pour tout $B \in \mathcal{G}, A \cup B$

23. Supposons que B soit un ensemble, $\{A_i \mid i \in I\}$ est une famille indexée d'ensembles, et $I \neq \emptyset$.

(a) Quelles stratégies de preuve sont utilisées dans la preuve suivante de l'équation $B \cap (\bigcup_{i \in J_e} A_i) = \bigcup_{i \in J_e} (B \cap A_i)$?

Preuve. Soit x arbitraire. Supposons que $x \in B \cap (\bigcup_{i \in J_e} A_i)$. Alors $x \in B$ et $x \in \bigcup_{i \in J_e} A_i$, donc nous pouvons choisir certains $i_0 \in J_e$ tel que $x \in A_{i_0}$. Puisque $x \in B$ et $x \in A_{i_0}$, $x \in B \cap A_{i_0}$. Par conséquent $x \in \bigcup_{i \in J_e} (B \cap A_i)$.

Supposons maintenant que $x \in \bigcup_{i \in J_e} (B \cap A_i)$. Alors nous pouvons choisir un $i_0 \in J_e$ tel que $x \in B \cap A_{i_0}$. Par conséquent $x \in B$ et $x \in A_{i_0}$. Puisque $x \in A_{i_0}$, $x \in \bigcup_{i \in J_e} A_i$. Puisque $x \in B$ et $x \in \bigcup_{i \in J_e} A_i$, $x \in B \cap (\bigcup_{i \in J_e} A_i)$.

Puisque x était arbitraire, nous avons montré que $\forall x [x \in B \cap (\bigcup_{i \in J_e} A_i) \leftrightarrow x \in \bigcup_{i \in J_e} (B \cap A_i)]$, donc $B \cap (\bigcup_{i \in J_e} A_i) = \bigcup_{i \in J_e} (B \cap A_i)$.

\square

(b) Démontrer que $B \setminus (\bigcup_{i \in J_e} A_i) = \bigcup_{i \in J_e} (B \setminus A_i)$.

(c) Pouvez-vous découvrir et prouver un théorème similaire sur $B \setminus (\bigcup_{i \in J_e} A_i)$? (Indice : essayez de deviner le théorème, puis essayez de le prouver. Si vous ne pouvez pas terminer la preuve, c'est peut-être parce que votre supposition était erronée. Modifiez votre supposition et réessayez.)

24. Supposons que $\{A_i \mid i \in J_e\}$ et $\{B_i \mid i \in I\}$ sont des familles d'ensembles indexées et $I \neq \emptyset$.

- (a) Démontrer que $\bigcup_{i \in Je} (A_i \setminus B_i) \subseteq (\bigcup_{i \in Je} A_i) \setminus (\bigcup_{i \in I} B_i)$.
- (b) Trouvez un exemple pour lequel $\bigcup_{i \in Je} (A_i \setminus B_i) \neq (\bigcup_{i \in Je} A_i) \setminus (\bigcup_{i \in Je} B_i)$.
25. Supposons que $\{A_i \mid i \in Je\}$ et $\{B_i \mid i \in I\}$ sont des familles d'ensembles indexées.
- (a) Démontrer que $\bigcup_{i \in Je} (A_i \cap B_i) \subseteq (\bigcup_{i \in Je} A_i) \cap (\bigcup_{i \in Je} B_i)$.
- (b) Trouvez un exemple pour lequel $\bigcup_{i \in Je} (A_i \cap B_i) \neq (\bigcup_{i \in Je} A_i) \cap (\bigcup_{i \in Je} B_i)$.
26. Démontrer que pour tous les entiers a et b , il existe un entier c tel que $a \mid c$ et $b \mid c$.
27. (a) Démontrer que pour tout entier n , $15 \mid n$ ssi $3 \mid n$ et $5 \mid n$.
- (b) Démontrer qu'il n'est pas vrai que pour tout entier n , $60 \mid n$ ssi $6 \mid n$ et $10 \mid n$.

3.5 Preuves impliquant des disjonctions

Supposons qu'une donnée de votre preuve soit de la forme $P \vee Q$. Cette donnée vous indique que P ou Q est vraie, mais ne vous dit pas laquelle. Ainsi, vous devez prendre en compte deux possibilités. Une façon de faire la preuve serait de les considérer tour à tour. Autrement dit, supposez d'abord que P est vraie et utilisez cette hypothèse pour prouver votre objectif. Supposez ensuite que Q est vraie et donnez une autre preuve que l'objectif est vrai. Bien que vous ne sachiez pas laquelle de ces hypothèses est correcte, la donnée $P \vee Q$ vous indique que *l'une* d'elles doit l'être. Quelle qu'elle soit, vous avez démontré qu'elle implique l'objectif. Ainsi, l'objectif doit être vrai.

Les deux possibilités considérées séparément dans ce type de preuve – la possibilité que P soit vraie et la possibilité que Q soit vraie – sont appelées *cas*. La valeur donnée de $P \vee Q$ justifie l'utilisation de ces deux cas en garantissant qu'ils couvrent toutes les possibilités. Les mathématiciens disent dans cette situation que les cas sont *exhaustifs*. Toute preuve peut être décomposée en deux ou plusieurs cas à tout moment, à condition que ces cas soient exhaustifs.

Pour utiliser une donnée de la forme $P \vee Q$:

Décomposez votre preuve en cas. Pour le cas 1, supposez que P est vraie et utilisez cette hypothèse pour prouver l'objectif. Pour le cas 2, supposez que Q est vraie et fournissez une autre preuve de l'objectif.

Travail à partir de zéro

Avant d'utiliser la stratégie :

<i>Givens</i>	<i>Goal</i>
$P \vee Q$	—
—	—

Après avoir utilisé la stratégie :

Case 1:	<i>Givens</i>	<i>Goal</i>
	P	—
	—	—
Case 2:	<i>Givens</i>	<i>Goal</i>
	Q	—
	—	—

Forme de l'épreuve finale :

Cas 1. P est vrai.

[La preuve du but va ici.]

Cas 2. Q est vrai.

[La preuve du but va ici.]

Puisque nous connaissons $P \vee Q$, ces cas couvrent toutes les possibilités. Par conséquent, l'objectif doit être vrai.

Exemple 3.5.1. Supposons que A , B et C soient des ensembles. Démontrer que si $A \subseteq C$ et $B \subseteq C$ alors $A \cup B \subseteq C$.

Travail à partir de zéro

On suppose que $A \subseteq C$ et $B \subseteq C$, et on prouve que $A \cup B \subseteq C$. L'écriture du but à l'aide de symboles logiques nous donne les données et le but suivants :

<i>Givens</i>	<i>Goal</i>
$A \subseteq C$	$\forall x(x \in A \cup B \rightarrow x \in C)$
$B \subseteq C$	—

Pour prouver l'objectif, nous laissons x arbitraire, supposons $x \in A \cup B$, et essayez de prouver $x \in C$. Ainsi, nous avons maintenant un nouveau x donné $\in A \cup B$, que nous écrivons $x \in A \vee x \in B$, et notre objectif est maintenant $x \in C$.

<i>Givens</i>	<i>Goal</i>
$A \subseteq C$	$x \in C$
$B \subseteq C$	—
$x \in A \vee x \in B$	—

Comme l'objectif ne peut être analysé plus en détail à ce stade, nous examinons de plus près les données. La première donnée sera utile si nous rencontrons un objet élément de A , car elle nous permettrait de conclure immédiatement que cet objet doit également être élément de C . De même, la deuxième donnée sera utile si nous rencontrons un élément de B . Gardant à l'esprit que nous devons être attentifs aux éléments de A ou B qui pourraient apparaître, nous passons à la troisième donnée. Comme cette donnée est de forme $P \vee Q$, nous tentons une démonstration par cas. Pour le premier cas, nous

supposons $x \in A$, et pour le second nous supposons $x \in B$. Dans le premier cas nous avons donc les données et le but suivants :

<i>Givens</i>	<i>Goal</i>
$A \subseteq C$	
$B \subseteq C$	
$x \in A$	$x \in C$

Nous avons déjà décidé que si jamais nous rencontrions un élément de A , nous pouvons utiliser le premier donné pour conclure qu'il s'agit également d'un élément de C . Puisque nous avons maintenant $x \in A$ étant donné, nous pouvons conclure que $x \in C$, qui est notre objectif. Le raisonnement pour le second cas est assez similaire, utilisant la seconde donnée au lieu de la première.

Solution

Théorème. *Supposons que UN, Groupe C sont des ensembles. Si $A \subseteq C$ et $B \subseteq C$ alors $A \cup B \subseteq C$.*

Preuve. Supposons que $A \subseteq C$ et $B \subseteq C$, et soit x un élément arbitraire de $A \cup B$. Alors soit $x \in A$ ou $x \in B$.

Cas 1. $x \in A$. Alors puisque $A \subseteq C$, $x \in C$.

Cas 2. $x \in B$. Alors puisque $B \subseteq C$, $x \in C$.

Puisque nous savons que soit $x \in A$ ou $x \in B$, ces cas couvrent toutes les possibilités, nous pouvons donc conclure que $x \in C$. Puisque x est un élément arbitraire de $A \cup B$, cela signifie que $A \cup B \subseteq C$.

□

Notez que les cas de cette preuve ne sont pas *exclusifs*. Autrement dit, il est possible que $x \in A$ et $x \in B$ est vrai, donc certaines valeurs de x pourraient correspondre aux deux cas. Il n'y a rien de mal à cela. Les cas d'une preuve doivent couvrir toutes les possibilités, mais il n'y a aucun inconvénient à couvrir certaines possibilités plus d'une fois. Autrement dit, les cas doivent être exhaustifs, mais pas exclusifs.

La preuve par cas est parfois utile pour prouver un objectif de la forme $P \vee Q$. Si vous pouvez prouver P dans certains cas et Q dans d'autres, alors, tant que vos cas sont exhaustifs, vous pouvez conclure que $P \vee Q$ est vrai. Cette méthode est particulièrement utile si l'une des données a également la forme d'une disjonction, car vous pouvez alors utiliser les cas suggérés par cette donnée.

Pour prouver un but de la forme $P \vee Q$:

preuve en cas. Dans chaque cas, prouvez P ou Q .

Exemple 3.5.2. Supposons que A , B et C sont des ensembles. Démontrer que $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Travail à partir de zéro

Parce que le but est $\forall x (x \in A \setminus (B \setminus C) \rightarrow x \in (A \setminus B) \cup C)$, nous laissons x arbitraire, supposons $x \in A \setminus (B \setminus C)$, et essayez de prouver $x \in (A \setminus B) \cup C$. L'écriture de ces énoncés sous forme de symboles logiques nous donne :

$$\begin{array}{ccc} \text{Givens} & & \text{Goal} \\ x \in A \wedge \neg(x \in B \wedge x \notin C) & & (x \in A \wedge x \notin B) \vee x \in C \end{array}$$

Nous divisons le donné en deux donnés distincts, $x \in A$ et $\neg(x \in B \wedge x \notin C)$, et comme la seconde est une affirmation négative, nous utilisons l'une des lois de De Morgan pour la réexprimer comme l'affirmation positive $x \notin B \vee x \in C$.

$$\begin{array}{ccc} \text{Givens} & & \text{Goal} \\ x \in A \\ x \notin B \vee x \in C & & (x \in A \wedge x \notin B) \vee x \in C \end{array}$$

Maintenant, la seconde donnée et le but sont tous deux des disjonctions, nous allons donc essayer de considérer les deux cas $x \notin B$ et $x \in C$ suggéré par le second donné. Selon notre stratégie pour prouver des buts de la forme $P \vee Q$, si dans chaque cas nous pouvons prouver $x \in A \wedge x \notin B$ ou prouver $x \in C$, alors la preuve sera complète. Pour le premier cas, nous supposons $x \notin B$.

$$\begin{array}{ccc} \text{Givens} & & \text{Goal} \\ x \in A \\ x \notin B & & (x \in A \wedge x \notin B) \vee x \in C \end{array}$$

Dans ce cas, l'objectif est clairement vrai, car en fait, nous pouvons conclure que $x \in A \wedge x \notin B$. Pour le deuxième cas, nous supposons $x \in C$, et encore une fois le but est clairement vrai.

Solution

Théorème. Supposons que UN , Groupe C sont des ensembles. Alors $UN \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Preuve. Supposons que $x \in UN \setminus (B \setminus C)$. Alors $x \in UN$ et $x \notin B \setminus C$. Puisque $x \notin B \setminus C$, il s'ensuit que soit $x \notin B$ soit $x \in C$. Nous examinerons ces cas séparément.

Cas 1. $x \notin B$. Alors puisque $x \in UN$, $x \in A \setminus B$, donc $x \in (A \setminus B) \cup C$.

Cas 2. $x \in C$. Alors clairement $x \in (A \setminus B) \cup C$.

Puisque x est un élément arbitraire de $UN \setminus (B \setminus C)$, nous pouvons conclure que $UN \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

□

Parfois, vous pouvez trouver utile de décomposer une preuve en cas même si les cas ne sont pas suggérés par une donnée de la forme $P \vee Q$.

Toute preuve peut être décomposée en cas à tout moment, à condition que les cas épuisent toutes les possibilités.

Exemple 3.5.3. Démontrer que pour tout entier x , le reste de la division de x^2 par 4 est soit 0, soit 1.

Travail à partir de zéro

Nous commençons par laisser x être un entier arbitraire, puis essayons de prouver que le reste lorsque x^2 est divisé par 4 est soit 0, soit 1.

$$\begin{array}{c} \text{Given} \\ x \in \mathbb{Z} \end{array} \qquad \qquad \begin{array}{c} \text{Goal} \\ (x^2 \div 4 \text{ has remainder } 0) \vee (x^2 \div 4 \text{ has remainder } 1) \end{array}$$

L'objectif étant une disjonction, décomposer la preuve en cas semble une approche plausible, mais rien ne permet de déterminer les cas à utiliser. Cependant, tester quelques valeurs de x suggère les cas appropriés :

x	x^2	quotient of $x^2 \div 4$	remainder of $x^2 \div 4$
1	1	0	1
2	4	1	0
3	9	2	1
4	16	4	0
5	25	6	1
6	36	9	0

Il apparaît que le reste est nul lorsque x est pair et nul lorsque x est impair. Voici les cas que nous allons utiliser. Ainsi, pour le cas 1, nous supposons que x est pair et essayons de prouver que le reste est nul ; pour le cas 2, nous supposons que x est impair et prouvons que le reste est nul. Puisque chaque entier est pair ou impair, ces cas sont exhaustifs.

En complétant la définition de *pair*, voici nos données et notre objectif pour le cas 1 :

$$\begin{array}{c} \text{Given} \\ x \in \mathbb{Z} \\ \exists k \in \mathbb{Z}(x = 2k) \end{array} \qquad \qquad \begin{array}{c} \text{Goal} \\ x^2 \div 4 \text{ has remainder } 0 \end{array}$$

Nous utilisons immédiatement la seconde donnée et posons k comme un entier particulier pour lequel $x = 2k$. Alors $x^2 = (2k)^2 = 4k^2$, donc clairement, lorsque nous divisons x^2 par 4, le quotient est k^2 et le reste est 0.

Le cas 2 est assez similaire :

$$\begin{array}{c} \text{Given} \\ x \in \mathbb{Z} \\ \exists k \in \mathbb{Z}(x = 2k + 1) \end{array} \qquad \qquad \begin{array}{c} \text{Goal} \\ x^2 \div 4 \text{ has remainder } 1 \end{array}$$

Encore une fois, nous utilisons la seconde donnée immédiatement et laissons k représenter un entier pour lequel $x = 2k + 1$. Alors $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$, donc clairement, lorsque nous divisons x^2 par 4, le quotient est $k^2 + k$ et le reste est 1.

$1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, donc lorsque x^2 est divisé par 4, le quotient est $k^2 + k$ et le reste est 1.

Solution

Théorème. Pour chaque entier x , le reste lorsque x^2 est divisé par 4 est soit 0 ou 1 .

Preuve . Supposons que x soit un entier. Considérons deux cas.

Cas 1. x est pair. Alors $x = 2k$ pour un entier k , donc $x^2 = 4k^2$. De toute évidence, le reste lorsque x^2 est divisé par 4 est nul.

Cas 2. x est impair. Alors $x = 2k + 1$ pour un entier k , donc $x^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. Dans ce cas, le reste de la division de x^2 par 4 est 1.

□

Parfois, dans la preuve d'un objectif de la forme $P \vee Q$, il est difficile de décomposer la preuve en cas. Voici une méthode souvent utile. Supposons simplement que P est vrai dans le cas 1 et qu'il est faux dans le cas 2. P est certainement vrai ou faux, ces cas sont donc exhaustifs. Dans le premier cas, vous avez supposé que P est vrai, donc l'objectif $P \vee Q$ est certainement vrai. Ainsi, aucun raisonnement supplémentaire n'est nécessaire dans le cas 1. Dans le second cas, vous avez supposé que P est faux, donc la seule façon pour que l'objectif $P \vee Q$ soit vrai est que Q soit vrai. Ainsi, pour compléter ce cas , vous devez essayer de prouver Q .

Pour prouver un but de la forme $P \vee Q$:

Si P est vrai, alors l'objectif $P \vee Q$ est clairement vrai ; il suffit donc de se préoccuper du cas où P est faux. Dans ce cas, on peut compléter la preuve en prouvant que Q est vrai.

Travail à partir de zéro

Avant d'utiliser la stratégie :

$$\begin{array}{ccc} \text{Givens} & & \text{Goal} \\ \hline & & P \vee Q \end{array}$$

Après avoir utilisé la stratégie :

$$\begin{array}{ccc} \text{Givens} & & \text{Goal} \\ \hline & & Q \\ & & \hline & & \neg P \end{array}$$

Forme de l'épreuve finale :

Si P est vrai, alors bien sûr $P \vee Q$ est vrai. Supposons maintenant que P soit faux.

[La preuve de Q va ici.]

Ainsi, $P \vee Q$ est vrai.

Ainsi, cette stratégie pour prouver $P \vee Q$ suggère de transformer le problème en ajoutant $\neg P$ comme nouvelle donnée et en changeant le but en Q . Il est intéressant de noter que c'est exactement la même transformation que vous utiliseriez pour prouver le but $\neg P \rightarrow Q$! Cela n'est pas vraiment surprenant, car nous savons déjà que les affirmations $P \vee Q$ et $\neg P \rightarrow Q$ sont équivalentes. Mais nous avons déduit cette équivalence auparavant de la table de vérité pour le connecteur conditionnel, et cette table de vérité a pu être difficile à comprendre au début. Peut-être que le raisonnement que nous avons donné rend cette équivalence, et donc la table de vérité pour le connecteur conditionnel, plus naturelles.

Bien sûr, les rôles de P et Q pourraient être inversés en utilisant cette stratégie. Ainsi, vous pouvez également prouver $P \vee Q$ en supposant que Q est faux et en prouvant P .

Exemple 3.5.4. Démontrer que pour tout nombre réel x , si $x^2 \geq x$ alors $x \leq 0$ ou $x \geq 1$.

Travail à partir de zéro

Notre objectif est $\forall x (x^2 \geq x \rightarrow (x \leq 0 \vee x \geq 1))$, donc pour commencer, nous laissons x un nombre réel arbitraire, supposons $x^2 \geq x$ et définissons $x \leq 0 \vee x \geq 1$ comme objectif :

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ x^2 \geq x & & x \leq 0 \vee x \geq 1 \end{array}$$

Selon notre stratégie, pour prouver cet objectif, nous pouvons soit supposer $x > 0$ et prouver $x \geq 1$, soit supposer $x < 1$ et prouver $x \leq 0$. L'hypothèse selon laquelle x est positif semble plus susceptible d'être utile dans le raisonnement sur les inégalités, nous adoptons donc la première approche.

$$\begin{array}{ccc} \text{Given} & & \text{Goal} \\ x^2 \geq x & & x \geq 1 \\ x > 0 & & \end{array}$$

La preuve est maintenant simple. Puisque $x > 0$, on peut diviser l'inégalité donnée $x^2 \geq x$ par x pour obtenir l'objectif $x \geq 1$.

Solution

Théorème. Pour chaque nombre réel x , si $x^2 \geq x$ alors soit $x \leq 0$ ou $x \geq 1$.

Preuve. Supposons que $x^2 \geq x$. Si $x \leq 0$, alors bien sûr $x \leq 0$ ou $x \geq 1$. Supposons maintenant que $x > 0$. Nous pouvons alors diviser les deux côtés de l'inégalité $x^2 \geq x$ par x pour conclure que $x \geq 1$. Ainsi, soit $x \leq 0$, soit $x \geq 1$.

□

L'équivalence de $P \vee Q$ et $\neg P \rightarrow Q$ suggère également une règle d'inférence appelée *syllogisme disjonctif* pour utiliser un énoncé donné de la forme $P \vee Q$:

Pour utiliser une donnée de la forme $P \vee Q$:

Si l'on vous donne également $\neg P$, ou si vous pouvez prouver que P est faux, vous pouvez alors utiliser cette donnée pour conclure que Q est vrai. De même, si l'on vous donne $\neg Q$ ou si vous pouvez prouver que Q est faux, vous pouvez alors conclure que P est vrai.

En fait, cette règle est celle que nous avons utilisée dans notre premier exemple de raisonnement déductif au [chapitre 1](#)!

Une fois de plus, nous terminons cette section avec une preuve que vous pourrez lire sans avoir recours à une analyse préliminaire du travail de base.

Théorème 3.5.5. *Supposer m et n sont des entiers. Si mn est pair, alors soit m est pair ou n est pair.*

Preuve. Supposons que mn soit pair. On peut alors choisir un entier k tel que $mn = 2k$. Si m est pair alors il n'y a plus rien à prouver, donc supposons que m soit impair. Alors $m = 2j + 1$ pour un entier j . En substituant cela dans l'équation $mn = 2k$, on obtient $(2j + 1)n = 2k$, donc $2jn + n = 2k$, et donc $n = 2k - 2jn = 2(k - jn)$. Puisque $k - jn$ est un entier, il s'ensuit que n est pair.

□

Commentaire. La forme générale de la preuve est la suivante :

Supposons que mn soit pair.

Si m est pair, alors soit m est pair, soit n est pair. Supposons maintenant que m ne soit pas pair. Alors m est impair.

[La preuve que n est pair va ici.]

Par conséquent, soit m est pair, soit n est pair.

Par conséquent, si mn est pair, alors soit m est pair, soit n est pair.

Les hypothèses selon lesquelles mn est pair et m est impair conduisent, par instantiation existentielle, aux équations $mn = 2k$ et $m = 2j + 1$. Bien que la démonstration ne le dise pas explicitement, vous devez déterminer par vous-même que pour prouver que n est pair, il

suffit de trouver un entier c tel que $n = 2c$. Une algèbre simple conduit à l'équation $n = 2(k - jn)$, donc le choix $c = k - jn$ fonctionne.

Exercices

- \triangleright *1. Supposons que A , B et C sont des ensembles. Démontrer que $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.
- \triangleright 2. Supposons que A , B et C sont des ensembles. Démontrer que $(A \cup B) \setminus C \subseteq A \cup (B \setminus C)$.
- \triangleright 3. Supposons que A et B sont des ensembles. Démontrer que $A \setminus (A \setminus B) = A \cap B$.
- \triangleright 4. Supposons que A , B et C sont des ensembles. Démontrer que $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.
- \triangleright *5. Supposons que $A \cap C \subseteq B \cap C$ et $A \cup C \subseteq B \cup C$. Démontrer que $A \subseteq B$.
- \triangleright 6. Rappelons de [la section 1.4](#) que la différence symétrique de deux ensembles A et B est l'ensemble $AB = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Démontrer que si $AB \subseteq A$ alors $B \subseteq A$.
- \triangleright 7. Supposons que A , B et C sont des ensembles. Démontrer que $A \cup C \subseteq B \cup C$ ssi $A \setminus C \subseteq B \setminus C$.
- \triangleright *8. Démontrer que pour tout ensemble A et B , $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
- \triangleright 9. Démontrer que pour tout ensemble A et B , si $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$ alors soit $A \subseteq B$ soit $B \subseteq A$.
- 10. Supposons que x et y soient des nombres réels et $x = 0$. Démontrer que $y + 1/x = 1 + y/x$ ssi $x = 1$ ou $y = 1$.
- 11. Démontrer que pour tout nombre réel x , si $|x - 3| > 3$ alors $x^2 > 6x$.
(Indice : Selon la définition de $|x - 3|$, si $x - 3 \geq 0$ alors $|x - 3| = x - 3$, et si $x - 3 < 0$ alors $|x - 3| = 3 - x$. Le moyen le plus simple d'utiliser ce fait est de décomposer votre preuve en cas. Supposons que $x - 3 \geq 0$ dans le cas 1, et $x - 3 < 0$ dans le cas 2.)
- 12. Démontrer que pour tout nombre réel x , $|2x - 6| > x$ ssi $|x - 4| > 2$.
(Indice : Lisez l'indice de [l'exercice 11.](#))
- 13. (a) Démontrer que pour tous les nombres réels a et b , $|a| \leq b$ ssi $-b \leq a \leq b$.
(b) Démontrer que pour tout nombre réel x , $-|x| \leq x \leq |x|$. (Indice : utilisez la partie (a).)
(c) Démontrer que pour tous les nombres réels x et y , $|x + y| \leq |x| + |y|$. (C'est ce qu'on appelle l'*inégalité triangulaire*. Une façon de le

prouver est de combiner les parties (a) et (b), mais vous pouvez également le faire en considérant plusieurs cas.)

- (d) Démontrer que pour tous les nombres réels x et y , $|x + y| \geq |x| - |y|$. (Indice : Commencez par l'équation $|x| = |(x + y) + (-y)|$ puis appliquez l'inégalité triangulaire au côté droit.)
14. Démontrer que pour tout entier x , $x^2 + x$ est pair.
15. Démontrer que pour chaque entier x , le reste lorsque x^4 est divisé par 8 est soit 0, soit 1.
16. Supposons que \mathcal{F} et \mathcal{G} soient des familles d'ensembles non vides.
- P_D (a) Démontrer que $\bigcup(\mathcal{F} \cup \mathcal{G}) = (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.
- (b) Démontrer que $B \cup (\bigcup \mathcal{F}) = \bigcup_{A \in \mathcal{F}} (B \cup A)$.
- (c) Pouvez-vous découvrir et prouver un théorème similaire sur $\bigcap(\mathcal{F} \cup \mathcal{G})$?
17. Supposons que \mathcal{F} soit une famille d'ensembles non vide et que B soit un ensemble.
- P_D (a) Démontrer que $B \cup (\bigcup \mathcal{F}) = \bigcup(\mathcal{F} \cup \{B\})$.
- (b) Démontrer que $B \cup (\bigcap \mathcal{F}) = \bigcap_{A \in \mathcal{F}} (B \cup A)$.
- (c) Pouvez-vous découvrir et prouver des théorèmes similaires sur $B \cap (\bigcup \mathcal{F})$ et $B \cap (\bigcap \mathcal{F})$?
18. Supposons que \mathcal{F} , \mathcal{G} et \mathcal{H} soient des familles d'ensembles non vides et que pour tout $A \in \mathcal{F}$ et chaque $B \in \mathcal{G}$, $A \cup B \in \mathcal{H}$. Démontrer que $\bigcap \mathcal{H} \subseteq (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.
- D 19. Supposons que A et B sont des ensembles. Démontrer que $\forall x (x \in \text{Un } \Delta B \leftrightarrow (x \in A \leftrightarrow x \notin B))$.
- *20. Supposons que A , B et C sont des ensembles. Démontrer que $A \Delta B$ et C sont disjoints ssi $A \cap C = B \cap C$.
- D 21. Supposons que A , B et C sont des ensembles. Démontrer que $AB \subseteq C$ ssi $A \cup C = B \cup C$.
- D 22. Supposons que A , B et C sont des ensembles. Démontrer que $C \subseteq A \Delta B$ ssi $C \subseteq A \cup B$ et $A \cap B \cap C = \emptyset$.
- *23. Supposons que A , B et C sont des ensembles.
- (a) Démontrer que $A \setminus C \subseteq (A \setminus B) \cup (B \setminus C)$.
- (b) Démontrer que $AC \subseteq (AB) \cup (BC)$.
- *24. Supposons que A , B et C sont des ensembles.
- (a) Démontrer que $(A \cup B)C \subseteq (AC) \cup (BC)$.

(b) Trouvez un exemple d'ensembles A , B et C tels que $(A \cup B) \Delta C \neq (A \Delta C) \cup (B \Delta C)$

25. Supposons que A , B et C soient des ensembles.

(a) Démontrer que $(A \Delta C) \cap (B \Delta C) \subseteq (A \cap B) \Delta C$.

(b) Est-il toujours vrai que $(A \cap B) \Delta C \subseteq (A \Delta C) \cap (B \Delta C)$? Donnez une preuve ou un contre-exemple.

26. Supposons que A , B et C soient des ensembles. Considérons les ensembles $(A \setminus B) \Delta C$ et $(A \Delta C) \setminus (B \Delta C)$. Pouvez-vous prouver que l'un est un sous-ensemble de l'autre ? Justifiez vos conclusions par des preuves ou des contre-exemples.

27. Considérons le théorème putatif suivant.

Théorème? Pour chaque nombre réel x , si $|x - 3| < 3$ alors $0 < x < 6$.

La preuve suivante est-elle correcte ? Si oui, quelles stratégies de preuve utilise-t-elle ? Si non, peut-elle être corrigée ? Le théorème est-il correct ?

Preuve. Soit x un nombre réel arbitraire, et supposons $|x - 3| < 3$. On considère deux cas :

Cas 1. $x - 3 \geq 0$. Alors $|x - 3| = x - 3$. En plaçant cela dans l'hypothèse que $|x - 3| < 3$, nous obtenons $x - 3 < 3$, donc clairement $x < 6$.

Cas 2. $x - 3 < 0$. Alors $|x - 3| = 3 - x$, donc l'hypothèse $|x - 3| < 3$ signifie que $3 - x < 3$. Par conséquent $3 < 3 + x$, donc $0 < x$.

Puisque nous avons prouvé que $0 < x$ et $x < 6$, nous pouvons conclure que $0 < x < 6$.

□

28. Considérez le théorème putatif suivant.

Théorème? Pour tous les ensembles UN , Groupe C , si $A \setminus B \subseteq C$ et CA alors $A \cap B = \emptyset$.

La preuve suivante est-elle correcte ? Si oui, quelles stratégies de preuve utilise-t-elle ? Si non, peut-elle être corrigée ? Le théorème est-il correct ?

Preuve. Supposons que $A \setminus B \subseteq C$ et AC . Puisque AC , nous pouvons choisir un x tel que $x \in A$ et $x \notin C$. Puisque $x \notin C$ et $A \setminus B \subseteq C$, $x \notin A \setminus B$. Par conséquent, soit $x \notin A$, soit $x \in B$. Mais nous savons déjà que $x \in A$, il s'ensuit donc que $x \in B$. Puisque $x \in A$ et $x \in B$, $x \in A \cap B$. Par conséquent $A \cap B \neq \emptyset$.

□

29. Considérons le théorème putatif suivant.

Théorème ? $\forall x \in \mathbb{R} \exists y \in \mathbb{R} (xy^2 \neq y - x)$.

La preuve suivante est-elle correcte ? Si oui, quelles stratégies de preuve utilise-t-elle ? Si non, peut-elle être corrigée ? Le théorème est-il correct ?

Preuve. Soit x un nombre réel arbitraire.

Cas 1. $x = 0$. Soit $y = 1$. Alors $xy^2 = 0$ et $y - x = 1 - 0 = 1$, donc $xy^2 \neq y - x$

Cas 2. $x = 0$. Soit $y = 0$. Alors $xy^2 = 0$ et $y - x \neq -x = 0$, donc $xy^2 \neq y - x$.

Comme ces cas sont exhaustifs, nous avons montré que $\exists y \in \mathbb{R} (\ xy^2 \neq y - x)$. Puisque x est arbitraire, cela montre que $\forall x \in \mathbb{R} \ \exists y \in \mathbb{R} (\ xy^2 \neq y - x)$.

□

30. Démontrer que si $\forall xP(x) \rightarrow \exists xQ(x)$ alors $\exists x(P(x) \rightarrow Q(x))$.
(Indice : Rappelez-vous que $P \rightarrow Q$ est équivalent à $\neg P \vee Q$.)

31. Considérons le théorème putatif suivant.

Théorème? Supposer *UN Groupe C* sont des ensembles et $A \subseteq B \cup C$. Alors soit $A \subseteq B$ ou $A \subseteq C$.

La preuve suivante est-elle correcte ? Si oui, quelles stratégies de preuve utilise-t-elle ? Si non, peut-elle être corrigée ? Le théorème est-il correct ?

Preuve. Soit x un élément arbitraire de A . Puisque $A \subseteq B \cup C$, il s'ensuit que $x \in B$ ou $x \in C$.

Cas 1. $x \in B$. Puisque x était un élément arbitraire de A , il s'ensuit que $\forall x \in \text{Un} (x \in B)$, ce qui signifie que $A \subseteq B$.

Cas 2. $x \in C$. De même, puisque x est un élément arbitraire de A , nous pouvons conclure que $A \subseteq C$.

Ainsi, soit $A \subseteq B$, soit $A \subseteq C$.

□

D 32. Supposons que A , B et C soient des ensembles et que $A \subseteq B \cup C$.

Démontrer que soit $A \subseteq B$ soit $A \cap C \neq \emptyset$.

33. Démontrer que $\exists x (P(x) \rightarrow \forall yP(y))$. (Remarque : supposons que l'univers du discours n'est pas l'ensemble vide.)

3.6 Preuves d'existence et d'unicité

Dans cette section, nous considérons des preuves dont le but est de la forme $\exists! xP(x)$. Rappelons que cette formule signifie « il existe exactement un x tel que $P(x)$ », et comme nous l'avons vu dans [la section 2.2](#), elle peut être considérée comme une abréviation de la formule $\exists x(P(x) \wedge \forall y(P(y) \wedge y \neq x))$. Selon les stratégies de preuve présentées dans les sections précédentes, nous pourrions donc prouver ce but en trouvant une valeur particulière de x pour laquelle nous pourrions prouver à la fois $P(x)$ et $\forall y(P(y) \wedge y \neq x)$. La dernière partie de cette preuve impliquerait de prouver une affirmation négative, mais nous pouvons la réexprimer sous la forme d'une affirmation positive équivalente :

$$\neg \exists y(P(y) \wedge y \neq x)$$

est équivalent à $\forall y \neg(P(y) \wedge y \neq x)$ (loi de négation du quantificateur),

ce qui équivaut à $\forall y (\neg P(y) \vee y = x)$ (loi de De Morgan),

ce qui équivaut à $\forall y (P(y) \rightarrow y = x)$ (loi conditionnelle).

Ainsi, nous voyons que $\exists! xP(x)$ pourrait également s'écrire comme $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$. En fait, comme le montre l'exemple suivant, plusieurs autres formules sont également équivalentes à $\exists! xP(x)$, et elles suggèrent d'autres approches pour prouver des objectifs de cette forme.

Exemple 3.6.1. Démontrer que les formules suivantes sont toutes équivalentes :

1. $\exists X(P(X) \wedge \forall y(P(y) \rightarrow y = X))$.
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$.
3. $\exists xP(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$.

Travail à partir de zéro

Si nous prouvons directement que chacune de ces affirmations est équivalente à chacune des autres, nous aurons alors trois biconditionnelles à prouver : affirmation 1 ssi affirmation 2, affirmation 1 ssi affirmation 3 et affirmation 2 ssi affirmation 3. Si nous prouvons chaque biconditionnelle par les méthodes de la [section 3.4](#), chacune

impliquera deux preuves conditionnelles, ce qui nous nécessitera un total de six preuves conditionnelles. Heureusement, il existe une méthode plus simple. Nous allons prouver que l'affirmation 1 implique l'affirmation 2, l'affirmation 2 implique l'affirmation 3 et l'affirmation 3 implique l'affirmation 1 – soit trois conditions. Bien que nous ne donnions pas de preuve séparée que l'affirmation 2 implique l'affirmation 1, cela découlera du fait que l'affirmation 2 implique l'affirmation 3 et l'affirmation 3 implique l'affirmation 1. De même, les deux autres conditionnelles découlent des trois que nous allons prouver. Les mathématiciens utilisent presque toujours un tel raccourci lorsqu'ils prouvent que plusieurs affirmations sont toutes équivalentes. Étant donné que nous allons prouver trois instructions conditionnelles, notre preuve comportera trois parties, que nous appellerons $1 \rightarrow 2$, $2 \rightarrow 3$ et $3 \rightarrow 1$. Nous devrons élaborer notre stratégie pour les trois parties séparément.

$1 \rightarrow 2$. Nous supposons l'énoncé 1 et démontrons l'énoncé 2. Puisque l'énoncé 1 commence par un quantificateur existentiel, nous choisissons un nom, disons x_0 , pour un objet pour lequel $P(x_0)$ et $\forall y (P(y) \rightarrow y = x_0)$ sont tous deux vrais. Ainsi, nous avons maintenant la situation suivante :

<i>Givens</i>	<i>Goal</i>
$P(x_0)$ $\forall y (P(y) \rightarrow y = x_0)$	$\exists x \forall y (P(y) \leftrightarrow y = x)$

Notre objectif commence également avec un quantificateur existentiel, donc pour le prouver nous devons essayer de trouver une valeur de x qui rende le reste de l'énoncé vrai. Bien sûr, le choix évident est $x = x_0$. En remplaçant x_0 par x , nous voyons que nous devons maintenant prouver $\forall y (P(y) \leftrightarrow y = x_0)$. Nous posons y arbitraire et prouvons les deux directions de la biconditionnelle. La direction \rightarrow est claire par la deuxième donnée. Pour la direction \leftarrow , supposons $y = x_0$. Nous avons également $P(x_0)$ comme donnée, et en remplaçant y par x_0 dans cette donnée nous obtenons $P(y)$.

$2 \rightarrow 3$. L'énoncé 2 est un énoncé existentiel ; on considère donc x_0 comme un objet tel que $\forall y (P(y) \leftrightarrow y = x_0)$. L'objectif, l'énoncé 3, est une conjonction ; on le traite donc comme deux objectifs distincts.

<i>Givens</i>	<i>Goals</i>
$\forall y (P(y) \leftrightarrow y = x_0)$	$\exists x P(x)$ $\forall y \forall z ((P(y) \wedge P(z)) \rightarrow y = z)$

Pour prouver le premier objectif, nous devons choisir une valeur pour x , et bien sûr, la valeur évidente est à nouveau $x = x_0$. Ainsi, nous devons prouver P

(x_0). La manière naturelle d'utiliser notre seule donnée est de remplacer y par quelque chose ; et pour prouver l'objectif $P(x_0)$, la valeur évidente à remplacer est x_0 . Cela nous donne $P(x_0) \leftrightarrow x_0 = x_0$. Bien sûr, $x_0 = x_0$ est vrai, donc par la direction \leftarrow de la biconditionnelle, nous obtenons $P(x_0)$.

Pour le deuxième objectif, nous laissons y et z arbitraires, supposons $P(y)$ et $P(z)$ et essayons de prouver $y = z$.

<i>Givens</i>	<i>Goal</i>
$\forall y(P(y) \leftrightarrow y = x_0)$	
$P(y)$	
$P(z)$	

En insérant chacun des y et z dans la première donnée, nous obtenons $P(y) \leftrightarrow y = x_0$ et $P(z) \leftrightarrow z = x_0$. Puisque nous avons supposé $P(y)$ et $P(z)$, cette fois nous utilisons les directions \rightarrow de ces biconditionnelles pour conclure que $y = x_0$ et $z = x_0$. Notre objectif $y = z$ suit clairement.

3 \rightarrow 1. Puisque l'énoncé 3 est une conjonction, nous le traitons comme deux données distinctes. Le premier est un énoncé existentiel ; nous supposons donc que x_0 représente un objet tel que $P(x_0)$ soit vrai. Pour prouver l'énoncé 1, nous posons à nouveau $x = x_0$, ce qui nous donne la situation suivante :

<i>Givens</i>	<i>Goal</i>
$P(x_0)$	
$\forall y\forall z((P(y) \wedge P(z)) \rightarrow y = z)$	$P(x_0) \wedge \forall y(P(y) \rightarrow y = x_0)$

Nous connaissons déjà la première moitié de l'objectif ; il ne nous reste donc plus qu'à prouver la seconde. Pour cela, posons y comme arbitraire, supposons $P(y)$ et définissons $y = x_0$ comme objectif.

<i>Givens</i>	<i>Goal</i>
$P(x_0)$	
$\forall y\forall z((P(y) \wedge P(z)) \rightarrow y = z)$	
$P(y)$	$y = x_0$

Mais maintenant nous connaissons à la fois $P(y)$ et $P(x_0)$, donc l'objectif $y = x_0$ découle de la deuxième donnée.

Solution

Théorème. *Les éléments suivants sont équivalents :*

1. $\exists X(P(X) \wedge \forall y(P(y) \rightarrow y = X))$.
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$.
3. $\exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$.

Preuve . 1 → 2. Par l'énoncé 1, nous pouvons soit x_0 un objet tel que $P(x_0)$ et $\forall y (P(y) \rightarrow y = x_0)$. Pour prouver l'énoncé 2 nous montrerons que $\forall y (P(y) \leftrightarrow y = x_0)$. Soit y un objet quelconque. Nous connaissons déjà la direction \rightarrow de la biconditionnelle. Pour la direction \leftarrow , supposons $y = x_0$. Alors puisque nous connaissons $P(x_0)$, nous pouvons conclure $P(y)$.

2 → 3. Par l'énoncé 2, choisissons x_0 tel que $\forall y (P(y) \leftrightarrow y = x_0)$. Alors, en particulier, $P(x_0) \leftrightarrow x_0 = x_0$, et puisque clairement $x_0 = x_0$, il s'ensuit que $P(x_0)$ est vrai. Ainsi, $\exists x P(x)$. Pour prouver la seconde moitié de l'énoncé 3, soit y et z arbitraires et supposons $P(y)$ et $P(z)$. Alors par notre choix de x_0 (comme quelque chose pour lequel $\forall y (P(y) \leftrightarrow y = x_0)$ est vrai), il s'ensuit que $y = x_0$ et $z = x_0$, donc $y = z$.

3 → 1. Par la première moitié de l'énoncé 3, soit x_0 un objet tel que $P(x_0)$. L'énoncé 1 suivra si nous pouvons montrer que $\forall y (P(y) \rightarrow y = x_0)$, donc supposons $P(y)$. Puisque nous avons maintenant à la fois $P(x_0)$ et $P(y)$, par la seconde moitié de l'énoncé 3 nous pouvons conclure que $y = x_0$, comme requis.

□

Puisque les trois énoncés du théorème sont équivalents à $\exists! x P(x)$, on peut prouver un but de cette forme en prouvant l'un des trois énoncés du théorème. La technique la plus courante pour prouver un but de la forme $\exists! x P(x)$ est probablement de prouver l'énoncé 3 du théorème.

Pour prouver un but de la forme $\exists! x P(x)$:

Démontrer $\exists x P(x)$ et $\forall y \forall z ((P(y) \wedge P(z)) \rightarrow y = z)$. Le premier de ces objectifs montre qu'il existe un x tel que $P(x)$ est vrai, et le second montre qu'il est unique. Les deux parties de la preuve sont donc parfois appelées « *existence* » et « *unicité* ». Chaque partie est prouvée à l'aide des stratégies décrites précédemment.

Forme de l'épreuve finale :

Existence : [La preuve de $\exists x P(x)$ va ici.]

Unicité : [Preuve de $\forall y \forall z ((P(y) \wedge P(z)) \rightarrow y = z)$ va ici.]

Exemple 3.6.2. Démontrer qu'il existe un unique ensemble A tel que pour tout ensemble B , $A \cup B = B$.

Travail à partir de zéro

Notre objectif est $\exists! AP(A)$, où $P(A)$ est l'énoncé $\forall B (A \cup B = B)$. Selon notre stratégie, nous pouvons le prouver en prouvant séparément l'existence et l'unicité. Pour la partie existence de la preuve, nous devons prouver $\exists AP(A)$. Nous essayons donc de trouver une valeur de A qui rende $P(A)$ vrai. Il n'existe pas de formule pour trouver cet ensemble A , mais si vous réfléchissez à la signification de l'énoncé $P(A)$, vous devriez comprendre que le bon choix est $A = \emptyset$. En remplaçant A par cette valeur, nous voyons que pour compléter la partie existence de la preuve, nous devons montrer que $\forall B (\emptyset \cup B = B)$. C'est clairement vrai. (En cas de doute, résolvez la preuve !)

Pour la partie de la preuve d'unicité, nous prouvons $\forall C \forall D ((P(C) \wedge P(D)) \rightarrow C = D)$. Pour ce faire, nous posons C et D arbitraires, supposons $P(C)$ et $P(D)$, et prouvons $C = D$. En exprimant la signification des affirmations $P(C)$ et $P(D)$, nous obtenons les données et l'objectif suivants :

$$\begin{array}{ll} \text{Givens} & \text{Goal} \\ \forall B (C \cup B = B) & C = D \\ \forall B (D \cup B = B) & \end{array}$$

Pour utiliser les données, il faut essayer de trouver un substitut pour B dans chacune d'elles. Un choix astucieux simplifie le reste de la preuve : on remplace D par C dans la première donnée, et C par D dans la seconde. Cela nous donne $C \cup D = D$ et $D \cup C = C$. Mais il est clair que $C \cup D = D \cup C$. (Si vous ne voyez pas pourquoi, prouvez-le !) L'objectif $C = D$ suit immédiatement.

Solution

Théorème. *Il existe un ensemble unique UN tel que pour tout ensemble B, A ∪ B = B.*

Preuve. Existence : Clairement $\forall B (\emptyset \cup B = B)$, donc \emptyset a la propriété requise.

Unicité : Supposons $\forall B (C \cup B = B)$ et $\forall B (D \cup B = B)$. En appliquant la première de ces hypothèses à D , nous voyons que $C \cup D = D$, et en appliquant la seconde à C , nous obtenons $D \cup C = C$. Mais il est clair que $C \cup D = D \cup C$, donc $C = D$.

□

Parfois, une affirmation de la forme $\exists! xP(x)$ est prouvée en prouvant l'affirmation 1 de [l'exemple 3.6.1](#). Cela conduit à la stratégie de preuve suivante.

Pour prouver un but de la forme $\exists! xP(x)$:

Démontrer $\exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x))$, en utilisant les stratégies des sections précédentes.

Exemple 3.6.3. Démontrer que pour tout nombre réel x , si $x = 2$ alors il existe un unique nombre réel y tel que $2y/(y+1) = x$.

Travail à partir de zéro

Notre objectif est $\forall x (x \neq 2 \rightarrow \exists! y (2y/(y+1) = x))$. Nous supposons donc x arbitraire, supposons $x \neq 2$ et prouvons $\exists! y (2y/(y+1) = x)$. Selon la stratégie précédente, nous pouvons prouver cet objectif en prouvant l'énoncé équivalent.

$$\exists y \left(\frac{2y}{y+1} = x \wedge \forall z \left(\frac{2z}{z+1} = x \rightarrow z = y \right) \right).$$

Commençons par trouver une valeur de y qui rende vraie l'équation $2y/(y+1) = x$. Autrement dit, résolvons cette équation pour y :

$$\frac{2y}{y+1} = x \Rightarrow 2y = x(y+1) \Rightarrow y(2-x) = x \Rightarrow y = \frac{x}{2-x}.$$

Notez que $x \neq 2$ est une donnée, donc la division par $2-x$ à la dernière étape est logique. Bien sûr, ces étapes n'apparaîtront pas dans la preuve. Posons simplement $y = x/(2-x)$ et essayons de prouver à la fois $2y/(y+1) = x$ et $\forall z (2z/(z+1) = x \rightarrow z = y)$.

Givens	Goals
$x \neq 2$	$\frac{2y}{y+1} = x$
$y = \frac{x}{2-x}$	$\forall z \left(\frac{2z}{z+1} = x \rightarrow z = y \right)$

Le premier objectif est facile à vérifier en remplaçant simplement $x/(2-x)$ par y . Pour le second, supposons que z soit arbitraire, supposons que $2z/(z+1) = x$ et prouvons que $z = y$:

Existence and Uniqueness Proofs	
Givens	Goal
$x \neq 2$	$z = y$
$y = \frac{x}{2-x}$	
$\frac{2z}{z+1} = x$	

Nous pouvons maintenant montrer que $z = y$ en résolvant pour z dans la troisième donnée :

$$\frac{2z}{z+1} = x \Rightarrow 2z = x(z+1) \Rightarrow z(2-x) = x \Rightarrow z = \frac{x}{2-x} = y.$$

Notez que les étapes suivies ici sont exactement les mêmes que celles utilisées précédemment pour déterminer y . Il s'agit d'un schéma courant dans les preuves d'existence et d'unicité. Bien que le travail préliminaire nécessaire pour établir une preuve d'existence ne doive pas figurer dans la preuve, ce travail préliminaire, ou un raisonnement similaire, peut parfois servir à prouver l'unicité de l'objet dont l'existence est démontrée.

Solution

Théorème. Pour chaque nombre réel x , si $x \neq 2$ alors il existe un unique réel nombre y tel que $2y/(y+1) = x$.

Preuve. Soit x un nombre réel arbitraire, et supposons $x \neq 2$. Soit $y = x/(2-x)$, qui est défini puisque $x \neq 2$. Alors

$$\frac{2y}{y+1} = \frac{\frac{2x}{2-x}}{\frac{x}{2-x} + 1} = \frac{\frac{2x}{2-x}}{\frac{2}{2-x}} = \frac{2x}{2} = x.$$

Pour voir que cette solution est unique, supposons que $z/(z+1) = x$. Alors $z = x(z+1)$, donc $z(2-x) = x$. Puisque $x = 2$, nous pouvons diviser les deux côtés par $2-x$ pour obtenir $z = x/(2-x) = y$.

□

Le théorème de [l'exemple 3.6.1](#) peut également servir à formuler des stratégies d'utilisation de données de la forme $\exists! xP(x)$. Encore une fois, l'énoncé 3 du théorème est celui le plus souvent utilisé.

Pour utiliser une donnée de la forme $\exists! xP(x)$:

Considérez ceci comme deux affirmations données, $\exists xP(x)$ et $\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$. Pour utiliser la première affirmation, vous devriez probablement choisir un nom, disons x_0 , pour représenter un objet tel que $P(x_0)$ est vrai. La seconde vous indique que si jamais vous rencontrez deux objets y et z tels que $P(y)$ et $P(z)$ sont tous deux vrais, vous pouvez conclure que $y = z$.

Exemple 3.6.4. Supposons que A , B et C soient des ensembles, que A et B soient non disjoints, que A et C soient non disjoints et que A possède exactement un élément. Démontrer que B et C ne sont pas disjoints.

Travail à partir de zéro

<i>Givens</i>	<i>Goal</i>
$A \cap B \neq \emptyset$	
$A \cap C \neq \emptyset$	
$\exists! x(x \in A)$	

Nous traitons la dernière donnée comme deux données distinctes, comme le suggère notre stratégie. En écrivant la signification des autres données et de l'objectif, nous obtenons la situation suivante :

<i>Givens</i>	<i>Goal</i>
$\exists x(x \in A \wedge x \in B)$	
$\exists x(x \in A \wedge x \in C)$	
$\exists x(x \in A)$	
$\forall y \forall z((y \in A \wedge z \in A) \rightarrow y = z)$	$\exists x(x \in B \wedge x \in C)$

Pour prouver l'objectif, nous devons trouver un élément de B et de C . Pour ce faire, nous nous tournons vers les données. La première

donnée nous indique que nous pouvons choisir un nom, disons b , pour un élément tel que $b \in A$ et $b \in B$. De même, par la seconde donnée, nous pouvons laisser c être quelque chose tel que $c \in A$ et $c \in C$. À ce stade, la troisième donnée est redondante. Nous savons déjà qu'il y a quelque chose dans A , car en fait nous savons déjà que $b \in A$ et $c \in A$. On peut tout aussi bien passer à la dernière donnée, qui dit que si jamais on rencontre deux objets qui sont des éléments de A , on peut conclure qu'ils sont égaux. Mais comme nous venons de le constater, nous savons que $b \in A$ et $c \in A$! On peut donc conclure que $b = c$. Puisque $b \in B$ et $b = c \in C$, nous avons trouvé quelque chose qui est un élément à la fois de B et de C , comme requis pour prouver l'objectif.

Solution

Théorème. *Supposer UN, Groupe C sont des ensembles, UN et B ne sont pas disjoints, UN et C ne sont pas disjoints, et A a exactement un élément. Alors B et C ne sont pas disjoints .*

Preuve . Puisque A et B ne sont pas disjoints, on peut poser b tel que $b \in A$ et $b \in B$. De même, puisque A et C ne sont pas disjoints, il existe un objet c tel que $c \in A$ et $c \in C$. Puisque A n'a qu'un seul élément, nous devons avoir $b = c$. Ainsi, $b = c \in B \cap C$ et donc B et C ne sont pas disjoints.

□

Exercices

- *1. Démontrer que pour chaque nombre réel x , il existe un nombre réel unique y tel que $x^2y = x - y$.
- 2. Démontrer qu'il existe un nombre réel unique x tel que pour tout nombre réel y , $xy + x - 4 = 4y$.
- 3. Démontrer que pour tout nombre réel x , si $x = 0$ et $x = 1$, alors il existe un nombre réel unique y tel que $y/x = y - x$.
- *4. Démontrer que pour tout nombre réel x , si $x = 0$, alors il existe un nombre réel unique y tel que pour tout nombre réel z , $zy = z/x$.
- 5. Rappelons que si \mathcal{F} est une famille d'ensembles, alors $\bigcup \mathcal{F} = \{x \mid \exists A (\ A \in \mathcal{F} \wedge x \in A\)\}$. Supposons que nous définissions un nouvel ensemble $\bigcup! \mathcal{F}$ par la formule $\bigcup! \mathcal{F} = \{x \mid \exists! A (\ A \in \mathcal{F} \wedge x \in A\)\}$.
 - (a) Démontrer que pour toute famille d'ensembles \mathcal{F} , $\bigcup! \mathcal{F} \subseteq \bigcup \mathcal{F}$.

(b) Une famille d'ensembles \mathcal{F} est dite *deux à deux disjointe* si chaque paire d'éléments distincts de \mathcal{F} est disjointe ; c'est-à-dire, $\forall A \in \mathcal{F} \forall B \in \mathcal{F} (A \neq B \rightarrow A \cap B = \emptyset)$. Démontrer que pour toute famille d'ensembles \mathcal{F} , $\bigcup \mathcal{F} = \bigcup \mathcal{F}$ si \mathcal{F} est deux à deux disjoint.

*6. Soit U un ensemble quelconque.

(a) Prouver qu'il existe un unique $A \in \mathcal{P}(U)$ tel que pour tout $B \in \mathcal{P}(U)$, $A \cup B = B$.

(b) Prouver qu'il existe un unique $A \in \mathcal{P}(U)$ tel que pour tout $B \in \mathcal{P}(U)$, $A \cup B = A$.

*7. Soit U un ensemble quelconque.

(a) Prouver qu'il existe un unique $A \in \mathcal{P}(U)$ tel que pour tout $B \in \mathcal{P}(U)$, $A \cap B = B$.

(b) Prouver qu'il existe un unique $A \in \mathcal{P}(U)$ tel que pour tout $B \in \mathcal{P}(U)$, $A \cap B = A$.

*8. Soit U un ensemble quelconque.

(a) Démontrer que pour chaque $A \in \mathcal{P}(U)$ il existe un B unique $\in \mathcal{P}(U)$ tel que pour tout $C \in \mathcal{P}(U)$, $C \setminus A = C \cap B$.

(b) Démontrer que pour chaque $A \in \mathcal{P}(U)$ il existe un B unique $\in \mathcal{P}(U)$ tel que pour tout $C \in \mathcal{P}(U)$, $C \cap A = C \setminus B$.

D 9. Rappelez-vous que vous avez montré dans [l'exercice 14](#) de la section [1.4](#) que la différence symétrique est associative ; en d'autres termes, pour tous les ensembles A , B et C , $A \Delta (B \Delta C) = (A \Delta B) \Delta C$. Vous trouverez peut-être également utile dans ce problème de noter que la différence symétrique est clairement commutative ; en d'autres termes, pour tous les ensembles A et B , $A \Delta B = B \Delta A$.

(a) Démontrer qu'il existe un élément neutre unique pour la différence symétrique. Autrement dit, il existe un ensemble unique X tel que pour tout ensemble A , $A \Delta X = A$.

(b) Démontrer que chaque ensemble possède une unique inverse pour l'opération de différence symétrique. Autrement dit, pour tout ensemble A , il existe un unique ensemble B tel que $A \Delta B = X$, où X est l'élément neutre de la partie (a).

(c) Démontrer que pour tout ensemble A et B , il existe un ensemble unique C tel que $A \Delta C = B$.

(d) Démontrer que pour tout ensemble A , il existe un ensemble unique $B \subseteq A$ tel que pour tout ensemble $C \subseteq A$, $B \Delta C = A \setminus C$.

D 10. Supposons que A soit un ensemble, et pour toute famille d'ensembles \mathcal{F} , si $\bigcup \mathcal{F} = A$ alors $A \in \mathcal{F}$. Démontrer que A a exactement un élément.

- _D *11. Supposons que \mathcal{F} soit une famille d'ensembles qui possède la propriété que pour tout $\mathcal{G} \subseteq \mathcal{F}$, $\bigcup \mathcal{G} \in \mathcal{F}$. Démontrer qu'il existe un ensemble unique A tel que $A \in \mathcal{F}$ et $\forall B \in \mathcal{F}(B \subseteq A)$.
12. (a) Supposons que $P(x)$ soit une affirmation avec une variable libre x . Trouvez une formule, en utilisant les symboles logiques que nous avons étudiés, qui signifie « il existe exactement deux valeurs de x pour lesquelles $P(x)$ est vraie ».
- (b) Sur la base de votre réponse à la partie (a), concevez une stratégie de preuve pour prouver une affirmation de la forme « il y a exactement deux valeurs de x pour lesquelles $P(x)$ est vrai ».
- (c) Démontrer qu'il existe exactement deux solutions à l'équation $x^3 = x^2$.
13. (a) Démontrer qu'il existe un nombre réel unique c tel qu'il existe un nombre réel unique x tel que $x^2 + 3x + c = 0$. (En d'autres termes, il existe un nombre réel unique c tel que l'équation $x^2 + 3x + c = 0$ ait exactement une solution.)
- (b) Montrez qu'il n'existe *pas* un nombre réel unique x tel qu'il existe un nombre réel unique c tel que $x^2 + 3x + c = 0$. (Indice : vous devriez être capable de prouver que pour *tout* nombre réel x , il existe un nombre réel unique c tel que $x^2 + 3x + c = 0$.)

3.7 Autres exemples de preuves

Jusqu'à présent, la plupart de nos preuves ont consisté en des applications assez simples des techniques de preuve présentées. Nous terminons ce chapitre par quelques exemples de preuves un peu plus complexes. Ces preuves utilisent les techniques de ce chapitre, mais, pour diverses raisons, elles sont légèrement plus difficiles que la plupart de nos autres. Preuves précédentes. Certaines sont simplement plus longues et nécessitent l'application de stratégies de preuve supplémentaires. D'autres nécessitent des choix stratégiques judicieux. Dans certains cas, la stratégie à utiliser est évidente, mais une certaine perspicacité est nécessaire pour comprendre précisément comment l'utiliser. Nos exemples précédents, destinés uniquement à illustrer et à clarifier les techniques de preuve, ont pu donner une impression mécanique et fastidieuse de rédaction de preuves. Nous espérons qu'en étudiant ces exemples plus complexes, vous commencerez à comprendre que le raisonnement mathématique peut aussi être surprenant et beau.

Certaines techniques de preuve sont particulièrement difficiles à appliquer. Par exemple, pour prouver un objectif de la forme $\exists x P(x)$, la méthode la plus évidente consiste à essayer de trouver une valeur de x qui rende l'énoncé $P(x)$ vrai. Cependant, il n'est pas toujours évident de trouver cette valeur. Utiliser une donnée de la forme $\forall x P(x)$ est similaire. Vous souhaiterez probablement insérer une valeur particulière pour x , mais pour finaliser la preuve, vous devrez peut-être faire un choix judicieux. Les preuves qui doivent être décomposées en cas sont également parfois difficiles à comprendre. Il est parfois difficile de savoir quand et lesquels utiliser.

Nous commençons par réexaminer les preuves de l'introduction. Certains aspects de ces preuves vous ont probablement semblé quelque peu mystérieux lors de leur lecture. Voyez s'ils vous semblent plus clairs maintenant que vous comprenez mieux comment les preuves sont construites. Nous présenterons chaque preuve exactement comme elle apparaissait dans l'introduction, puis nous la suivrons d'un commentaire expliquant les techniques de preuve utilisées.

Théorème 3.7.1. *Supposer n est un entier supérieur à 1 et n n'est pas premier. Alors $2^n - 1$ n'est pas premier.*

Preuve. Puisque n n'est pas premier, il existe des entiers positifs a et b tels que $a < n$, $b < n$, et $n = ab$. Soit $x = 2^b - 1$ et $y = 1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}$. Alors

$$\begin{aligned} xy &= (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= 2^b \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= (2^b + 2^{2b} + 2^{3b} + \dots + 2^{ab}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= 2^{ab} - 1 \\ &= 2^n - 1. \end{aligned}$$

Puisque $b < n$, nous pouvons conclure que $x = 2^b - 1 < 2^n - 1$. De plus, puisque $ab = n > a$, il s'ensuit que $b > 1$. Par conséquent, $x = 2^b - 1 > 2^1 - 1 = 1$, donc $y < xy = 2^n - 1$. Ainsi, nous avons montré que $2^n - 1$ peut s'écrire comme le produit de deux entiers positifs x et y , tous deux plus petits que $2^n - 1$, donc $2^n - 1$ n'est pas premier.

□

Commentaire. On nous donne que n n'est pas premier, et nous devons prouver que $2^n - 1$ n'est pas premier. Ces deux affirmations sont négatives, mais heureusement, il est facile de les reformuler sous forme positive. Dire qu'un entier supérieur à 1 n'est pas premier signifie qu'il peut s'écrire comme le produit de deux entiers positifs plus petits. Ainsi, l'hypothèse que n n'est pas premier signifie $\exists a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+ (ab = n \wedge a < n \wedge b < n)$, et ce que nous devons prouver est que $2^n - 1$ n'est

pas premier, ce qui signifie $\exists x \in \mathbb{Z}^+ \exists y \in \mathbb{Z}^+ (xy = 2^n - 1 \wedge x < 2^n - 1 \wedge y < 2^n - 1)$. Dans la deuxième phrase de la preuve, nous appliquons l'instanciation existentielle à l'hypothèse que n n'est pas premier, et le reste de la preuve est consacré à présenter les nombres x et y avec les propriétés requises pour prouver que $2^n - 1$ n'est pas premier.

Comme d'habitude dans les démonstrations d'énoncés existentiels, la démonstration n'explique pas comment les valeurs de x et y ont été choisies ; elle démontre simplement que ces valeurs fonctionnent. Une fois les valeurs de x et y données, l'objectif restant à démontrer est : $xy = 2^n - 1 \wedge x < 2^n - 1 \wedge y < 2^n - 1$. Bien entendu, il s'agit de trois objectifs distincts, démontrés un par un. Les démonstrations de ces trois objectifs ne font appel qu'à l'algèbre élémentaire.

L'un des aspects intéressants de cette démonstration est le calcul utilisé pour montrer que $xy = 2^n - 1$. Les formules pour x et y sont quelque peu compliquées, et leur produit paraît encore plus compliqué à première vue. Quelle agréable surprise que la plupart des termes de ce produit s'annulent et que, comme par magie, la réponse $2^n - 1$ apparaisse. Bien sûr, on comprend rétrospectivement que c'est ce calcul qui a motivé le choix de x et y . Un aspect de ce calcul peut cependant vous inquiéter. L'utilisation de « \cdots » dans les formules indique que la démonstration dépend d'une structure de calcul non explicitée. Nous donnerons une démonstration plus rigoureuse de $xy = 2^n - 1$ au [chapitre 6](#), après avoir présenté la méthode de démonstration par induction mathématique (voir [le théorème 6.5.2](#)).

Théorème 3.7.2. *Il existe une infinité de nombres premiers .*

Preuve . Supposons qu'il n'y ait qu'un nombre fini de nombres premiers. Soit p_1, p_2, \dots, p_n une liste de tous les nombres premiers. Soit $m = p_1 p_2 \cdots p_n + 1$. Notons que m n'est pas divisible par p_1 , puisque diviser m par p_1 donne un quotient de $p_2 p_3 \cdots p_n$ et un reste de 1. De même, m n'est divisible par aucun des nombres p_2, p_3, \dots, p_n .

Nous utilisons maintenant le fait que tout entier supérieur à 1 est soit premier, soit peut s'écrire comme un produit de nombres premiers. (Nous verrons une démonstration de ce fait au [chapitre 6](#) – voir [le théorème 6.4.2](#).) De toute évidence, m est supérieur à 1, donc m est soit premier, soit un produit de nombres premiers. Supposons d'abord que m soit premier. Notons que m est supérieur à tous les nombres de la liste p_1, p_2, \dots, p_n , nous avons donc trouvé un nombre premier qui ne figure pas dans cette liste. Mais cela contredit notre

hypothèse selon laquelle il s'agissait d'une liste de *tous* les nombres premiers.

Supposons maintenant que m soit un produit de nombres premiers. Soit q l'un des nombres premiers de ce produit. Alors m est divisible par q . Or, nous avons déjà vu que m n'est divisible par aucun des nombres de la liste p_1, p_2, \dots, p_n , ce qui contredit à nouveau l'hypothèse selon laquelle cette liste inclurait tous les nombres premiers.

Puisque l'hypothèse selon laquelle il existe un nombre fini de nombres premiers a conduit à une contradiction, il doit y avoir une infinité de nombres premiers.

□

Commentaire . Étant donné *qu'infini* signifie *non fini*, l'énoncé du théorème pourrait être considéré comme une affirmation négative. Il n'est donc pas surprenant que la démonstration procède par contradiction. L'hypothèse d'un nombre fini de nombres premiers signifie qu'il existe un entier naturel n tel qu'il y ait n nombres premiers, et l'affirmation qu'il y ait n nombres premiers signifie qu'il existe une liste de nombres distincts p_1, p_2, \dots, p_n telle que chaque nombre de la liste soit premier, et qu'il n'y ait aucun nombre premier qui ne soit pas dans cette liste. Ainsi, la deuxième phrase de la démonstration applique l'instanciation existentielle pour introduire les nombres n et p_1, p_2, \dots, p_n dans la démonstration. À ce stade de la démonstration, nous avons la situation suivante :

<i>Givens</i>	<i>Goal</i>
p_1, p_2, \dots, p_n are all prime $\neg \exists q (q \text{ is prime} \wedge q \notin \{p_1, p_2, \dots, p_n\})$	Contradiction

La seconde donnée pourrait être reformulée par une affirmation positive, mais puisqu'il s'agit d'une preuve par contradiction, une autre approche raisonnable serait d'essayer d'atteindre une contradiction en prouvant que $\exists q (q \text{ est premier} \wedge q \notin \{p_1, p_2, \dots, p_n\})$. C'est la stratégie utilisée dans la preuve. Ainsi, le but du reste de la preuve est de montrer qu'il existe un nombre premier qui ne fait pas partie de la liste p_1, p_2, \dots, p_n – un « nombre premier non listé ».

Puisque notre objectif est maintenant une affirmation existentielle, il n'est pas surprenant que l'étape suivante de la preuve consiste à introduire le nouveau nombre m , sans aucune explication sur son choix. Ce qui est surprenant, c'est que m puisse être ou non le nombre premier non listé que nous recherchons. Le problème est que m pourrait ne pas être premier. Tout ce dont nous sommes sûrs, c'est que

m est soit premier, soit un produit de nombres premiers. Puisque cette affirmation est une disjonction, elle suggère une preuve par cas, et c'est la méthode utilisée dans la suite de la preuve. Bien que les cas ne soient pas explicitement étiquetés comme tels dans la preuve, il est important de comprendre que la suite de la preuve prend la forme d'une preuve par cas. Dans le cas 1, nous supposons que m est premier, et dans le cas 2, nous supposons qu'il est un produit de nombres premiers. Dans les deux cas, nous sommes capables de produire un nombre premier non listé, comme requis pour compléter la preuve.

Notre prochaine preuve utilise la notation factorielle. Rappelons que pour tout entier positif n , la factorielle n est le nombre $n! = 1 \cdot 2 \cdot 3 \cdots n$.

Théorème 3.7.3. *Pour chaque entier positif n , il existe une séquence de n entiers positifs consécutifs ne contenant aucun nombre premier.*

Preuve. Supposons que n soit un entier strictement positif. Soit $x = (n + 1)! + 2$. Nous allons montrer qu'aucun des nombres $x, x + 1, x + 2, \dots, x + (n - 1)$ n'est premier. Puisqu'il s'agit d'une suite de n entiers strictement positifs consécutifs, ceci démontrera le théorème.

Pour voir que x n'est pas premier, notez que

$$\begin{aligned} x &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 2 \\ &= 2 \cdot (1 \cdot 3 \cdot 4 \cdots (n + 1) + 1). \end{aligned}$$

Ainsi, x peut être écrit comme un produit de deux entiers positifs plus petits, donc x n'est pas premier.

De même, nous avons

$$\begin{aligned} x + 1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 3 \\ &= 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n + 1) + 1), \end{aligned}$$

Donc $x + 1$ n'est pas premier non plus. En général, considérons tout nombre $x + i$, où $0 \leq i \leq n - 1$. On a alors

$$\begin{aligned} x + i &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + (i + 2) \\ &= (i + 2) \cdot (1 \cdot 2 \cdot 3 \cdots (i + 1) \cdot (i + 3) \cdots (n + 1) + 1), \end{aligned}$$

donc $x + i$ n'est pas premier.

□

Commentaire. Une suite de n entiers positifs consécutifs est une suite de la forme $x, x + 1, x + 2, \dots, x + (n - 1)$, où x est un entier positif. Ainsi, la forme logique de l'énoncé à prouver est $\forall n > 0 \exists x > 0 \forall i (0 \leq i \leq n - 1 \rightarrow x + i \text{ n'est pas premier})$, où toutes les variables s'étendent sur les entiers. Le plan général de la preuve est exactement ce à quoi on s'attendrait pour une preuve d'un énoncé de cette forme : nous posons $n > 0$ arbitraire, spécifions une valeur pour x , soit i arbitraire, puis

supposons que $0 \leq i \leq n - 1$ et prouvons que $x + i$ n'est pas premier. Comme dans la preuve du [théorème 3.7.1](#), pour prouver que $x + i$ n'est pas premier, nous montrons comment l'écrire comme un produit de deux entiers positifs plus petits.

Avant de démontrer que $x + i$ n'est pas premier, où i est un entier arbitraire compris entre 0 et $n - 1$, la preuve inclut des vérifications que x et $x + 1$ ne sont pas premiers. Ces vérifications sont totalement inutiles et ne sont incluses que pour faciliter la lecture de la preuve.

Exemple 3.7.4. Démontrer qu'il existe un nombre réel unique m possédant les deux propriétés suivantes :

1. Pour tout nombre réel x , $x^2 + 2x + 3 \geq m$.
2. Si y est un nombre réel ayant pour propriété que pour tout nombre réel x , $x^2 + 2x + 3 \geq y$, alors $m \geq y$.

Travail à partir de zéro

Il est pratique de nommer la propriété 1. On dira que m est une *borne inférieure* pour l'expression $x^2 + 2x + 3$ si la propriété 1 est vérifiée ; autrement dit, si pour tout nombre réel x , $x^2 + 2x + 3 \geq m$. La propriété 2 stipule alors que si y est une borne inférieure pour $x^2 + 2x + 3$, alors $m \geq y$. Autrement dit, aucune borne inférieure ne peut être supérieure à m ; m est donc la borne inférieure *maximale*. (Nous reviendrons sur les bornes inférieures et les bornes inférieures maximales dans [la section 4.4 du chapitre 4.](#))

Nous devrons prouver l'existence et l'unicité du nombre m . Pour la partie de la preuve concernant l'existence, le plus difficile est de trouver la bonne valeur pour m . On peut trouver un indice sur la façon de choisir m en complétant le carré :

$$x^2 + 2x + 3 = x^2 + 2x + 1 + 2 = (x + 1)^2 + 2.$$

Puisque $(x + 1)^2$ ne peut pas être négatif, pour tout nombre réel x nous aurons $x^2 + 2x + 3 = (x + 1)^2 + 2 \geq 2$, donc $m = 2$ fonctionnera dans la propriété 1 – en d'autres termes, 2 est une borne inférieure pour $x^2 + 2x + 3$. Bien sûr, tout nombre plus petit serait également une borne inférieure, mais la propriété 2 exige que m soit la plus grande borne inférieure, donc m ne peut pas être inférieur à 2. Peut-être que $m = 2$ est le bon choix. Voyons si nous pouvons prouver la propriété 2 avec ce choix de m .

Pour prouver que la propriété 2 est vraie avec $m = 2$, il faut prouver $\forall y [\forall x (x^2 + 2x + 3 \geq y) \rightarrow 2 \geq y]$. La méthode la plus simple consiste à

poser y comme arbitraire, à supposer $\forall x (x^2 + 2x + 3 \geq y)$, puis à prouver $2 \geq y$, ce qui nous donne la situation suivante :

$$\begin{array}{c} \text{Given} \\ \forall x(x^2 + 2x + 3 \geq y) \end{array} \quad \begin{array}{c} \text{Goal} \\ 2 \geq y \end{array}$$

La manière naturelle d'utiliser notre donnée est de remplacer x par une valeur. En considérant l'objectif, nous voyons que si seulement $x \leq 2$ et $x^2 + 2x + 3 = 2$ existait, alors insérer cette valeur de x dans la donnée nous mènerait directement à l'objectif. En résolvant l'équation $x^2 + 2x + 3 = 2$, nous constatons que poser $x = -1$ complète la preuve.

Il nous reste à prouver l'unicité de m . Pour cela, nous supposerons que m_1 et m_2 sont deux nombres possédant les propriétés 1 et 2, puis nous prouverons que $m_1 = m_2$. Ceci nous donne les données et l'objectif suivants :

$$\begin{array}{c} \text{Given} \\ \begin{aligned} \forall x(x^2 + 2x + 3 \geq m_1) \\ \forall x(x^2 + 2x + 3 \geq m_2) \\ \forall y[\forall x(x^2 + 2x + 3 \geq y) \rightarrow m_1 \geq y] \\ \forall y[\forall x(x^2 + 2x + 3 \geq y) \rightarrow m_2 \geq y] \end{aligned} \end{array} \quad \begin{array}{c} \text{Goal} \\ m_1 = m_2 \end{array}$$

Nous devrions probablement appliquer linstanciation universelle à une ou plusieurs données, mais lesquelles et quelles valeurs devrions-nous remplacer ? Lobservation clé est que les deux premières données suggèrent qu'il serait utile de remplacer y par m_1 ou m_2 dans les troisième et quatrième données. En fait, nous poserons $y = m_2$ dans la troisième donnée et $y = m_1$ dans la quatrième. (Vous pourriez vouloir comparer cela à la stratégie que nous avons utilisée pour la preuve d'unicité dans [l'exemple 3.6.2](#).) Cela nous donne $m_1 \geq m_2$ et $m_2 \geq m_1$, et l'objectif $m_1 = m_2$ en découle.

Solution

Théorème. Il existe un nombre réel unique m avec les deux propriétés suivantes :

1. Pour tout nombre réel x , $x^2 + 2x + 3 \geq m$.
2. Si y est un nombre réel ayant pour propriété que pour tout nombre réel x , $x^2 + 2x + 3 \geq y$, alors $m \geq y$.

Preuve. Existence : Soit $m = 2$. Pour prouver la propriété 1, soit x un nombre réel arbitraire. Alors

$$x^2 + 2x + 3 = (x + 1)^2 + 2 \geq 2 = m,$$

comme requis. Cela montre que 2 est une borne inférieure pour $x^2 + 2x + 3$.

Pour la propriété 2, soit y un nombre arbitraire possédant la propriété que pour tout x , $x^2 + 2x + 3 \geq y$. En particulier, en posant $x = -1$, on trouve que

$$y \leq (-1)^2 + 2(-1) + 3 = 2 = m.$$

Comme y est arbitraire, cela prouve la propriété 2.

Unicité : Supposons que m_1 et m_2 possèdent tous deux les propriétés 1 et 2. Autrement dit, m_1 et m_2 sont tous deux des bornes inférieures pour $x^2 + 2x + 3$, et si y est une borne inférieure quelconque, alors $m_1 \geq y$ et $m_2 \geq y$. En appliquant ce dernier fait à $y = m_1$ et $y = m_2$, nous obtenons $m_1 \geq m_2$ et $m_2 \geq m_1$, donc $m_1 = m_2$.

□

Pour les lecteurs familiarisés avec la définition des limites en calcul différentiel et intégral, nous donnons un exemple supplémentaire illustrant comment les démonstrations impliquant des limites peuvent être réalisées grâce aux techniques présentées dans ce chapitre. Les lecteurs qui ne connaissent pas cette définition sont invités à ignorer cet exemple.

Exemple 3.7.5. Montrer que

$$\lim_{x \rightarrow 3} \frac{2x^2 - 5x - 3}{x - 3} = 7.$$

Travail à partir de zéro

Selon la définition des limites, notre objectif signifie que pour tout nombre positif, il existe un nombre positif δ tel que si x est un nombre tel que $0 < |x - 3| < \delta$, alors $|(\frac{2x^2 - 5x - 3}{x - 3}) - 7| < \epsilon$. En traduisant cela en symboles logiques, nous avons

$$\forall \epsilon > 0 \exists \delta > 0 \forall x \left(0 < |x - 3| < \delta \rightarrow \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| < \epsilon \right).$$

Nous commençons donc par poser un nombre positif arbitraire et essayons ensuite de trouver un nombre positif δ pour lequel nous pouvons prouver

$$\forall x \left(0 < |x - 3| < \delta \rightarrow \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| < \epsilon \right).$$

le travail de recherche de δ n'apparaîtra pas dans la démonstration. Dans la démonstration finale, nous écrirons simplement « Soit $\delta = (\text{un nombre positif})$ » et nous procéderons ensuite à la démonstration.

$$\forall x \left(0 < |x - 3| < \delta \rightarrow \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| < \epsilon \right).$$

Avant de calculer la valeur de δ , voyons à quoi ressemblera la suite de la preuve. Compte tenu de la forme de l'objectif à ce stade, nous devrions procéder en supposant x arbitraire, en supposant $0 < |x - 3| < \delta$, puis en prouvant $|[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon$. Ainsi, la preuve entière aura la forme suivante :

Soit ϵ un nombre positif arbitraire.

Soit $\delta = (\text{un nombre positif})$.

Soit x arbitraire.

Supposons que $0 < |x - 3| < \delta$.

[Preuve de $|[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon$ va ici.]

Par conséquent $0 < |x - 3| < \delta \rightarrow |[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon$.

Puisque x est arbitraire, nous pouvons conclure que $\forall x (0 < |x - 3| < \delta \rightarrow |[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon)$.

Par conséquent, $\exists \delta > 0 \forall x (0 < |x - 3| < \delta \rightarrow |[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon)$. Puisque ϵ était arbitraire, il s'ensuit que $\forall \epsilon > 0 \exists \delta > 0 \forall x (0 < |x - 3| < \delta \rightarrow |[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon)$.

Il reste deux étapes à franchir : déterminer la valeur de δ et compléter la preuve de $|[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon$. *Nous commencerons par la deuxième étape, et au cours de son exécution, la valeur à utiliser pour δ deviendra claire*. Les données et l'objectif de cette deuxième étape sont les suivants :

Given		Goal
$\epsilon > 0$		
$\delta = (\text{some positive number})$		
$0 < x - 3 < \delta$		
		$\left \frac{2x^2 - 5x - 3}{x - 3} - 7 \right < \epsilon$

Tout d'abord, notons que nous avons $0 < |x - 3|$ comme donnée, donc $x = 3$ et donc la fraction $(2x^2 - 5x - 3)/(x - 3)$ est définie. En factorisant le numérateur, nous trouvons que

$$\begin{aligned} \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| &= \left| \frac{(2x + 1)(x - 3)}{x - 3} - 7 \right| \\ &= |2x + 1 - 7| = |2x - 6| = 2|x - 3|. \end{aligned}$$

Nous avons maintenant comme donnée que $|x - 3| < \delta$, donc $2|x - 3| < 2\delta$. En combinant cela avec l'équation précédente, nous obtenons $|[(2x^2 - 5x - 3)/(x - 3) - 7]| < 2\delta$, et notre objectif est $|[(2x^2 - 5x - 3)/(x - 3) - 7]| < \epsilon$. Ainsi, si nous choisissons δ tel que $2\delta = \epsilon$, nous aurons terminé. Autrement dit, nous devrions poser $\delta = \epsilon/2$. Notons que puisque $\epsilon > 0$, c'est un nombre positif, comme requis.

Solution

Théorème. $\lim_{x \rightarrow 3} \frac{2x^2 - 5x - 3}{x - 3} = 7$.

Preuve. Supposons $\epsilon > 0$. Soit $\delta = \epsilon/2$, qui est aussi clairement positif. Soit x un nombre réel arbitraire, et supposons que $0 < |x - 3| < \delta$. Alors

$$\begin{aligned} \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| &= \left| \frac{(2x + 1)(x - 3)}{x - 3} - 7 \right| = |2x + 1 - 7| \\ &= |2x - 6| = 2|x - 3| < 2\delta = 2\left(\frac{\epsilon}{2}\right) = \epsilon. \end{aligned}$$

□

Exercices

D *1. Supposons que \mathcal{F} soit une famille d'ensembles. Démontrer qu'il existe un unique ensemble A possédant les deux propriétés suivantes :

- (a) $\mathcal{F} \subseteq \mathcal{P}(A)$.
- (b) $\forall B (\mathcal{F} \subseteq \mathcal{P}(B) \rightarrow A \subseteq B)$.

(Indice : essayez d'abord un exemple. Soit $\mathcal{F} = \{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}\}$. Pouvez-vous trouver l'ensemble A qui a les propriétés (a) et (b) ?)

2. Démontrer qu'il existe un nombre réel positif unique m qui possède les deux propriétés suivantes :

- (a) Pour tout nombre réel positif x , $\frac{x}{x+1} < m$.
- (b) Si y est un nombre réel positif ayant pour propriété que pour tout nombre réel positif x , $\frac{x}{x+1} < y$, alors $m \leq y$.
- D 3. Supposons que A et B soient des ensembles. Que pouvez-vous démontrer à propos de $\mathcal{P}(A \setminus B) \setminus (\mathcal{P}(A) \setminus \mathcal{P}(B))$? (Non, ce n'est pas égal à \emptyset . Essayez quelques exemples et voyez ce que vous obtenez.)

D 4. Supposons que A , B et C soient des ensembles. Démontrer que les affirmations suivantes sont équivalentes :

- (une) ($\bigcup_{i \in I} A_i$) \cap ($\bigcup_{j \in J} B_j$) $= \emptyset$.
- (b) $A \cap B \subseteq C \subseteq A \cup B$. (Remarque : il s'agit d'une manière abrégée de dire que $A \cap B \subseteq C$ et $C \subseteq A \cup B$.)
- (c) $\bigcup_{i \in I} A_i \subseteq \bigcup_{j \in J} B_j$.
- *5. Supposons que $\{A_i \mid i \in I\}$ est une famille d'ensembles. Démontrer que si $P(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} \mathcal{P}(A_i)$, alors il y a un $i \in I$ tel que $\forall j \in I$ ($A_j \subseteq A_i$).

6. Supposons que \mathcal{F} soit une famille d'ensembles non vide. Soient $I = \bigcup \mathcal{F}$ et $J = \bigcup \mathcal{F}$. Supposons également que $J \neq \emptyset$, et remarquons qu'il en résulte que pour tout $X \in \mathcal{F}$, $X \neq \emptyset$, et aussi que $I \neq \emptyset$. Enfin, supposons que $\{A_i \mid i \in I\}$ est une famille d'ensembles indexés.

- (a) Démontrer que $\bigcup_{i \in J} A_i = \bigcup_{x \in F} (\bigcup_{i \in X} U_n)_i$.
- (b) Démontrer que $\bigcup_{i \in J} A_i = \bigcup_{x \in \mathcal{F}} (\bigcup_{i \in X} U_n)_i$.
- (c) Démontrer que $\bigcup_{i \in J} U_n \subseteq \bigcup_{x \in \mathcal{F}} (\bigcup_{i \in X} A_i)$. Est-il toujours vrai que $\bigcup_{i \in J} A_i = \bigcup_{x \in \mathcal{F}} (\bigcup_{i \in X} A_i)$? Donnez une preuve ou un contre-exemple pour justifier votre réponse.
- (d) Découvrir et prouver un théorème reliant $\bigcup_{i \in J} A_i$ et $\bigcup_{x \in \mathcal{F}} (\bigcup_{i \in X} U_n)_i$.

7. Prouver que $\lim_{x \rightarrow 2} \frac{3x^2 - 12}{x - 2} = 12$.

*8. Démontrer que si $\lim_{x \rightarrow c} f(x) = L$ et $L > 0$, alors il existe un nombre $\delta > 0$ tel que pour tout x , si $0 < |x - c| < \delta$ alors $f(x) > 0$.

9. Démontrer que si $\lim_{x \rightarrow c} f(x) = L$ alors $\lim_{x \rightarrow c} 7f(x) = 7L$.

10. Considérez le théorème putatif suivant.

Théorème? Il y a des nombres irrationnels a et b tel que a^b est rationnel.

La preuve suivante est-elle correcte ? Si oui, quelles stratégies de preuve utilise-t-elle ? Sinon, peut-elle être corrigée ? Le théorème est-il correct ? (Remarque : la preuve utilise le fait que $\sqrt{2}$ est irrationnel, ce que nous démontrerons au [chapitre 6](#) – voir [le théorème 6.4.5](#).)

Preuve. Soit $\sqrt{2}^{\sqrt{2}}$ c'est rationnel, soit c'est irrationnel.

Cas 1. $\sqrt{2}^{\sqrt{2}}$ est rationnel. Soit $a = b = \sqrt{2}$. Alors a et b sont irrationnels, et $a^b = \sqrt{2}^{\sqrt{2}}$ que nous supposons dans ce cas est rationnel.

Cas 2. $\sqrt{2}^{\sqrt{2}}$ est irrationnel. Soit $a = \sqrt{2}^{\sqrt{2}}$ et $b = \sqrt{2}$. Alors, a est irrationnel par hypothèse, et nous savons que b est également irrationnel. De plus,

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = (\sqrt{2})^2 = 2,$$

□

ce qui est rationnel.

4

Rapports

4.1 Paires ordonnées et produits cartésiens

Au [chapitre 1](#), nous avons abordé les ensembles de vérité pour les énoncés contenant une seule variable libre. Dans ce chapitre, nous étendons cette idée aux énoncés comportant plusieurs variables libres.

Par exemple, supposons que $P(x, y)$ soit une affirmation avec deux variables libres x et y . Nous ne pouvons pas dire que cette affirmation est vraie ou fausse tant que nous n'avons pas spécifié deux valeurs – une pour x et une pour y . Ainsi, si nous voulons que l'ensemble de vérité identifie quelles affectations de valeurs aux variables libres rendent l'affirmation vraie, alors l'ensemble de vérité devra contenir non pas des valeurs individuelles, mais des paires de valeurs. Nous spécifierons une paire de valeurs en écrivant les deux valeurs entre parenthèses séparées par une virgule. Par exemple, soit $D(x, y)$ signifie « x divise y ». Alors $D(6, 18)$ est vrai, puisque $6 \mid 18$, donc la paire de valeurs $(6, 18)$ est une affectation de valeurs aux variables x et y qui rend l'affirmation $D(x, y)$ vraie. Notez que 18 ne divise pas 6 , donc la paire de valeurs $(18, 6)$ rend l'affirmation $D(x, y)$ fausse. Il faut donc distinguer les couples $(18, 6)$ et $(6, 18)$. L'ordre des valeurs étant différent, nous appellerons un couple (a, b) un *couple ordonné*, de première coordonnée a et de seconde coordonnée b .

Vous avez probablement déjà vu des paires ordonnées en étudiant des points dans le plan xy . L'utilisation des coordonnées x et y pour identifier des points dans le plan consiste à attribuer à chaque point du plan une paire ordonnée, dont les coordonnées sont ses coordonnées x et y . Ces paires doivent être ordonnées car, par exemple, les points $(2, 5)$ et $(5, 2)$ sont des points différents dans le plan. Dans ce cas, les coordonnées des paires ordonnées sont des nombres réels, mais les paires ordonnées peuvent avoir n'importe quelle valeur. Par exemple, supposons que $C(x, y)$ représente l'énoncé « x a y enfants ». Dans cet énoncé, la variable x couvre l'ensemble de toutes les personnes, et y couvre l'ensemble de toutes les personnes. Ensemble de tous les nombres naturels. Ainsi, les seules paires ordonnées qu'il est judicieux

de considérer lors de l'analyse des affectations de valeurs aux variables x et y dans cette affirmation sont celles dont la première coordonnée est une personne et la seconde un nombre naturel. Par exemple, l'affectation (Prince Charles, 2) rend l'affirmation $C(x, y)$ vraie, car le Prince Charles a bien deux enfants, tandis que l'affectation (Angelina Jolie, 37) la rend fausse. Notez que l'affectation (2, Prince Charles) est absurde, car elle conduirait à l'affirmation absurde « 2 a des enfants du Prince Charles ».

En général, si $P(x, y)$ est une affirmation dans laquelle x s'étend sur un ensemble A et y sur un ensemble B , alors les seules attributions de valeurs à x et y qui auront un sens dans $P(x, y)$ seront des paires ordonnées dont la première coordonnée est un élément de A et la seconde provient de B . On en fait donc la définition suivante :

Définition 4.1.1. Supposons que A et B soient des ensembles. Alors, le *produit cartésien* de A et B , noté $A \times B$, est l'ensemble de tous les couples ordonnés dont la première coordonnée est un élément de A et la seconde un élément de B . Autrement dit,

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

Exemple 4.1.2.

1. Si $A = \{\text{rouge, vert}\}$ et $B = \{2, 3, 5\}$ alors

$$A \times B = \{(\text{rouge}, 2), (\text{rouge}, 3), (\text{rouge}, 5), (\text{vert}, 2), (\text{vert}, 3), (\text{vert}, 5)\}.$$

2. Si P = l'ensemble de toutes les personnes alors

$$\begin{aligned} P \times \mathbb{N} &= \{(p, n) \mid p \text{ is a person and } n \text{ is a natural number}\} \\ &= \{(\text{Prince Charles}, 0), (\text{Prince Charles}, 1), (\text{Prince Charles}, 2), \dots, \\ &\quad (\text{Angelina Jolie}, 0), (\text{Angelina Jolie}, 1), \dots\}. \end{aligned}$$

Ce sont les paires ordonnées qui ont du sens en tant qu'affectations de valeurs aux variables libres x et y dans l'instruction $C(x, y)$.

3. $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \text{ et } y \text{ sont des nombres réels}\}$. Ce sont les coordonnées de tous les points du plan. Pour des raisons évidentes, cet ensemble est parfois noté \mathbb{R}^2 .

L'introduction d'un nouveau concept mathématique nous permet de mettre en pratique nos techniques de démonstration en démontrant certaines propriétés fondamentales de ce nouveau concept. Voici un théorème donnant quelques propriétés fondamentales des produits cartésiens.

Théorème 4.1.3. Supposer UN, B, C , et D sont des ensembles .

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
3. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
4. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.
5. $Un \times \emptyset = \emptyset \times A = \emptyset$.

Preuve de 1. Soit p un élément arbitraire de $A \times (B \cap C)$. Alors, par définition du produit cartésien, p doit être une paire ordonnée dont la première coordonnée est un élément de A et la seconde coordonnée est un élément de $B \cap C$. En d'autres termes, $p = (x, y)$ pour certains $x \in A$ et $y \in B \cap C$. Puisque $y \in B \cap C$, $y \in B$ et $y \in C$. Puisque $x \in A$ et $y \in B$, $p = (x, y) \in A \times B$, et de même $p \in A \times C$. Ainsi, $p \in (A \times B) \cap (A \times C)$. Puisque p est un élément arbitraire de $A \times (B \cap C)$, il s'ensuit que $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

Soit maintenant p un élément arbitraire de $(A \times B) \cap (A \times C)$. Alors $p \in A \times B$, donc $p = (x, y)$ pour certains $x \in A$ et $y \in B$. De plus, $(x, y) = p \in A \times C$, donc $y \in C$. Puisque $y \in B$ et $y \in C$, $y \in B \cap C$. Ainsi, $p = (x, y) \in A \times (B \cap C)$. Puisque p est un élément arbitraire de $(A \times B) \cap (A \times C)$ nous pouvons conclure que $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$, donc $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Commentaire. Avant de continuer avec les preuves des autres parties, nous donnons un bref commentaire sur la preuve qui vient d'être donnée. L'énoncé 1 est une équation entre deux ensembles, donc comme nous l'avons vu dans [l'exemple 3.4.5](#), il y a deux approches naturelles que nous pourrions adopter pour la prouver. Nous pourrions prouver $\forall p [p \in A \times (B \cap C) \leftrightarrow p \in (A \times B) \cap (A \times C)]$ ou nous pourrions prouver à la fois $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$ et $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$. Dans cette preuve, nous avons adopté la deuxième approche. Le premier paragraphe donne la preuve que $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$, et le deuxième donne la preuve que $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

Français Dans la première de ces démonstrations, nous adoptons l'approche habituelle en posant p comme un élément arbitraire de $A \times (B \cap C)$ puis en prouvant $p \in (A \times B) \cap (A \times C)$. Puisque $p \in A \times (B \cap C)$ signifie $\exists x \exists y (x \in A \wedge y \in B \cap C \wedge p = (x, y))$, nous introduisons immédiatement les variables x et y par instanciation existentielle. Le reste de la démonstration consiste simplement à élaborer les définitions des opérations de théorie des ensembles impliquées. La démonstration de l'inclusion inverse dans le deuxième paragraphe est similaire.

Notez que dans les deux parties de cette démonstration, nous avons introduit un objet arbitraire p qui s'est avéré être une paire ordonnée, et nous avons donc pu dire que $p = (x, y)$ pour certains objets x et y . Dans la plupart des démonstrations impliquant des produits cartésiens,

les mathématiciens suppriment cette étape. Si cela est clair dès le départ, Pour qu'un objet soit une paire ordonnée, on l'appelle généralement (x, y) dès le départ. Nous suivrons cette pratique dans nos démonstrations.

Nous laissons les preuves des énoncés 2 et 3 en exercices (voir [exercice 5](#)).

Preuve de 4. Soit (x, y) un élément arbitraire de $(A \times B) \cup (C \times D)$. Alors soit $(x, y) \in A \times B$ soit $(x, y) \in C \times D$.

Cas 1. $(x, y) \in A \times B$. Alors $x \in A$ et $y \in B$, donc clairement $x \in A \cup C$ et $y \in B \cup D$. Par conséquent $(x, y) \in (A \cup C) \times (B \cup D)$.

Cas 2. $(x, y) \in C \times D$. Un argument similaire montre que $(x, y) \in (A \cup C) \times (B \cup D)$.

Étant donné que (x, y) est un élément arbitraire de $(A \times B) \cup (C \times D)$, il s'ensuit que $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Preuve de 5. Supposons que $A \times \emptyset = \emptyset$. Alors $A \times \emptyset$ possède au moins un élément, et par définition du produit cartésien, cet élément doit être une paire ordonnée (x, y) pour certains $x \in A$ et $y \in \emptyset$. Mais cela est impossible, car \emptyset n'a aucun élément. Ainsi, $A \times \emptyset = \emptyset$. La preuve que $\emptyset \times A = \emptyset$ est similaire.

Commentaire. L'énoncé 4 stipule qu'un ensemble est un sous-ensemble d'un autre, et la démonstration suit le schéma habituel pour les énoncés de ce type : nous partons d'un élément quelconque du premier ensemble, puis démontrons qu'il est un élément du second. Il est clair que l'élément quelconque du premier ensemble doit être une paire ordonnée ; nous l'avons donc écrite comme telle dès le début.

Ainsi, pour le reste de la preuve, nous avons $(x, y) \in (A \times B) \cup (C \times D)$ comme donnée, et le but est de prouver que $(x, y) \in (A \cup C) \times (B \cup D)$. La donnée signifie $(x, y) \in A \times B \vee (x, y) \in C \times D$, donc la preuve par cas est une stratégie appropriée. Dans chaque cas, il est facile de prouver l'objectif.

L'énoncé 5 signifie que $A \times \emptyset = \emptyset \wedge \emptyset \times A = \emptyset$. Nous traitons donc cela comme deux objectifs et prouvons que $A \times \emptyset = \emptyset$ et $\emptyset \times A = \emptyset$ séparément. Dire qu'un ensemble est égal à l'ensemble vide est en fait une affirmation négative, même si cela peut ne pas sembler le cas à première vue, car cela signifie que l'ensemble n'a *aucun* élément. Il n'est donc pas surprenant que la preuve que $A \times \emptyset = \emptyset$ procède par contradiction. L'hypothèse que $A \times \emptyset = \emptyset$ signifie $\exists p (p \in A \times \emptyset)$, notre prochaine étape consiste donc à introduire un nom pour un élément de $A \times \emptyset$. Une fois de plus, il est clair que le nouvel objet introduit dans la preuve est une paire ordonnée, nous l'avons donc écrite comme une

paire ordonnée (x, y) dès le début. Écrire la signification de $(x, y) \in A \times \emptyset$ conduit immédiatement à une contradiction.

La preuve que $\emptyset \times A = \emptyset$ est semblable, mais le simple *fait de l'affirmer ne suffit pas à la prouver*. Ainsi, l'affirmation de la similitude de cette partie de la preuve indique que la seconde partie de la preuve est laissée en exercice. Il est conseillé de travailler mentalement les détails de cette preuve (ou, si nécessaire, de les écrire sur papier) pour être sûr qu'une preuve similaire à celle de la première moitié fonctionnera réellement.

Comme l'ordre des coordonnées dans une paire ordonnée est important, $A \times B$ et $B \times A$ ont des significations différentes. Est-il possible que $A \times B = B \times A$? Cela pourrait se produire si $A = B$. *De toute évidence*, si $A = B$, alors $A \times B = A \times A = B \times A$. Existe-t-il d'autres possibilités?

Voici une preuve incorrecte que $A \times B = B \times A$ seulement si $A = B$: Les premières coordonnées des paires ordonnées dans $A \times B$ proviennent de A , et les premières coordonnées des paires ordonnées dans $B \times A$ proviennent de B . Mais si $A \times B = B \times A$, alors les premières coordonnées de ces deux ensembles doivent être les mêmes, donc $A = B$.

Français Ceci est un bon exemple de pourquoi il est important de s'en tenir aux règles d'écriture de preuves que nous avons étudiées plutôt que de se laisser convaincre par n'importe quel raisonnement qui semble plausible. Le raisonnement informel du paragraphe précédent est incorrect, et nous pouvons trouver l'erreur en essayant de reformuler ce raisonnement sous forme de preuve formelle. Supposons $A \times B = B \times A$. Pour prouver que $A = B$, nous pourrions laisser x être arbitraire, puis essayer de prouver $x \in A \rightarrow x \in B$ et $x \in B \rightarrow x \in A$. Pour le premier de ces cas, nous supposerons $x \in A$ et essaierons de prouver $x \in B$. Maintenant, la preuve incorrecte suggère que nous devrions essayer de montrer que x est la première coordonnée d'une paire ordonnée dans $A \times B$, puis utiliser le fait que $A \times B = B \times A$. Nous pourrions le faire en essayant de trouver un objet $y \in B$, puis en formant la paire ordonnée (x, y) . On aurait alors $(x, y) \in A \times B$ et $A \times B = B \times A$, et il s'ensuivrait que $(x, y) \in B \times A$ et donc $x \in B$. Mais comment trouver un objet $y \in B$? On ne dispose d'aucune information sur B , si ce n'est que $A \times B = B \times A$. En fait, B pourrait être le Ensemble vide ! C'est là le défaut de la preuve. Si $B = \emptyset$, il sera impossible de choisir $y \in B$, et la preuve s'effondrera. Pour des raisons similaires, l'autre moitié de la preuve ne fonctionnera pas si $A = \emptyset$.

Non seulement nous avons trouvé la faille dans la preuve, mais nous pouvons maintenant déterminer comment la corriger. Nous devons prendre en compte la possibilité que A ou B soient l'ensemble vide.

Théorème 4.1.4. *Supposons UN et B sont des ensembles. Alors $A \times B = B \times A$ si et seulement si $A = \emptyset$, $B = \emptyset$ ou $A = B$.*

Preuve. (\rightarrow) Supposons que $A \times B = B \times A$. Si $A = \emptyset$ ou $B = \emptyset$, alors il n'y a plus rien à prouver, donc supposons $A = \emptyset$ et $B = \emptyset$. Nous allons montrer que $A = B$. Soit x arbitraire, et supposons $x \in A$. Puisque $B = \emptyset$ nous pouvons choisir un $y \in B$. Alors $(x, y) \in A \times B = B \times A$, donc $x \in B$.

Supposons maintenant que $x \in B$. Puisque $A = \emptyset$ nous pouvons choisir un $z \in A$. Par conséquent $(x, z) \in B \times A = A \times B$, donc $x \in A$. Ainsi $A = B$, comme requis.

(\leftarrow) Supposons que $A = \emptyset$, $B = \emptyset$ ou $A = B$.

Cas 1. $A = \emptyset$. Alors $A \times B = \emptyset \times B = \emptyset = B \times \emptyset = B \times A$.

Cas 2. $B = \emptyset$. Similaire au cas 1.

Cas 3. $A = B$. Alors $A \times B = A \times A = B \times A$.

Commentaire . Bien sûr, l'énoncé à prouver est un énoncé ssi, nous prouvons donc les deux directions séparément. Pour la direction \rightarrow , notre objectif est $A = \emptyset \vee B = \emptyset \vee A = B$, qui pourrait s'écrire comme $(A = \emptyset \vee B = \emptyset) \vee A = B$, donc par l'une de nos stratégies pour les disjonctions du [chapitre 3](#), nous pouvons supposer $\neg(A = \emptyset \vee B = \emptyset)$ et prouver $A = B$. Notez que par l'une des lois de De Morgan, $\neg(A = \emptyset \vee B = \emptyset)$ est équivalent à $A = \emptyset \wedge B = \emptyset$, nous traitons donc cela comme deux hypothèses, $A = \emptyset$ et $B = \emptyset$. Bien sûr, nous aurions pu procéder différemment, par exemple en supposant $A = B$ et $B = \emptyset$, puis en prouvant $A = \emptyset$. Mais rappelons-nous du commentaire de la partie 5 du [théorème 4.1.3](#) que $A = \emptyset$ et $B = \emptyset$ sont en fait des énoncés négatifs, donc comme il est généralement préférable de travailler avec des énoncés positifs que négatifs, nous avons intérêt à les nier tous les deux pour obtenir les hypothèses $A = \emptyset$ et $B = \emptyset$, puis à prouver l'énoncé positif $A = B$. Les hypothèses $A = \emptyset$ et $B = \emptyset$ sont des énoncés existentiels, elles sont donc utilisées dans la preuve pour justifier l'introduction de y et z . La preuve que $A = B$ procède de manière évidente, en introduisant un objet arbitraire x , puis en prouvant $x \in A \leftrightarrow x \in B$.

Pour la direction \leftarrow de la preuve, nous avons $A = \emptyset \vee B = \emptyset \vee A = B$ comme donnée ; il est donc naturel d'utiliser la preuve par cas. Dans chaque cas, l'objectif est facile à prouver.

Ce théorème illustre mieux la réalité mathématique que la plupart des exemples que nous avons vus jusqu'à présent. Généralement, lorsqu'on cherche la réponse à une question mathématique, on ne connaît pas à l'avance la réponse. On peut deviner la réponse et avoir une idée de la manière dont la démonstration pourrait se dérouler, mais cette hypothèse peut être erronée et l'idée de démonstration erronée.

Ce n'est qu'en transformant cette idée en démonstration formelle, conformément aux règles du [chapitre 3](#), que l'on peut être sûr que la réponse est correcte. Souvent, en essayant de construire une démonstration formelle, on découvre une faille dans son raisonnement, comme nous l'avons vu précédemment, et il faut parfois revoir ses idées pour la corriger. Le théorème et la démonstration finaux sont souvent le fruit d'erreurs et de corrections répétées. Bien sûr, lorsque les mathématiciens rédigent leurs théorèmes et leurs démonstrations, ils suivent notre règle selon laquelle les démonstrations servent à justifier les théorèmes et non à expliquer les processus de pensée ; elles ne décrivent donc pas toutes les erreurs commises. Mais ce n'est pas parce que les mathématiciens n'expliquent pas leurs erreurs dans leurs preuves que vous devez penser qu'ils n'en font pas !

Maintenant que nous savons comment utiliser les paires ordonnées et les produits cartésiens pour parler de l'attribution de valeurs à des variables libres, nous sommes prêts à définir des ensembles de vérité pour les instructions contenant deux variables libres.

Définition 4.1.5. Supposons que $P(x, y)$ soit une affirmation à deux variables libres dans laquelle x s'étend sur un ensemble A et y sur un autre ensemble B . Alors, $A \times B$ est l'ensemble de toutes les affectations de valeurs à x et y qui ont un sens dans l'affirmation $P(x, y)$. L'*ensemble de vérité* de $P(x, y)$ est le sous-ensemble de $A \times B$ constitué des affectations qui rendent l'affirmation vraie. Autrement dit, l'ensemble de vérité de $P(x, y)$ est l'ensemble $\{(a, b) \in A \times B \mid P(a, b)\}$.

Exemple 4.1.6. Quels sont les ensembles de vérité des affirmations suivantes ?

1. « x a y enfants », où x s'étend sur l'ensemble P de toutes les personnes et y s'étend sur \mathbb{N} .
2. « x est situé dans y », où x s'étend sur l'ensemble C de toutes les villes et y s'étend sur l'ensemble N de tous les pays.
3. « $y = 2x - 3$ », où x et y s'étendent sur \mathbb{R} .

Solutions

1. $\{(p, n) \in P \times \mathbb{N} \mid \text{la personne } p \text{ a } n \text{ enfants}\} = \{\text{(Prince Charles, 2), ...}\}$.
2. $\{(c, n) \in C \times N \mid \text{la ville } c \text{ est située dans le pays } n\} = \{\text{(New York, États-Unis), (Tokyo, Japon), (Paris, France), ...}\}$.

3. $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x - 3\} = \{(0, -3), (1, -1), (2, 1), \dots\}$. Vous savez probablement déjà que les paires ordonnées de cet ensemble sont les coordonnées de points du plan situés le long d'une droite, appelée graphe de l'équation $y = 2x - 3$. Ainsi, vous pouvez considérer le graphe de l'équation comme une image de son ensemble de vérité !

Français De nombreux faits sur les ensembles de vérité pour les énoncés à une variable libre que nous avons discutés au [chapitre 1](#) s'appliquent aux ensembles de vérité pour les énoncés à deux variables libres. Par exemple, supposons que T soit l'ensemble de vérité d'un énoncé $P(x, y)$, où x s'étend sur un ensemble A et y sur B . Alors, pour tout $a \in A$ et $b \in B$, l'énoncé $(a, b) \in T$ a la même signification que $P(a, b)$. De plus, si $P(x, y)$ est vrai pour tout $x \in A$ et $y \in B$, alors $T = A \times B$, et si $P(x, y)$ est faux pour tout $x \in A$ et $y \in B$, alors $T = \emptyset$. Si S est l'ensemble de vérité d'un autre énoncé $Q(x, y)$, alors l'ensemble de vérité de l'énoncé $P(x, y) \wedge Q(x, y)$ est $T \cap S$, et l'ensemble de vérité de $P(x, y) \vee Q(x, y)$ est $T \cup S$.

Bien que nous nous concentrions sur les paires ordonnées dans la suite de ce chapitre, il est possible de travailler avec des triplets ordonnés, des quadruplets ordonnés, etc. Ceux-ci peuvent être utilisés pour parler d'ensembles de vérité pour des énoncés contenant trois variables libres ou plus. Par exemple, soit $L(x, y, z)$ l'énoncé « x a vécu à y pendant z ans », où x couvre l'ensemble P de toutes les personnes, y couvre l'ensemble C de toutes les villes et z couvre \mathbb{N} . Ensuite, les affectations de valeurs Les variables libres qui ont du sens dans cette affirmation seraient des triplets ordonnés (p, c, n) , où p est une personne, c est une ville et n est un nombre naturel. L'ensemble de tous ces triplets ordonnés s'écrirait $P \times C \times \mathbb{N}$, et l'ensemble de vérité de l'affirmation $L(x, y, z)$ serait l'ensemble $\{(p, c, n) \in P \times C \times \mathbb{N} \mid \text{la personne } p \text{ a vécu dans la ville } c \text{ pendant } n \text{ années}\}$.

Exercices

- *1. Quels sont les ensembles de vérité des affirmations suivantes ?
Enumérez quelques éléments de chaque ensemble de vérité.
- (a) « x est un parent de y », où x et y s'étendent tous deux sur l'ensemble P de toutes les personnes.
 - (b) « Il y a quelqu'un qui vit à x et qui fréquente y », où x s'étend sur l'ensemble C de toutes les villes et y s'étend sur l'ensemble U de toutes les universités.

2. Quels sont les ensembles de vérité des affirmations suivantes ?
 Enumérez quelques éléments de chaque ensemble de vérité.
- (a) « x vit dans y », où x s'étend sur l'ensemble P de toutes les personnes et y s'étend sur l'ensemble C de toutes les villes.
- (b) « La population de x est y », où x s'étend sur l'ensemble C de toutes les villes et y s'étend sur \mathbb{N} .
3. Les ensembles de vérité des énoncés suivants sont des sous-ensembles de \mathbb{R}_2 . Citez quelques éléments de chaque ensemble de vérité. Dessinez une image montrant tous les points du plan dont les coordonnées sont dans l'ensemble de vérité.
- (a) $y = x^2 - x - 2$.
- (b) $y < x$.
- (c) Soit $y = x^2 - x - 2$, soit $y = 3x - 2$.
- (d) $y < x$, et soit $y = x^2 - x - 2$ soit $y = 3x - 2$.
- *4. Soit $A = \{1, 2, 3\}$, $B = \{1, 4\}$, $C = \{3, 4\}$ et $D = \{5\}$. Calculer tous les ensembles mentionnés dans [le théorème 4.1.3](#) et vérifier que toutes les parties du théorème sont vraies.
5. Démontrer les parties 2 et 3 du [théorème 4.1.3](#).
- *6. Quel est le problème avec la preuve suivante selon laquelle pour tout ensemble A , B , C et D , $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$? (Notez qu'il s'agit de l'inverse de l'inclusion dans la partie 4 du [théorème 4.1.3](#).)
- Preuve.* Supposons que $(x, y) \in (A \cup C) \times (B \cup D)$. Alors $x \in A \cup C$ et $y \in B \cup D$, donc soit $x \in A$ soit $x \in C$, et soit $y \in B$ soit $y \in D$. Nous considérons ces cas séparément.
- Cas 1. $x \in A$ et $y \in B$. Alors $(x, y) \in A \times B$.
- Cas 2. $x \in C$ et $y \in D$. Alors $(x, y) \in C \times D$.
- Ainsi, soit $(x, y) \in A \times B$ soit $(x, y) \in C \times D$, donc $(x, y) \in (A \times B) \cup (C \times D)$.
-
7. Si A a m éléments et B a n éléments, combien d'éléments $A \times B$ a-t-il ?
- *8. Est-il vrai que pour tous les ensembles A , B et C , $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$? Donnez une preuve ou un contre-exemple pour justifier votre réponse.
9. Démontrer que pour tous les ensembles A , B et C , $A \times (B \Delta C) = (A \times B) \setminus (A \times C)$.
- *10. Démontrer que pour tous les ensembles A , B , C et D , $(A \setminus C) \times (B \setminus D) \subseteq (A \times B) \setminus (C \times D)$.

11. Démontrer que pour tous ensembles A, B, C et D , $(A \times B) \setminus (C \times D) = [A \times (B \setminus D)] \cup [(A \setminus C) \times B]$.
12. Démontrer que pour tout ensemble A, B, C et D , si $A \times B$ et $C \times D$ sont disjoints, alors soit A et C sont disjoints, soit B et D sont disjoints.
13. Supposons que $I = \emptyset$. Démontrer que pour toute famille indexée d'ensembles $\{A_i \mid i \in I\}$ et tout ensemble B , $(\cap_{i \in I} A_i) \times B = \cap_{i \in I} (A_i \times B)$. Où dans la preuve l'hypothèse que $I = \emptyset$ est-elle utilisée ?
14. Supposons que $\{A_i \mid i \in I\}$ et $\{B_i \mid i \in I\}$ soient des familles d'ensembles indexées.
- (a) Démontrer que $\cup_{i \in I} (A_i \times B_i) \subseteq (\cup_{i \in I} A_i) \times (\cup_{i \in I} B_i)$.
- (b) Pour chaque $(i, j) \in I \times I$ soit $C_{(i, j)} = A_i \times B_j$, et soit $P = I \times I$. Démontrer que $\cup_{p \in P} C_p = (\cup_{i \in I} B_i)$

*15. Ce problème a été suggéré par le professeur Alan Taylor de l'Union College, New York. Considérons le théorème putatif suivant.

Théorème? Pour tous les ensembles UN, B, C , et D , si $A \times B \subseteq C \times D$ alors $A \subseteq C$ et $B \subseteq D$.

La preuve suivante est-elle correcte ? Si oui, quelles stratégies de preuve utilise-t-elle ? Si non, peut-elle être corrigée ? Le théorème est-il correct ?

Preuve. Supposons que $A \times B \subseteq C \times D$. Soit a un élément arbitraire de A et soit b un élément arbitraire de B . Alors $(a, b) \in A \times B$, donc puisque $A \times B \subseteq C \times D$, $(a, b) \in C \times D$. Par conséquent $a \in C$ et $b \in D$. Puisque a et b sont des éléments arbitraires de A et B , respectivement, cela montre que $A \subseteq C$ et $B \subseteq D$.

□

4.2 Relations

Supposons que $P(x, y)$ soit une affirmation comportant deux variables libres x et y . On peut souvent considérer une telle affirmation comme l'expression d'une *relation* entre x et y . L'ensemble de vérité de l'affirmation $P(x, y)$ est un ensemble de paires ordonnées qui enregistre les cas où cette relation est vérifiée. En fait, il est souvent utile de considérer tout ensemble de paires ordonnées de cette manière, comme un enregistrement des cas où une relation est vérifiée. C'est la raison d'être de la définition suivante.

Définition 4.2.1. Supposons que A et B soient des ensembles. Alors un ensemble $R \subseteq A \times B$ est appelé une *relation de UN à B*.

Si x est compris entre A et y entre B , alors l'ensemble de vérité de toute affirmation $P(x, y)$ sera clairement une relation de A vers B . Cependant, notez que [la définition 4.2.1](#) n'exige pas qu'un ensemble de paires ordonnées soit défini comme l'ensemble de vérité d'une affirmation pour que cet ensemble soit une relation. Bien que la réflexion sur les ensembles de vérité ait motivé cette définition, celle-ci ne dit rien explicitement à ce sujet. Selon la définition, *tout sous-ensemble de $A \times B$ doit être qualifié de relation de A vers B* .

Exemple 4.2.2. Voici quelques exemples de relations d'un ensemble à un autre.

1. Soit $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$ et $R = \{(1, 3), (1, 5), (3, 3)\}$. Alors $R \subseteq A \times B$, donc R est une relation de A vers B .
2. Soit $G = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x > y\}$. Alors G est une relation de \mathbb{R} vers \mathbb{R} .
3. Soit $A = \{1, 2\}$ et $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Soit $E = \{(x, y) \in A \times B \mid x \in y\}$. Alors E est une relation de A vers B . Dans ce cas, $E = \{(1, \{1\}), (1, \{1, 2\}), (2, \{2\}), (2, \{1, 2\})\}$.

Pour les trois exemples suivants, soit S l'ensemble de tous les étudiants de votre école, R l'ensemble de toutes les chambres d'étudiants, P l'ensemble de tous les professeurs et C l'ensemble de tous les cours.

4. Soit $L = \{(s, r) \in S \times R \mid \text{l'étudiant } s \text{ vit dans la chambre universitaire } r\}$. Alors L est une relation de S vers R .
5. Soit $E = \{(s, c) \in S \times C \mid \text{l'étudiant } s \text{ est inscrit au cours } c\}$. Alors E est une relation de S vers C .
6. Soit $T = \{(c, p) \in C \times P \mid \text{le cours } c \text{ est enseigné par le professeur } p\}$. Alors T est une relation de C vers P .

Jusqu'ici, nous nous sommes principalement concentrés sur le développement de vos compétences en rédaction. Une autre compétence importante en mathématiques est la capacité à comprendre et à appliquer. Nouvelles définitions. Voici les définitions de plusieurs nouveaux concepts impliquant des relations. Nous donnerons bientôt des exemples illustrant ces concepts, mais commencez par vérifier si vous pouvez les comprendre à partir de leurs définitions.

Définition 4.2.3. Supposons que R soit une relation de A vers B . Alors, le *domaine* de R est l'ensemble

$$\text{Dom}(R) = \{a \in A \mid \exists b \in B ((a, b) \in R)\}.$$

La portée de R est l'ensemble

$$\text{Ran}(R) = \{b \in B \mid \exists a \in A ((a, b) \in R)\}.$$

L'inverse de R est la relation R^{-1} de B vers A définie comme suit :

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

Supposons enfin que R soit une relation de A vers B et que S soit une relation de B vers C . La composition de S et R est alors la relation $S \circ R$ de A vers C définie comme suit :

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B ((a, b) \in R \text{ et } (b, c) \in S)\}.$$

Notez que nous avons supposé que les secondes coordonnées des paires dans R et les premières coordonnées des paires dans S proviennent toutes deux du même ensemble B , car c'est la situation dans laquelle nous nous intéresserons le plus souvent à $S \circ R$. Cependant, cette restriction n'est pas vraiment nécessaire, comme nous vous demandons de le montrer dans [l'exercice 15](#).

Selon [la définition 4.2.3](#), le domaine d'une relation de A à B est l'ensemble contenant toutes les premières coordonnées des paires ordonnées de la relation. Il s'agit généralement d'un sous-ensemble de A , mais pas nécessairement de la totalité de A . Prenons par exemple la relation L de la partie 4 de [l'exemple 4.2.2](#), qui associe les étudiants à leurs chambres universitaires. Le domaine de L contiendrait tous les étudiants apparaissant comme première coordonnée d'une paire ordonnée de L – autrement dit, tous les étudiants qui vivent dans une chambre universitaire – mais ne contiendrait pas, par exemple, les étudiants qui vivent dans des appartements hors campus. En appliquant la définition plus précisément, nous obtenons

$$\begin{aligned}\text{Dom}(L) &= \{s \in S \mid \exists r \in R((s, r) \in L)\} \\ &= \{s \in S \mid \exists r \in R(\text{the student } s \text{ lives in the dorm room } r)\} \\ &= \{s \in S \mid \text{the student } s \text{ lives in some dorm room}\}.\end{aligned}$$

De même, l'étendue d'une relation est l'ensemble contenant toutes les secondes coordonnées de ses paires ordonnées. Par exemple, l'étendue de la relation L serait la Ensemble de toutes les chambres de résidence universitaire occupées par un étudiant. Les chambres inoccupées ne sont pas comprises dans la plage de L .

L'inverse d'une relation contient exactement les mêmes paires ordonnées que la relation d'origine, mais l'ordre des coordonnées de chaque paire est inversé. Ainsi, dans le cas de la relation L , si Joe Smith habite la chambre 213 Davis Hall, alors $(\text{Joe Smith}, 213 \text{ Davis Hall}) \in L$ et $(213 \text{ Davis Hall}, \text{Joe Smith}) \in L^{-1}$. En général, pour tout étudiant s et

chambre r , on aurait $(r, s) \in L^{-1}$ ssi $(s, r) \in L$. Prenons un autre exemple : la relation G de la partie 2 de [l'exemple 4.2.2](#). Elle contient toutes les paires ordonnées de nombres réels (x, y) pour lesquels x est supérieur à y . On pourrait l'appeler la relation « supérieur à ». Son inverse est

$$\begin{aligned} G^{-1} &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (y, x) \in G\} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y > x\} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}. \end{aligned}$$

En d'autres termes, l'inverse de la relation « supérieur à » est la relation « inférieur à » !

Le concept le plus complexe introduit dans [la définition 4.2.3](#) est celui de la composition de deux relations. Prenons comme exemple les relations E et T des parties 5 et 6 de [l'exemple 4.2.2](#). Rappelons que E est une relation de l'ensemble S des étudiants à l'ensemble C des cours, et que T est une relation de C à l'ensemble P des professeurs. Selon [la définition 4.2.3](#), la composition $T \circ E$ est la relation de S à P définie comme suit :

$$\begin{aligned} T \circ E &= \{(s, p) \in S \times P \mid \exists c \in C((s, c) \in E \text{ and } (c, p) \in T)\} \\ &= \{(s, p) \in S \times P \mid \exists c \in C(\text{the student } s \text{ is enrolled in the course } c \\ &\quad \text{and the course } c \text{ is taught by the professor } p)\} \\ &= \{(s, p) \in S \times P \mid \text{the student } s \text{ is enrolled in some course taught} \\ &\quad \text{by the professor } p\}. \end{aligned}$$

Ainsi, si Joe Smith est inscrit en Biologie 12 et que Biologie 12 est enseignée par le professeur Evans, alors $(\text{Joe Smith}, \text{Biologie 12}) \in E$ et $(\text{Biologie 12}, \text{professeur Evans}) \in T$, et donc $(\text{Joe Smith}, \text{professeur Evans}) \in T \circ E$. En général, si s est un étudiant particulier et p est un professeur particulier, alors $(s, p) \in T \circ E$ ssi il existe un cours c tel que $(s, c) \in E$ et $(c, p) \in T$. Cette notation peut sembler à première vue rétrograde. Si $(s, c) \in E$ et $(c, p) \in T$, alors vous pourriez être tenté d'écrire $(s, p) \in E \circ T$, mais selon notre définition, la notation correcte est $(s, p) \in T \circ E$. La raison pour laquelle nous avons choisi d'écrire les compositions de relations de cette manière deviendra claire au [chapitre 5](#). Pour le moment, vous devrez simplement faire attention à ce détail de notation lorsque vous travaillerez avec des compositions de relations.

Exemple 4.2.4. Soient S , R , C et P les ensembles d'étudiants, de chambres, de cours et de professeurs de votre établissement, comme précédemment, et L , E et T les relations définies dans les parties 4 à 6 de [l'exemple 4.2.2](#). Décrivez les relations suivantes.

1. E^{-1} .
2. $E \circ L^{-1}$.

3. $E^{-1} \circ E$.

4. $E \circ E^{-1}$.

5. $T \circ (E \circ L^{-1})$.

6. $(T \circ E) \circ L^{-1}$.

Solutions

1. $E^{-1} = \{(c, s) \in C \times S \mid (s, c) \in E\} = \{(c, s) \in C \times S \mid \text{l'étudiant } s \text{ est inscrit au cours } c\}$. Par exemple, si Joe Smith est inscrit en Biologie 12, alors $(\text{Joe Smith}, \text{Biologie 12}) \in E$ et $(\text{Biologie 12}, \text{Joe Smith}) \in E^{-1}$.

2. Étant donné que L^{-1} est une relation de R à S et E est une relation de S à C , $E \circ L^{-1}$ sera la relation de R à C définie comme suit.

$$\begin{aligned} E \circ L^{-1} &= \{(r, c) \in R \times C \mid \exists s \in S((r, s) \in L^{-1} \text{ and } (s, c) \in E)\} \\ &= \{(r, c) \in R \times C \mid \exists s \in S((s, r) \in L \text{ and } (s, c) \in E)\} \\ &= \{(r, c) \in R \times C \mid \exists s \in S(\text{the student } s \text{ lives in the dorm room } r \text{ and is enrolled in the course } c)\} \\ &= \{(r, c) \in R \times C \mid \text{some student who lives in the room } r \text{ is enrolled in the course } c\}. \end{aligned}$$

Revenons à notre étudiant préféré Joe Smith, inscrit en Biologie 12 et résidant dans la chambre 213 Davis Hall. Nous avons $(213 \text{ Davis Hall}, \text{Joe Smith}) \in L^{-1}$ et $(\text{Joe Smith}, \text{Biologie 12}) \in E$. D'après la définition de la composition, il s'ensuit que $(213 \text{ Davis Hall}, \text{Biologie 12}) \in E \circ L^{-1}$.

3. Parce que E est une relation de S à C et E^{-1} est une relation de C à S , $E^{-1} \circ E$ est la relation de S à S définie comme suit.

$$\begin{aligned} E^{-1} \circ E &= \{(s, t) \in S \times S \mid \exists c \in C((s, c) \in E \text{ and } (c, t) \in E^{-1})\} \\ &= \{(s, t) \in S \times S \mid \exists c \in C(\text{the student } s \text{ is enrolled in the course } c, \text{ and so is the student } t)\} \\ &= \{(s, t) \in S \times S \mid \text{there is some course that the students } s \text{ and } t \text{ are both enrolled in}\}. \end{aligned}$$

(Notez qu'un élément arbitraire de $S \times S$ s'écrit (s, t) , et non (s, s) , car nous ne voulons pas supposer que les deux coordonnées sont égales.)

4. Ceci est différent du dernier exemple ! Puisque E^{-1} est une relation de C vers S et E est une relation de S vers C , $E \circ E^{-1}$ est une relation de C vers C . Sa définition est la suivante.

$$\begin{aligned} E \circ E^{-1} &= \{(c, d) \in C \times C \mid \exists s \in S((c, s) \in E^{-1} \text{ and } (s, d) \in E)\} \\ &= \{(c, d) \in C \times C \mid \exists s \in S(\text{the student } s \text{ is enrolled in the course } c, \text{ and he or she is also enrolled in the course } d)\} \\ &= \{(c, d) \in C \times C \mid \text{there is some student who is enrolled in both of the courses } c \text{ and } d\}. \end{aligned}$$

5. Nous avons vu dans la partie 2 que $E \circ L^{-1}$ est une relation de R à C , et T est une relation de C à P , donc $T \circ (E \circ L^{-1})$ est la relation de R à P définie comme suit.

$$\begin{aligned} T \circ (E \circ L^{-1}) &= \{(r, p) \in R \times P \mid \exists c \in C ((r, c) \in E \circ L^{-1} \text{ and } (c, p) \in T)\} \\ &= \{(r, p) \in R \times P \mid \exists c \in C (\text{some student who lives in the room } r \text{ is enrolled in the course } c, \text{ and } c \text{ is taught by the professor } p)\} \\ &= \{(r, p) \in R \times P \mid \text{some student who lives in the room } r \text{ is enrolled in some course taught by the professor } p\}. \end{aligned}$$

$$\begin{aligned} (T \circ E) \circ L^{-1} &= \{(r, p) \in R \times P \mid \exists s \in S ((r, s) \in L^{-1} \text{ and } (s, p) \in T \circ E)\} \\ &= \{(r, p) \in R \times P \mid \exists s \in S (\text{the student } s \text{ lives in the room } r, \text{ and is enrolled in some course taught by the professor } p)\} \\ &= \{(r, p) \in R \times P \mid \text{some student who lives in the room } r \text{ is enrolled in some course taught by the professor } p\}. \end{aligned}$$

6.

Notez que nos réponses aux parties 3 et 4 de [l'exemple 4.2.4](#) étaient différentes, la composition des relations n'est donc pas commutative. En revanche, nos réponses aux parties 5 et 6 se sont avérées identiques. Est-ce une coïncidence, ou est-il généralement vrai que la composition des relations est associative ? Souvent, l'examen d'exemples d'un nouveau concept suggère des règles générales qui pourraient s'y appliquer. Bien qu'un contre-exemple suffise à démontrer l'inexactitude d'une règle, il ne faut jamais l'accepter comme correcte sans preuve. Le théorème suivant résume certaines des propriétés fondamentales des nouveaux concepts que nous avons introduits.

Théorème 4.2.5. Supposer R est une relation de UN à B , S est une relation de B à C , et T est une relation de C à D . Alors :

1. $(R^{-1})^{-1} = R$.
2. $\text{Dom}(R^{-1}) = \text{Ran}(R)$.
3. $\text{Ran}(R^{-1}) = \text{Dom}(R)$.
4. $T \circ (S \circ R) = (T \circ S) \circ R$.
5. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Preuve. Nous prouverons 1, 2 et la moitié de 4, et laisserons le reste en exercices. (Voir [exercice 7.](#))

1. Notons tout d'abord que R^{-1} est une relation de B vers A , donc $(R^{-1})^{-1}$ est une relation de A vers B , tout comme R . Pour voir que $(R^{-1})^{-1} = R$, soit (a, b) un couple ordonné arbitraire dans $A \times B$. Alors

$$(a, b) \in (R^{-1})^{-1} \text{ssi } (b, a) \in R^{-1} \text{ssi } (a, b) \in R.$$

2. Notons d'abord que $\text{Dom}(R^{-1})$ et $\text{Ran}(R)$ sont tous deux des sous-ensembles de B . Soit maintenant b un élément arbitraire de B . Alors

$$\begin{aligned} b \in \text{Dom}(R^{-1}) &\text{ iff } \exists a \in A((b, a) \in R^{-1}) \\ &\text{ iff } \exists a \in A((a, b) \in R) \text{ iff } b \in \text{Ran}(R). \end{aligned}$$

4. De toute évidence, $T \circ (S \circ R)$ et $(T \circ S) \circ R$ sont tous deux des relations de A à D . Soit (a, d) un élément arbitraire de $A \times D$.

Premièrement, supposons que $(a, d) \in T \circ (S \circ R)$. Par définition de composition, cela signifie que nous pouvons choisir un $c \in C$ tel que $(a, c) \in S \circ R$ et $(c, d) \in T$. Puisque $(a, c) \in S \circ R$, nous pouvons à nouveau utiliser la définition de composition et choisir un $b \in B$ tel que $(a, b) \in R$ et $(b, c) \in S$. Maintenant, puisque $(b, c) \in S$ et $(c, d) \in T$, nous pouvons conclure que $(b, d) \in T \circ S$. De même, puisque $(a, b) \in R$ et $(b, d) \in T \circ S$, il s'ensuit que $(a, d) \in (T \circ S) \circ R$.

Supposons maintenant que $(a, d) \in (T \circ S) \circ R$. Un argument similaire, laissé au lecteur, montre que $(a, d) \in T \circ (S \circ R)$. Ainsi, $T \circ (S \circ R) = (T \circ S) \circ R$.

□

Commentaire. L'énoncé 1 signifie $\forall p (p \in (R^{-1})^{-1} \leftrightarrow p \in R)$, donc la preuve doit procéder en introduisant un objet arbitraire p puis en prouvant $p \in (R^{-1})^{-1} \leftrightarrow p \in R$. Mais comme R et $(R^{-1})^{-1}$ sont tous deux des relations de A à B , nous pourrions penser à l'univers sur lequel p s'étend comme étant $A \times B$, donc p doit être une paire ordonnée. Ainsi, dans la preuve précédente, nous l'avons écrit comme une paire ordonnée (a, b) dès le début. La preuve de l'énoncé biconditionnel $(a, b) \in (R^{-1})^{-1} \leftrightarrow (a, b) \in R$ utilise la méthode, introduite dans [l'exemple 3.4.5](#), consistant à enchaîner une séquence d'équivalences.

Français Les preuves des énoncés 2 et 4 sont similaires, sauf que la preuve biconditionnelle de l'énoncé 4 ne peut pas être facilement réalisée en enchaînant des équivalences, nous prouvons donc les deux directions séparément. Une seule direction a été prouvée. La clé de cette preuve est de reconnaître que l'énoncé $(a, d) \in T \circ (S \circ R)$ donné est un énoncé existentiel, car il signifie $\exists c \in C ((a, c) \in S \circ R \text{ et } (c, d) \in T)$, nous devrions donc introduire une nouvelle variable c dans la preuve pour représenter un élément de C tel que $(a, c) \in S \circ R$ et $(c, d) \in T$. De même, $(a, c) \in S \circ R$ est un énoncé existentiel, il suggère donc d'introduire la variable b . Une fois ces nouvelles variables introduites, il est facile de prouver le but $(a, d) \in (T \circ S) \circ R$.

L'énoncé 5 du [théorème 4.2.5](#) mérite peut-être quelques commentaires. Tout d'abord, notez que le membre de droite de l'équation est $R^{-1} \circ S^{-1}$, et non $S^{-1} \circ R^{-1}$; l'ordre des relations a été inversé. On vous demande de démontrer l'affirmation 5 dans [l'exercice 7](#), mais il peut être utile d'essayer d'abord un exemple. Nous avons déjà vu que, pour les relations E et T des parties 5 et 6 de [l'exemple 4.2.2](#),

$$T \circ E = \{(s, p) \in S \times P \mid \text{the student } s \text{ is enrolled in some course taught by the professor } p\}.$$

Il s'ensuit que

$$(T \circ E)^{-1} = \{(p, s) \in P \times S \mid \text{the student } s \text{ is enrolled in some course taught by the professor } p\}.$$

Pour calculer $E^{-1} \circ T^{-1}$, notons d'abord que T^{-1} est une relation de P vers C et E^{-1} est une relation de C vers S , donc $E^{-1} \circ T^{-1}$ est une relation de P vers S . Maintenant, en appliquant la définition de composition, nous obtenons

$$\begin{aligned} E^{-1} \circ T^{-1} &= \{(p, s) \in P \times S \mid \exists c \in C((p, c) \in T^{-1} \text{ and } (c, s) \in E^{-1})\} \\ &= \{(p, s) \in P \times S \mid \exists c \in C((c, p) \in T \text{ and } (s, c) \in E)\} \\ &= \{(p, s) \in P \times S \mid \exists c \in C(\text{the course } c \text{ is taught by the professor } p \text{ and the student } s \text{ is enrolled in the course } c)\} \\ &= \{(p, s) \in P \times S \mid \text{the student } s \text{ is enrolled in some course taught by the professor } p\}. \end{aligned}$$

Ainsi, $(T \circ E)^{-1} = E^{-1} \circ T^{-1}$.

Exercices

*1. Trouvez les domaines et les domaines des relations suivantes.

- (a) $\{(p, q) \in P \times P \mid \text{la personne } p \text{ est un parent de la personne } q\}$, où P est l'ensemble de toutes les personnes vivantes.
 (b) $\{(x, y) \in \mathbb{R}^2 \mid y > x^2\}$.

2. Trouvez les domaines et les domaines des relations suivantes.

- (a) $\{(p, q) \in P \times P \mid \text{la personne } p \text{ est un frère de la personne } q\}$, où P est l'ensemble de toutes les personnes vivantes.
 (b) $\{(x, y) \in \mathbb{R}^2 \mid y^2 = 1 - 2/(x^2 + 1)\}$.

3. Soient L et E les relations définies dans les parties 4 et 5 de [l'exemple 4.2.2](#). Décrivez les relations suivantes :

- (a) $L^{-1} \circ L$.
 (b) $E \circ (L^{-1} \circ L)$.

4. Soient E et T les relations définies dans les parties 5 et 6 de [l'exemple 4.2.2](#). De plus, comme dans cet exemple, soit C l'ensemble des cours de votre établissement, et soit $D = \{\text{lundi, mardi, mercredi, jeudi, vendredi}\}$. Soit $M = \{(c, d) \in C \times D \mid \text{le cours } c \text{ a lieu le jour } j\}$. Décrivez les relations suivantes :

- (a) $M \circ E$.
- (b) $M \circ T^{-1}$.

*5. Supposons que $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, $R = \{(1, 4), (1, 5), (2, 5), (3, 6)\}$ et $S = \{(4, 5), (4, 6), (5, 4), (6, 6)\}$. Notez que R est une relation de A vers B et S est une relation de B vers B . Trouvez les relations suivantes :

- (a) $S \circ R$.
- (b) $S \circ S^{-1}$.

6. Supposons que $A = \{1, 2, 3\}$, $B = \{4, 5\}$, $C = \{6, 7, 8\}$, $R = \{(1, 7), (3, 6), (3, 7)\}$ et $S = \{(4, 7), (4, 8), (5, 6)\}$. Notez que R est une relation de A vers C et S est une relation de B vers C . Trouvez les relations suivantes :

- (a) $S^{-1} \circ R$.
- (b) $R^{-1} \circ S$.

7. (a) Démontrez la partie 3 du [théorème 4.2.5](#) en imitant la preuve de la partie 2 dans le texte.

(b) Donnez une preuve alternative de la partie 3 du [théorème 4.2.5](#) en montrant qu'elle découle des parties 1 et 2.

(c) Complétez la preuve de la partie 4 du [théorème 4.2.5](#).

(d) Démontrer la partie 5 du [théorème 4.2.5](#).

*8. Soit $E = \{(p, q) \in P \times P \mid \text{la personne } p \text{ est un ennemi de la personne } q\}$, et $F = \{(p, q) \in P \times P \mid \text{la personne } p \text{ est un ami de la personne } q\}$, où P est l'ensemble de tous les individus. Que signifie l'expression « l'ennemi de son ennemi est son ami » à propos des relations E et F ?

9. Supposons que R soit une relation de A à B et que S soit une relation de B à C .

(a) Démontrer que $\text{Dom}(S \circ R) \subseteq \text{Dom}(R)$.

(b) Démontrer que si $\text{Ran}(R) \subseteq \text{Dom}(S)$ alors $\text{Dom}(S \circ R) = \text{Dom}(R)$.

(c) Formuler et prouver des théorèmes similaires sur $\text{Ran}(S \circ R)$.

10. Supposons que R et S soient des relations de A vers B . Les affirmations suivantes doivent-elles être vraies ? Justifiez vos réponses par des preuves ou des contre-exemples.

(a) $R \subseteq \text{Dom}(R) \times \text{Ran}(R)$.

(b) Si $R \subseteq S$ alors $R^{-1} \subseteq S^{-1}$.

$$(c) (R \cup S)^{-1} = R^{-1} \cup S^{-1}.$$

*11. Supposons que R soit une relation de A à B et S soit une relation de B à C . Démontrer que $S \circ R = \emptyset$ ssi $\text{Ran}(R)$ et $\text{Dom}(S)$ sont disjoints.

^P D12. Supposons que R soit une relation de A à B et que S et T soient des relations de B à C .

(a) Démontrer que $(S \circ R) \setminus (T \circ R) \subseteq (S \setminus T) \circ R$.

(b) Quel est le problème avec la preuve suivante selon laquelle $(S \setminus T) \circ R \subseteq (S \circ R) \setminus (T \circ R)$?

Preuve. Supposons que $(a, c) \in (S \setminus T) \circ R$. Alors on peut choisir un $b \in B$ tel que $(a, b) \in R$ et $(b, c) \in S \setminus T$, donc $(b, c) \in S$ et $(b, c) \notin T$. Puisque $(a, b) \in R$ et $(b, c) \in S$, $(a, c) \in S \circ R$. De même, puisque $(a, b) \in R$ et $(b, c) \notin T$, $(a, c) \notin T \circ R$. Donc $(a, c) \in (S \circ R) \setminus (T \circ R)$. Étant donné que (a, c) était arbitraire, cela montre que $(S \setminus T) \circ R \subseteq (S \circ R) \setminus (T \circ R)$.

(c) Doit-il être vrai que $(S \setminus T) \circ R \subseteq (S \circ R) \setminus (T \circ R)$? Justifiez votre réponse par une preuve ou un contre-exemple.

13. Supposons que R et S soient des relations de A vers B et que T soit une relation de B vers C . Les affirmations suivantes doivent-elles être vraies ? Justifiez vos réponses par des preuves ou des contre-exemples.

(a) Si R et S sont disjoints, alors R^{-1} et S^{-1} le sont aussi.

(b) Si R et S sont disjoints, alors $T \circ R$ et $T \circ S$ le sont aussi.

(c) Si $T \circ R$ et $T \circ S$ sont disjoints, alors R et S le sont aussi.

^P D14. Supposons que R soit une relation de A vers B , et que S et T soient des relations de B vers C . Les affirmations suivantes doivent-elles être vraies ? Justifiez vos réponses par des preuves ou des contre-exemples.

(a) Si $S \subseteq T$ alors $S \circ R \subseteq T \circ R$.

(b) $(S \cap T) \circ R \subseteq (S \circ R) \cap (T \circ R)$.

(c) $(S \cap T) \circ R = (S \circ R) \cap (T \circ R)$.

(d) $(S \cup T) \circ R = (S \circ R) \cup (T \circ R)$.

15. Supposons que R soit une relation de A vers B et S une relation de C vers D . Démontrer qu'il existe un ensemble E tel que R soit une relation de A vers E et S une relation de E vers D . Par conséquent, la définition de $S \circ R$ de [la définition 4.2.3](#) peut être appliquée. De plus, cette définition donne le même résultat quel que soit l'ensemble E utilisé.

4.3 En savoir plus sur les relations

Bien que nous ayons défini les relations comme des ensembles de paires ordonnées, il est parfois utile de pouvoir les apprêhender autrement. Souvent, même un léger changement de notation peut nous aider à voir les choses différemment. Une notation alternative que les mathématiciens utilisent parfois pour les relations est motivée par le fait qu'en mathématiques, on exprime souvent une relation entre deux objets x et y en plaçant un symbole entre eux. Par exemple, les notations $x = y$, $x < y$, $x \in y$ et $x \subseteq y$ expriment quatre relations mathématiques importantes entre x et y . En imitant ces notations, si R est une relation de A vers B , $x \in A$ et $y \in B$, les mathématiciens écrivent parfois xRy pour signifier $(x, y) \in R$.

Français Par exemple, si L est la relation définie dans la partie 4 de l'[exemple 4.2.2](#), alors pour tout étudiant s et chambre universitaire r , sLr signifie $(s, r) \in L$, ou en d'autres termes, l'étudiant s vit dans la chambre universitaire r . De même, si E et T sont les relations définies dans les parties 5 et 6 de l'[exemple 4.2.2](#), alors sEc signifie que l'étudiant s est inscrit au cours c , et cTp signifie que le cours c est enseigné par le professeur p . La définition de la composition de relations aurait pu être énoncée en disant que si R est une relation de A vers B et S est une relation de B vers C , alors $S \circ R = \{(a, c) \in A \times C \mid \exists b \in B (aRb \text{ et } bSc)\}$.

Une autre façon d'envisager les relations est de les représenter par des dessins. [La figure 4.1](#) illustre la relation $R = \{(1, 3), (1, 5), (3, 3)\}$ de la partie 1 de l'[exemple 4.2.2](#). Rappelons qu'il s'agit d'une relation de l'ensemble $A = \{1, 2, 3\}$ à l'ensemble $B = \{3, 4, 5\}$. Sur la figure, chacun de ces ensembles est représenté par un ovale, dont les éléments sont représentés par des points à l'intérieur. Chaque couple $(a, b) \in R$ est représenté par une flèche allant du point représentant a au point représentant b . Par exemple, il existe une flèche allant du point à l'intérieur de A , étiqueté 1, au point à l'intérieur de B , étiqueté 5, car le couple $(1, 5)$ est un élément de R .

En général, toute relation R d'un ensemble A vers un ensemble B peut être représentée par une telle image. Les points représentant les éléments de A et B dans une telle image sont appelés *sommets*, et les flèches représentant les paires ordonnées dans R sont appelées *arêtes*. La disposition exacte des sommets représentant les éléments de A et B sur la page importe peu ; l'important est que les arêtes correspondent précisément aux paires ordonnées dans R . Dessiner ces images peut vous aider à comprendre les concepts abordés dans la section

précédente. Par exemple, vous devriez être capable de vous convaincre que vous pouvez trouver le domaine de R en localisant les sommets de A dont les arêtes pointent dans le sens opposé. De même, l'ensemble de R serait constitué des éléments de B dont les sommets ont des arêtes pointant vers eux. Pour la relation R illustrée à [la figure 4.1](#), nous avons $\text{Dom}(R) = \{1, 3\}$ et $\text{Ran}(R) = \{3, 5\}$. Une image de R^{-1} ressemblerait exactement à une image de R mais avec les directions de toutes les flèches inversées.

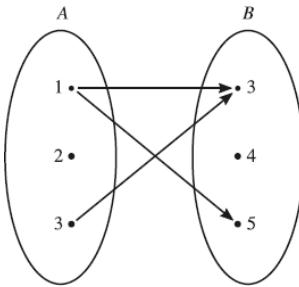


Figure 4.1.

Les images illustrant la composition de deux relations sont un peu plus difficiles à comprendre. Prenons l'exemple des relations E et T des parties 5 et 6 de [l'exemple 4.2.2](#). [La figure 4.2](#) montre à quoi pourraient ressembler les deux relations. (L'image complète peut être assez grande si votre établissement compte de nombreux étudiants, cours et professeurs.) On voit sur cette image que, par exemple, Joe Smith suit les cours de biologie 12 et de mathématiques 21, que la biologie 12 est enseignée par le professeur Evans et que les mathématiques 21 sont enseignées par le professeur Andrews. Ainsi, en appliquant la définition de composition, on constate que les couples (Joe Smith, professeur Evans) et (Joe Smith, professeur Andrews) sont tous deux des éléments de la relation $T \circ E$.

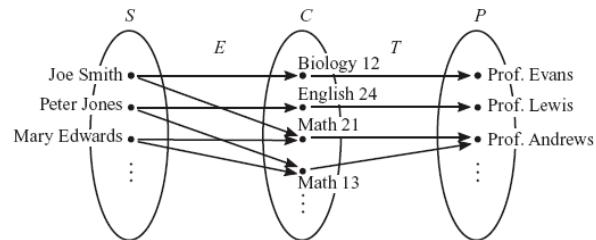


Figure 4.2.

Pour voir plus clairement comment la composition $T \circ E$ est représentée dans cette image, notez d'abord que pour tout étudiant s , cours c et professeur p , il y a une flèche de s à c ssi sEc , et il existe une flèche de c à p ssi cTp . Ainsi, selon la définition de la composition,

$$\begin{aligned}
T \circ E &= \{(s, p) \in S \times P \mid \exists c \in C (sEc \text{ and } cTp)\} \\
&= \{(s, p) \in S \times P \mid \exists c \in C (\text{in Figure 4.2, there is an arrow} \\
&\quad \text{from } s \text{ to } c \text{ and an arrow from } c \text{ to } p)\} \\
&= \{(s, p) \in S \times P \mid \text{in Figure 4.2, you can get from } s \text{ to } p \text{ in} \\
&\quad \text{two steps by following the arrows}\}.
\end{aligned}$$

Par exemple, en commençant au sommet étiqueté Mary Edwards, nous pouvons arriver au professeur Andrews en deux étapes (en passant par Math 21 ou Math 13), nous pouvons donc conclure que $(\text{Mary Edwards}, \text{Prof. Andrews}) \in T \circ E$.

Dans certaines situations, nous représentons les relations d'une manière légèrement différente. Par exemple, si A est un ensemble et $R \subseteq A \times A$, alors, selon [la définition 4.2.1](#), R serait appelé une relation de A vers A . Une telle relation est aussi parfois appelée *relation sur A* (ou une *relation binaire sur A*). Des relations de ce type apparaissent souvent en mathématiques ; en fait, nous en avons déjà vu quelques-unes. Par exemple, nous avons décrit la relation G dans la partie 2 de [l'exemple 4.2.2](#) comme une relation de \mathbb{R} vers \mathbb{R} , mais dans notre nouvelle terminologie, nous pourrions l'appeler une relation (ou une relation binaire) sur \mathbb{R} . La relation $E^{-1} \circ E$ de [l'exemple 4.2.4](#) était une relation sur l'ensemble S , et $E \circ E^{-1}$ était une relation sur C .

Exemple 4.3.1. Voici d'autres exemples de relations sur des ensembles.

1. Soit $A = \{1, 2\}$ et $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ comme dans la partie 3 de [l'exemple 4.2.2](#). Soit

$$\begin{aligned}
S &= \{(x, y) \in B \times B \mid x \subseteq y\} \\
&= \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{2\}), \\
&\quad (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}.
\end{aligned}$$

Alors S est une relation sur B .

2. Supposons que A soit un ensemble. Soit $i_A = \{(x, y) \in A \times A \mid x = y\}$. Alors i_A est une relation sur A . (On l'appelle *relation d'identité* sur A .) Par exemple, si $A = \{1, 2, 3\}$, alors $i_A = \{(1, 1), (2, 2), (3, 3)\}$. On peut aussi définir i_A en écrivant $i_A = \{(x, x) \mid x \in A\}$.
3. Pour tout nombre réel positif r , soit $D_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \text{ et } y \text{ diffèrent de moins de } r\}$, ou en d'autres termes $|x - y| < r$. Alors D_r est une relation sur \mathbb{R} .

Supposons que R soit une relation sur un ensemble A . Si nous utilisions la méthode décrite précédemment pour dessiner une image de R , alors nous devrions dessiner deux copies de l'ensemble A et puis tracer des arêtes d'une copie de A à l'autre pour représenter les paires ordonnées dans R . Une façon plus simple de dessiner l'image serait de

ne dessiner qu'une seule copie de A , puis de connecter les sommets représentant les éléments de A avec des arêtes pour représenter les paires ordonnées dans R . Par exemple, [la figure 4.3](#) montre une image de la relation S de la partie 1 de [l'exemple 4.3.1](#). Des images comme celle de [la figure 4.3](#) sont appelées *graphes orientés*.

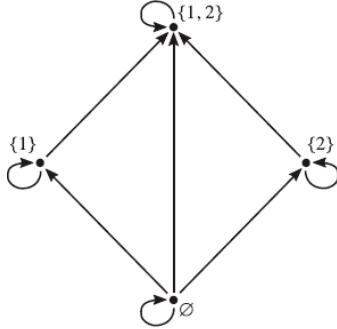


Figure 4.3.

Notez que dans ce graphe orienté, il existe une arête de \emptyset vers lui-même, car $(\emptyset, \emptyset) \in S$. Les arêtes comme celle-ci qui vont d'un sommet à lui-même sont appelées *boucles*. En fait, dans [la figure 4.3](#), il y a une boucle à chaque sommet, car S a la propriété que $\forall x \in B ((x, x) \in S)$. Nous décrivons cette situation en disant que S est *réflexif*.

Définition 4.3.2. Supposons que R soit une relation sur A .

1. On dit que R est *réflexif sur A* (ou simplement *réflexif*, si A ressort clairement du contexte) si $\forall x \in A (xRx)$, ou en d'autres termes $\forall x \in A ((x, x) \in R)$.
2. R est *symétrique* si $\forall x \in A \forall y \in A (xRy \rightarrow yRx)$.
3. R est *transitif* si $\forall x \in A \forall y \in A \forall z \in A ((xRy \wedge yRz) \rightarrow xRz)$.

Comme nous l'avons vu dans [l'exemple 4.3.1](#), si R est réflexif sur A , alors le graphe orienté représentant R comportera des boucles à tous ses sommets. Si R est symétrique, alors chaque arête de x à y comportera également une arête de y à x . Si x et y sont distincts, il en résulte que deux arêtes relieront x et y , une pointant dans chaque direction. Ainsi, si R est symétrique, alors toutes les arêtes, sauf les boucles, seront viendront par paires. Si R est transitif, alors chaque fois qu'il existe une arête de x vers y et de y vers z , il existe également une arête de x vers z .

Exemple 4.3.3. La relation G de la partie 2 de [l'exemple 4.2.2](#) est-elle réflexive ? Est-elle symétrique ? Transitive ? Les relations de [l'exemple 4.3.1 sont-elles](#) réflexives, symétriques ou transitives ?

Solution

Rappelons que la relation G de [l'exemple 4.2.2](#) est une relation sur \mathbb{R} et que pour tout nombre réel x et y , xGy signifie $x > y$. Ainsi, dire que G est réflexif signifierait que $\forall x \in \mathbb{R} (xGx)$, ou en d'autres termes $\forall x \in \mathbb{R} (x > x)$, ce qui est clairement faux. Dire que G est symétrique signifierait que $\forall x \in \mathbb{R} \forall y \in \mathbb{R} (x > y \rightarrow y > x)$, ce qui est également clairement faux. Enfin, dire que G est transitif signifierait que $\forall x \in \mathbb{R} \forall y \in \mathbb{R} \forall z \in \mathbb{R} ((x > y \wedge y > z) \rightarrow x > z)$, ce qui est vrai. Ainsi, G est transitif, mais pas réflexif ou symétrique.

L'analyse des relations dans [l'exemple 4.3.1](#) est similaire. Pour la relation S dans la partie 1, nous utilisons le fait que pour tout x et y dans B , xSy signifie $x \subseteq y$. Comme nous l'avons déjà observé, S est réflexive, car $\forall x \in B (x \subseteq x)$, mais il n'est pas vrai que $\forall x \in B \forall y \in B (x \subseteq y \rightarrow y \subseteq x)$. Par exemple, $\{1\} \subseteq \{1, 2\}$, mais $\{1, 2\} \not\subseteq \{1\}$. Vous pouvez le voir dans [la figure 4.3](#) en notant qu'il y a une arête de $\{1\}$ vers $\{1, 2\}$ mais pas de $\{1, 2\}$ vers $\{1\}$. Ainsi, S n'est pas symétrique. S est transitif, car l'énoncé $\forall x \in B \forall y \in B \forall z \in B ((x \subseteq y \wedge y \subseteq z) \rightarrow x \subseteq z)$ est vrai.

Français Pour tout ensemble A la relation d'identité i_A sera réflexive, symétrique et transitive, car les énoncés $\forall x \in A (x = x)$, $\forall x \in A \forall y \in A (x = y \rightarrow y = x)$ et $\forall x \in A \forall y \in A \forall z \in A ((x = y \wedge y = z) \rightarrow x = z)$ sont tous clairement vrais. Enfin, supposons que r est un nombre réel positif et considérons la relation D_r . Pour tout nombre réel x , $|x - x| = 0 < r$, donc $(x, x) \in D_r$. Ainsi, D_r est réflexive. De plus, pour tout nombre réel x et y , $|x - y| = |y - x|$, donc si $|x - y| < r$ alors $|y - x| < r$. Par conséquent, si $(x, y) \in D_r$ alors $(y, x) \in D_r$, donc D_r est symétrique. Mais D_r n'est pas transitif. Pour comprendre pourquoi, soit x un nombre réel quelconque. Soit $y = x + 2r/3$ et $z = y + 2r/3 = x + 4r/3$. Alors $|x - y| = 2r/3 < r$ et $|y - z| = 2r/3 < r$, mais $|x - z| = 4r/3 > r$. Ainsi, $(x, y) \in D_r$ et $(y, z) \in D_r$, mais $(x, z) \notin D_r$.

Vous avez peut-être déjà deviné que les propriétés des relations définies dans [la définition 4.3.2](#) sont liées aux opérations définies dans [la définition 4.2.3](#). Dire qu'une relation R est symétrique revient à inverser les rôles de deux variables, ce qui peut rappeler la définition de R^{-1} . La définition de La transitivité d'une relation implique l'enchaînement de deux paires ordonnées, tout comme la définition de la composition des relations. Le théorème suivant précise ces connexions.

Théorème 4.3.4. Supposer R est une relation sur un ensemble UN .

1. R est réflexif ssi $i_A \subseteq R$, où comme précédemment i_A est la relation d'identité sur A .

2. R est symétrique ssi $R = R^{-1}$.

3. R est transitif ssi $R \circ R \subseteq R$.

Preuve. Nous prouverons 2 et laisserons les preuves de 1 et 3 en exercices (voir [exercices 7](#) et [8](#)).

2. (\rightarrow) Supposons que R soit symétrique. Soit (x, y) un élément arbitraire de R . Alors xRy , donc puisque R est symétrique, yRx . Ainsi, $(y, x) \in R$, donc par définition de R^{-1} , $(x, y) \in R^{-1}$. Puisque (x, y) était arbitraire, il s'ensuit que $R \subseteq R^{-1}$.

Supposons maintenant que $(x, y) \in R^{-1}$. Alors $(y, x) \in R$, donc puisque R est symétrique, $(x, y) \in R$. Ainsi, $R^{-1} \subseteq R$, donc $R = R^{-1}$.

(\leftarrow) Supposons $R = R^{-1}$, et soient x et y des éléments arbitraires de A . Supposons xRy . Alors $(x, y) \in R$, donc puisque $R = R^{-1}$, $(x, y) \in R^{-1}$. Par définition de R^{-1} cela signifie $(y, x) \in R$, donc yRx . Ainsi, $\forall x \in A \forall y \in A (xRy \rightarrow yRx)$, donc R est symétrique.

□

Commentaire. Cette preuve est assez simple. L'énoncé à prouver est un énoncé ssi, nous prouvons donc les deux directions séparément. Dans la \rightarrow moitié, nous devons prouver que $R = R^{-1}$, et cela se fait en prouvant à la fois $R \subseteq R^{-1}$ et $R^{-1} \subseteq R$. Chacun de ces objectifs est prouvé en prenant un élément arbitraire du premier ensemble et en montrant qu'il est dans le second ensemble. Dans la \leftarrow moitié, nous devons prouver que R est symétrique, ce qui signifie $\forall x \in A \forall y \in A (xRy \rightarrow yRx)$. Nous utilisons la stratégie évidente de poser x et y comme des éléments arbitraires de A , en supposant xRy , et en prouvant yRx .

Exercices

*1. Soit $L = \{a, b, c, d, e\}$ et $W = \{\text{bad}, \text{bed}, \text{cab}\}$. Soit $R = \{(l, w) \in L \times W \mid \text{la lettre } l \text{ apparaît dans le mot } w\}$. Dessinez un diagramme (comme celui de [la figure 4.1](#)) de R .

2. Soit $A = \{\text{chat, chien, oiseau, rat}\}$, et soit $R = \{(x, y) \in A \times A \mid \text{il y a au moins une lettre qui apparaît dans les deux mots } x \text{ et } y\}$. Dessinez un graphe orienté (comme celui de [la figure 4.3](#)) pour la relation R . R est-il réflexif ? Symétrique ? Transitif ?

*3. Soit $A = \{1, 2, 3, 4\}$. Tracez un graphe orienté pour i_A , la relation d'identité sur A .

4. Lister les paires ordonnées dans les relations représentées par les graphes orientés de [la figure 4.4](#). Déterminer si chaque relation est réflexive, symétrique ou transitive.

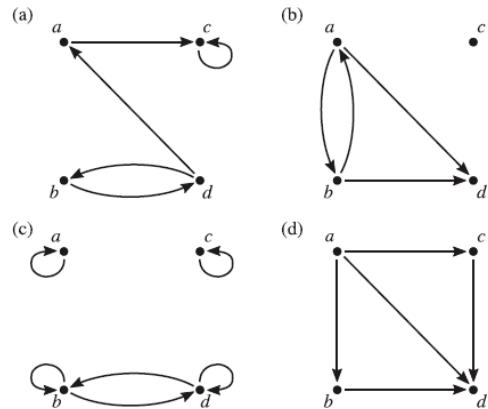


Figure 4.4.

*5. [La figure 4.5](#) montre deux relations R et S . Trouvez $S \circ R$.

6. Supposons que r et s soient deux nombres réels positifs. Soient D_r et D_s définis comme dans la partie 3 de [l'exemple 4.3.1](#). Quel est $D_r \circ D_s$? Justifiez votre réponse par une preuve. (Indice : Dans votre preuve, vous pourriez trouver utile d'utiliser l'inégalité triangulaire ; voir [l'exercice 13\(c\) de la section 3.5](#).)

*7. Démontrer la partie 1 du [théorème 4.3.4](#).

8. Démontrer la partie 3 du [théorème 4.3.4](#).

9. Supposons que A et B sont des ensembles.

(a) Montrer que pour toute relation R de A à B , $R \circ i_A = R$.

(b) Montrer que pour toute relation R de A à B , $i_B \circ R = R$.

*10. Supposons que S soit une relation sur A . Soit $D = \text{Dom}(S)$ et $R = \text{Ran}(S)$. Démontrer que $i_D \subseteq S^{-1} \circ S$ et $i_R \subseteq S \circ S^{-1}$.

11. Supposons que R soit une relation sur A . Démontrer que si R est réflexive alors $R \subseteq R \circ R$.

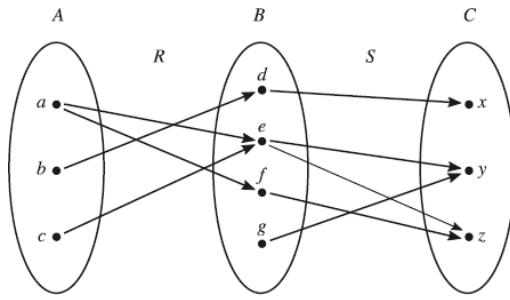


Figure 4.5.

12. Supposons que R soit une relation sur A .

- (a) Démontrer que si R est réflexif, alors R^{-1} l'est aussi.
- (b) Démontrer que si R est symétrique, alors R^{-1} l'est aussi.
- (c) Démontrer que si R est transitif, alors R^{-1} l'est aussi.

*13. Supposons que R_1 et R_2 soient des relations sur A . Pour chaque partie, donnez une preuve ou un contre-exemple pour justifier votre réponse.

- (a) Si R_1 et R_2 sont réflexifs, $R_1 \cup R_2$ doit-il être réflexif ?
- (b) Si R_1 et R_2 sont symétriques, $R_1 \cup R_2$ doit-il être symétrique ?
- (c) Si R_1 et R_2 sont transitifs, $R_1 \cup R_2$ doit-il être transitif ?

14. Supposons que R_1 et R_2 soient des relations sur A . Pour chaque partie, donnez une preuve ou un contre-exemple pour justifier votre réponse.

- (a) Si R_1 et R_2 sont réflexifs, $R_1 \cap R_2$ doit-il être réflexif ?
- (b) Si R_1 et R_2 sont symétriques, $R_1 \cap R_2$ doit-il être symétrique ?
- (c) Si R_1 et R_2 sont transitifs, $R_1 \cap R_2$ doit-il être transitif ?

15. Supposons que R_1 et R_2 soient des relations sur A . Pour chaque partie, donnez une preuve ou un contre-exemple pour justifier votre réponse.

- (a) Si R_1 et R_2 sont réflexifs, $R_1 \setminus R_2$ doit-il être réflexif ?
- (b) Si R_1 et R_2 sont symétriques, $R_1 \setminus R_2$ doit-il être symétrique ?
- (c) Si R_1 et R_2 sont transitifs, $R_1 \setminus R_2$ doit-il être transitif ?

16. Supposons que R et S soient des relations réflexives sur A . Démontrer que $R \circ S$ est réflexive.

*17. Supposons que R et S soient des relations symétriques sur A . Démontrer que $R \circ S$ est symétrique ssi $R \circ S = S \circ R$.

18. Supposons que R et S soient des relations transitives sur A . Démontrer que si $S \circ R \subseteq R \circ S$ alors $R \circ S$ est transitive.

19. Considérez le théorème putatif suivant.

Théorème? Supposer R est une relation sur A , et définir une relation S sur $\mathcal{P}(A)$ comme suit :

$$S = \{(X, \text{Oui}) \in \mathcal{P}(\text{UNE}) \times \mathcal{P}(\text{UNE}) \mid \exists X \in X \exists y \in Y (xRy)\}.$$

Si R est transitif, alors S l'est aussi .

(a) Quel est le problème avec la preuve suivante du théorème ?

Preuve . Supposons que R soit transitif. Supposons que $(X, Y) \in S$ et $(Y, Z) \in S$. Alors par définition de S , xRy et yRz , où $x \in X, y \in Y$ et $z \in Z$. Puisque xRy , yRz et R sont transitifs, xRz . Mais alors puisque $x \in X$ et $z \in Z$, il résulte de la définition de S que $(X, Z) \in S$. Ainsi, S est transitif. \square

(b) Le théorème est-il correct ? Justifiez votre réponse par une preuve ou un contre-exemple.

*20. Supposons que R soit une relation sur A . Soit $B = \{X \in \mathcal{P}(A) \mid X \neq \emptyset\}$, et définissons une relation S sur B comme suit :

$$S = \{(X, \text{Oui}) \in B \times B \mid \forall x \in X \forall y \in Y (xRy)\}.$$

Démontrer que si R est transitif, alors S l'est aussi . Pourquoi l'ensemble vide a-t-il dû être exclu de l'ensemble B pour que cette preuve fonctionne ?

21. Supposons que R soit une relation sur A , et définissons une relation S sur $\mathcal{P}(A)$ comme suit :

$$S = \{(X, \text{Oui}) \in \mathcal{P}(\text{UNE}) \times \mathcal{P}(\text{UNE}) \mid \forall x \in X \exists y \in Y (xRy)\}.$$

Pour chaque partie, donnez soit une preuve, soit un contre-exemple pour justifier votre réponse.

- (a) Si R est réflexif, S doit-il être réflexif ?
- (b) Si R est symétrique, S doit-il être symétrique ?
- (c) si R est transitif, S doit-il être transitif ?

22. Considérons le théorème putatif suivant :

Théorème? Supposer R est une relation sur A . Si R est symétrique et transitif, alors R est réflexif .

La preuve suivante est-elle correcte ? Si oui, quelles stratégies de preuve utilise-t-elle ? Si non, peut-elle être corrigée ? Le théorème est-il correct ?

Preuve . Soit x un élément quelconque de A . Soit y un élément quelconque de A tel que xRy . Puisque R est symétrique, il en résulte

que yRx . Mais alors, par transitivité, puisque xRy et yRx nous pouvons conclure que xRx . Puisque x est arbitraire, nous avons montré que $\forall x \in A (xRx)$, donc R est réflexif.

□

- *23. Ce problème a été suggéré par le professeur William Zwicker de l'Union College de New York. Supposons que A soit un ensemble et que $\mathcal{F} \subseteq \mathcal{P}(A)$. Soit $R = \{(a, b) \in A \times A \mid \text{pour tout } X \subseteq A \setminus \{a, b\}, \text{ si } X \cup \{a\} \in \mathcal{F} \text{ alors } X \cup \{b\} \in \mathcal{F}\}$. Montrer que R est transitif.
 - 24. Soit $R = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid |m - n| \leq 1\}$, qui est une relation sur \mathbb{N} . Notons que $R \subseteq \mathbb{Z} \times \mathbb{Z}$, donc R est aussi une relation sur \mathbb{Z} . Cet exercice illustre pourquoi, dans la partie 1 de [la définition 4.3.2](#), nous avons défini l'expression « R est réflexif sur A » plutôt que simplement « R est réflexif ».
- (a) R est-il réflexif sur \mathbb{N} ?
 (b) R est-il réflexif sur \mathbb{Z} ?

4.4 Relations de commande

Considérons la relation $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$. Vous devriez pouvoir vérifier par vous-même qu'elle est réflexive et transitive, mais pas symétrique. Elle n'est pas symétrique de manière assez extrême car il existe de nombreuses paires (x, y) telles que xLy est vraie mais yLx est fausse. En fait, la seule façon pour que xLy et yLx soient toutes deux vraies est si $x \leq y$ et $y \leq x$, et donc $x = y$. On dit donc que L est *antisymétrique*. Voici la définition générale.

Définition 4.4.1. Supposons que R soit une relation sur un ensemble A . Alors R est dit *antisymétrique* si $\forall x \in A \forall y \in A ((xRy \wedge yRx) \rightarrow x = y)$.

Nous avons déjà vu une relation possédant de nombreuses propriétés identiques à L . Regardons à nouveau la relation S définie dans la partie 1 de [l'exemple 4.3.1](#). Rappelons que dans cet exemple, nous posons $A = \{1, 2\}$, $B = \mathcal{P}(A)$ et $S = \{(x, y) \in B \times B \mid x \subseteq y\}$. Ainsi, si x et y sont des éléments de B , alors xSy signifie $x \subseteq y$. Nous avons vérifié dans la section précédente que S est réflexive et transitive, mais pas symétrique. En fait, S est également antisymétrique, car pour tout ensemble x et y , si $x \subseteq y$ et $y \subseteq x$ alors $x = y$. Il peut être utile de consulter à nouveau [la figure 4.3](#) de la section précédente, qui montre le graphe orienté représentant S .

Intuitivement, L et S sont deux relations qui ont un rapport avec la comparaison des tailles de deux objets. Chacune des affirmations $x \leq y$

et $x \subseteq y$ peut être interprétée comme indiquant que, d'une certaine manière, y est « au moins aussi grand que » x . On pourrait dire que chacune de ces affirmations précise l'*ordre* x et y entrent en jeu. Ceci motive la définition suivante.

Définition 4.4.2. Supposons que R soit une relation sur un ensemble A . Alors R est dite *partielle ordre sur A* (ou juste un *ordre partiel* si A ressort clairement du contexte) s'il est réflexif, transitif et antisymétrique. On parle alors d'*ordre total sur A* (ou juste un *total ordre*) s'il s'agit d'un ordre partiel, et qu'en plus il possède la propriété suivante :

$$\forall x \in A \forall y \in A (xRy \vee yRx).$$

Les relations L et S que nous venons de considérer sont toutes deux des ordres partiels. S n'est pas un ordre total, car il n'est pas vrai que $\forall x \in B \forall y \in B (x \subseteq y \vee y \subseteq x)$. Par exemple, si nous posons $x = \{1\}$ et $y = \{2\}$, alors $x \not\subseteq y$ et $y \not\subseteq x$. Ainsi, bien que nous puissions penser que la relation S indique un sens dans lequel un élément de B pourrait être au moins aussi grand qu'un autre, elle ne nous donne pas un moyen de comparer *chaque* paire d'éléments de B . Pour certaines paires, telles que $\{1\}$ et $\{2\}$, S ne choisit aucun des deux comme étant au moins aussi grand que l'autre. C'est le sens dans lequel l'ordre est *partiel*. D'un autre côté, L est un ordre total, car si x et y sont deux nombres réels quelconques, alors soit $x \leq y$, soit $y \leq x$. Ainsi, L nous donne un moyen de comparer *deux* nombres réels.

Exemple 4.4.3. Lesquelles des relations suivantes sont des ordres partiels ? Lesquelles sont des ordres totaux ?

1. Soit A un ensemble quelconque, et soit $B = \mathcal{P}(A)$ et $S = \{(x, y) \in B \times B \mid x \subseteq y\}$.
2. Soit $A = \{1, 2\}$ et $B = \mathcal{P}(A)$ comme précédemment. Soit

$$\begin{aligned} R &= \{(x, y) \in B \times B \mid y \text{ has at least as many elements as } x\} \\ &= \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{2\}), \\ &\quad (\{1\}, \{1, 2\}), (\{2\}, \{1\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}. \end{aligned}$$

$$3. D = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x \text{ divise } y\}.$$

$$4. G = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq y\}.$$

Solutions

1. Ceci n'est qu'une généralisation d'un des exemples présentés précédemment, et il est facile de vérifier qu'il s'agit d'un ordre partiel. Tant que A comporte au moins deux éléments, il ne s'agit pas d'un ordre total. Pour comprendre pourquoi, notez que si a et b

sont des éléments distincts de A , alors $\{a\}$ et $\{b\}$ sont des éléments de B pour lesquels $\{a\} \not\subseteq \{b\}$ et $\{b\} \not\subseteq \{a\}$.

2. Notons que $(\{1\}, \{2\}) \in R$ et $(\{2\}, \{1\}) \in R$, mais bien sûr, $\{1\} \neq \{2\}$. Ainsi, R n'est pas antisymétrique, et donc pas un ordre partiel. Bien que R ait été défini en sélectionnant des couples (x, y) dans lesquels y est, dans un certain sens, au moins aussi grand que x , il ne satisfait pas à la définition d'un ordre partiel. Cet exemple montre que notre description des ordres partiels comme des relations indiquant un sens où un objet est au moins aussi grand qu'un autre ne doit pas être prise trop au sérieux. sérieusement. C'était la *motivation* de la définition de l'ordre partiel, mais ce n'est pas la définition elle-même.
3. De toute évidence, tout entier positif est divisible par lui-même, donc D est réflexif. De plus, comme nous l'avons montré dans [le théorème 3.3.7](#), si $x | y$ et $y | z$ alors $x | z$. Ainsi, si $(x, y) \in D$ et $(y, z) \in D$ alors $(x, z) \in D$, donc D est transitif. Finalement, supposons $(x, y) \in D$ et $(y, x) \in D$. Alors $x | y$ et $y | x$, et comme x et y sont positifs il s'ensuit que $x \leq y$ et $y \leq x$, donc $x = y$. Ainsi, D est antisymétrique, donc c'est un ordre partiel. Il est facile de trouver des exemples illustrant que D n'est pas un ordre total. Par exemple, $(3, 5) \notin D$ et $(5, 3) \notin D$.

Vous avez peut-être été surpris d'apprendre que D est un ordre partiel. Il ne semble pas impliquer de comparaison de tailles, contrairement aux autres ordres partiels que nous avons vus. Cependant, nous avons montré qu'il partage avec ces autres relations les propriétés importantes de réflexivité, de transitivité et d'antisymétrie. C'est d'ailleurs l'une des raisons pour lesquelles des définitions telles que [la définition 4.4.2 ont été formulées](#). Elles nous aident à identifier des similitudes entre des choses qui, à première vue, pourraient ne pas sembler similaires du tout.

4. Vous devriez être capable de vérifier par vous-même que G est un ordre total. Notez que, dans ce cas, il semble plus raisonnable de considérer xGy comme signifiant que y est au moins aussi *petit* que x plutôt qu'au moins aussi *grand*. La définition d'ordre partiel, bien que motivée par la réflexion sur les ordres unidirectionnels, s'applique en réalité aux ordres bidirectionnels. En effet, cet exemple pourrait vous amener à supposer que si R est un ordre partiel sur A , alors R^{-1} l'est aussi. Vous devrez démontrer cette conjecture dans [l'exercice 13](#).

Jusqu'à présent, nous avons toujours utilisé des lettres pour nommer nos relations, mais il arrive que les mathématiciens les représentent par des symboles plutôt que par des lettres. Par exemple, dans la partie

4 de [l'exemple 4.4.3.](#), nous avons utilisé la lettre G comme nom de relation. Or, dans cet exemple, pour tous les nombres réels x et y , xGy signifiait la même chose que $x \geq y$. Cela suggère que nous n'avions pas vraiment besoin d'introduire la lettre G ; nous aurions simplement pu considérer le symbole \geq comme le nom de la relation. En utilisant cette notation, nous pourrions dire que \geq est un ordre total sur \mathbb{R} .

Voici un autre exemple d'ordre partiel. Soit A l'ensemble de tous les mots anglais, et soit $R = \{(x, y) \in A \times A \mid$ toutes les lettres du mot x apparaissent, consécutivement et dans le bon ordre, dans le mot $y\}$. Par exemple, (can, cannot), (tar, start) et (ball, ball) sont tous des éléments de R , mais (can, anchor) et (can, carnival) ne le sont pas. Vous devriez pouvoir vérifier que R est réflexif, transitif et antisymétrique, donc R est un ordre partiel. Considérons maintenant l'ensemble $B = \{\text{me, men, tame, mental}\} \subseteq A$. Il est clair que de nombreuses paires ordonnées de mots de B sont dans la relation R , mais notez en particulier que les paires ordonnées (me, me), (me, men), (me, tame) et (me, mental) sont toutes dans R . Si l'on considère xRy comme ce qui signifie que y est dans un certain sens au moins aussi grand que x , alors nous pourrions dire que le mot *me* est le *plus petit* élément de B , dans le sens où il est plus petit que tout le reste de l'ensemble.

Tous les ensembles de mots n'ont pas un élément qui soit le plus petit dans ce sens. Par exemple, considérons l'ensemble $C = \{\text{a, me, men, tame, mental}\} \subseteq A$. Chacun des mots *men*, *tame* et *mental* est plus grand qu'au moins un autre mot de l'ensemble, mais ni *a* ni *me* ne l'est. Nous appellerons *a* et *me* les éléments *minimaux* de C . Cependant, notez que ni *a* ni *me* ne sont le plus petit élément de C au sens décrit dans le paragraphe précédent, car aucun n'est plus petit que l'autre. L'ensemble C possède deux éléments minimaux, mais aucun élément de plus petit.

Ces exemples pourraient susciter plusieurs questions sur les plus petits éléments et les éléments minimaux. L'ensemble C possède deux éléments minimaux, mais B n'en possède qu'un seul. Un ensemble peut-il avoir plus d'un plus petit élément ? Tant que nous n'avons pas clarifié cette question, nous devrions considérer un objet comme étant *le* plus petit élément d'un ensemble, plutôt que *le* plus petit élément. Si un ensemble ne possède qu'un seul élément minimal, doit-il être le plus petit élément ? Un ensemble peut-il avoir un plus petit élément et un élément minimal différents ? Les réponses à ces questions seraient-elles différentes si nous nous concentrions sur les ordres *totaux* plutôt que sur tous les ordres partiels ? Avant de tenter de répondre à ces questions, il convient de préciser les définitions des termes *plus petit* et *minimal*.

Définition 4.4.4. Supposons que R soit un ordre partiel sur un ensemble A , $B \subseteq A$ et $b \in B$. Alors b est appelé un R -*plus petit* élément

de B (ou simplement un *plus petit* élément si R est clair d'après le contexte) si $\forall x \in B$ (bRx). Il est appelé un R - élément *minimal* (ou simplement un élément *minimal*) si $\neg\exists x \in B$ ($xRb \wedge x = b$).

Exemple 4.4.5.

1. Soit $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, comme précédemment. Soit $B = \{x \in \mathbb{R} \mid x \geq 7\}$. B possède -t-il des éléments L -plus petits ou L -minimaux ? Qu'en est-il de l'ensemble $C = \{x \in \mathbb{R} \mid x > 7\}$? Comme mentionné précédemment, on pourrait se passer de la lettre L et se demander *quels sont les éléments* \leq - plus petits ou \leq -minimaux de B et C .
2. Soit D la relation de divisibilité définie dans la partie 3 de [l'exemple 4.4.3](#). Soit $B = \{3, 4, 5, 6, 7, 8, 9\}$. B possède-t-il des éléments D plus petits ou D minimaux ?
3. Soit $S = \{(X, Y) \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \mid X \subseteq Y\}$, qui est un ordre partiel sur l'ensemble $\mathcal{P}(\mathbb{N})$. Soit $\mathcal{F} = \{X \in \mathcal{P}(\mathbb{N}) \mid 2 \in X \text{ et } 3 \in X\}$. Notez que les éléments de F ne sont pas des nombres naturels, mais *des ensembles* de nombres naturels. Par exemple, $\{1, 2, 3\}$ et $\{n \in \mathbb{N} \mid n \text{ est premier}\}$ sont tous deux des éléments de \mathcal{F} . \mathcal{F} possède -t-il des éléments S -plus petits ou S -minimaux ? Qu'en est-il de l'ensemble $G = \{X \in \mathcal{P}(\mathbb{N}) \mid \text{soit } 2 \in X \text{ soit } 3 \in X\}$?

Solutions

1. Clairement, $7 \leq x$ pour tout $x \in B$, donc $\forall x \in B$ ($7 Lx$) et donc 7 est un plus petit élément de B . C'est aussi un élément minimal, puisque rien dans B n'est plus petit que 7, donc $\neg\exists x \in B$ ($xL7 \wedge x \neq 7$). Il n'y a pas d'autres plus petits éléments ou éléments minimaux. Notons que 7 n'est *pas* un plus petit élément ou élément minimal de C , puisque $7 \notin C$. Selon la [définition 4.4.4](#), un plus petit élément ou élément minimal d'un ensemble doit en fait être un élément de l'ensemble. En fait, C n'a pas d'éléments plus petits ou minimaux.
2. Tout d'abord, notez que 6 et 9 ne sont pas minimaux car tous deux sont divisibles par 3, et 8 n'est pas minimal car il est divisible par 4. Tous les autres éléments de B sont des éléments minimaux, mais aucun n'est un plus petit élément.
3. L'ensemble $\{2, 3\}$ est le plus petit élément de \mathcal{F} , car 2 et 3 sont des éléments de tout ensemble de \mathcal{F} et donc $\forall X \in \mathcal{F}$ ($\{2, 3\} \subseteq X$). C'est aussi un élément minimal, car aucun autre élément de \mathcal{F} n'en est un sous-ensemble, et il n'existe pas d'autres éléments plus petits ou

minimaux. L'ensemble \mathcal{G} possède deux éléments minimaux, $\{2\}$ et $\{3\}$. Tout autre ensemble de \mathcal{G} doit contenir l'un de ces deux éléments comme sous-ensemble, donc aucun autre ensemble ne peut être minimal. Aucun des deux ensembles n'est le plus petit, car aucun n'est un sous-ensemble de l'autre.

Nous sommes maintenant prêts à répondre à certaines des questions que nous avons soulevées avant [la définition 4.4.4](#).

Théorème 4.4.6. *Supposer R est un ordre partiel sur un ensemble A , et $B \subseteq A$.*

1. *Si B possède un plus petit élément, alors ce plus petit élément est unique. On peut donc parler de **le** le plus petit élément de B plutôt que **un** le plus petit élément.*
2. *Supposons que b soit le plus petit élément de B . Alors b est également un élément minimal de B , et c'est le seul élément minimal.*
3. *Si R est un ordre total et b est un élément minimal de B , alors b est le plus petit élément de B .*

Travail à partir de zéro

Ces preuves sont un peu plus difficiles que les précédentes dans ce chapitre, nous faisons donc un peu de travail de base avant les preuves.

1. Bien sûr, commençons par supposer que B possède un plus petit élément, et comme il s'agit d'une affirmation existentielle, nous introduisons immédiatement un nom, disons b , pour un plus petit élément de B . Il faut prouver que b est le seul plus petit élément. Comme nous l'avons vu à [la section 3.6](#), cela peut s'écrire $\forall c (c \text{ est un plus petit élément de } B \rightarrow b = c)$, donc notre prochaine étape devrait être de poser c arbitraire, de supposer qu'il est aussi un plus petit élément, et de prouver que $b = c$.

À ce stade, nous ne savons pas grand-chose sur b et c . Nous savons qu'ils sont tous deux des éléments de B , mais nous ne savons même pas quels types d'objets sont dans B – qu'il s'agisse de nombres, d'ensembles ou d'autres types d'objets – donc cela ne nous aide pas beaucoup à décider comment prouver que $b = c$. Le seul autre fait que nous savons sur b et c est qu'ils sont tous deux les plus petits éléments de B , ce qui signifie $\forall x \in B (bRx)$ et $\forall x \in B (cRx)$. La façon la plus prometteuse d'utiliser ces instructions est de remplacer x par une valeur dans chaque instruction. Ce que nous remplaçons devrait être un élément de B , et nous ne connaissons que deux éléments de B à ce stade, b et c . En les remplaçant tous les deux dans les deux instructions, nous obtenons bRb , bRc , cRb et cRc . Bien sûr, nous connaissons déjà

bRb et cRc , puisque R est réflexif. Mais quand on voit que bRc et cRb , on devrait penser à l'antisymétrie. Puisque R est un ordre partiel, il est antisymétrique ; ainsi, de bRc et cRb , il résulte que $b = c$.

2. Notre premier objectif est de prouver que b est un élément minimal de B , ce qui signifie $\neg \exists x \in B (xRb \wedge x \neq b)$. Comme il s'agit d'une affirmation négative, il peut être utile de la reformuler sous une forme positive équivalente :

$$\begin{aligned} \neg \exists x \in B (xRb \wedge x \neq b) &\text{ iff } \forall x \in B \neg (xRb \wedge x \neq b) \\ &\text{ iff } \forall x \in B (\neg xRb \vee x = b) \\ &\text{ iff } \forall x \in B (xRb \rightarrow x = b). \end{aligned}$$

Ainsi, pour prouver que b est minimal, nous pourrions laisser x être un élément arbitraire de B , supposer que xRb et prouver que $x = b$.

Il est judicieux de faire le point sur ce que nous savons actuellement sur b et x . Nous connaissons xRb et b est le plus petit élément de B , ce qui signifie $\forall x \in B (bRx)$. Si nous appliquons ce dernier fait à notre x arbitraire, alors, comme dans la première partie, nous pouvons utiliser l'antisymétrie pour compléter la preuve.

Il nous reste à prouver que b est le seul élément minimal, et comme dans la partie 1, cela signifie $\forall c (c \text{ est un élément minimal de } B \rightarrow b = c)$. Soit donc c arbitraire et supposons que c est un élément minimal de B , et nous devons prouver que $b = c$. L'hypothèse que c est un élément minimal de B signifie que $c \in B$ et $\neg x \in B (xRc \wedge x = c)$, mais comme précédemment, nous pouvons réexprimer cette dernière affirmation sous la forme positive équivalente $\forall x \in B (xRc \rightarrow x = c)$. Pour utiliser cette affirmation, nous devons remplacer x par quelque chose, et parce que notre objectif est Pour montrer que $b = c$, remplacer x par b semble judicieux. Cela nous donne $bRc \rightarrow b = c$; si seulement nous pouvions montrer bRc , nous pourrions compléter la preuve en utilisant le modus ponens pour conclure que $b = c$. Mais nous savons que b est le plus petit élément de B ; donc, bien sûr, bRc est vrai.

3. Bien sûr, commençons par supposer que R est un ordre total et que b est un élément minimal de B . Il faut prouver que b est le plus petit élément de B , ce qui signifie $\forall x \in B (bRx)$. Soit donc x un élément arbitraire de B et essayons de prouver bRx .

Nous savons, d'après les exemples que nous avons vus, que les éléments minimaux dans les ordres *partiels* ne sont pas toujours les plus petits éléments, donc l'hypothèse que R est un ordre *total* doit être cruciale. L'hypothèse que R est total signifie $\forall x \in A \forall y \in A (xRy \vee yRx)$, donc pour l'utiliser, nous devons remplacer x et y . Les seuls candidats probables pour remplacer x sont b et notre objet arbitraire x , et en les remplaçant, nous obtenons $xRb \vee bRx$. Notre objectif est bRx , donc cela ressemble certainement à un progrès. Si seulement nous pouvions exclure la possibilité que xRb , nous aurions terminé. Voyons donc si nous pouvons prouver $\neg xRb$.

Comme il s'agit d'une affirmation négative, nous tentons une preuve par contradiction. Supposons xRb . Quelle affirmation donnée pouvons-nous contredire ? La seule donnée que nous n'avons pas encore utilisée est la minimisation de b , et comme il s'agit d'une affirmation négative, c'est l'endroit naturel pour chercher une contradiction. Pour contredire la minimisation de b , nous devrions essayer de montrer que $\exists x \in B (xRb \wedge x \neq b)$. Mais nous avons déjà supposé xRb ; si nous pouvions montrer que $x \neq b$, ce serait terminé.

Vous devriez essayer de prouver $x = b$ à ce stade. Vous n'arriverez à rien. En fait, nous avons commencé par considérer x comme un élément arbitraire de B , ce qui signifie qu'il pourrait être n'importe quel élément de B , y compris b . Nous avons ensuite supposé que xRb , mais comme R est réflexif, cela n'exclut pas la possibilité que $x = b$. Il n'y a vraiment aucun espoir de prouver que $x \neq b$. Nous semblons bloqués.

Revoyons notre plan de preuve. Nous devions démontrer que $\forall x \in B (bRx)$, donc nous posons x comme un élément arbitraire de B et nous essayons de démontrer bRx . Nous nous heurtions maintenant à des problèmes liés à la possibilité que $x = b$. Mais si notre objectif ultime est de démontrer bRx , alors la possibilité que $x = b$ ne pose finalement aucun problème. Puisque R est réflexif, si $x = b$ alors bRx sera bien sûr vrai !

Maintenant, comment structurer la rédaction finale de la preuve ? Il semble que notre raisonnement pour établir bRx doive être différent selon que $x = b$ ou non. Cela suggère *une preuve par cas*. Dans le cas 1, nous supposons que $x = b$ et utilisons le fait que R est réflexif pour compléter la preuve. Dans le cas 2, nous supposons que $x = b$ et pouvons alors utiliser notre ligne d'attaque initiale, en commençant par le fait que R est total.

Preuve .

1. Supposons que b soit le plus petit élément de B , et que c soit également le plus petit élément de B . Puisque b est le plus petit élément, $\forall x \in B (bRx)$, on a donc en particulier bRc . De même, puisque c est le plus petit élément, cRb . Mais puisque R est un ordre partiel, il doit être antisymétrique ; ainsi, à partir de bRc et cRb , on peut conclure que $b = c$.
2. Soit x un élément quelconque de B et supposons que xRb . Puisque b est le plus petit élément de B , nous devons avoir bRx , et par antisymétrie, il en résulte que $x = b$. Ainsi, il ne peut y avoir $x \in B$ tel que xRb et $x \neq b$; b est donc un élément minimal.

Pour voir qu'il est le seul, supposons que c soit aussi un élément minimal. Puisque b est le plus petit élément de B , bRc . Mais alors ,

puisque c est minimal, nous devons avoir $b = c$. Ainsi, b est le seul élément minimal de B .

3. Supposons que R soit un ordre total et que b soit un élément minimal de B . Soit x un élément arbitraire de B . Si $x = b$, alors puisque R est réflexif, bRx . Supposons maintenant que $x \neq b$. Puisque R est un ordre total, nous savons que xRb ou bRx . Or, xRb ne peut être vrai, car en combinant xRb avec notre hypothèse que $x \neq b$, nous pourrions conclure que b n'est pas minimal, ce qui contredirait notre hypothèse qu'il est minimal. Ainsi, bRx doit être vrai. Puisque x est arbitraire, nous pouvons conclure que $\forall x \in B (bRx)$, donc b est le plus petit élément de B .

□

Lors de la comparaison de sous-ensembles d'un ensemble A , les mathématiciens utilisent souvent l'ordre partiel $S = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid X \subseteq Y\}$, bien que cela ne soit pas toujours explicite. Rappelons que si $\mathcal{F} \subseteq \mathcal{P}(A)$ et $X \in \mathcal{F}$, alors selon [la définition 4.4.4](#), X est le S -plus petit élément de \mathcal{F} si $\forall Y \in \mathcal{F} (X \subseteq Y)$. En d'autres termes, dire qu'un élément de \mathcal{F} est le plus petit élément signifie qu'il est un sous-ensemble de chaque élément de \mathcal{F} . De même, les mathématiciens parlent parfois d'un ensemble comme étant le plus petit avec une certaine propriété. Généralement, cela signifie que l'ensemble a la propriété en question, et de plus, il est un sous-ensemble de chaque ensemble qui a la propriété. Par exemple, nous pourrions décrire notre conclusion dans la partie 3 de [l'exemple 4.4.5](#) en disant que $\{2, 3\}$ est le plus petit ensemble $X \subseteq \mathbb{N}$ avec la propriété que $2 \in X$ et $3 \in X$. Nous verrons plus d'exemples de cette idée dans les chapitres suivants.

Exemple 4.4.7.

1. Trouvez le plus petit ensemble de nombres réels X tels que $5 \in X$ et pour tous les nombres réels x et y , si $x \in X$ et $x < y$ alors $y \in X$.
2. Trouvez le plus petit ensemble de nombres réels X tels que $X \neq \emptyset$ et pour tous les nombres réels x et y , si $x \in X$ et $x < y$ alors $y \in X$.

Solutions

1. Une autre façon de formuler la question serait de dire que nous recherchons le plus petit élément de la famille des ensembles $\mathcal{F} = \{X \subseteq \mathbb{R} \mid 5 \in X \text{ et } \forall x \forall y ((x \in X \wedge x < y) \rightarrow y \in X)\}$, où il est entendu que *le plus petit* signifie le plus petit par rapport à l'ordre partiel des sous-ensembles. Maintenant, pour tout ensemble $x \in \mathcal{F} \Leftrightarrow$ nous savons que $5 \in X$, et nous savons que $\forall x \forall y ((x \in X \wedge x < y) \rightarrow y \in X)$.

X). En particulier, puisque $5 \in X$ nous pouvons dire que $\forall y (5 < y \rightarrow y \in X)$. Ainsi, si nous posons $A = \{y \in \mathbb{R} \mid 5 \leq y\}$, alors nous pouvons conclure que $\forall X \in \mathcal{F} (A \subseteq X)$. Mais il est facile de voir que $A \in \mathcal{F}$, donc A est le plus petit élément de \mathcal{F} .

2. Nous devons trouver le plus petit élément de la famille des ensembles $\mathcal{F} = \{X \subseteq \mathbb{R} \mid X \neq \emptyset \text{ et } \forall x \forall y ((x \in X \wedge x < y) \rightarrow y \in X)\}$. L'ensemble $A = \{y \in \mathbb{R} \mid 5 \leq y\}$ de la partie 1 est un élément de \mathcal{F} , mais ce n'est pas le plus petit élément, ni même un élément minimal, car l'ensemble $A = \{y \in \mathbb{R} \mid 6 \leq y\}$ est plus petit – en d'autres termes, $A \subseteq A$ et $A = A$. Mais A n'est pas non plus le plus petit élément, car $A = \{y \in \mathbb{R} \mid 7 \leq y\}$ est encore plus petit. En fait, cette famille n'a pas de plus petit élément, ni même d'élément minimal. On vous demande de vérifier cela dans [l'exercice 12](#). Cet exemple montre qu'il faut être prudent lorsqu'on parle du plus petit ensemble possédant une propriété. Il se peut qu'un tel plus petit ensemble n'existe pas !

Vous avez probablement déjà deviné comment définir les éléments maximaux et les plus grands dans les ensembles partiellement ordonnés. Supposons que R soit un ordre partiel sur A , $B \subseteq A$ et $b \in B$. On dit que b est le *plus grand élément* de B si $\forall x \in B (xRb)$, et qu'il est un élément *maximal de B* si $\neg \exists x \in B (bRx \wedge b \neq x)$. Bien sûr, ces définitions sont assez similaires à celles de [la définition 4.4.4](#). [L'exercice 14](#) vous demande de déterminer certains liens entre ces idées. Une autre idée connexe utile est le concept de borne supérieure ou inférieure pour un ensemble.

Définition 4.4.8. Supposons que R soit un ordre partiel sur A , $B \subseteq A$ et $a \in A$. Alors a est appelé *borne inférieure* de B si $\forall x \in B (aRx)$. De même, c'est un *ordre supérieur. borne* pour B si $\forall x \in B (xRa)$.

Notez qu'une borne inférieure pour B n'a pas besoin d'être un élément de B . C'est la seule différence entre les bornes inférieures et les plus petits éléments. Un plus petit élément de B est simplement une borne inférieure qui est aussi un élément de B . Par exemple, dans la partie 1 de [l'exemple 4.4.5](#), nous avons conclu que 7 n'était pas un plus petit élément de l'ensemble $C = \{x \in \mathbb{R} \mid x > 7\}$ car $7 \notin C$. Mais 7 est une borne inférieure pour C . En fait, il en est de même pour tout nombre réel inférieur à 7, mais pas pour tout nombre supérieur à 7. Ainsi, l'ensemble de toutes les bornes inférieures de C est l'ensemble $\{x \in \mathbb{R} \mid x \leq 7\}$, et 7 est son plus grand élément. Nous disons que 7 est la *plus grande borne inférieure* de l'ensemble C .

Définition 4.4.9. Supposons que R soit un ordre partiel sur A et $B \subseteq A$. Soit U l'ensemble des bornes supérieures de B et L l'ensemble des bornes inférieures. Si U possède un plus petit élément, alors ce plus petit élément est appelé la *plus petite borne supérieure* de B . Si L possède un plus grand élément, alors ce plus grand élément est appelé le *plus grand . limite inférieure* de B . Les expressions « *plus petite limite supérieure* » et « *plus grande limite inférieure* » sont parfois abrégées par *lub .* et *glb .*

Exemple 4.4.10.

1. Soit $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, un ordre total sur \mathbb{R} . Soit $B = \{1/n \mid n \in \mathbb{Z}^+\} = \{1, 1/2, 1/3, 1/4, 1/5, \dots\} \subseteq \mathbb{R}$. B possède-t-il des bornes supérieures ou inférieures ? A-t-il une plus petite borne supérieure ou une plus grande borne inférieure ?
2. Soit A l'ensemble de tous les mots anglais, et R l'ordre partiel sur A décrit après [l'exemple 4.4.3](#). Soit $B = \{\text{hold}, \text{up}\}$. B a-t-il une borne supérieure ou inférieure ? A-t-il une borne supérieure minimale ou une borne inférieure maximale ?

Solutions

1. De toute évidence, le plus grand élément de B est 1. C'est aussi une borne supérieure pour B , comme l'est tout nombre supérieur à 1. Par définition, une borne supérieure pour B doit être au moins aussi grande que chaque élément de B , donc en particulier elle doit être au moins aussi grande que 1. Ainsi, aucun nombre inférieur à 1 n'est une borne supérieure pour B , donc l'ensemble des bornes supérieures pour B est $\{x \in \mathbb{R} \mid x \geq 1\}$. *De toute évidence, le plus petit élément de cet ensemble est 1, donc 1 est la borne supérieure de B .*

De toute évidence, 0 est une borne inférieure pour B , comme tout nombre négatif. Par ailleurs, supposons que a soit un nombre positif. Alors, pour un entier n suffisamment grand, nous aurons $1/n < a$. (Vous devriez vous convaincre que tout entier n supérieur à $1/a$ ferait l'affaire.) Ainsi, $\forall x \in B$ ($a \leq x$), et donc a n'est pas une borne inférieure pour B . Ainsi, l'ensemble des bornes inférieures pour B est $\{x \in \mathbb{R} \mid x \leq 0\}$, et le glb de B est 0.

2. Il est clair que *holdup* et *uphold* sont des bornes supérieures pour B . En fait, aucun mot plus court ne pourrait être une borne supérieure ; ils sont donc tous deux des éléments minimaux de l'ensemble de toutes les bornes supérieures. D'après la partie 2 du [théorème 4.4.6](#), un ensemble comportant plusieurs éléments minimaux ne peut avoir de plus petit élément ; l'ensemble de toutes

les bornes supérieures de B n'a donc pas de plus petit élément, et donc B n'a pas de plus petite borne supérieure.

Les mots *hold* et *up* n'ont aucune lettre en commun, donc B n'a pas de limite inférieure.

Notez que dans la partie 1 de [l'exemple 4.4.10](#), le plus grand élément de B s'est également avéré être sa plus petite borne supérieure. On peut se demander si les plus grands éléments sont Les plus petits éléments sont-ils toujours des bornes supérieures ? On vous demande de prouver que c'est le cas dans [l'exercice 20](#). Un autre fait intéressant concernant cet exemple est que, bien que B n'ait pas de plus petit élément, il avait une borne inférieure supérieure. Ce n'était pas une coïncidence. Il est important de noter, concernant les nombres réels, que *tout* ensemble non vide de nombres réels ayant une borne inférieure possède une borne inférieure supérieure et, de même, tout ensemble non vide de nombres réels ayant une borne supérieure possède une borne supérieure inférieure. La démonstration de ce fait dépasse le cadre de ce livre, mais il est important de comprendre qu'il s'agit d'un fait particulier concernant les nombres réels ; il ne s'applique pas à tous les ordres partiels, ni même à tous les ordres totaux. Par exemple, l'ensemble B de la deuxième partie de [l'exemple 4.4.10](#) possédait des bornes supérieures, mais pas de borne supérieure inférieure.

Nous terminons cette section en examinant une fois de plus comment ces nouveaux concepts s'appliquent à l'ordre partiel des sous-ensembles sur $\mathcal{P}(A)$, pour tout ensemble A . Il s'avère que dans cet ordre partiel, les plus petites bornes supérieures et les plus grandes bornes inférieures sont nos vieilles amies unions et intersections.

Théorème 4.4.11. *Supposer UN est un ensemble, $\mathcal{F} \subseteq \mathcal{P}(A)$, et $\mathcal{F} \neq \emptyset$. Alors la plus petite borne supérieure de \mathcal{F} (dans l'ordre partiel du sous-ensemble) est $\bigcap \mathcal{F}$ et la plus grande borne inférieure de \mathcal{F} est $\bigcap \mathcal{F}$.*

Preuve . Voir [exercice 23](#) .

Exercices

*1. Dans chaque cas, dites si R est ou non un ordre partiel sur A . Si oui, est-ce un ordre total ?

(a) $A = \{a, b, c\}$, $R = \{(a, a), (b, a), (b, b), (b, c), (c, c)\}$.

(b) $A = \mathbb{R}$, $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| \leq |y|\}$.

(c) $A = \mathbb{R}$, $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| < |y| \text{ ou } x = y\}$.

2. Dans chaque cas, dites si R est ou non un ordre partiel sur A . Si oui, est-ce un ordre total ?

(a) A = l'ensemble de tous les mots anglais, $R = \{(x, y) \in A \times A \mid \text{le mot } y \text{ apparaît au moins aussi tard dans l'ordre alphabétique que le mot } x\}$.

(b) A = l'ensemble de tous les mots anglais, $R = \{(x, y) \in A \times A \mid \text{la première lettre du mot } y \text{ apparaît au moins aussi tard dans l'alphabet que la première lettre du mot } x\}$.

(c) A = l'ensemble de tous les pays du monde, $R = \{(x, y) \in A \times A \mid \text{la population du pays } y \text{ est au moins aussi grande que la population du pays } x\}$.

3. Dans chaque cas, trouvez tous les éléments minimaux et maximaux de B . Trouvez également, s'ils existent, les plus grands et les plus petits éléments de B , ainsi que la plus petite borne supérieure et la plus grande borne inférieure de B .

(a) R = la relation représentée dans le graphe orienté de [la figure 4.6](#), $B = \{2, 3, 4\}$.

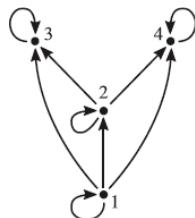


Figure 4.6.

(b) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, $B = \{x \in \mathbb{R} \mid 1 \leq x < 2\}$.

(c) $R = \{(x, y) \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \mid x \subseteq y\}$, $B = \{x \in \mathcal{P}(\mathbb{N}) \mid x \text{ a au plus 5 éléments}\}$.

*4. Supposons que R soit une relation sur A . On pourrait penser que R ne peut être à la fois antisymétrique et symétrique, mais ce n'est pas vrai. Démontrer que R est à la fois antisymétrique et symétrique ssi $R \subseteq i_A$.

5. Supposons que R soit un ordre partiel sur A et $B \subseteq A$. Démontrer que $R \cap (B \times B)$ est un ordre partiel sur B .
6. Supposons que R_1 et R_2 soient des ordres partiels sur A . Pour chaque partie, donnez une preuve ou un contre-exemple pour justifier votre réponse.
- $R_1 \cap R_2$ doit-il être un ordre partiel sur A ?
 - $R_1 \cup R_2$ doit-il être un ordre partiel sur A ?
7. Supposons que R_1 soit un ordre partiel sur A_1 , R_2 soit un ordre partiel sur A_2 et $A_1 \cap A_2 = \emptyset$.
- Démontrer que $R_1 \cup R_2$ est un ordre partiel sur $A_1 \cup A_2$.
 - Démontrer que $R_1 \cup R_2 \cup (A_1 \times A_2)$ est un ordre partiel sur $A_1 \cup A_2$.
 - Supposons que R_1 et R_2 soient des ordres totaux. Les ordres partiels des parties (a) et (b) sont-ils également des ordres totaux ?
- *8. Supposons que R soit un ordre partiel sur A et que S soit un ordre partiel sur B . Définissez une relation T sur $A \times B$ comme suit : $T = \{((a, b), (a', b')) \in (A \times B) \times (A \times B) \mid aRa' \text{ et } bSb'\}$. Montrez que T est un ordre partiel sur $A \times B$. Si R et S sont tous deux des ordres totaux, T sera-t-il également un ordre total ?
9. Supposons que R soit un ordre partiel sur A et que S soit un ordre partiel sur B . Définissez une relation L sur $A \times B$ comme suit : $L = \{((a, b), (a', b')) \in (A \times B) \times (A \times B) \mid aRa' \text{ et si } a = a' \text{ alors } bSb'\}$. Montrez que L est un ordre partiel sur $A \times B$. Si R et S sont tous deux des ordres totaux, L sera-t-il également un ordre total ?
10. Supposons que R soit un ordre partiel sur A . Pour tout $x \in A$, soit $P_x = \{a \in A \mid aRx\}$. Démontrer que $\forall x \in A \forall y \in A (xRy \leftrightarrow P_x \subseteq P_y)$.
- *11. Soit D la relation de divisibilité définie dans la partie 3 de [l'exemple 4.4.3](#). Soit $B = \{x \in \mathbb{Z} \mid x > 1\}$. B possède-t-il des éléments minimaux ? Si oui, lesquels ? B possède-t-il un plus petit élément ? Si oui, lequel ?
12. Démontrer que, comme indiqué dans la partie 2 de [l'exemple 4.4.7](#), $\{X \subseteq \mathbb{R} \mid X \neq \emptyset \text{ et } \forall x \forall y ((x \in X \wedge x < y) \rightarrow y \in X)\}$ n'a pas d'élément minimal.
13. Supposons que R soit un ordre partiel sur A . Démontrer que R^{-1} est aussi un ordre partiel sur A . Si R est un ordre total, R^{-1} sera-t-il aussi un ordre total ?
- *14. Supposons que R soit un ordre partiel sur A , $B \subseteq A$ et $b \in B$. [L'exercice 13](#) montre que R^{-1} est également un ordre partiel sur A .

- (a) Démontrer que b est le R -plus grand élément de B ssi c'est le R^{-1} -plus petit élément de B .
- (b) Démontrer que b est un élément R -maximal de B ssi c'est un élément R^{-1} -minimal de B .
15. Supposons que R_1 et R_2 soient des ordres partiels sur A , $R_1 \subseteq R_2$, $B \subseteq A$ et $b \in B$.
- (a) Démontrer que si b est le R_1 -plus petit élément de B , alors il est également le R_2 -plus petit élément de B .
- (b) Démontrer que si b est un élément R_2 -minimal de B , alors il est également un élément R_1 -minimal de B .
16. Supposons que R soit un ordre partiel sur A , $B \subseteq A$ et $b \in B$. Démontrer que si b est le plus grand élément de B , alors b est aussi un élément maximal de B , et c'est le seul élément maximal.
- *17. Si un sous-ensemble d'un ensemble partiellement ordonné possède exactement un élément minimal, cet élément doit-il être le plus petit élément ? Justifiez votre réponse par une preuve ou un contre-exemple.
18. Supposons que R soit un ordre partiel sur A , $B_1 \subseteq A$, $B_2 \subseteq A$, $\forall x \in B_1 \exists y \in B_2 (xRy)$ et $\forall x \in B_2 \exists y \in B_1 (xRy)$.
- (a) Démontrer que pour tout $x \in A$, x est une borne supérieure de B_1 ssi x est une borne supérieure de B_2 .
- (b) Démontrer que si B_1 et B_2 sont disjoints alors aucun d'eux n'a d'élément maximal.
19. Considérez le théorème putatif suivant.

Théorème? Supposer R est une commande totale sur UN et $B \subseteq A$. Alors chaque l'élément de B est soit le plus petit élément de B soit le plus grand élément de B .

- (a) Quel est le problème avec la preuve suivante du théorème ?

Preuve . Supposons que $b \in B$. Soit x un élément arbitraire de B . Puisque R est un ordre total, soit bRx soit xRb .

Cas 1. bRx . Puisque x est arbitraire, nous pouvons conclure que $\forall x \in B (bRx)$, donc b est le plus petit élément de R .

Cas 2. xRb . Puisque x est arbitraire, nous pouvons conclure que $\forall x \in B (xRb)$, donc b est le plus grand élément de R .

Ainsi, b est soit le plus petit élément de B , soit le plus grand élément de B . Puisque b est arbitraire, chaque élément de B est soit son plus petit élément, soit son plus grand élément.

(b) Le théorème est-il correct ? Justifiez votre réponse par une preuve ou un contre-exemple.

20. Supposons que R soit un ordre partiel sur A , $B \subseteq A$ et $b \in B$.

(a) Démontrer que si b est le plus petit élément de B , alors il est aussi la plus grande borne inférieure de B .

(b) Démontrer que si b est le plus grand élément de B , alors il est aussi la plus petite borne supérieure de B .

*21. Supposons que R soit un ordre partiel sur A et $B \subseteq A$. Soit U l'ensemble de toutes les bornes supérieures pour B .

(a) Démontrer que U est fermé vers le haut ; c'est-à-dire démontrer que si $x \in U$ et xRy , alors $y \in U$.

(b) Démontrer que chaque élément de B est une borne inférieure pour U

(c) Démontrer que si x est la plus grande borne inférieure de U , alors x est la plus petite borne supérieure de B .

22. Supposons que R soit un ordre partiel sur A , $B_1 \subseteq A$, $B_2 \subseteq A$, x_1 est la plus petite borne supérieure de B_1 et x_2 est la plus petite borne supérieure de B_2 . Démontrer que si $B_1 \subseteq B_2$ alors $x_1 Rx_2$.

23. Démontrer [le théorème 4.4.11](#).

*24. Supposons que R soit une relation sur A . Soit $S = R \cup R^{-1}$.

(a) Montrer que S est une relation symétrique sur A et $R \subseteq S$.

(b) Montrez que si T est une relation symétrique sur A et $R \subseteq T$ alors $S \subseteq T$.

Notez que cet exercice montre que S est le plus petit élément de l'ensemble $\mathcal{F} = \{ T \subseteq A \times A \mid R \subseteq T \text{ et } T \text{ est symétrique} \}$; autrement dit, c'est la plus petite relation symétrique sur A qui contient R comme sous-ensemble. La relation S est appelée la *clôture symétrique* de R .

25. Supposons que R soit une relation sur A . Soit $\mathcal{F} = \{ T \subseteq A \times A \mid R \subseteq T \text{ et } T \text{ est transitive}\}$.

(a) Montrer que $\mathcal{F} \neq \emptyset$.

(b) Montrer que $\cap \mathcal{F}$ est une relation transitive sur A et $R \subseteq \cap \mathcal{F}$.

(c) Montrer que $\cap \mathcal{F}$ est la plus petite relation transitive sur A qui contient R comme sous-ensemble. La relation $\cap \mathcal{F}$ est appelée la *clôture transitive* de R .

26. Supposons que R_1 et R_2 soient des relations sur A et $R_1 \subseteq R_2$.

(a) Soient S_1 et S_2 les fermetures symétriques de R_1 et R_2 , respectivement. Démontrer que $S_1 \subseteq S_2$. (Voir [l'exercice 24](#) pour la définition d'une fermeture symétrique.)

(b) Soient T_1 et T_2 les fermetures transitives de R_1 et R_2 , respectivement. Démontrer que $T_1 \subseteq T_2$. (Voir [l'exercice 25](#) pour la définition d'une fermeture transitive.)

*27. Supposons que R_1 et R_2 soient des relations sur A , et soit $R = R_1 \cup R_2$.

(a) Soient S_1 , S_2 et S les fermetures symétriques de R_1 , R_2 et R , respectivement. Démontrer que $S_1 \cup S_2 = S$. (Voir [l'exercice 24](#) pour la définition d'une fermeture symétrique.)

(b) Soient T_1 , T_2 et T les fermetures transitives de R_1 , R_2 et R , respectivement. Démontrer que $T_1 \cup T_2 \subseteq T$ et donner un exemple montrant qu'il peut arriver que $T_1 \cup T_2 \neq T$. (Voir [l'exercice 25](#) pour la définition d'une fermeture transitive.)

28. Supposons que A soit un ensemble.

(a) Démontrer que si A possède au moins deux éléments, alors il n'existe pas de plus grande relation antisymétrique sur A . Autrement dit, il n'existe pas de relation R sur A telle que R soit antisymétrique, et pour toute relation antisymétrique S sur A , $S \subseteq R$.

(b) Supposons que R soit un ordre total sur A . Démontrer que R est une relation antisymétrique maximale sur A . En d'autres termes, il n'existe pas de relation antisymétrique S sur A telle que $R \subseteq S$ et $R \neq S$.

29. Supposons que R soit une relation sur A . On dit que R est *irréflexif* si $\forall x \in A ((x, x) \notin R)$. R est dit *ordre partiel strict* sur A s'il est irréflexif et transitif. On dit *ordre total strict* s'il est un ordre partiel strict et que de plus $\forall x \in A \forall y \in A (xRy \vee yRx \vee x = y)$. (Notez que la terminologie ici est quelque peu trompeuse, car un ordre partiel strict n'est pas un ordre partiel particulier. Ce n'est pas du tout un ordre partiel, puisqu'il n'est pas réflexif !)

(a) Soit $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$. Montrer que L est un ordre total strict sur \mathbb{R} .

(b) Montrer que si R est un ordre partiel sur A , alors $R \setminus i_A$ est un ordre partiel strict sur A , et si R est un ordre total sur A , alors $R \setminus i_A$ est un ordre total strict sur A .

(c) Montrer que si R est un ordre partiel strict sur A , alors $R \cup i_A$ est un ordre partiel sur A , et si R est un ordre total strict sur A , alors $R \cup i_A$ est un ordre total sur A .

30. Supposons que R soit une relation sur A , et soit T la clôture transitive de R . Démontrer que si R est symétrique, alors T l'est aussi. (Indice : Supposons que R est symétrique. Démontrer que $R \subseteq$

T^{-1} et que T^{-1} est transitive. Que conclure de T et T^{-1} ? Voir [l'exercice 25](#) pour la définition de la clôture transitive.)

4.5 Relations d'équivalence

Nous avons vu dans [l'exemple 4.3.3](#) que la relation d'identité i_A sur tout ensemble A est toujours réflexive, symétrique et transitive. Les relations combinant cette combinaison de propriétés sont fréquentes en mathématiques et possèdent des propriétés importantes que nous étudierons dans cette section. Ces relations sont appelées *relations d'équivalence*.

Définition 4.5.1. Supposons que R soit une relation sur un ensemble A . On dit alors que R est une *relation d'équivalence sur A* (ou simplement une *relation d'équivalence* si A ressort clairement du contexte) si elle est réflexive, symétrique et transitive.

Comme nous l'avons observé précédemment, la relation d'identité i_A sur un ensemble A est une relation d'équivalence. Par exemple, soit T l'ensemble de tous les triangles, et soit C la relation de congruence des triangles. Autrement dit, $C = \{(s, t) \in T \times T \mid \text{le triangle } s \text{ est congru au triangle } t\}$. (Rappelons qu'un triangle est congru à un autre s'il peut être déplacé sans le déformer de manière à ce qu'il coïncide avec l'autre.) De toute évidence, tout triangle est congru à lui-même, donc C est réflexif. De plus, si le triangle s est congru au triangle t , alors t est congru à s , donc C est symétrique ; et si r est congru à s et s est congru à t , alors r est congru à t , donc C est transitif. Ainsi, C est une relation d'équivalence sur T .

Prenons un autre exemple : soit P l'ensemble de toutes les personnes, et soit $B = \{(p, q) \in P \times P \mid \text{la personne } p \text{ a le même anniversaire que la personne } q\}$. (Par « même anniversaire », nous entendons le même mois et le même jour, mais pas nécessairement la même année.) Tout le monde a le même anniversaire que lui, donc B est réflexif. Si p a le même anniversaire que q , alors q a le même anniversaire que p , donc B est symétrique. Et si p a le même anniversaire que q et q a le même anniversaire que r , alors p a le même anniversaire que r , donc B est transitif. Par conséquent, B est une relation d'équivalence.

Il peut être instructif d'examiner la relation B de plus près. Nous pouvons penser à cette relation comme divisant l'ensemble P de toutes les personnes en 366 catégories, une pour chaque anniversaire possible. (Rappelez-vous, certaines personnes sont nées le 29 février !)

Une paire ordonnée de personnes sera un élément de B si les personnes viennent de la même catégorie, mais ne sera pas un élément de B si les personnes viennent de catégories différentes. Nous pourrions penser à ces catégories comme formant une famille de sous-ensembles de P , que nous pourrions écrire comme une famille indexée comme suit. Tout d'abord, soit D l'ensemble de tous les anniversaires possibles. En d'autres termes, $D = \{1er janv., 2 janv., 3 janv., \dots, 30 déc., 31 déc.\}$. Maintenant, pour chaque $d \in D$, soit $P_d = \{p \in P \mid \text{la personne } p \text{ est née le jour } d\}$. Alors la famille $\mathcal{F} = \{P_d \mid d \in D\}$ est une famille indexée de sous-ensembles de P . Les éléments de \mathcal{F} sont appelés *équivalence classes* pour la relation B , et chaque personne est un élément d'une seule de ces classes d'équivalence. La relation B est constituée des couples $(p, q) \in P \times P$ tels que les personnes p et q appartiennent à la même classe d'équivalence. Autrement dit,

$$\begin{aligned} B &= \{(p, q) \in P \times P \mid \exists d \in D (p \in P_d \text{ and } q \in P_d)\} \\ &= \{(p, q) \in P \times P \mid \exists d \in D ((p, q) \in P_d \times P_d)\} \\ &= \bigcup_{d \in D} (P_d \times P_d). \end{aligned}$$

Nous appellerons la famille \mathcal{F} une *partition* de P car elle décompose l'ensemble P en éléments disjoints. Il s'avère que toute relation d'équivalence sur un ensemble A détermine une partition de A , dont les éléments sont les classes d'équivalence de cette relation. Mais avant de pouvoir expliquer en détail pourquoi cela est vrai, nous devons définir plus précisément les termes *partition* et *classe d'équivalence*.

Définition 4.5.2. Supposons que A soit un ensemble et que $\mathcal{F} \subseteq \mathcal{P}(A)$. On dira que \mathcal{F} est *deux à deux disjoint* si chaque paire d'éléments distincts de \mathcal{F} est disjointe, autrement dit $\forall X \in \mathcal{F} \forall Y \in \mathcal{F} (X = Y \rightarrow X \cap Y = \emptyset)$. (Ce concept a été abordé dans [l'exercice 5 de la section 3.6](#).) \mathcal{F} est dite une *partition* de A si elle possède les propriétés suivantes :

1. $\bigcup \mathcal{F} = A$.
2. \mathcal{F} est deux à deux disjoint.
3. $\forall x \in \mathcal{F} (X \neq \emptyset)$.

Par exemple, supposons que $A = \{1, 2, 3, 4\}$ et $\mathcal{F} = \{\{2\}, \{1, 3\}, \{4\}\}$. Alors $\bigcap \mathcal{F} = \{2\} \cup \{1, 3\} \cup \{4\} = \{1, 2, 3, 4\} = A$, donc \mathcal{F} satisfait la première clause de la définition de la partition. De plus, aucun

ensemble de \mathcal{F} n'a d'éléments en commun, donc \mathcal{F} est deux à deux disjoint, et clairement tous les ensembles de \mathcal{F} sont non vides. Ainsi, \mathcal{F} est une partition de A . D'autre part, la famille $\mathcal{G} = \{\{1, 2\}, \{1, 3\}, \{4\}\}$ n'est pas deux à deux disjointe, car $\{1, 2\} \cap \{1, 3\} = \{1\} \neq \emptyset$, donc ce n'est pas une partition de A . La famille $\mathcal{H} = \{\emptyset, \{2\}, \{1, 3\}, \{4\}\}$ n'est pas non plus une partition de A , car elle ne remplit pas la troisième exigence de la définition.

Définition 4.5.3. Supposons que R soit une relation d'équivalence sur un ensemble A , et $x \in A$. Alors la *classe d'équivalence de x en ce qui concerne R* est l'ensemble

$$[x]_R = \{y \in A \mid yRx\}.$$

Si R est clair d'après le contexte, alors nous écrivons simplement $[x]$ au lieu de $[x]_R$. L'ensemble de toutes les classes d'équivalence des éléments de A est appelé *A modulo R*, et est noté A/R . Ainsi,

$$A/R = \{[x]_R \mid x \in A\} = \{X \subseteq A \mid \exists x \in A (X = [x]_R)\}.$$

Dans le cas d'une relation de même anniversaire B , si p est une personne quelconque, alors selon la [définition 4.5.3](#),

$$\begin{aligned}[p]_B &= \{q \in P \mid qBp\} \\ &= \{q \in P \mid \text{the person } q \text{ has the same birthday as the person } p\}.\end{aligned}$$

Par exemple, si John est né le 10 août, alors

$$\begin{aligned}[\text{John}]_B &= \{q \in P \mid \text{the person } q \text{ has the same birthday as John}\} \\ &= \{q \in P \mid \text{the person } q \text{ was born on August 10}\}.\end{aligned}$$

Dans la notation introduite précédemment, il s'agit simplement de l'ensemble P_d , pour $d = 10$ août. En fait, il est maintenant clair que pour toute personne p , si l'on considère d comme la date de naissance de p , alors $[p]_B = P_d$. Ceci est en accord avec notre affirmation précédente selon laquelle les ensembles P_d sont les classes d'équivalence pour la relation d'équivalence B . Selon [la définition 4.5.3](#), l'ensemble de toutes ces classes d'équivalence est appelé *P modulo B*:

$$P/B = \{[p]_B \mid p \in P\} = \{P_d \mid d \in D\}.$$

On vous demande de donner une preuve plus précise de cette équation dans [l'exercice 6](#). Comme nous l'avons observé précédemment, cette famille est une partition de P .

Prenons un autre exemple. Soit S la relation sur \mathbb{R} définie comme suit :

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{Z}\}.$$

Français Par exemple, $(5,73, 2,73) \in S$ et $(-1,27, 2,73) \in S$, puisque $5,73 - 2,73 = 3 \in \mathbb{Z}$ et $-1,27 - 2,73 = -4 \in \mathbb{Z}$, mais $(1,27, 2,73) \notin S$, puisque $1,27 - 2,73 = -1,46 \notin \mathbb{Z}$. Clairement pour tout $x \in \mathbb{R}$, $x - x = 0 \in \mathbb{Z}$, donc $(x, x) \in S$, et donc S est réflexif. Pour voir que S est symétrique, supposons $(x, y) \in S$. Français Par la définition de S , cela signifie que $x - y \in \mathbb{Z}$. Mais alors $y - x = -(x - y) \in \mathbb{Z}$ aussi, puisque le négatif de tout entier est aussi un entier, donc $(y, x) \in S$. Puisque (x, y) était un élément arbitraire de S , cela montre que S est symétrique. Enfin, pour voir que S est transitif, supposons que $(x, y) \in S$ et $(y, z) \in S$. Alors $x - y \in \mathbb{Z}$ et $y - z \in \mathbb{Z}$. Puisque la somme de deux entiers est un entier, il s'ensuit que $x - z = (x - y) + (y - z) \in \mathbb{Z}$, donc $(x, z) \in S$, comme requis. Ainsi, S est une relation d'équivalence sur \mathbb{R} .

À quoi ressemblent les classes d'équivalence pour cette relation d'équivalence ? Nous avons déjà observé que $(5,73, 2,73) \in S$ et $(-1,27, 2,73) \in S$, donc $5,73 \in [2,73]$ et $-1,27 \in [2,73]$. En fait, il est facile de voir quels seront les autres éléments de cette classe d'équivalence :

$$[2,73] = \{ \dots, -1,27, -0,27, 0,73, 1,73, 2,73, 3,73, 4,73, 5,73, \dots \}.$$

Autrement dit, la classe d'équivalence contient tous les nombres réels positifs de la forme « $.\underline{73}$ » et tous les nombres réels négatifs de la forme « $-\underline{27}$ ». En général, pour tout nombre réel x , la classe d'équivalence de x contient tous les nombres réels qui diffèrent de x d'un nombre entier :

$$[x] = \{ \dots, x - 3, x - 2, x - 1, x, x + 1, x + 2, x + 3, \dots \}.$$

Voici quelques faits sur ces classes d'équivalence que vous pourriez essayer de vérifier par vous-même. Comme vous pouvez le constater dans la dernière équation, x est toujours un élément de $[x]$. Si nous choisissons un nombre $x \in [2,73]$, alors $[x]$ sera exactement égal à $[2,73]$. Par exemple, en prenant $x = 4,73$, nous trouvons que

$$[4,73] = \{ \dots, -1,27, -0,27, 0,73, 1,73, 2,73, 3,73, 4,73, 5,73, \dots \} = [2,73].$$

Ainsi, $[4,73]$ et $[2,73]$ ne sont que deux noms différents pour le même ensemble. Mais si l'on choisit $x \notin [2,73]$, alors $[x]$ sera différent de $[2,73]$. Par exemple,

$$[1,3] = \{ \dots, -1,7, -0,7, 0,3, 1,3, 2,3, 3,3, 4,3, \dots \}.$$

En fait, on peut voir à partir de ces équations que [1.3] et [2.73] n'ont aucun élément en commun. Autrement dit, [1.3] est en réalité *disjoint* de [2.73]. En général, pour deux nombres réels x et y , les classes d'équivalence $[x]$ et $[y]$ sont soit identiques, soit disjointes. Chaque classe d'équivalence possède de nombreux noms différents, mais différentes classes d'équivalence sont disjointes. Puisque $[x]$ contient toujours x comme élément, chaque classe d'équivalence est non vide et chaque nombre réel x appartient à une seule classe d'équivalence, à savoir $[x]$. Autrement dit, l'ensemble de toutes les classes d'équivalence, \mathbb{R}/S , est une partition de \mathbb{R} . Ceci illustre une fois de plus que les classes d'équivalence déterminées par une relation d'équivalence forment toujours une partition.

Théorème 4.5.4. *Supposer R est une relation d'équivalence sur un ensemble A . Alors A/R est une partition de A .*

La démonstration du [théorème 4.5.4](#) sera plus facile à comprendre si nous démontrons d'abord quelques faits concernant les classes d'équivalence. Les faits démontrés principalement dans le but de les utiliser pour démontrer un théorème sont généralement appelés *lemmes*.

Lemme 4.5.5. *Supposer R est une relation d'équivalence sur A . Alors :*

1. *Pour tout $x \in A$, $x \in [x]$.*
2. *Pour tout $x \in A$ et $y \in A$, $y \in [x]$ ssi $[y] = [x]$.*

Preuve.

1. Soit $x \in A$ arbitraire. Puisque R est réflexif, xRx . Par conséquent, par définition de classe d'équivalence, $x \in [x]$.
2. (\rightarrow) Supposons $y \in [x]$. Alors par définition de la classe d'équivalence, yRx . Supposons maintenant $z \in [y]$. Alors zRy . Puisque zRy et yRx , par transitivité de R nous pouvons conclure que zRx , donc $z \in [x]$. Puisque z est arbitraire, cela montre que $[y] \subseteq [x]$.

Supposons maintenant que $z \in [x]$, donc zRx . Nous connaissons déjà yRx , et comme R est symétrique nous pouvons conclure que xRy . En appliquant la transitivité à zRx et xRy , nous pouvons conclure que zRy , donc $z \in [y]$. Par conséquent $[x] \subseteq [y]$, donc $[x] = [y]$.

(\leftarrow) Supposons que $[y] = [x]$. Par la partie 1, nous savons que $y \in [y]$, donc puisque $[y] = [x]$, il s'ensuit que $y \in [x]$.

□

Commentaire.

1. Selon la définition des classes d'équivalence, $x \in [x]$ signifie xRx . Ceci nous amène à appliquer le fait que R est réflexif.
2. Bien sûr, la forme ssi du but nous conduit à prouver les deux directions séparément. Pour la direction \rightarrow , le but est $[y] = [x]$, et, comme $[y]$ et $[x]$ sont des ensembles, nous pouvons le prouver en prouvant que $[y] \subseteq [x]$ et $[x] \subseteq [y]$. Nous prouvons Chacune de ces affirmations est vérifiée par la méthode habituelle, qui consiste à prendre un élément arbitraire d'un ensemble et à prouver qu'il appartient à l'autre. Tout au long de la démonstration, nous utilisons à plusieurs reprises la définition des classes d'équivalence, comme nous l'avons fait pour la démonstration de l'affirmation 1.

Preuve du théorème 4.5.4. Pour prouver que A/R est une partition de A , nous devons prouver les trois propriétés de [la définition 4.5.2](#). Pour la première, nous devons montrer que $\bigcup(A/R) = A$, ou en d'autres termes que $\bigcup_{x \in A} [x] = A$. Maintenant, chaque classe d'équivalence dans A/R est un sous-ensemble de A , il devrait donc être clair que leur union est aussi un sous-ensemble de A . Ainsi, $\bigcup(A/R) \subseteq A$, donc tout ce que nous devons montrer pour terminer la preuve est que $A \subseteq \bigcup(A/R)$. Pour prouver cela, supposons $x \in A$. Alors par [le lemme 4.5.5](#), $x \in [x]$, et bien sûr $[x] \in A/R$, donc $x \in \bigcup(A/R)$. Ainsi, $\bigcup(A/R) = A$.

Pour voir que A/R est deux à deux disjoint, supposons que X et Y soient deux éléments de A/R , et $X \cap Y \neq \emptyset$. Par définition de A/R , X et Y sont des classes d'équivalence, nous devons donc avoir $X = [x]$ et $Y = [y]$ pour certains $x, y \in A$. Puisque $X \cap Y \neq \emptyset$, nous pouvons choisir un z tel que $z \in X \cap Y = [x] \cap [y]$. Maintenant, d'après [le lemme 4.5.5](#), puisque $z \in [x]$ et $z \in [y]$, il s'ensuit que $[x] = [z] = [y]$. Ainsi, $X = Y$. Ceci montre que si $X \neq Y$ alors $X \cap Y = \emptyset$, donc A/R est deux à deux disjoint.

Enfin, pour la dernière clause de la définition de la partition, supposons $X \in A/R$. Comme précédemment, cela signifie que $X = [x]$ pour un certain $x \in A$. Maintenant, par [le lemme 4.5.5](#), $x \in [x] = X$, donc $X \neq \emptyset$, comme requis.

□

Commentaire. Nous avons donné une raison intuitive pour laquelle $\bigcup(A/R) \subseteq A$, mais si vous n'êtes pas sûr de la raison pour laquelle cela est correct, vous devriez écrire une preuve formelle. (Vous pouvez également consulter [l'exercice 16 de la section 3.3](#).) La preuve que $A \subseteq \bigcup(A/R)$ est simple.

La définition de deux à deux disjoint suggère que pour prouver que A/R est deux à deux disjoint, nous devrions poser X et Y comme des éléments arbitraires de A/R , puis prouver que $X \neq Y \rightarrow X \cap Y = \emptyset$. Rappelons que l'affirmation selon laquelle un ensemble est vide est en

réalité une affirmation négative, donc l'antécédent et le conséquent de cette condition sont tous deux négatifs. Cela suggère qu'il sera probablement plus facile de prouver la contraposée, nous supposons donc $X \cap Y \neq \emptyset$ et prouvons $X = Y$. Les données $X \in A/R$, $Y \in A/R$ et $X \cap Y \neq \emptyset$ sont toutes des affirmations existentielles, nous les utilisons donc pour introduire les variables x , y et z . Le lemme 4.5.5 s'occupe maintenant de la preuve que $X = Y$ ainsi que de la preuve de la clause finale dans la définition de la partition.

Le théorème 4.5.4 montre que si R est une relation d'équivalence sur A alors A/R est une partition de A . En fait, il s'avère que *chaque* partition de A apparaît de cette manière.

Théorème 4.5.6. *Supposer UN est un ensemble et \mathcal{F} est une partition de A. Ensuite, il y a un relation d'équivalence R sur A telle que $A/R = \mathcal{F}$.*

Avant de démontrer ce théorème, il peut être utile d'aborder brièvement la stratégie de démonstration. La conclusion du théorème étant une affirmation existentielle, nous devrions chercher à trouver une relation d'équivalence R telle que $A/R = \mathcal{F}$. Il est clair que pour différents choix de $\mathcal{F} \Leftrightarrow$ nous devrons choisir R différemment ; la définition de R devrait donc dépendre de \mathcal{F} d'une manière ou d'une autre. L'exemple des personnes ayant le même anniversaire, présenté au début de cette section, peut vous aider à comprendre comment procéder. Rappelons que dans cet exemple, la relation d'équivalence B était constituée de toutes les paires de personnes (p, q) telles que p et q étaient dans le même ensemble dans la partition $\{P_d \mid d \in D\}$. En fait, nous avons constaté que nous pouvions également exprimer cela en disant que $B = \bigcup_{d \in D} (P_d \times P_d)$. Cela suggère que dans la preuve du théorème 4.5.6, nous devrions laisser R être l'ensemble de toutes les paires $(x, y) \in A \times A$ telles que x et y sont dans le même ensemble dans la partition \mathcal{F} . Une autre façon d'écrire cela serait $R = \bigcup_{X \in \mathcal{F}} (X \times X)$.

Par exemple, reprenons l'exemple d'une partition donnée après la définition 4.5.2. Dans cet exemple, nous avions $A = \{1, 2, 3, 4\}$ et $\mathcal{F} = \{\{2\}, \{1, 3\}, \{4\}\}$. Définissons maintenant une relation R sur A comme suggéré au paragraphe précédent. Cela nous donne :

$$\begin{aligned} R &= \bigcup_{X \in \mathcal{F}} (X \times X) \\ &= (\{2\} \times \{2\}) \cup (\{1, 3\} \times \{1, 3\}) \cup (\{4\} \times \{4\}) \\ &= \{(2, 2)\} \cup \{(1, 1), (1, 3), (3, 1), (3, 3)\} \cup \{(4, 4)\} \\ &= \{(2, 2), (1, 1), (1, 3), (3, 1), (3, 3), (4, 4)\}. \end{aligned}$$

Le graphe orienté de cette relation est présenté dans [la figure 4.7](#). Nous allons vous permettre de vérifier que R est une relation d'équivalence et que les classes d'équivalence sont

$$[2] = \{2\}, [1] = [3] = \{1, 3\}, [4] = \{4\}.$$

Ainsi, l'ensemble de toutes les classes d'équivalence est $A/R = \{\{2\}, \{1, 3\}, \{4\}\}$, ce qui est exactement le même que la partition \mathcal{F} avec laquelle nous avons commencé.

Bien entendu, le raisonnement qui nous a conduit à la formule $R = \bigcup_{X \in \mathcal{F}} (X \times X)$ ne fera pas partie de la preuve du [théorème 4.5.6](#). Lors de la rédaction de la preuve, nous pouvons simplement définir R de cette manière, puis vérifier qu'il s'agit d'une relation d'équivalence sur A et que $A/R = \mathcal{F}$. La démonstration pourrait être plus facile à suivre si nous démontrons d'abord quelques lemmes.

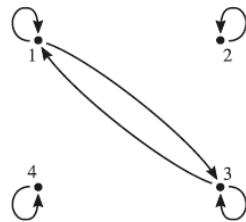


Figure 4.7.

Lemme 4.5.7. Supposer A est un ensemble et \mathcal{F} est une partition de A . Soit $R = \bigcup_{X \in \mathcal{F}} (X \times X)$. Alors R est une relation d'équivalence sur A . Nous appellerons R la relation d'équivalence déterminée par \mathcal{F} .

Preuve . Nous allons prouver que R est réflexif et vous laissons le reste à faire dans [l'exercice 8](#). Soit x un élément arbitraire de A . Puisque \mathcal{F} est une partition de A , $\bigcup \mathcal{F} = A$, donc $x \in \bigcup \mathcal{F}$. Ainsi, nous pouvons choisir un $X \in \mathcal{F}$ tel que $x \in X$. Mais alors $(x, x) \in X \times X$, donc $(x, x) \in \bigcup_{X \in \mathcal{F}} (X \times X) = R$. Par conséquent, R est réflexif.

□

Commentaire . Après avoir posé x comme élément arbitraire de A , nous devons prouver que $(x, x) \in R$. Puisque $R = \bigcup_{X \in \mathcal{F}} (X \times X)$, cela signifie que nous devons prouver $\exists X \in \mathcal{F} ((x, x) \in X \times X)$, ou en d'autres termes $\exists X \in \mathcal{F} (x \in X)$. Mais cela signifie simplement que $x \in \bigcup \mathcal{F}$, cela

suggère donc d'utiliser la première clause de la définition de la partition, qui dit que $\bigcup \mathcal{F} = A$.

Lemme 4.5.8. *Supposer UN est un ensemble et \mathcal{F} est une partition de A . Soit R être la Relation d'équivalence déterminée par \mathcal{F} . Supposons $X \in \mathcal{F}$ et $x \in X$. Alors $[x]_R = X$.*

Preuve. Supposons $y \in [x]_R$. Alors $(y, x) \in R$, donc par définition de R il doit y avoir un $Y \in \mathcal{F}$ tel que $(y, x) \in Y \times Y$, et donc $y \in Y$ et $x \in Y$. Puisque $x \in X$ et $x \in Y$, $X \cap Y \neq \emptyset$, et puisque \mathcal{F} est deux à deux disjoint, il s'ensuit que $X = Y$. Ainsi, puisque $y \in Y, y \in X$. Puisque y est un élément arbitraire de $[x]_R$, nous pouvons conclure que $[x]_R \subseteq X$.

Supposons maintenant $y \in X$. Alors $(y, x) \in X \times X$, donc $(y, x) \in R$ et donc $y \in [x]_R$. Ainsi $X \subseteq [x]_R$, donc $[x]_R = X$.

□

Commentaire. Pour prouver que $[x]_R = X$, nous prouvons que $[x]_R \subseteq X$ et que $X \subseteq [x]_R$. Pour le premier, nous commençons avec un $y \in [x]_R$ arbitraire et prouvons que $y \in X$. En écrivant la définition de $[x]_R$, nous obtenons $(y, x) \in R$, et comme R a été défini comme étant $\bigcup_{Y \in \mathcal{F}} (Y \times Y)$, cela signifie $\exists \exists Y \in \mathcal{F} ((y, x) \in Y \times Y)$. Bien sûr, puisqu'il s'agit d'une déclaration existentielle, nous introduisons immédiatement la nouvelle variable Y par instanciation existentielle. Puisque cela nous donne $y \in Y$ et que notre objectif est $y \in X$, il n'est pas surprenant que la preuve soit complétée en prouvant que $Y = X$.

La preuve que $X \subseteq [x]_R$ utilise également les définitions de $[x]_R$ et R , mais est plus simple.

Preuve du théorème 4.5.6. Soit $R = \bigcup_{X \in \mathcal{F}} (X \times X)$. Nous avons déjà vu que R est une relation d'équivalence, il suffit donc de vérifier que $A/R = \mathcal{F}$. Pour le voir, supposons $X \in A/R$. Cela signifie que $X = [x]$ pour un certain $x \in A$. Puisque \mathcal{F} est une partition, nous savons que $\bigcup \mathcal{F} = A$, donc $x \in \bigcup \mathcal{F}$ et donc nous pouvons choisir un certain $Y \in \mathcal{F}$ tel que $x \in Y$. Mais alors, d'après le lemme 4.6.8, $[x] = Y$. Ainsi $X = Y \in \mathcal{F}$, donc $A/R \subseteq \mathcal{F}$.

Supposons maintenant que $X \in \mathcal{F}$. Alors, puisque \mathcal{F} est une partition, $X \neq \emptyset$, nous pouvons donc choisir un $x \in X$. Par conséquent, d'après le lemme 4.6.8, $X = [x] \in A/R$, donc $\mathcal{F} \subseteq A/R$. Ainsi, $A/R = \mathcal{F}$.

□

Commentaire. Nous prouvons que $A/R = \mathcal{F}$ en prouvant que $A/R \subseteq \mathcal{F}$ et $\mathcal{F} \subseteq A/R$. Pour le premier, nous prenons un $X \in A/R$ arbitraire et prouvons que $X \in \mathcal{F}$. Puisque $X \in A/R$ signifie $\exists x \in A (X = [x])$, nous introduisons immédiatement la nouvelle variable x pour représenter un élément de A tel que $X = [x]$. La preuve que $x \in \mathcal{F}$ procède maintenant par la voie légèrement détournée de trouver un ensemble $Y \in \mathcal{F}$ tel que $X = Y$. Ceci est motivé par [le lemme 4.5.8](#), qui suggère une manière de montrer qu'un élément de \mathcal{F} est égal à $[x] = X$. La preuve que $\mathcal{F} \subseteq A/R$ repose également sur [le lemme 4.5.8](#).

Nous avons vu comment une relation d'équivalence R sur un ensemble A peut être utilisée pour définir une partition A/R de A et aussi comment une partition \mathcal{F} de A peut être utilisée pour définir une relation d'équivalence $\bigcup_{X \in \mathcal{F}} (X \times X)$ sur A . La preuve du [théorème 4.5.6](#) démontre une relation intéressante entre ces opérations. Si vous commencez avec une partition \mathcal{F} de A , utilisez \mathcal{F} pour définir la relation d'équivalence $R = \bigcup_{X \in \mathcal{F}} (X \times X)$, puis utilisez R pour définir une partition A/R , vous revenez alors à votre point de départ. En d'autres termes, la partition finale A/R est la même que la partition originale \mathcal{F} . Vous pourriez vous demander si la même idée fonctionnerait dans l'autre ordre. En d'autres termes, supposons que vous commenciez avec une relation d'équivalence R sur A , utilisez R pour définir une partition $\mathcal{F} = A/R$, puis utilisez \mathcal{F} pour définir une relation d'équivalence $S = \bigcup_{X \in \mathcal{F}} (X \times X)$. La relation d'équivalence finale S serait-elle identique à la relation d'équivalence initiale R ? [L'exercice 10](#) vous demande de démontrer que la réponse est oui.

Nous terminons cette section en examinant quelques exemples supplémentaires de relations d'équivalence. La définition suivante donne une famille de relations d'équivalence très utile.

Définition 4.5.9. Supposons que m soit un entier positif. Pour tout entier x et y , on dira que x est *congru à et modulo* m si $\exists k \in \mathbb{Z} (x - y = km)$. En d'autres termes, x est congru à y modulo m ssi $m | (x - y)$.

Nous utiliserons la notation $x \equiv y \pmod{m}$ pour signifier que x est congru à y modulo m .

Par exemple, $12 \equiv 27 \pmod{5}$, car $12 - 27 = -15 = (-3) \cdot 5$. Maintenant, pour tout entier positif m , nous pouvons considérer la relation $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod{m}\}$. Comme nous l'avons mentionné dans la section précédente, les mathématiciens utilisent parfois des symboles plutôt que des lettres pour nommer les relations. Dans ce cas, motivés par la notation de [la définition 4.5.9](#), nous utiliserons le symbole \equiv_m comme nom pour cette relation. Ainsi, pour tout entier x et y , $x \equiv_m y$ signifie la même chose que $x \equiv y \pmod{m}$. Il s'avère que cette relation est un autre exemple de relation d'équivalence.

Théorème 4.5.10. *Pour chaque entier positif m , \equiv_m est une relation d'équivalence sur \mathbb{Z} .*

Preuve. Nous vérifierons la transitivité pour \equiv_m et vous laisserons vérifier la réflexivité et la symétrie dans [l'exercice 11](#). Pour voir que \equiv_m est transitif, supposons que $x \equiv_m y$ et $y \equiv_m z$. Cela signifie que $x \equiv y \pmod{m}$ et $y \equiv z \pmod{m}$, ou en d'autres termes $m \mid (x - y)$ et $m \mid (y - z)$. Par conséquent, d'après [l'exercice 18\(a\)](#) de [la section 3.3](#), $m \mid [(x - y) + (y - z)]$. Mais $(x - y) + (y - z) = x - z$, il s'ensuit donc que $m \mid (x - z)$, et donc $x \equiv_m z$.

□

Nous reviendrons davantage sur ces relations d'équivalence plus loin dans ce livre, notamment au [chapitre 7](#).

Les relations d'équivalence apparaissent souvent lorsqu'on souhaite regrouper des éléments d'un ensemble ayant un point commun. Par exemple, si vous avez étudié les vecteurs dans un précédent cours de mathématiques ou de physique, on vous a peut-être expliqué que les vecteurs peuvent être considérés comme des flèches. Mais on vous a probablement aussi expliqué que des flèches différentes pointant dans la même direction et de même longueur doivent être considérées comme représentant le même vecteur. Voici une explication plus claire de la relation entre vecteurs et flèches. Soit A l'ensemble de toutes les flèches, et soit $R = \{(x, y) \in A \times A \mid \text{les flèches } x \text{ et } y \text{ pointent dans la même direction et ont la même longueur}\}$. Nous vous laissons vérifier par vous-même que R est une relation d'équivalence sur A . Chaque classe d'équivalence est constituée de flèches de même longueur et pointant dans la même direction. Nous pouvons maintenant

considérer les vecteurs comme étant représentés, non pas par des flèches, mais par des classes d'équivalence de flèches.

Les étudiants familiarisés avec la programmation informatique pourraient être intéressés par notre prochain exemple. Supposons que P soit l'ensemble de tous les programmes informatiques, et que pour tout programme p et q , nous disions que p et q sont *équivalents* s'ils produisent toujours le même résultat avec la même entrée. Soit $R = \{(p, q) \in P \times P \mid \text{les programmes } p \text{ et } q \text{ sont équivalents}\}$. Il est facile de vérifier que R est une relation d'équivalence sur P . Les classes d'équivalence regroupent les programmes qui produisent le même résultat avec la même entrée.

Exercices

- *1. Trouvez toutes les partitions de l'ensemble $A = \{1, 2, 3\}$.
2. Trouvez toutes les relations d'équivalence sur l'ensemble $A = \{1, 2, 3\}$.
- *3. Soit W = l'ensemble de tous les mots de la langue anglaise. Parmi les relations suivantes sur W , *lesquelles* sont des relations d'équivalence ? Pour celles qui sont des relations d'équivalence, quelles sont les classes d'équivalence ?
 - (a) $R = \{(x, y) \in W \times W \mid \text{les mots } x \text{ et } y \text{ commencent par la même lettre}\}$.
 - (b) $S = \{(x, y) \in W \times W \mid \text{les mots } x \text{ et } y \text{ ont au moins une lettre en commun}\}$.
 - (c) $T = \{(x, y) \in W \times W \mid \text{les mots } x \text{ et } y \text{ ont le même nombre de lettres}\}$.
4. Parmi les relations suivantes sur $\mathbb{R} \setminus \{0\}$ sont des relations d'équivalence ? Pour celles qui sont des relations d'équivalence, quelles sont les classes d'équivalence ?
 - (a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{N}\}$.
 - (b) $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{Q}\}$.
 - (c) $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \exists n \in \mathbb{Z} (y = x \cdot 10^n)\}$.
5. Soit L l'ensemble de toutes les droites non verticales du plan. Parmi les relations suivantes sur L , *lesquelles* sont des relations d'équivalence ? Pour celles qui sont des relations d'équivalence, quelles sont les classes d'équivalence ?
 - (a) $R = \{(k, l) \in L \times L \mid \text{les droites } k \text{ et } l \text{ ont la même pente}\}$.
 - (b) $S = \{(k, l) \in L \times L \mid \text{les lignes } k \text{ et } l \text{ sont perpendiculaires}\}$.
 - (c) $T = \{(k, l) \in L \times L \mid k \cap x = l \cap x \text{ et } k \cap y = l \cap y\}$, où x et y sont les axes x et y . (Nous traitons ici les lignes comme des ensembles de points.)

- *6. Dans la discussion de la relation d'équivalence de même anniversaire B suivant [la définition 4.5.3](#), nous avons affirmé que $P/B = \{P_d \mid d \in D\}$. Donnez un Preuve précise de cette affirmation. En élaborant la preuve, vous constaterez qu'il faut faire une hypothèse sur les anniversaires des personnes (une hypothèse très raisonnable) pour que la preuve soit valide. Quelle est cette hypothèse ?
7. Soit T l'ensemble de tous les triangles, et soit $S = \{(s, t) \in T \times T \mid$ les triangles s et t sont semblables}. (Rappelons que deux triangles sont semblables si les angles de l'un sont égaux aux angles correspondants de l'autre.) Vérifiez que S est une relation d'équivalence.
8. Complétez la preuve du [lemme 4.5.7](#).
9. Supposons que R et S soient des relations d'équivalence sur A et que $A/R = A/S$. Démontrer que $R = S$.
- *10. Supposons que R soit une relation d'équivalence sur A . Soit $\mathcal{F} = A/R$, et soit S la relation d'équivalence déterminée par \mathcal{F} . Autrement dit, $S = \bigcup_{X \in \mathcal{F}} (X \times X)$. Démontrer que $S = R$.
11. Soit \equiv_m la relation « congruence modulo m » définie dans le texte, pour un entier positif m .
- (a) Complétez la preuve du [théorème 4.5.10](#) en montrant que \equiv_m est réflexif et symétrique.
- (b) Trouvez toutes les classes d'équivalence pour \equiv_2 et \equiv_3 . Combien y a-t-il de classes d'équivalence dans chaque cas ? En général, combien de classes d'équivalence pensez-vous qu'il y ait pour \equiv_m ?
12. Démontrer que pour tout entier n , soit $n^2 \equiv 0 \pmod{4}$, soit $n^2 \equiv 1 \pmod{4}$.
- *13. Supposons que m soit un entier positif. Démontrer que pour tous les entiers a, a', b et b' , si $a' \equiv a \pmod{m}$ et $b' \equiv b \pmod{m}$ alors $a' + b' \equiv a + b \pmod{m}$ et $ab \equiv a'b' \pmod{m}$.
14. Supposons que R soit une relation d'équivalence sur A et $B \subseteq A$. Soit $S = R \cap (B \times B)$.
- (a) Démontrer que S est une relation d'équivalence sur B .
- (b) Démontrer que pour tout $x \in B$, $[x]_S = [x]_R \cap B$.
15. Supposons que $B \subseteq A$ et définissons une relation R sur $\mathcal{P}(A)$ comme suit :

$$R = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid XY \subseteq B\}.$$

- (a) Démontrer que R est une relation d'équivalence sur $\mathcal{P}(A)$.
 (b) Démontrer que pour chaque $X \in \mathcal{P}(A)$ il existe exactement un $Y \in [X]_R$ tel que $Y \cap B = \emptyset$.

*16. Supposons que \mathcal{F} et \mathcal{G} sont des partitions de A , \mathcal{H} une partition de B et que A et B soient disjoints. Démontrer que $\mathcal{F} \cup \mathcal{G}$ est une partition de $A \cup B$.

17. Supposons que R soit une relation d'équivalence sur A , S soit une relation d'équivalence sur B , et A et B soient disjoints.

- (a) Démontrer que $R \cup S$ est une relation d'équivalence sur $A \cup B$.
 (b) Démontrer que pour tout $x \in A$, $[x]_{R \cup S} = [x]_R$, et pour tout $y \in B$, $[y]_{R \cup S} = [y]_S$.

(c) Démontrer que $(A \cup B)/(R \cup S) = (A/R) \cup (B/S)$.

18. Supposons que \mathcal{F} et \mathcal{G} soient des partitions d'un ensemble A . On définit une nouvelle famille d'ensembles $\mathcal{F} \cdot \mathcal{G}$ comme suit :

$$\mathcal{F} \cdot \mathcal{G} = \{Z \in \mathcal{P}(A) \mid Z \neq \emptyset \text{ et } \exists X \in \mathcal{F} \exists Y \in \mathcal{G} (Z = X \cap Y)\}.$$

Démontrer que $\mathcal{F} \cdot \mathcal{G}$ est une partition de A .

19. Soit $\mathcal{F} = \{\mathbb{R}^-, \mathbb{R}^+, \{0\}\}$ et $\mathcal{G} = \{\mathbb{Z}, \mathbb{R} \setminus \mathbb{Z}\}$, et notons que \mathcal{F} et \mathcal{G} sont des partitions de \mathbb{R} . Énumérez les éléments de $\mathcal{F} \cdot \mathcal{G}$. (Voir [l'exercice 18](#) pour la signification de la notation utilisée ici.)

*20. Supposons que R et S soient des relations d'équivalence sur un ensemble A . Soit $T = R \cap S$.

- (a) Démontrer que T est une relation d'équivalence sur A .
 (b) Démontrer que pour tout $x \in A$, $[x]_T = [x]_R \cap [x]_S$.
 (c) Démontrer que $A/T = (A/R) \cdot (A/S)$. (Voir [l'exercice 18](#) pour la signification de la notation utilisée ici.)

21. Supposons que \mathcal{F} soit une partition de A et que \mathcal{G} soit une partition de B . On définit une nouvelle famille d'ensembles $\mathcal{F} \otimes \mathcal{G}$ comme suit :

$$\mathcal{F} \otimes \mathcal{G} = \{Z \in \mathcal{P}(A \times B) \mid \exists X \in \mathcal{F} \exists Y \in \mathcal{G} (Z = X \times Y)\}.$$

Démontrer que $\mathcal{F} \otimes \mathcal{G}$ est une partition de $A \times B$.

*22. Soit $\mathcal{F} = \{\mathbb{R}^-, \mathbb{R}^+, \{0\}\}$, qui est une partition de \mathbb{R} . Lister les éléments de $\mathcal{F} \otimes \mathcal{F}$ et les décrire géométriquement comme des

sous-ensembles du plan xy . (Voir [l'exercice 21](#) pour la signification de la notation utilisée ici.)

23. Supposons que R soit une relation d'équivalence sur A et que S soit une relation d'équivalence sur B . Définissons une relation T sur $A \times B$ comme suit :

$$T = \{((a, b), (a', b')) \in (A \times B) \times (A \times B) \mid aRa' \text{ et } bSb'\}.$$

- (a) Démontrer que T est une relation d'équivalence sur $A \times B$.
 - (b) Démontrer que si $a \in A$ et $b \in B$ alors $[(a, b)]_T = [a]_R \times [b]_S$.
 - (c) Démontrer que $(A \times B)/T = (A/R) \otimes (B/S)$. (Voir [l'exercice 21](#) pour la signification de la notation utilisée ici.)
- *24. Supposons que R et S soient des relations sur un ensemble A , et que S soit une relation d'équivalence. On dira que R est *compatible* avec S si, pour tout x, y, x' et y' dans A , si xSx' et ySy' alors xRy ssi $x'Ry'$.
- (a) Démontrer que si R est compatible avec S , alors il existe une relation unique T sur A/S telle que pour tout x et y dans A , $[x]_S T [y]_S$ ssi xRy .
 - (b) Supposons que T soit une relation sur A/S et pour tout x et y dans A , $[x]_S T [y]_S$ ssi xRy . Démontrer que R est compatible avec S .
25. Supposons que R soit une relation sur A et que R soit réflexive et transitive. (Une telle relation est appelée un *préordre* sur A .) Soit $S = R \cap R^{-1}$.
- (a) Démontrer que S est une relation d'équivalence sur A .
 - (b) Démontrer qu'il existe une relation unique T sur A/S telle que pour tout x et y dans A , $[x]_S T [y]_S$ iff xRy . (Indice : utilisez [l'exercice 24](#).)
 - (c) Démontrer que T est un ordre partiel sur A/S , où T est la relation de la partie (b).
26. Soit $I = \{1, 2, \dots, 100\}$, $A = \mathcal{P}(I)$, et $R = \{(X, Y) \in A \times A \mid Y \text{ a au moins autant d'éléments que } X\}$.
- (a) Démontrer que R est un préordre sur A . (Voir [l'exercice 25](#) pour la définition du *préordre*.)
 - (b) Soient S et T définis comme dans [l'exercice 25](#). Décrivez les éléments de A/S et l'ordre partiel T . Combien d'éléments possède A/S ? T est-il un ordre total?
27. Supposons que A soit un ensemble. Si \mathcal{F} et \mathcal{G} sont des partitions de A , alors on dira que \mathcal{F} raffine \mathcal{G} si $\forall X \in \mathcal{F} \exists Y \in \mathcal{G} (X \subseteq Y)$. Soit P

l'ensemble de toutes les partitions de A , et soit $R = \{(\mathcal{F}, \mathcal{G}) \in P \times P \mid \mathcal{F}$ raffine $\mathcal{G}\}$.

- (a) Démontrer que R est un ordre partiel sur P .
- (b) Supposons que S et T soient des relations d'équivalence sur A . Soient $\mathcal{F} = A/S$ et $\mathcal{G} = A/T$. Démontrer que $S \subseteq T$ ssi \mathcal{F} raffine \mathcal{G} .
- (c) Supposons que \mathcal{F} et \mathcal{G} soient des partitions de A . Démontrer que $\mathcal{F} \cdot \mathcal{G}$ est la plus grande borne inférieure de l'ensemble $\{\mathcal{F}, \mathcal{G}\}$ dans l'ordre partiel R . (Voir [l'exercice 18](#) pour la signification de la notation utilisée ici.)

5

Fonctions

5.1 Fonctions

Supposons que P soit l'ensemble de toutes les personnes, et soit $H = \{(p, n) \in P \times \mathbb{N} \mid \text{la personne } p \text{ a } n \text{ enfants}\}$. Alors H est une relation de P vers \mathbb{N} , et elle possède la propriété importante suivante : pour tout $p \in P$, il existe *exactement un* $n \in \mathbb{N}$ tel que $(p, n) \in H$. Les mathématiciens expriment cela en disant que H est une *fonction* de P vers \mathbb{N} .

Définition 5.1.1. Supposons que F soit une relation de A vers B . Alors F est dite *fonction de A vers B* si pour tout $a \in A$ il existe exactement un $b \in B$ tel que $(a, b) \in F$. Autrement dit, dire que F est une fonction de A vers B signifie :

$$\forall a \in A \exists! b \in B ((a, b) \in F).$$

Pour indiquer que F est une fonction de A vers B , nous écrirons $F : A \rightarrow B$.

Exemple 5.1.2.

1. Soit $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ et $F = \{(1, 5), (2, 4), (3, 5)\}$. F est-elle une fonction de A vers B ?
2. Soit $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ et $G = \{(1, 5), (2, 4), (1, 6)\}$. G est-elle une fonction de A vers B ?
3. Soit C l'ensemble des villes et N l'ensemble des pays, et soit $L = \{(c, n) \in C \times N \mid \text{la ville } c \text{ est dans le pays } n\}$. L est-elle une fonction de C dans N ?
4. Soit P l'ensemble de toutes les personnes, et soit $C = \{(p, q) \in P \times P \mid \text{la personne } p \text{ est un parent de la personne } q\}$. C est-elle une fonction de P dans P ?
5. Soit P l'ensemble de toutes les personnes, et soit $D = \{(p, x) \in P \times \mathcal{P}(P) \mid x = \text{l'ensemble de tous les enfants de } p\}$. D est-elle une

fonction de P dans $\mathcal{P}(P)$?

6. Soit A un ensemble quelconque. Rappelons que $i_A = \{(a, a) \mid a \in A\}$ est appelée la relation d'identité sur A . Est-ce une fonction de A vers A ?
7. Soit $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$. Est-ce que f est une fonction de \mathbb{R} dans \mathbb{R} ?

Solutions

1. Oui. Notez que 1 est apparié à 5 dans la relation F , mais qu'il n'est apparié à aucun autre élément de B . De même, 2 n'est apparié qu'à 4 et 3 à 5. Autrement dit, chaque élément de A apparaît comme la première coordonnée d'une seule paire ordonnée dans F . Par conséquent, F est une fonction de A vers B . Notez que la définition d'une fonction n'exige pas que chaque élément de B soit apparié à un seul élément de A . Ainsi, peu importe que 5 apparaisse comme la seconde coordonnée de deux paires différentes dans F et que 6 n'apparaisse dans aucune paire ordonnée.
2. Non. G n'est pas une fonction de A vers B pour deux raisons. Premièrement, 3 n'est associé à aucun élément de B dans la relation G , ce qui contrevient à l'exigence selon laquelle tout élément de A doit être associé à un élément de B . Deuxièmement, 1 est associé à deux éléments différents de B , 5 et 6, ce qui contrevient à l'exigence selon laquelle chaque élément de A doit être associé à un seul élément de B .
3. Si nous faisons l'hypothèse raisonnable que chaque ville se trouve dans exactement un pays, alors L est une fonction de C à N .
4. Parce que certaines personnes n'ont pas d'enfants et que certaines personnes en ont plus d'un, C n'est pas une fonction de P vers P .
5. Oui, D est une fonction de P dans $\mathcal{P}(P)$. Chaque personne p est appariée à un seul ensemble $x \subseteq P$, à savoir l'ensemble de tous les enfants de p . Notons que dans la relation D , une personne p est appariée à l'ensemble constitué de tous les enfants de p , et non à ces enfants eux-mêmes. Même si p n'a pas exactement un enfant, il n'en reste pas moins vrai qu'il existe un seul ensemble contenant précisément les enfants de p et rien d'autre.
6. Oui. Chaque $a \in A$ est apparié dans la relation i_A à un seul élément de A , à savoir a lui-même. Autrement dit, $(a, a) \in i_A$, mais pour tout $a' \neq a$, $(a, a') \notin i_A$. Ainsi, on peut appeler i_A la fonction identité sur A .

7. Oui. Pour chaque nombre réel x , il existe exactement une valeur de y , à savoir $y = x^2$, telle que $(x, y) \in f$.

Supposons $f : A \rightarrow B$. Si $a \in A$, alors nous savons qu'il existe exactement un $b \in B$ tel que $(a, b) \in f$. Cet unique b est appelé « valeur de f en a », ou « image de a par f », ou « résultat de l'application f à a », ou simplement « f de a », et s'écrit $f(a)$. Autrement dit, pour tout $a \in A$ et tout $b \in B$, $b = f(a)$ si et seulement si $(a, b) \in f$. Par exemple, pour la fonction $F = \{(1, 5), (2, 4), (3, 5)\}$ dans la partie 1 de [l'exemple 5.1.2](#), nous pourrions dire que $F(1) = 5$, puisque $(1, 5) \in F$. De même, $F(2) = 4$ et $F(3) = 5$. Si L est la fonction dans la partie 3 et c est une ville quelconque, alors $L(c)$ serait l'unique pays n tel que $(c, n) \in L$. En d'autres termes, $L(c)$ = le pays dans lequel c est situé. Par exemple, $L(\text{Paris}) = \text{France}$. Pour la fonction D dans la partie 5, nous pourrions dire que pour toute personne p , $D(p)$ = l'ensemble de tous les enfants de p . Si A est un ensemble quelconque et $a \in A$, alors $(a, a) \in i_A$, donc $i_A(a) = a$. Et si f est la fonction de la partie 7, alors pour tout nombre réel x , $f(x) = x^2$.

Une fonction f d'un ensemble A vers un autre ensemble B est souvent spécifiée en donnant une règle permettant de déterminer $f(a)$ pour tout $a \in A$. Par exemple, si A est l'ensemble de toutes les personnes et $B = \mathbb{R}^+$, alors on pourrait définir une fonction f de A vers B par la règle selon laquelle, pour tout $a \in A$, $f(a)$ = la taille de a en pouces. Bien que cette définition ne précise pas explicitement quels couples ordonnés sont des éléments de f , on peut le déterminer en utilisant notre règle selon laquelle, pour tout $a \in A$ et $b \in B$, $(a, b) \in f$ si et seulement si $b = f(a)$. Ainsi,

$$\begin{aligned} f &= \{(a, b) \in A \times B \mid b = f(a)\} \\ &= \{(a, b) \in A \times B \mid b = a's \text{ height in inches}\}. \end{aligned}$$

Par exemple, si Joe Smith mesure 68 pouces, alors $(\text{Joe Smith}, 68) \in f$ et $f(\text{Joe Smith}) = 68$.

Il est souvent utile de considérer une fonction f de A vers B comme représentant une règle associant, à chaque $a \in A$, un objet correspondant $b = f(a) \in B$. Cependant, il est important de se rappeler que, bien qu'une fonction puisse être définie en donnant une telle règle, elle n'a pas besoin d'être définie de cette manière. Tout sous-ensemble de $A \times B$ qui satisfait aux exigences de [la définition 5.1.1](#) est une fonction de A vers B .

Exemple 5.1.3. Voici d'autres exemples de fonctions définies par des règles.

1. Supposons que chaque étudiant se voit attribuer un conseiller pédagogique qui est un professeur. Soit S l'ensemble des étudiants et P l'ensemble des professeurs. On peut alors définir une fonction f de S vers P selon la règle selon laquelle, pour tout étudiant s , $f(s)$ = le conseiller pédagogique de s . Autrement dit,

$$\begin{aligned} f &= \{(s, p) \in S \times P \mid p = f(s)\} \\ &= \{(s, p) \in S \times P \mid \text{the professor } p \text{ is the academic advisor of} \\ &\quad \text{the student } s\}. \end{aligned}$$

2. Nous pouvons définir une fonction g de \mathbb{Z} vers \mathbb{R} par la règle selon laquelle pour tout $x \in \mathbb{Z}$, $g(x) = 2x + 3$. Alors

$$\begin{aligned} g &= \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = g(x)\} \\ &= \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = 2x + 3\} \\ &= \{\dots, (-2, -1), (-1, 1), (0, 3), (1, 5), (2, 7), \dots\}. \end{aligned}$$

3. Soit h la fonction de \mathbb{R} dans \mathbb{R} définie par la règle selon laquelle pour tout $x \in \mathbb{R}$, $h(x) = 2x + 3$. Notons que la formule de $h(x)$ est identique à celle de $g(x)$ dans la partie 2. Cependant, h et g ne sont pas la même fonction. On peut le constater en notant que, par exemple, $(\pi, 2\pi + 3) \in h$ mais $(\pi, 2\pi + 3) \notin g$, puisque $\pi \notin \mathbb{Z}$. (Pour plus d'informations sur la relation entre g et h , voir [l'exercice 7\(c\)](#).)

Notez que lorsqu'une fonction f de A à B est spécifiée en donnant une règle pour trouver $f(a)$, la règle doit déterminer la valeur de $f(a)$ pour *chaque* $a \in A$. Parfois, lorsque les mathématiciens énoncent une telle règle, ils ne précisent pas explicitement qu'elle s'applique à tout $a \in A$. Par exemple, un mathématicien pourrait dire « soit f la fonction de \mathbb{R} dans \mathbb{R} définie par la formule $f(x) = x^2 + 7$ ». Il est entendu dans ce cas que l'équation $f(x) = x^2 + 7$ s'applique à tout $x \in \mathbb{R}$ même si elle n'a pas été explicitement formulée. Cela signifie que vous pouvez remplacer x par *n'importe quel nombre réel* dans cette équation, et l'équation résultante sera vraie. Par exemple, vous pouvez conclure que $f(3) = 3^2 + 7 = 16$. De même, si w est un nombre réel, alors vous pouvez écrire $f(w) = w^2 + 7$, ou même $f(2w - 3) = (2w - 3)^2 + 7 = 4w^2 - 12w + 16$.

Puisqu'une fonction f de A vers B est entièrement déterminée par la règle de recherche de $f(a)$, deux fonctions définies par des règles équivalentes doivent être égales. Plus précisément, nous avons le théorème suivant :

Théorème 5.1.4. *Supposer f et g sont des fonctions de UN à B . Si $\forall a \in A$ ($f(a) = g(a)$), alors $f = g$.*

Preuve. Supposons que $\forall a \in A (f(a) = g(a))$, et soit (a, b) un élément arbitraire de f . Alors $b = f(a)$. Mais par notre hypothèse $f(a) = g(a)$, donc $b = g(a)$ et donc $(a, b) \in g$. Ainsi, $f \subseteq g$. Un argument similaire montre que $g \subseteq f$, donc $f = g$.

Commentaire. Puisque f et g sont des ensembles, nous prouvons $f = g$ en prouvant $f \subseteq g$ et $g \subseteq f$. Chacun de ces objectifs est prouvé en montrant qu'un élément arbitraire d'un ensemble doit être un élément de l'autre. Notons que, maintenant que nous avons prouvé [le théorème 5.1.4](#), nous disposons d'une autre méthode pour prouver que deux fonctions f et g d'un ensemble A vers un autre ensemble B sont égales. À l'avenir, pour prouver $f = g$, nous prouverons généralement $\forall a \in A (f(a) = g(a))$ puis appliquerons [le théorème 5.1.4](#).

Les fonctions étant des relations d'un type particulier, les concepts introduits au [chapitre 4](#) concernant les relations peuvent également leur être appliqués. Par exemple, supposons que $f : A \rightarrow B$. Alors f est une relation de A vers B ; il est donc logique de parler du domaine de définition de f , qui est un sous-ensemble de A , et de l'ensemble image de f , qui est un sous-ensemble de B . Selon la définition d'une fonction, chaque élément de A doit apparaître comme la première coordonnée d'un couple ordonné (en fait, un seul) dans f ; le domaine de définition de f doit donc être tout A . Mais l'ensemble image de f ne doit pas nécessairement être tout B . Les éléments de l'ensemble image de f seront les secondes coordonnées de tous les couples ordonnés de f , et la seconde coordonnée d'un couple ordonné de f est ce que nous avons appelé l'image de sa première coordonnée. Ainsi, l'ensemble image de f pourrait également être décrit comme l'ensemble de toutes les images des éléments de A par f :

$$\text{Ran}(f) = \{f(a) \mid a \in A\}.$$

Par exemple, pour la fonction f définie dans la partie 1 de [l'exemple 5.1.3](#), $\text{Ran}(f) = \{f(s) \mid s \in S\} =$ l'ensemble de tous les conseillers des étudiants.

Français Nous pouvons dessiner des diagrammes de fonctions exactement de la même manière que nous avons dessiné des diagrammes pour les relations au [chapitre 4](#). Si $f : A \rightarrow B$, alors comme précédemment, chaque paire ordonnée $(a, b) \in f$ serait représentée dans le diagramme par une arête reliant a à b . Par définition de fonction, chaque $a \in A$ apparaît comme la première coordonnée d'exactement une paire ordonnée dans f , et la deuxième coordonnée de cette paire ordonnée est $f(a)$. Ainsi, pour chaque $a \in A$ il y aura exactement une arête provenant de a , et elle reliera a à $f(a)$. Par exemple, [la figure 5.1 montre à quoi](#) ressemblerait le diagramme de la fonction L définie dans la partie 3 de [l'exemple 5.1.2](#).

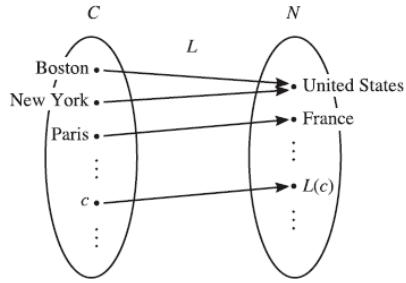


Figure 5.1.

La définition de la composition de relations s'applique également aux fonctions. Si $f: A \rightarrow B$ et $g: B \rightarrow C$, alors f est une relation de A vers B et g est une relation de B vers C , donc $g \circ f$ sera une relation de A vers C . En fait, il s'avère que $g \circ f$ est une fonction de A vers C , comme le montre le théorème suivant.

Théorème 5.1.5. Supposer $f: A \rightarrow B$ et $g: B \rightarrow C$. Alors $g \circ f: A \rightarrow C$, et pour tout $a \in A$, la valeur de $g \circ f$ en a est donnée par la formule $(g \circ f)(a) = g(f(a))$.

Travail à partir de zéro

Français Avant de prouver ce théorème, il peut être utile de discuter du travail de base pour la preuve. Selon la définition d'une fonction, pour montrer que $g \circ f: A \rightarrow C$ nous devons prouver que $\forall a \in A \exists! c \in C ((a, c) \in g \circ f)$, nous commencerons donc par poser a comme élément arbitraire de A , puis nous essaierons de prouver que $\exists! c \in C ((a, c) \in g \circ f)$. Comme nous l'avons vu dans [la section 3.6](#), nous pouvons prouver cette affirmation en prouvant séparément l'existence et l'unicité. Pour prouver l'existence, nous devrions essayer de trouver un $c \in C$ tel que $(a, c) \in g \circ f$. Pour l'unicité, nous devons supposer que $(a, c_1) \in g \circ f$ et $(a, c_2) \in g \circ f$, puis essayer de prouver que $c_1 = c_2$.

Preuve. Soit a un élément arbitraire de A . Il faut montrer qu'il existe un unique $c \in C$ tel que $(a, c) \in g \circ f$.

Existence : Soit $b = f(a) \in B$. Soit $c = g(b) \in C$. Alors $(a, b) \in f$ et $(b, c) \in g$, donc par définition de composition de relations, $(a, c) \in g \circ f$. Ainsi, $\exists c \in C ((a, c) \in g \circ f)$.

Unicité : Supposons que $(a, c_1) \in g \circ f$ et $(a, c_2) \in g \circ f$. Alors par définition de composition, on peut choisir $b_1 \in B$ tel que $(a, b_1) \in f$ et $(b_1, c_1) \in g$, et on peut aussi choisir $b_2 \in B$ tel que $(a, b_2) \in f$ et $(b_2, c_2) \in g$. Puisque f est une fonction, il ne peut y avoir qu'un seul $b \in B$ tel que $(a, b) \in f$. Ainsi, puisque (a, b_1) et (a, b_2) sont tous deux des éléments de f , il s'ensuit que $b_1 = b_2$. Mais en appliquant maintenant le

même raisonnement à g , puisque $(b_1, c_1) \in g$ et $(b_1, c_2) = (b_2, c_2) \in g$, il s'ensuit que $c_1 = c_2$, comme requis.

Ceci complète la preuve que $g \circ f$ est une fonction de A vers C . Enfin, pour dériver la formule de $(g \circ f)(a)$, notez que nous avons montré dans la moitié de la preuve que pour tout $a \in A$, si nous posons $b = f(a)$ et $c = g(b)$, alors $(a, c) \in g \circ f$. Ainsi,

$$(g \circ f)(a) = c = g(b) = g(f(a)).$$

Lorsque nous avons introduit pour la première fois l'idée de la composition de deux relations au [chapitre 4](#), nous avons souligné que la notation était quelque peu particulière et avons promis d'en expliquer la raison dans ce chapitre. Nous pouvons fournir maintenant cette explication. La notation utilisée pour la composition de relations est qu'elle conduit à la formule pratique $(g \circ f)(x) = g(f(x))$ dérivée du [théorème 5.1.5](#). Notez que, les fonctions étant des relations d'un type particulier, tout ce que nous avons démontré sur la composition de relations s'applique à la composition de fonctions. En particulier, d'après [le théorème 4.2.5](#), nous savons que la composition de fonctions est associative.

Exemple 5.1.6. Voici quelques exemples de compositions de fonctions.

- Soient C et N les ensembles de toutes les villes et de tous les pays, respectivement, et soit $L : C \rightarrow N$ la fonction définie dans la partie 3 de [l'exemple 5.1.2](#). Ainsi, pour toute ville c , $L(c)$ = le pays où c est située. Soit B l'ensemble de tous les bâtiments situés dans les villes, et définissons $F : B \rightarrow C$ par la formule $F(b)$ = la ville où se trouve le bâtiment b . Alors $L \circ F : B \rightarrow N$. Par exemple, $F(\text{Tour Eiffel}) = \text{Paris}$, donc, d'après la formule du [théorème 5.1.5](#),

$$\begin{aligned}(L \circ F)(\text{Eiffel Tower}) &= L(F(\text{Eiffel Tower})) \\ &= L(\text{Paris}) = \text{France}.\end{aligned}$$

En général, pour chaque bâtiment $b \in B$,

$$\begin{aligned}(L \circ F)(b) &= L(F(b)) = L(\text{the city in which } b \text{ is located}) \\ &= \text{the country in which } b \text{ is located.}\end{aligned}$$

Un diagramme de cette fonction est présenté dans [la Figure 5.2](#).

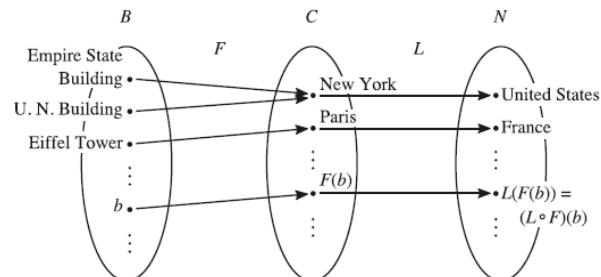


Figure 5.2.

2. Soit $g : \mathbb{Z} \rightarrow \mathbb{R}$ la fonction de la partie 2 de [l'exemple 5.1.3](#), définie par la formule $g(x) = 2x + 3$. Soit $f : \mathbb{Z} \rightarrow \mathbb{Z}$ définie par la formule $f(n) = n^2 - 3n + 1$. Alors $g \circ f : \mathbb{Z} \rightarrow \mathbb{R}$. Par exemple, $f(2) = 2^2 - 3 \cdot 2 + 1 = -1$, donc $(g \circ f)(2) = g(f(2)) = g(-1) = 1$. En général, pour tout $n \in \mathbb{Z}$,

$$\begin{aligned}(g \circ f)(n) &= g(f(n)) = g(n^2 - 3n + 1) = 2(n^2 - 3n + 1) + 3 \\ &= 2n^2 - 6n + 5.\end{aligned}$$

Exercices

- *1. (a) Soit $A = \{1, 2, 3\}$, $B = \{4\}$ et $f = \{(1, 4), (2, 4), (3, 4)\}$. f est-elle une fonction de A vers B ?
 (b) Soit $A = \{1\}$, $B = \{2, 3, 4\}$ et $f = \{(1, 2), (1, 3), (1, 4)\}$. f est-elle une fonction de A vers B ?
 (c) Soit C l'ensemble de toutes les voitures immatriculées dans votre état, et soit S l'ensemble de toutes les suites finies de lettres et de chiffres. Soit $L = \{(c, s) \in C \times S \mid \text{le numéro d'immatriculation de la voiture } c \text{ est } s\}$. L est-il une fonction de C vers S ?
 2. (a) Soit f la relation représentée par le graphique de [la figure 5.3](#). Est-ce que f est une fonction de A vers B ?

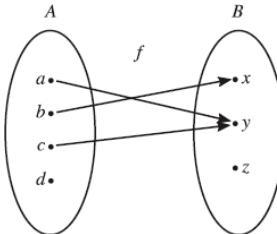


Figure 5.3.

- (b) Soit W l'ensemble de tous les mots de la langue anglaise, et soit A l'ensemble de toutes les lettres de l'alphabet. Soit $f = \{(w, a) \in W \times A \mid \text{la lettre } a \text{ apparaît dans le mot } w\}$, et soit $g = \{(w, a) \in W \times A \mid \text{la lettre } a \text{ est la première lettre du mot } w\}$. Est-ce que f est une fonction de W vers A ? Et g ?
 (c) John, Mary, Susan et Fred sortent dîner et s'assoient à une table ronde. Soit $P = \{\text{John, Mary, Susan, Fred}\}$, et soit $R = \{(p, q) \in P \times P \mid \text{la personne } p \text{ est assise immédiatement à droite de la personne } q\}$. R est-elle une fonction de P dans P ?
 *3. (a) Soit $A = \{a, b, c\}$, $B = \{a, b\}$, et $f = \{(a, b), (b, b), (c, a)\}$. Alors $f : A \rightarrow B$. Que sont $f(a)$, $f(b)$ et $f(c)$?

(b) Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ la fonction définie par la formule $f(x) = x^2 - 2x$. Quelle est $f(2)$?

(c) Soit $f = \{(x, n) \in \mathbb{R} \times \mathbb{Z} \mid n \leq x < n + 1\}$. Alors $f : \mathbb{R} \rightarrow \mathbb{Z}$. Qu'est-ce que $f(\pi)$? Qu'est-ce que $f(-\pi)$?

4. (a) Soit N l'ensemble des pays et C l'ensemble des villes. Soit $H : N \rightarrow C$ la fonction définie par la règle selon laquelle pour tout pays n , $H(n)$ = la capitale du pays n . Quelle est $H(\text{Italie})$?

(b) Soit $A = \{1, 2, 3\}$ et $B = \mathcal{P}(A)$. Soit $F : B \rightarrow B$ la fonction définie par la formule $F(X) = A \setminus X$. Quelle est $F(\{1, 3\})$?

(c) Soit $f : \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ la fonction définie par la formule $f(x) = (x+1, x-1)$. Quelle est $f(2)$?

*5. Soit L la fonction définie dans la partie 3 de [l'exemple 5.1.2](#) et soit H la fonction définie dans [l'exercice 4\(a\)](#). Décrire $L \circ H$ et $H \circ L$.

6. Soient f et g des fonctions de \mathbb{R} dans \mathbb{R} définies par les formules suivantes :

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

Trouvez les formules pour $(f \circ g)(x)$ et $(g \circ f)(x)$.

*7. Supposons que $f : A \rightarrow B$ et $C \subseteq A$. L'ensemble $f \cap (C \times B)$, qui est une relation de C vers B , est appelé la *restriction* de f à C , et est parfois noté $f \upharpoonright C$. En d'autres termes,

$$f \upharpoonright C = f \cap (C \times B).$$

(a) Démontrer que $f \upharpoonright C$ est une fonction de C vers B et que pour tout $c \in C$, $f(c) = (f \upharpoonright C)(c)$.

(b) Supposons $g : C \rightarrow B$. Démontrer que $g = f \upharpoonright C$ ssi $g \subseteq f$.

(c) Soient g et h les fonctions définies dans les parties 2 et 3 de [l'exemple 5.1.3](#). Montrer que $g = h \upharpoonright \mathbb{Z}_4$

8. Supposons $f : A \rightarrow B$ et $g \subseteq f$. Démontrer qu'il existe un ensemble $A' \subseteq A$ tel que $g : A' \rightarrow B$.

9. Supposons que $f : A \rightarrow B$, $B \neq \emptyset$ et $A \subseteq A'$. Démontrer qu'il existe une fonction $g : A' \rightarrow B$ telle que $f \subseteq g$.

10. Supposons que f et g soient des fonctions de A vers B et que $f = g$. Démontrer que fg n'est pas une fonction.

11. Supposons que A soit un ensemble. Montrer que A est la seule relation sur A qui soit à la fois une relation d'équivalence sur A et une fonction de A vers A .

12. Supposons $f : A \rightarrow C$ et $g : B \rightarrow C$.

(a) Démontrer que si A et B sont disjoints, alors $f \cup g : A \cup B \rightarrow C$.

(b) Démontrer que $f \cup g : A \cup B \rightarrow C$ ssi $f \upharpoonright (A \cap B) = g \upharpoonright (A \cap B)$. (Voir [l'exercice 7](#) pour la signification de la notation utilisée ici.)

13. Supposons que R soit une relation de A à B , S soit une relation de B à C , $\text{Ran}(R) = \text{Dom}(S) = B$, et $S \circ R : A \rightarrow C$.

(a) Démontrer que $S : B \rightarrow C$.

(b) Donnez un exemple pour montrer qu'il n'est pas nécessaire que $R : A \rightarrow B$.

14. Supposons que $f : A \rightarrow B$ et que S soit une relation sur B . Définissons une relation R sur A comme suit :

$$R = \{(x, y) \in A \times A \mid (f(x), f(y)) \in S\}.$$

(a) Démontrer que si S est réflexif, alors R l'est aussi.

(b) Démontrer que si S est symétrique, alors R l'est aussi.

(c) Démontrer que si S est transitif, alors R l'est aussi.

15. Supposons que $f : A \rightarrow B$ et que R soit une relation sur A . Définissons une relation S sur B comme suit :

$$S = \{(x, y) \in B \times B \mid \exists u \in A \exists v \in A (f(u) = x \wedge f(v) = y \wedge (u, v) \in R)\}.$$

Justifiez vos réponses aux questions suivantes avec des preuves ou des contre-exemples.

(a) Si R est réflexif, doit-il en être de même pour S ?

(b) Si R est symétrique, doit-il en être de même pour S ?

(c) Si R est transitif, doit-il en être de même pour S ?

16. Supposons que A et B soient des ensembles, et soit $\mathcal{F} = \{f \mid f : A \rightarrow B\}$.

Supposons également que R soit une relation sur B , et définissons une relation S sur \mathcal{F} comme suit :

$$S = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \forall x \in A ((f(x), g(x)) \in R)\}.$$

Justifiez vos réponses aux questions suivantes avec des preuves ou des contre-exemples.

(a) Si R est réflexif, doit-il en être de même pour S ?

(b) Si R est symétrique, doit-il en être de même pour S ?

(c) Si R est transitif, doit-il en être de même pour S ?

17. Supposons que A soit un ensemble non vide et $f : A \rightarrow A$.

(a) Supposons qu'il existe un $a \in A$ tel que $\forall x \in A (f(x) = a)$. (Dans ce cas, f est appelée une fonction *constante*.) Démontrer que pour tout $g : A \rightarrow A$, $f \circ g = f$.

(b) Supposons que pour tout $g : A \rightarrow A$, $f \circ g = f$. Démontrer que f est une fonction constante. (Indice : que se passe-t-il si g est une fonction constante?)

18. Soit $\mathcal{F} = \{f \mid f : \mathbb{R} \rightarrow \mathbb{R}\}$. Soit $R = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \exists a \in \mathbb{R} \forall x > a (f(x) = g(x))\}$.

(a) Soient $f : \mathbb{R} \rightarrow \mathbb{R}$ et $g : \mathbb{R} \rightarrow \mathbb{R}$ les fonctions définies par les formules $f(x) = |x|$ et $g(x) = x$. Montrer que $(f, g) \in R$.

(b) Démontrer que R est une relation d'équivalence.

19. Soit $\mathcal{F} = \{f \mid f: \mathbb{Z}^+ \rightarrow \mathbb{R}\}$. Pour $g \in \mathcal{F}$, on définit l'ensemble $O(g)$ comme suit :

$$O(g) = \{f \in \mathcal{F} \mid \exists a \in \mathbb{Z}^+ \exists c \in \mathbb{R}^+ \forall x > a (|f(x)| \leq c|g(x)|)\}.$$

(Si $f \in O(g)$, alors les mathématiciens disent que « f est grand-oh de g »)

(a) Soient $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ et $g: \mathbb{Z}^+ \rightarrow \mathbb{R}$ définis par les formules $f(x) = 7x + 3$ et $g(x) = x^2$. Démontrer que $f \in O(g)$, mais $g \notin O(f)$.

(b) Soit $S = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid f \in O(g)\}$. Démontrer que S est un préordre, mais pas un ordre partiel. (Voir [l'exercice 25 de la section 4.5](#) pour la définition de préordre.)

(c) Supposons que $f_1 \in O(g)$ et $f_2 \in O(g)$, et que s et t soient des nombres réels. Définissez une fonction $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ par la formule $f(x) = sf_1(x) + tf_2(x)$. Démontrez que $f \in O(g)$. (Indice : L'inégalité triangulaire peut vous être utile. Voir [l'exercice 13\(c\) de la section 3.5](#).)

20. (a) Supposons $g: A \rightarrow B$ et soit $R = \{(x, y) \in A \times A \mid g(x) = g(y)\}$. Montrer que R est une relation d'équivalence sur A .

(b) Supposons que R soit une relation d'équivalence sur A et soit $g: A \rightarrow A/R$ la fonction définie par la formule $g(x) = [x]_R$. Montrer que $R = \{(x, y) \in A \times A \mid g(x) = g(y)\}$.

21. Supposons que $f: A \rightarrow B$ et que R soit une relation d'équivalence sur A . On dira que f est compatible avec R si $\forall x \in A \forall y \in A (xRy \rightarrow f(x) = f(y))$. (Vous pouvez comparer cet exercice à [l'exercice 24 de la section 4.5](#).)

(a) Supposons que f soit compatible avec R . Démontrer qu'il existe une fonction unique $h: A/R \rightarrow B$ telle que pour tout $x \in A$, $h([x]_R) = f(x)$.

(b) Supposons $h: A/R \rightarrow B$ et pour tout $x \in A$, $h([x]_R) = f(x)$. Démontrer que f est compatible avec R .

22. Soit $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \equiv y \pmod{5}\}$. Notons que d'après [le théorème 4.5.10](#) et [l'exercice 14 de la section 4.5](#), R est une relation d'équivalence sur \mathbb{N} .

(a) Démontrer qu'il existe une unique fonction $h: \mathbb{N}/R \rightarrow \mathbb{N}/R$ telle que pour tout entier naturel x , $h([x]_R) = [x^2]_R$. (Indice : utilisez [l'exercice 21](#).)

(b) Montrer qu'il n'existe pas de fonction $h: \mathbb{N}/R \rightarrow \mathbb{N}/R$ telle que pour tout nombre naturel x , $h([x]_R) = [2^x]_R$.

5.2 Un à un et sur

Dans la section précédente, nous avons vu que la composition de deux fonctions est à nouveau une fonction. Qu'en est-il des réciproques de fonctions ? Si $f: A \rightarrow B$, alors f est une relation de A vers B , donc f^{-1} est une relation de B vers A . S'agit-il d'une fonction de B vers A ? Nous répondrons à cette question dans la section suivante. Comme nous le verrons, la réponse dépend des deux propriétés suivantes des fonctions.

Définition 5.2.1. Supposons $f: A \rightarrow B$. On dira que f est *bijectif* si

$$\neg \exists a_1 \in A \exists a_2 \in A (f(a_1) = f(a_2) \wedge a_1 \neq a_2).$$

Nous disons que f cartes sur B (ou est simplement sur si B est clair d'après le contexte) si

$$\forall b \in B \exists a \in A (f(a) = b).$$

Les fonctions biunivoques sont parfois également appelées *injections*, et les fonctions onto sont parfois appelées *surjections*.

Notez que notre définition de la bijection commence par le symbole de négation \neg . Autrement dit, dire que f est bijective signifie qu'une certaine situation *ne se produit pas*. La situation qui ne doit pas se produire est celle où il existe deux éléments différents du domaine de définition de f , a_1 et a_2 , tels que $f(a_1) = f(a_2)$. Cette situation est illustrée par [la figure 5.4\(a\)](#). Ainsi, la fonction de [la figure 5.4\(a\)](#) n'est pas bijective. [La figure 5.4\(b\)](#) montre une fonction qui est bijective.

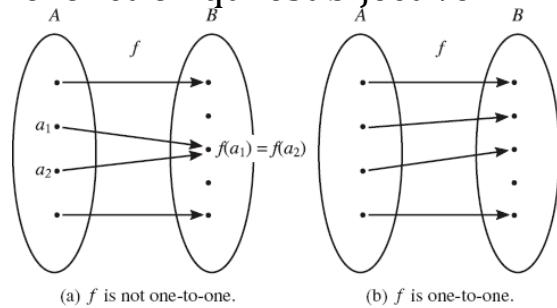


Figure 5.4.

Si $f: A \rightarrow B$, alors dire que f est sur signifie que tout élément de B est l'image par f d'un élément de A . Autrement dit, dans le diagramme de f , tout élément de B possède une arête pointant vers lui. Aucune des fonctions de [la figure 5.4](#) n'est sur, car dans les deux cas, il existe des éléments de B sans arêtes pointant vers eux. [La figure 5.5](#) montre deux fonctions sur.

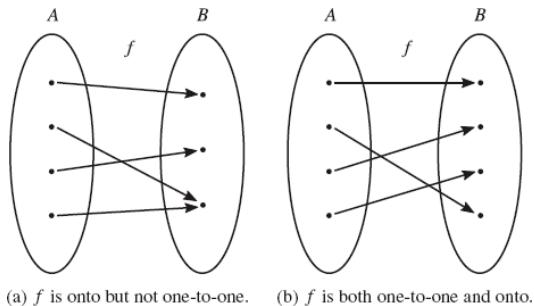


Figure 5.5.

Exemple 5.2.2. Les fonctions suivantes sont-elles bijectives ? Sont-elles sur ?

1. La fonction F de la partie 1 de [l'exemple 5.1.2](#).
2. La fonction L de la partie 3 de [l'exemple 5.1.2](#).
3. La fonction identité i_A , pour tout ensemble A .
4. La fonction g de la partie 2 de [l'exemple 5.1.3](#).
5. La fonction h de la partie 3 de [l'exemple 5.1.3](#).

Solutions

1. F n'est pas bijectif car $F(1) = 5 = F(3)$. Il n'est pas non plus sur, car $6 \in B$, mais il n'existe pas $a \in A$ tel que $F(a) = 6$.
2. L n'est pas bijectif car il existe de nombreuses paires de villes différentes c_1 et c_2 pour lesquelles $L(c_1) = L(c_2)$. Par exemple, $L(\text{Chicago}) = \text{États-Unis} = L(\text{Seattle})$. Dire que L est sur signifie que $\forall n \in N \exists c \in C (L(c) = n)$, ou en d'autres termes, pour chaque pays n , il existe une ville c telle que la ville c soit située dans le pays n . C'est probablement vrai, car il est peu probable qu'il existe un pays qui ne contienne aucune ville. Ainsi, L est probablement sur.
3. Pour décider si i_A est inexact, nous devons déterminer s'il existe deux éléments a_1 et a_2 de A tels que $i_A(a_1) = i_A(a_2)$ et $a_1 \neq a_2$. Mais comme nous l'avons vu dans [la section 5.1](#), pour tout $a \in A$, $i_A(a) = a$, donc $i_A(a_1) = i_A(a_2)$ signifie $a_1 = a_2$. Ainsi, il ne peut pas y avoir d'éléments a_1 et a_2 de A tels que $i_A(a_1) = i_A(a_2)$ et $a_1 \neq a_2$, donc i_A est exact.

Dire que i_A est sur signifie que pour tout $a \in A$, $a = i_A(b)$ pour un certain $b \in A$. Ceci est clairement vrai car, en fait, $a = i_A(a)$. Ainsi, i_A est également sur.

4. Comme dans la solution 3, pour déterminer si g est bijectif, il faut déterminer s'il existe des entiers n_1 et n_2 tels que $g(n_1) = g(n_2)$ et $n_1 \neq n_2$. D'après la définition de g , on a

$$\begin{aligned} g(n_1) = g(n_2) &\text{ iff } 2n_1 + 3 = 2n_2 + 3 \\ &\text{ iff } 2n_1 = 2n_2 \\ &\text{ iff } n_1 = n_2. \end{aligned}$$

Ainsi, il ne peut y avoir d'entiers n_1 et n_2 pour lesquels $g(n_1) = g(n_2)$ et $n_1 \neq n_2$. Autrement dit, g est bijectif. Cependant, g n'est pas sur, car, par exemple, il n'existe pas d'entier n pour lequel $g(n) = 0$. Pour comprendre pourquoi, supposons que n soit un entier et que $g(n) = 0$. Alors, par définition de g , on a $2n + 3 = 0$, donc $n = -3/2$. Mais cela contredit le fait que n soit un entier. Notons que le domaine de définition de g est \mathbb{Z} ; donc, pour que g soit sur, il faut que pour tout nombre réel y existe un entier n tel que $g(n) = y$. Puisque nous avons vu qu'il n'existe pas d'entier n tel que $g(n) = 0$, nous pouvons conclure que g n'est pas sur.

5. Cette fonction est à la fois bijective et sur. La vérification de la bijection de h est très similaire à celle de la solution 4, selon laquelle g est bijective, et elle est laissée au lecteur. Pour voir que h est sur, nous devons montrer que $\forall y \in \mathbb{R} \exists x \in \mathbb{R} (h(x) = y)$. Voici une brève preuve de cette affirmation. Soit y un nombre réel arbitraire. Soit $x = (y - 3)/2$. Alors $g(x) = 2x + 3 = 2((y - 3)/2) + 3 = y - 3 + 3 = y$. Ainsi, $\forall y \in \mathbb{R} \exists x \in \mathbb{R} (h(x) = y)$, donc h est sur.

Bien que la définition de bijectif soit plus facile à comprendre lorsqu'elle est formulée sous forme négative, comme dans [la définition 5.2.1](#), nous savons, depuis [le chapitre 3](#), que la définition sera plus facile à utiliser dans les démonstrations si nous la reformulons sous forme positive équivalente. Le théorème suivant montre comment procéder. Il fournit également une équivalence utile pour la définition d'onto.

Théorème 5.2.3. Supposer $f: A \rightarrow B$.

1. f est bijectifssi $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$.

2. f est surssi $\text{Ran}(f) = B$.

Preuve.

- Nous utilisons les règles des [chapitres 1](#) et [2](#) pour réexprimer les affirmations négatives en affirmations positives.

f is one-to-one iff $\neg \exists a_1 \in A \exists a_2 \in A (f(a_1) = f(a_2) \wedge a_1 \neq a_2)$
iff $\forall a_1 \in A \forall a_2 \in A (\neg(f(a_1) = f(a_2) \wedge a_1 \neq a_2))$
iff $\forall a_1 \in A \forall a_2 \in A (f(a_1) \neq f(a_2) \vee a_1 = a_2)$
iff $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$.

2. Nous relions d'abord la définition de onto à la définition de range.

f is onto iff $\forall b \in B \exists a \in A (f(a) = b)$
iff $\forall b \in B \exists a \in A ((a, b) \in f)$
iff $\forall b \in B (b \in \text{Ran}(f))$
iff $B \subseteq \text{Ran}(f)$.

Nous sommes maintenant prêts à prouver la partie 2 du théorème.

(\rightarrow) Supposons que f soit sur. Par l'équivalence qui vient d'être dérivée, nous avons $B \subseteq \text{Ran}(f)$, et par la définition de l'image, nous avons $\text{Ran}(f) \subseteq B$. Ainsi, il s'ensuit que $\text{Ran}(f) = B$.

(\leftarrow) Supposons que $\text{Ran}(f) = B$. Alors certainement $B \subseteq \text{Ran}(f)$, donc par équivalence, f est sur. \square

Commentaire . Il est souvent plus efficace d'écrire la preuve d'une instruction ssi sous forme d'une chaîne d'équivalences, si possible. Dans le cas de l'instruction 1, c'est facile, en utilisant les règles de la logique. Pour l'instruction 2, cette stratégie ne fonctionne pas tout à fait, mais elle nous donne une équivalence utile pour la preuve.

Exemple 5.2.4. Soit $A = \mathbb{R} \setminus \{-1\}$, et définissons $f: A \rightarrow \mathbb{R}$ par la formule

$$f(a) = \frac{2a}{a+1}.$$

Démontrer que f est bijectif mais pas sur.

Travail à partir de zéro

Français Par la partie 1 du [théorème 5.2.3](#), nous pouvons prouver que f est injective en prouvant l'énoncé équivalent $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$. Ainsi, nous posons a_1 et a_2 des éléments arbitraires de A , supposons $f(a_1) = f(a_2)$, puis prouvons $a_1 = a_2$. C'est la stratégie qui est presque toujours utilisée pour prouver qu'une fonction est injective. Les détails restants de la preuve n'impliquent que de l'algèbre simple et sont donnés plus loin.

Pour montrer que f n'est pas sur, nous devons prouver $\neg \forall x \in \mathbb{R} \exists a \in A (f(a) = x)$. En reformulant cela comme une affirmation positive, nous voyons que nous devons prouver $\exists x \in \mathbb{R} \forall a \in A (f(a) \neq x)$, nous devrions donc essayer de trouver un nombre réel particulier x tel que $\forall a \in A (f(a) \neq x)$. Malheureusement, la valeur que nous devrions utiliser pour x n'est pas du tout claire. Nous utiliserons une procédure quelque

peu inhabituelle pour surmonter cette difficulté. Au lieu d'essayer de prouver que f n'est pas sur, essayons de prouver qu'elle l'est ! Bien sûr, nous nous attendons à ce que cette preuve ne fonctionne pas, mais peut-être que comprendre *pourquoi* elle ne fonctionnera pas nous aidera à déterminer quelle valeur de x utiliser dans la preuve que f n'est pas sur.

Pour prouver que f est sur, il faudrait prouver $\forall x \in \mathbb{R} \exists a \in A (f(a) = x)$, donc on devrait soit x un nombre réel arbitraire et essayer de trouver un $a \in A$ tel que $f(a) = x$. En complétant la définition de f , on voit qu'il faut trouver $a \in A$ tel que

$$\frac{2a}{a+1} = x.$$

Pour trouver cette valeur de a , nous résolvons simplement l'équation pour a :

$$\frac{2a}{a+1} = x \Rightarrow 2a = ax + x \Rightarrow a(2-x) = x \Rightarrow a = \frac{x}{2-x}.$$

Ah ! La dernière étape de cette dérivation ne fonctionnerait pas si $x = 2$, car nous diviserions alors par 0. C'est la seule valeur de x qui semble poser problème lorsqu'on cherche une valeur de a pour laquelle $f(a) = x$. Peut-être $x = 2$ est-elle la valeur à utiliser pour prouver que f n'est pas correct.

Revenons maintenant à la preuve que f n'est pas sur. Si $x = 2$, pourachever la preuve, il faut montrer que $\forall a \in A (f(a) \neq 2)$. Pour ce faire, nous poserons a comme élément arbitraire de A , en supposant $f(a) = 2$, puis en essayant de déduire une contradiction. Les autres détails de la preuve ne sont pas difficiles.

Solution

Preuve . Pour voir que f est injectif, soit a_1 et a_2 des éléments arbitraires de A et supposons que $f(a_1) = f(a_2)$. En appliquant la définition de f , il s'ensuit que $2a_1/(a_1+1) = 2a_2/(a_2+1)$. Ainsi, $2a_1(a_2+1) = 2a_2(a_1+1)$. En multipliant les deux côtés, on obtient $2a_1a_2 + 2a_1 = 2a_1a_2 + 2a_2$, donc $2a_1 = 2a_2$ et donc $a_1 = a_2$.

Pour montrer que f n'est pas sur, nous allons prouver que $\forall a \in A (f(a) \neq 2)$. Supposons que $a \in A$ et $f(a) = 2$. En appliquant la définition de f , nous obtenons $2a/(a+1) = 2$. Ainsi, $2a = 2a + 2$, ce qui est clairement impossible. Ainsi, $2 \notin \text{Ran}(f)$, donc $\text{Ran}(f) \neq \mathbb{R}$ et donc f n'est pas sur.

□

Comme nous l'avons vu dans l'exemple précédent, pour prouver qu'une fonction f est injective, il est généralement plus facile de prouver

l'énoncé équivalent $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$ donné dans la partie 1 du [théorème 5.2.3](#). Bien sûr, ce n'est qu'un exemple du fait qu'il est généralement plus facile de prouver un énoncé positif qu'un énoncé négatif. Cette équivalence est également souvent utilisée dans les démonstrations où l'on nous *donne* qu'une fonction est injective, comme vous le verrez dans la preuve de la partie 1 du théorème suivant.

Théorème 5.2.5. *Supposer $f: A \rightarrow B$ et $g: B \rightarrow C$. Comme nous l'avons vu dans [le théorème 5.1.5](#), il s'ensuit que $g \circ f: A \rightarrow C$.*

1. Si f et g sont tous deux bijectifs, alors $g \circ f$ l'est aussi .
2. Si f et g sont tous deux sur, alors $g \circ f$ l'est aussi .

Preuve .

1. Supposons que f et g soient tous deux injectifs. Soient a_1 et a_2 des éléments arbitraires de A et supposons que $(g \circ f)(a_1) = (g \circ f)(a_2)$. D'après [le théorème 5.1.5](#), cela signifie que $g(f(a_1)) = g(f(a_2))$. Puisque g est injectif, il s'ensuit que $f(a_1) = f(a_2)$, et de même, puisque f est injectif, nous pouvons alors conclure que $a_1 = a_2$. Ainsi, $g \circ f$ est injectif.
2. Supposons que f et g soient tous deux sur, et soit c un élément arbitraire de C . Puisque g est sur, on peut trouver un $b \in B$ tel que $g(b) = c$. De même, puisque f est sur, il existe un $a \in A$ tel que $f(a) = b$. Alors $(g \circ f)(a) = g(f(a)) = g(b) = c$. Ainsi, $g \circ f$ est sur.

Commentaire .

1. Comme dans [l'exemple 5.2.4](#), nous prouvons que $g \circ f$ est injectif en prouvant que $\forall a_1 \in A \forall a_2 \in A ((g \circ f)(a_1) = (g \circ f)(a_2) \rightarrow a_1 = a_2)$. Ainsi, nous posons a_1 et a_2 des éléments arbitraires de A , supposons que $(g \circ f)(a_1) = (g \circ f)(a_2)$, ce qui signifie $g(f(a_1)) = g(f(a_2))$, puis prouvons que $a_1 = a_2$. La phrase suivante de la preuve indique que l'hypothèse que g est injectif est utilisée, mais la *manière dont* elle est utilisée n'est peut-être pas claire. Pour comprendre cette étape, écrivons ce que signifie dire que g est injectif. Comme nous l'avons observé précédemment, plutôt que d'utiliser la définition originale, qui est une affirmation négative, nous sommes probablement mieux lotis en utilisant l'énoncé positif équivalent $\forall b_1 \in B \forall b_2 \in B (g(b_1) = g(b_2) \rightarrow b_1 = b_2)$. La manière naturelle d'utiliser une donnée de cette forme est de

remplacer b_1 et b_2 . En remplaçant $f(a_1)$ et $f(a_2)$, nous obtenons $g(f(a_1)) = g(f(a_2)) \rightarrow f(a_1) = f(a_2)$, et puisque nous savons que $g(f(a_1)) = g(f(a_2))$, il s'ensuit par modus ponens que $f(a_1) = f(a_2)$. Rien de tout cela n'a été expliqué dans la preuve ; les lecteurs du *On attend* des preuves qu'elles le trouvent par elles-mêmes. Assurez-vous de comprendre comment, par un raisonnement similaire, vous pouvez passer de $f(a_1) = f(a_2)$ à $a_1 = a_2$ en appliquant le fait que f est bijectif.

2. Après avoir supposé que f et g sont tous deux sur, la forme du reste de la preuve est entièrement guidée par la forme logique de l'objectif de prouver que $g \circ f$ est sur. Puisque cela signifie $\forall c \in C \exists a \in A ((g \circ f)(a) = c)$, on pose c comme un élément arbitraire de C et on trouve ensuite un $a \in A$ pour lequel on peut prouver que $(g \circ f)(a) = c$.

□

Les fonctions à la fois bijectives et sur-exprimées sont particulièrement importantes en mathématiques. On les appelle parfois *correspondances bijectives* ou *bijections*. [La figure 5.5\(b\)](#) montre un exemple de correspondance bijective. Remarquez que, sur cette figure, A et B ont tous deux quatre éléments. En fait, vous devriez être capable de vous convaincre que s'il existe une correspondance bijective entre deux ensembles finis, alors ces ensembles doivent avoir le même nombre d'éléments. C'est l'une des raisons pour lesquelles les correspondances bijectives sont si importantes. Nous aborderons les correspondances bijectives entre ensembles infinis au [chapitre 8](#).

Voici un autre exemple de correspondance bijective. Supposons que A représente l'ensemble des spectateurs d'un concert à guichets fermés et que S représente l'ensemble des places assises. Soit $f : A \rightarrow S$ la fonction définie par la règle

$$f(a) = \text{the seat in which } a \text{ is sitting.}$$

Puisque différentes personnes ne seraient pas assises au même siège, f est biunivoque. Le concert étant complet, toutes les places sont prises, f est donc en ligne. Ainsi, f est une correspondance biunivoque. Même sans compter les personnes ni les sièges, on peut déduire que le nombre de spectateurs doit être égal au nombre de sièges dans la salle.

Exercices

1. Lesquelles des fonctions de [l'exercice 1](#) de [la section 5.1](#) sont bijectives ? Lesquelles sont sur ?

- *2. Lesquelles des fonctions de [l'exercice 2](#) de [la section 5.1](#) sont bijectives ? Lesquelles sont sur ?
3. Lesquelles des fonctions de [l'exercice 3](#) de [la section 5.1](#) sont bijectives ? Lesquelles sont sur ?
4. Lesquelles des fonctions de [l'exercice 4](#) de [la section 5.1](#) sont bijectives ? Lesquelles sont sur ?
- *5. Soit $A = \mathbb{R} \setminus \{1\}$, et soit $f: A \rightarrow A$ défini comme suit :

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

- (a) Montrez que f est bijectif et sur.
- (b) Montrer que $f \circ f = i_A$.
6. Supposons que a et b soient des nombres réels et que $a \neq 0$. Définissez $f: \mathbb{R} \rightarrow \mathbb{R}$ par la formule $f(x) = ax + b$. Montrez que f est bijectif et sur.
7. Définissez $f: \mathbb{R}^+ \rightarrow \mathbb{R}$ par la formule $f(x) = 1/x - x$.
- (a) Montrez que f est bijectif. (Indice : il peut être utile de prouver d'abord que si $0 < a < b$ alors $f(a) > f(b)$.)
- (b) Montrez que f est sur.
- (c) Définissez $g: \mathbb{R}^+ \rightarrow \mathbb{R}$ par la formule $g(x) = 1/x + x$. g est-il bijectif ? Est-il sur ?
8. Soit $A = \mathcal{P}(\mathbb{R})$. Définissons $f: \mathbb{R} \rightarrow A$ par la formule $f(x) = \{y \in \mathbb{R} \mid y^2 < x\}$.
- (a) Trouvez $f(2)$.
- (b) Est-ce que f est bijectif ? Est-ce sur ?
- *9. Soit $A = \mathcal{P}(\mathbb{R})$ et $B = \mathcal{P}(A)$. Définissons $f: B \rightarrow A$ par la formule $f(\mathcal{F}) = \bigcup \mathcal{F}$.
- (a) Trouvez $f(\{\{1, 2\}, \{3, 4\}\})$.
- (b) Est-ce que f est bijectif ? Est-ce sur ?
10. Supposons $f: A \rightarrow B$ et $g: B \rightarrow C$.
- (a) Démontrer que si $g \circ f$ est sur, alors g est sur.
- (b) Démontrer que si $g \circ f$ est bijectif, alors f est bijectif.
11. Supposons $f: A \rightarrow B$ et $g: B \rightarrow C$.
- (a) Démontrer que si f est sur et g n'est pas bijectif, alors $g \circ f$ n'est pas bijectif.
- (b) Démontrer que si f n'est pas sur et g est bijectif, alors $g \circ f$ n'est pas sur.
12. Supposons que $f: A \rightarrow B$. Définissons une fonction $g: B \rightarrow \mathcal{P}(A)$ par la formule $g(b) = \{a \in A \mid f(a) = b\}$. Démontrons que si f est sur, alors g est bijectif. Que se passe-t-il si f n'est pas sur ?

13. Supposons $f: A \rightarrow B$ et $C \subseteq A$. Dans [l'exercice 7 de la section 5.1](#), nous avons défini $f|C$ (la restriction de f à C), et vous avez montré que $f|C: C \rightarrow B$.

- (a) Démontrer que si f est bijectif, alors $f|C$ l'est aussi.
- (b) Démontrer que si $f|C$ est sur, alors f l'est aussi.
- (c) Donnez des exemples pour montrer que les réciproques des parties (a) et (b) ne sont pas toujours vraies.

14. Supposons que $f: A \rightarrow B$, et qu'il existe un $b \in B$ tel que $\forall x \in A (f(x) = b)$. (Ainsi, f est une fonction *constante*.)

- (a) Démontrer que si A a plus d'un élément, alors f n'est pas bijectif.
- (b) Démontrer que si B a plus d'un élément, alors f n'est pas sur.

15. Supposons que $f: A \rightarrow C$, $g: B \rightarrow C$, et que A et B soient disjoints.

Dans [l'exercice 12\(a\) de la section 5.1](#), vous avez démontré que $f \cup g: A \cup B \rightarrow C$. Supposons maintenant que f et g soient bijectifs. Démontrer que $f \cup g$ est bijectif ssi $\text{Ran}(f)$ et $\text{Ran}(g)$ sont disjoints.

16. Supposons que R soit une relation de A vers B , S une relation de B vers C , $\text{Ran}(R) = \text{Dom}(S) = B$ et $S \circ R: A \rightarrow C$. Dans [l'exercice 13\(a\) de la section 5.1](#), vous avez prouvé que $S: B \rightarrow C$. Démontrez maintenant que si S est bijectif alors $R: A \rightarrow B$.

17. Supposons que $f: A \rightarrow B$ et que R soit une relation sur A . Comme dans [l'exercice 15 de la section 5.1](#), définissons une relation S sur B comme suit :

$$S = \{(x, y) \in B \times B \mid \exists u \in A \exists v \in A (f(u) = x \wedge f(v) = y \wedge (u, v) \in R)\}.$$

- (a) Démontrer que si R est réflexif et f est sur, alors S est réflexif.
 - (b) Démontrer que si R est transitif et f est bijectif, alors S est transitif.
18. Supposons que R soit une relation d'équivalence sur A , et soit $g: A \rightarrow A/R$ défini par la formule $g(x) = [x]_R$, comme dans [l'exercice 20\(b\) de la section 5.1](#).

- (a) Montrez que g est sur.
- (b) Montrer que g est bijectif si et seulement si $R = i_A$.

19. Supposons que $f: A \rightarrow B$, R soit une relation d'équivalence sur A , et f soit compatible avec R . (Voir [l'exercice 21 de la section 5.1](#) pour la définition de *compatible*.) Dans [l'exercice 21\(a\) de la section 5.1](#), vous avez démontré qu'il existe une unique fonction $h: A/R \rightarrow B$ telle que pour tout $x \in A$, $h([x]_R) = f(x)$. Démontrons maintenant que h est bijectif ssi $\forall x \in A \forall y \in A (f(x) = f(y) \rightarrow xRy)$.

20. Supposons que A , B et C sont des ensembles et $f: A \rightarrow B$.

- (a) Démontrer que si f est sur, $g: B \rightarrow C$, $h: B \rightarrow C$, et $g \circ f = h \circ f$, alors $g = h$.
- (b) Supposons que C possède au moins deux éléments, et que pour toutes les fonctions g et h de B à C , si $g \circ f = h \circ f$ alors $g = h$.

Démontrer que f est sur.

21. Supposons que A , B et C sont des ensembles et $f: B \rightarrow C$.

(a) Démontrer que si f est bijectif, $g : A \rightarrow B$, $h : A \rightarrow B$ et $f \circ g = f \circ h$, alors $g = h$.

(b) Supposons que $A = \emptyset$, et pour toutes les fonctions g et h de A à B , si $f \circ g = f \circ h$ alors $g = h$. Démontrer que f est bijectif.

22. Soit $\mathcal{F} = \{f \mid f: \mathbb{R} \rightarrow \mathbb{R}\}$, et définissons une relation R sur \mathcal{F} comme suit :

$$R = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \exists h \in \mathcal{F} (f = h \circ g)\}.$$

(a) Soient f , g et h les fonctions de \mathbb{R} dans \mathbb{R} définies par les formules $f(x) = x^2 + 1$, $g(x) = x^3 + 1$ et $h(x) = x^4 + 1$. Démontrer que hRf , mais ce n'est pas le cas que gRf .

(b) Démontrer que R est un préordre. (Voir [l'exercice 25 de la section 4.5](#) pour la définition de préordre.)

(c) Démontrer que pour tout $f \in \mathcal{F}$, $fRi_{\mathbb{R}}$.

(d) Démontrer que pour tout $f \in \mathcal{F}$, $i_{\mathbb{R}}Rf$ ssi f est bijectif. (Indice pour le sens de droite à gauche : supposons que f soit bijectif. Soit $A = \text{Ran}(f)$, et soit $h = f^{-1} \cup ((\mathbb{R} \setminus A) \times \{0\})$. Démontrer maintenant que $h : \mathbb{R} \rightarrow \mathbb{R}$ et $i_{\mathbb{R}} = h \circ f$.)

(e) Supposons que $g \in \mathcal{F}$ soit une fonction constante ; autrement dit, il existe un nombre réel c tel que $\forall x \in \mathbb{R} (g(x) = c)$. Démontrer que pour tout $f \in \mathcal{F}$, gRf . (Indice : voir [l'exercice 17 de la section 5.1](#).)

(f) Supposons que $g \in \mathcal{F}$ soit une fonction constante. Démontrer que pour tout $f \in \mathcal{F}$, fRg ssi f est une fonction constante.

(g) Comme dans [l'exercice 25 de la section 4.5](#), si l'on pose $S = R \cap R^{-1}$, alors S est une relation d'équivalence sur \mathcal{F} . De plus, il existe une unique relation T sur \mathcal{F}/S telle que pour tout f et g dans \mathcal{F} , $[f]_S T [g]_S$ ssi $f Rg$, et T est un ordre partiel sur \mathcal{F}/S . Démontrer que l'ensemble de toutes les fonctions bijectives de \mathbb{R} à \mathbb{R} est le plus grand élément de \mathcal{F}/S dans l'ordre partiel T , et que l'ensemble de toutes les fonctions constantes de \mathbb{R} à \mathbb{R} est le plus petit élément.

23. Soit $f: \mathbb{N} \rightarrow \mathbb{N}$ défini par la formule $f(n) = n$. On pourrait aussi dire que $f: \mathbb{N} \rightarrow \mathbb{Z}$. Cet exercice illustrera pourquoi, dans [la définition 5.2.1](#), nous avons défini l'expression « f est appliqué à B » plutôt que simplement « f est appliqué à ».

(a) Est-ce que f est appliqué à \mathbb{N} ?

(b) Est-ce que f est appliquée à \mathbb{Z} ?

5.3 Inverses de fonctions

Nous sommes maintenant prêts à revenir à la question de savoir si l'inverse d'une fonction de A vers B est toujours une fonction de B vers A . Reprenons la fonction F de la partie 1 de [l'exemple 5.1.2](#). Rappelons que dans cet exemple, nous avions $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ et $F = \{(1, 5), (2, 4), (3, 5)\}$. Comme nous l'avons vu dans [l'exemple 5.1.2](#), F est une fonction de A vers B . Selon la définition de l'inverse d'une relation, $F^{-1} = \{(5, 1), (4, 2), (5, 3)\}$, ce qui est clairement une relation de B vers A . Or, F^{-1} n'est pas une fonction de B vers A pour deux raisons. Premièrement, $6 \in B$, mais 6 n'est associé à aucun élément de A dans la relation F^{-1} . Deuxièmement, 5 est associé à deux éléments différents de A , 1 et 3 . Ainsi, cet exemple montre que l'inverse d'une fonction de A vers B n'est pas toujours une fonction de B vers A .

Vous avez peut-être remarqué que les raisons pour lesquelles F^{-1} n'est pas une fonction de B vers A sont liées aux raisons pour lesquelles F n'est ni bijective ni sur, abordées dans la première partie de [l'exemple 5.2.2](#). Ceci suggère le théorème suivant.

Théorème 5.3.1. *Supposer $f: A \rightarrow B$. Si f est bijectif et sur, alors $f^{-1}: B \rightarrow A$.*

Preuve . Supposons que f soit bijectif et sur, et soit b un élément arbitraire de B . Pour montrer que f^{-1} est une fonction de B vers A , nous devons prouver que $\exists! a \in A ((b, a) \in f^{-1})$, nous prouvons donc l'existence et l'unicité séparément.

Existence : Puisque f est sur, il existe un $a \in A$ tel que $f(a) = b$. Ainsi, $(a, b) \in f$, donc $(b, a) \in f^{-1}$.

Unicité : Supposons que $(b, a_1) \in f^{-1}$ et $(b, a_2) \in f^{-1}$ pour un certain $a_1, a_2 \in A$. Alors $(a_1, b) \in f$ et $(a_2, b) \in f$, donc $f(a_1) = b = f(a_2)$. Puisque f est bijectif, il s'ensuit que $a_1 = a_2$.

□

Commentaire . La forme de la preuve est guidée par la forme logique de l'énoncé que $f^{-1}: B \rightarrow A$. Parce que cela signifie $\forall b \in B \exists! a \in A ((b, a) \in f^{-1})$, nous posons b un élément arbitraire de B et prouvons ensuite l'existence et l'unicité pour le $a \in A$ requis séparément. Notez que

l'hypothèse que f est sur est la clé de la moitié d'existence de la preuve, et l'hypothèse que f est bijectif est la clé de la moitié d'unicité.

Supposons que f soit une fonction quelconque d'un ensemble A vers un ensemble B . [Le théorème 5.3.1 stipule](#) qu'une condition suffisante pour que f^{-1} soit une fonction de B vers A est que f soit bijective et sur. Est-ce aussi une condition nécessaire ? Autrement dit, la réciproque du [théorème 5.3.1 est](#) -elle vraie ? (Si vous avez oublié la signification des mots *suffisant*, *nécessaire* et *réciproque*, consultez [la section 1.5](#) !) Nous montrerons dans [le théorème 5.3.4](#) que la réponse à cette question est oui. Autrement dit, si f^{-1} est une fonction de B vers A , alors f doit être bijective et sur.

Si $f^{-1} : B \rightarrow A$ alors, par définition de fonction, pour chaque $b \in B$, il existe exactement un $a \in A$ tel que $(b, a) \in f^{-1}$, et

$$\begin{aligned} f^{-1}(b) &= \text{the unique } a \in A \text{ such that } (b, a) \in f^{-1} \\ &= \text{the unique } a \in A \text{ such that } (a, b) \in f \\ &= \text{the unique } a \in A \text{ such that } f(a) = b. \end{aligned}$$

Ceci donne une autre façon utile de penser à f^{-1} . Si f^{-1} est une fonction de B vers A , alors c'est la fonction qui assigne, à chaque $b \in B$, l'unique $a \in A$ tel que $f(a) = b$. L'hypothèse du [théorème 5.3.1](#) selon laquelle f est bijectif et sur garantit qu'il existe exactement un tel a .

À titre d'exemple, considérons à nouveau la fonction f qui assigne à chaque spectateur d'un concert à guichets fermés sa place. Comme nous l'avons vu à la fin de la section précédente, f est une fonction bijective, sur l'ensemble A de tous les spectateurs, vers l'ensemble S de toutes les places de la salle. Ainsi, f^{-1} doit être une fonction de S vers A , et pour tout $s \in S$,

$$\begin{aligned} f^{-1}(s) &= \text{the unique } a \in A \text{ such that } f(a) = s \\ &= \text{the unique person } a \text{ such that the seat in which } a \text{ is sitting is } s \\ &= \text{the person who is sitting in the seat } s. \end{aligned}$$

En d'autres termes, la fonction f attribue à chaque personne le siège sur lequel elle est assise, et la fonction f^{-1} attribue à chaque siège la personne assise sur ce siège.

Puisque $f : A \rightarrow S$ et $f^{-1} : S \rightarrow A$, il résulte du [théorème 5.1.5](#) que $f^{-1} \circ f : A \rightarrow A$ et $f \circ f^{-1} : S \rightarrow S$. Quelles sont ces fonctions ? Pour déterminer quelle est la première fonction, soit a un élément arbitraire de A et calculons $(f^{-1} \circ f)(a)$.

$$\begin{aligned}
(f^{-1} \circ f)(a) &= f^{-1}(f(a)) \\
&= f^{-1}(\text{the seat in which } a \text{ is sitting}) \\
&= \text{the person sitting in the seat in which } a \text{ is sitting} \\
&= a.
\end{aligned}$$

Mais rappelons que pour tout $a \in A$, $i_A(a) = a$. Ainsi, nous avons montré que $\forall a \in A ((f^{-1} \circ f)(a) = i_A(a))$, donc par [le théorème 5.1.4](#), $f^{-1} \circ f = i_A$. De même, vous devriez pouvoir vérifier que $f \circ f^{-1} = i_S$.

Lorsque les mathématiciens découvrent un phénomène inhabituel comme celui-ci dans un exemple, ils se demandent toujours s'il s'agit d'une simple coïncidence ou s'il s'agit d'un modèle plus général. Autrement dit, pouvons-nous prouver un théorème affirmant que ce qui s'est produit dans cet exemple se produira également dans d'autres exemples ? Dans ce cas précis, il s'avère que oui.

Théorème 5.3.2. *Supposer f est une fonction de UN à B , et supposons que f^{-1} est une fonction de B vers A . Alors $f^{-1} \circ f = i_A$ et $f \circ f^{-1} = i_B$.*

Preuve. Soit a un élément arbitraire de A . Soit $b = f(a) \in B$. Alors $(a, b) \in f$, donc $(b, a) \in f^{-1}$ et donc $f^{-1}(b) = a$. Ainsi,

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = i_A(a).$$

Comme a est arbitraire, nous avons montré que $\forall a \in A ((f^{-1} \circ f)(a) = i_A(a))$, donc $f^{-1} \circ f = i_A$. La preuve de la seconde moitié du théorème est similaire et est laissée en exercice ([voir exercice 8](#)). □

Commentaire . Pour prouver que deux fonctions sont égales, on applique habituellement le théorème 5.1.4. Ainsi, puisque $f^{-1} \circ f$ et i_A sont toutes deux des fonctions de A dans A , pour prouver qu'elles sont égales on prouve que $\forall a \in A ((f^{-1} \circ f)(a) = i_A(a))$.

[Le théorème 5.3.2](#) dit que si $f : A \rightarrow B$ et $f^{-1} : B \rightarrow A$, alors chaque fonction annule l'effet de l'autre. Pour tout $a \in A$, l'application de la fonction f nous donne $f(a) \in B$. Selon [le théorème 5.3.2](#), $f^{-1}(f(a)) = (f^{-1} \circ f)(a) = i_A(a) = a$. Ainsi, l'application de f^{-1} à $f(a)$ annule l'effet de l'application de f , nous rendant l'élément original a . De même, pour tout $b \in B$, l'application de f^{-1} nous donne $f^{-1}(b) \in A$, et nous pouvons annuler l'effet de l'application de f^{-1} en appliquant f , puisque $f(f^{-1}(b)) = b$.

Par exemple, soit $f : \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = 2x$. On devrait pouvoir vérifier que f est bijective et sur, donc $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$, et

pour tout $x \in \mathbb{R}$,

$$f^{-1}(x) = \text{l'unique } y \text{ tel que } f(y) = x.$$

Français Parce que $f^{-1}(x)$ est l'unique solution pour y dans l'équation $f(y) = x$, nous pouvons trouver une formule pour $f^{-1}(x)$ en résolvant cette équation pour y . En complétant la définition de f dans l'équation, nous obtenons $2y = x$, donc $y = x/2$. Ainsi, pour tout $x \in \mathbb{R}$, $f^{-1}(x) = x/2$. Notez qu'appliquer f à n'importe quel nombre double le nombre et appliquer f^{-1} divise le nombre par deux, et chacune de ces opérations annule l'effet de l'autre. En d'autres termes, si vous doublez un nombre puis divisez le résultat par deux, vous récupérez le nombre de départ. De même, diviser par deux n'importe quel nombre puis doubler le résultat vous ramène au nombre initial.

Existe-t-il d'autres circonstances où la composition de deux fonctions est égale à la fonction identité ? L'étude de cette question conduit au théorème suivant.

Théorème 5.3.3. Supposer $f : A \rightarrow B$.

1. S'il existe une fonction $g : B \rightarrow A$ telle que $g \circ f = i_A$ alors f est bijectif.
2. S'il existe une fonction $g : B \rightarrow A$ telle que $f \circ g = i_B$ alors f est sur.

Preuve .

1. Supposons que $g : B \rightarrow A$ et $g \circ f = i_A$. Soient a_1 et a_2 des éléments arbitraires de A , et supposons que $f(a_1) = f(a_2)$. En appliquant g aux deux côtés de cette équation nous obtenons $g(f(a_1)) = g(f(a_2))$. Mais $g(f(a_1)) = (g \circ f)(a_1) = i_A(a_1) = a_1$, et de même, $g(f(a_2)) = a_2$. Ainsi, nous pouvons conclure que $a_1 = a_2$, et donc f est bijectif.

2. Voir [exercice 9](#).

□

Commentaire . L'hypothèse selon laquelle il existe un $g : B \rightarrow A$ tel que $g \circ f = i_A$ est une affirmation existentielle ; on imagine donc immédiatement qu'une fonction particulière g a été choisie. La preuve que f est bijective suit le modèle habituel pour ce type de preuve, basé sur [le théorème 5.2.3](#).

La boucle est bouclée. Le [théorème 5.3.1](#) montre que si f est une fonction bijective et sur de A vers B , alors f^{-1} est une fonction de B vers A . De cette conclusion, comme nous l'avons montré au [théorème 5.3.2](#),

il résulte que la composition de f avec son inverse doit être la fonction identité. Le [théorème 5.3.3](#) montre que lorsque la composition de deux fonctions est la fonction identité, nous revenons aux propriétés bijective et sur ! Ainsi, en combinant [les théorèmes 5.3.1](#) à 5.3.3, nous obtenons le théorème suivant.

Théorème 5.3.4. *Supposer $f : A \rightarrow B$. Alors les affirmations suivantes sont équivalentes.*

1. f est bijectif et sur.

2. $f^{-1} : B \rightarrow A$.

3. Il existe une fonction $g : B \rightarrow A$ telle que $g \circ f = i_A$ et $f \circ g = i_B$.

Preuve. 1 \rightarrow 2. C'est précisément ce que dit [le théorème 5.3.1](#).

2 \rightarrow 3. Supposons $f^{-1} : B \rightarrow A$. Soit $g = f^{-1}$ et appliquons [le théorème 5.3.2](#).

3 \rightarrow 1. Appliquer [le théorème 5.3.3](#).

□

Commentaire. Comme nous l'avons vu à [la section 3.6](#), la manière la plus simple de prouver l'équivalence de plusieurs énoncés est de démontrer un cercle d'implications. Dans ce cas, nous avons démontré le cercle 1 \rightarrow 2 \rightarrow 3 \rightarrow 1. Notez que les preuves de ces implications sont assez sommaires. Assurez-vous de bien comprendre les détails.

Par exemple, soit f et g des fonctions de \mathbb{R} dans \mathbb{R} définies par les formules suivantes :

$$f(x) = \frac{x+7}{5}, \quad g(x) = 5x - 7.$$

Alors pour tout nombre réel x ,

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{x+7}{5}\right) = 5 \cdot \frac{x+7}{5} - 7 = x + 7 - 7 = x.$$

Ainsi, $g \circ f = i_{\mathbb{R}}$. Un calcul similaire montre que $f \circ g = i_{\mathbb{R}}$. Ainsi, il résulte du [théorème 5.3.4](#) que f doit être injectif et sur, et f^{-1} doit aussi être une fonction de \mathbb{R} dans \mathbb{R} . Qu'est-ce que f^{-1} ? Bien sûr, une supposition logique serait que $f^{-1} = g$, mais cela ne découle pas réellement des théorèmes que nous avons prouvés. Vous pourriez le vérifier directement en résolvant pour $f^{-1}(x)$, en utilisant le fait que $f^{-1}(x)$ doit être l'unique solution pour y dans l'équation $f(y) = x$.

Cependant, il n'est pas nécessaire de vérifier. Le théorème suivant montre que f^{-1} doit être égal à g .

Théorème 5.3.5. Supposer $f : A \rightarrow B$, $g : B \rightarrow A$, $g \circ f = i_A$, et $f \circ g = i_B$. Alors $g = f^{-1}$.

Preuve. D'après [le théorème 5.3.4](#), $f^{-1} : B \rightarrow A$. Par conséquent, d'après [le théorème 5.3.2](#), $f^{-1} \circ f = i_A$. Ainsi,

$$\begin{aligned} g &= i_A \circ g && \text{(exercice 9 of Section 4.3)} \\ &= (f^{-1} \circ f) \circ g \\ &= f^{-1} \circ (f \circ g) && \text{(Theorem 4.2.5)} \\ &= f^{-1} \circ i_B \\ &= f^{-1} && \text{(exercice 9 of Section 4.3).} \end{aligned}$$

□

Commentaire. Cette démonstration aboutit rapidement à la conclusion souhaitée grâce à une utilisation judicieuse des théorèmes et exercices précédents. Pour une démonstration plus directe mais un peu plus longue, voir [l'exercice 10](#).

Exemple 5.3.6. Dans chaque partie, déterminer si f est bijective et sur. Si oui, trouver f^{-1} .

1. Soit $A = \mathbb{R} \setminus \{0\}$ et $B = \mathbb{R} \setminus \{2\}$, et définissons $f : A \rightarrow B$ par la formule

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

(Notez que pour tout $x \in A$, $1/x$ est défini et non nul, donc $f(x) \neq 2$ et donc $f(x) \in B$.)

2. Soit $A = \mathbb{R}$ et $B = \{x \in \mathbb{R} \mid x \geq 0\}$, et définissons $f : A \rightarrow B$ par la formule

$$f(x) = x^2.$$

Solutions

1. On peut vérifier directement que f est bijective et sur, mais nous n'allons pas nous en préoccuper. Nous allons simplement essayer de trouver une fonction $g : B \rightarrow A$ telle que $g \circ f = i_A$ et $f \circ g = i_B$. Nous savons par [les théorèmes 5.3.4](#) et [5.3.5](#) que si nous trouvons un tel g , alors nous pouvons conclure que f est bijectif et sur et $g = f^{-1}$.

Puisque nous espérons avoir $g = f^{-1}$, nous savons que pour tout $x \in B = \mathbb{R} \setminus \{2\}$, $g(x)$ doit être l'unique $y \in A$ tel que $f(y) = x$. Ainsi, pour trouver une formule pour $g(x)$, nous résolvons pour y dans l'équation $f(y) = x$. En complétant la définition de f , nous voyons que l'équation à résoudre est

$$\frac{1}{y} + 2 = x.$$

En résolvant cette équation, nous obtenons

$$\frac{1}{y} + 2 = x \Rightarrow \frac{1}{y} = x - 2 \Rightarrow y = \frac{1}{x-2}.$$

Ainsi, nous définissons $g : B \rightarrow A$ par la formule

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

(Notez que pour tout $x \in B$, $x \neq 2$, donc $1/(x-2)$ est défini et non nul, et donc $g(x) \in A$.) Vérifions que g a les propriétés requises. Pour tout $x \in A$, nous avons

$$g(f(x)) = g\left(\frac{1}{x} + 2\right) = \frac{1}{1/x + 2 - 2} = \frac{1}{1/x} = x.$$

Thus, $g \circ f = i_A$. Similarly, for any $x \in B$,

$$f(g(x)) = f\left(\frac{1}{x-2}\right) = \frac{1}{1/(x-2)} + 2 = x - 2 + 2 = x,$$

donc $f \circ g \neq i_B$. Par conséquent, comme nous l'avons observé précédemment, f doit être bijectif et sur, et $g = f^{-1}$.

2. En imitant la solution de la partie 1, essayons de trouver une fonction $g : B \rightarrow A$ telle que $g \circ f = i_A$ et $f \circ g = i_B$. Étant donné qu'appliquer f à un nombre met le nombre au carré et que nous voulons que g annule l'effet de f , une hypothèse raisonnable serait de laisser $g(x) = \sqrt{x}$. Voyons si cela fonctionne.

Pour tout $x \in B$ nous avons

$$f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x,$$

donc $f \circ g = i_B$. Mais pour $x \in A$ nous avons

$$g(f(x)) = g(x^2) = \sqrt{x^2},$$

et cela n'est pas toujours égal à x . Par exemple, $g(f(-3)) = \sqrt{(-3)^2} = \sqrt{9} = 3 \neq -3$. Ainsi, $g \circ f = i_A$. Cet exemple illustre que vous devez vérifier les deux $f \circ g = i_B$ et $g \circ f = i_A$. Il est possible que l'un fonctionne mais pas l'autre.

Qu'est-ce qui s'est passé ? Nous savons que si f^{-1} est une fonction de B vers A , alors pour tout $x \in B$, $f^{-1}(x)$ doit être l'unique solution pour y dans l'équation $f(y) = x$. En appliquant la définition de f nous donne $y^2 = x$, donc $y = \pm\sqrt{x}$. Ainsi, il n'y a pas de solution unique pour y dans l'équation $f(y) = x$; il y a deux solutions. Par exemple, lorsque $x = 9$ nous obtenons $y = \pm 3$. En d'autres termes, $f(3) = f(-3) = 9$. Mais cela signifie que f n'est pas bijective ! Ainsi, f^{-1} n'est pas une fonction de B vers A .

Les fonctions qui s'annulent sont fréquentes en mathématiques. Par exemple, si vous connaissez les logarithmes, vous reconnaîtrez les formules $10^{\log x} = x$ et $\log 10^x = x$. (Nous utilisons ici des logarithmes en base 10.) Nous pouvons reformuler ces formules dans le langage de cette section en définissant les fonctions $f: \mathbb{R} \rightarrow \mathbb{R}^+$ et $g: \mathbb{R}^+ \rightarrow \mathbb{R}$ comme suit :

$$f(x) = 10^x, \quad g(x) = \log x.$$

Alors pour tout $x \in \mathbb{R}$ nous avons $g(f(x)) = \log 10^x = x$, et pour tout $x \in \mathbb{R}^+$, $f(g(x)) = 10^{\log x} = x$. Ainsi, $g \circ f = i_{\mathbb{R}}$ et $f \circ g = i_{\mathbb{R}^+}$, donc $g = f^{-1}$. Autrement dit, la fonction logarithme est l'inverse de la fonction « élever 10 à la puissance ».

Nous avons vu un autre exemple de fonctions qui s'annulent dans [la section 4.5](#). Supposons que A soit un ensemble quelconque, soit \mathbb{E} l'ensemble de toutes les relations d'équivalence sur A , et soit \mathcal{P} l'ensemble de toutes les partitions de A . Définissons une fonction $f: \mathbb{E} \rightarrow \mathcal{P}$ par la formule $f(R) = A/R$, et définissons une autre fonction $g: \mathcal{P} \rightarrow \mathbb{E}$ par la formule

$$\begin{aligned} g(\mathcal{F}) &= \text{the equivalence relation determined by } \mathcal{F} \\ &= \bigcup_{X \in \mathcal{F}} (X \times X). \end{aligned}$$

Vous devriez vérifier que la preuve du [théorème 4.5.6](#) montre que $f \circ g = i_{\mathcal{P}}$, et [l'exercice 10 de la section 4.5](#) montre que $g \circ f = i_{\mathbb{E}}$. Ainsi, f est bijectif et sur, et $g = f^{-1}$. Une conséquence intéressante de ceci est que si A a un nombre fini d'éléments, alors nous pouvons dire que le nombre de relations d'équivalence sur A est exactement le même que le nombre de partitions de A , même si nous ne connaissons pas ce nombre.

Exercices

- *1. Soit R la fonction définie dans [l'exercice 2\(c\)](#) de [la section 5.1](#). Dans [l'exercice 2 de la section 5.2](#), vous avez montré que R est bijective et sur, donc $R^{-1}: P \rightarrow P$. Si $p \in P$, quelle est $R^{-1}(p)$?
- 2. Soit F la fonction définie dans [l'exercice 4\(b\)](#) de [la section 5.1](#). Dans [l'exercice 4 de la section 5.2](#), vous avez montré que F est bijective et sur, donc $F^{-1}: B \rightarrow B$. Si $X \in B$, quelle est $F^{-1}(X)$?
- *3. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule

$$f(x) = \frac{2x + 5}{3}.$$

Montrez que f est bijectif et sur, et trouvez une formule pour $f^{-1}(x)$. (Vous pouvez imiter la méthode utilisée dans l'exemple suivant [le théorème 5.3.2](#) ou dans [l'exemple 5.3.6](#).)

4. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = 2x^3 - 3$. Montrez que f est bijectif et sur, et trouvez une formule pour $f^{-1}(x)$.
- *5. Soit $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ défini par la formule $f(x) = 10^{2-x}$. Montrer que f est bijectif et sur, et trouver une formule pour $f^{-1}(x)$.
6. Soit $A = \mathbb{R} \setminus \{2\}$, et soit f la fonction de domaine A définie par la formule

$$f(x) = \frac{3x}{x-2}.$$

- (a) Montrer que f est une fonction bijective de A vers B pour un ensemble $B \subseteq \mathbb{R}$. Quel est l'ensemble B ?
- (b) Trouvez une formule pour $f^{-1}(x)$.
7. Dans l'exemple suivant [le théorème 5.3.4](#), nous avions $f(x) = (x+7)/5$ et avons trouvé que $f^{-1}(x) = 5x - 7$. Soient f_1 et f_2 des fonctions de \mathbb{R} dans \mathbb{R} définies par les formules

$$f_1(x) = x + 7, \quad f_2(x) = \frac{x}{5}.$$

- (a) Montrer que $f = f_2 \circ f_1$.
- (b) Selon la partie 5 du [théorème 4.2.5](#), $f^{-1} = (f_2 \circ f_1)^{-1} = f_1^{-1} \circ f_2^{-1}$. Vérifiez que cela est vrai en calculant $f_1^{-1} \circ f_2^{-1}$ directement.
8. (a) Démontrez la deuxième moitié du [théorème 5.3.2](#) en imitant la preuve de la première moitié.
- (b) Donnez une preuve alternative de la deuxième moitié du [théorème 5.3.2](#) en appliquant la première moitié à f^{-1} .
- *9. Démontrer la partie 2 du [théorème 5.3.3](#).
10. Utilisez la stratégie suivante pour donner une preuve alternative du [théorème 5.3.5](#) : Soit (b, a) un élément arbitraire de $B \times A$. Supposons que $(b, a) \in g$ et prouvons que $(b, a) \in f^{-1}$. Supposons ensuite que $(b, a) \in f^{-1}$ et prouvons que $(b, a) \in g$.
11. Supposons que $f: A \rightarrow B$ et $g: B \rightarrow A$
 - (a) Démontrer que si f est bijectif et $f \circ g = i_B$, alors $g = f^{-1}$.
 - (b) Démontrer que si f est sur et $g \circ f = i_A$, alors $g = f^{-1}$.
 - (c) Démontrer que si $f \circ g = i_B$ mais $g \circ f = i_A$, alors f est sur mais pas bijectif, et g est bijectif mais pas sur.

12. Supposons que $f: A \rightarrow B$ et que f soit bijectif. Démontrer qu'il existe un ensemble $B \subseteq A$ tel que $f^{-1}: B \rightarrow A$.
13. Supposons que $f: A \rightarrow B$ et que f soit sur. Soit $R = \{(x, y) \in A \times A \mid f(x) = f(y)\}$. D'après [l'exercice 20\(a\)](#) de [la section 5.1](#), R est une relation d'équivalence sur A .
- (a) Démontrer qu'il existe une fonction $h: A/R \rightarrow B$ telle que pour tout $x \in A$, $h([x]_R) = f(x)$. (Indice : voir [l'exercice 21](#) de [la section 5.1](#).)
 - (b) Démontrer que h est bijectif et sur. (Indice : voir [l'exercice 19](#) de [la section 5.2](#).)
 - (c) Il résulte de la partie (b) que $h^{-1}: B \rightarrow A/R$. Démontrer que pour tout $b \in B$, $h^{-1}(b) = \{x \in A \mid f(x) = b\}$.
 - (d) Supposons $g: B \rightarrow A$. Démontrer que $f \circ g = i_B$ ssi $\forall b \in B (g(b) \in h^{-1}(b))$.
14. Supposons $f: A \rightarrow B$, $g: B \rightarrow A$ et $f \circ g = i_B$. Soit $A' = \text{Ran}(g) \subseteq A$.
- (a) Démontrer que pour tout $x \in A'$, $(g \circ f)(x) = x$.
 - (b) Démontrer que $f|_{A'}$ est une fonction bijective de A' vers B et que $g = (f|_{A'})^{-1}$. (Voir [l'exercice 7](#) de [la section 5.1](#) pour la signification de la notation utilisée ici.)
15. Soit $B = \{x \in \mathbb{R} \mid x \geq 0\}$. Let $f: \mathbb{R} \rightarrow B$ and $g: B \rightarrow \mathbb{R}$ défini par les formules $f(x) = x^2$ and $g(x) = \sqrt{x}$. Comme nous l'avons vu dans la partie 2 de [l'exemple 5.3.6](#), $g \neq f^{-1}$. Montrer que $g = (f|_B)^{-1}$. (Indice : Voir [exercice 14](#).)
16. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = 4x - x^2$. Soit $B = \text{Ran}(f)$.
- (a) Trouvez B .
 - (b) Trouvez un ensemble $A \subseteq \mathbb{R}$ tel que $f|_A$ soit une fonction bijective de A à, et trouvez une formule pour $(f|_A)^{-1}(x)$. (Indice : voir [l'exercice 14](#).)
17. Supposons que A soit un ensemble, et que $\mathcal{F} = \{f \mid f: A \rightarrow A\}$ et $\mathcal{P} = \{f \in \mathcal{F} \mid f \text{ est bijectif et sur}\}$. Définissons une relation R sur \mathcal{F} comme suit :
- $$R = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \exists h \in \mathcal{P} (f = h^{-1} \circ g \circ h)\}.$$
- (a) Démontrer que R est une relation d'équivalence.
 - (b) Démontrer que si $f R g$ alors $(f \circ f) R (g \circ g)$.
 - (c) Pour tout $f \in \mathcal{F}$ et $a \in A$, si $f(a) = a$ alors on dit que a est une *constante fixe point* de f . Démontrer que si f a un point fixe et $f R g$, alors g a aussi un point fixe.
18. Supposons que $f: A \rightarrow C$, $g: B \rightarrow C$ et que g soit bijectif et sur. Démontrer qu'il existe une fonction $h: A \rightarrow B$ telle que $g \circ h = f$.

5.4 Fermetures

En mathématiques, on travaille souvent avec une fonction d'un ensemble vers lui-même. Dans ce cas, le concept suivant peut s'avérer utile.

Définition 5.4.1. Supposons $f: A \rightarrow A$ et $C \subseteq A$. On dira que C est fermé par f si $\forall x \in C (f(x) \in C)$.

Exemple 5.4.2.

1. Soit $A = \{a, b, c, d\}$ et $f = \{(a, c), (b, b), (c, d), (d, c)\}$. Alors $f: A \rightarrow A$. Soit $C_1 = \{a, c, d\}$ et $C_2 = \{a, b\}$. C_1 est-il fermé par f ? C_2 est-il?
2. Soient $f: \mathbb{R} \rightarrow \mathbb{R}$ et $g: \mathbb{R} \rightarrow \mathbb{R}$ définis par les formules $f(x) = x + 1$ et $g(x) = x - 1$. \mathbb{N} est-il fermé sous f ? Est-il fermé sous g ?
3. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = x^2$. Soient $C_1 = \{x \in \mathbb{R} \mid 0 < x < 1\}$ et $C_2 = \{x \in \mathbb{R} \mid 0 < x < 2\}$. C_1 est-il fermé sous f ? C_2 est-il?

Solutions

1. L'ensemble C_1 est fermé par f , car $f(a) = f(d) = c \in C_1$ et $f(c) = d \in C_1$. Cependant, C_2 n'est pas fermé par f , car $a \in C_2$ mais $f(a) = c \notin C_2$.
2. Pour tout entier naturel n , $n + 1$ est aussi un entier naturel, donc \mathbb{N} est fermé par f . Cependant, \mathbb{N} n'est pas fermé par g , car $0 \in \mathbb{N}$ mais $g(0) = -1 \notin \mathbb{N}$.
3. Pour tout nombre réel x , si $0 < x < 1$ alors $0 < x^2 < 1$ (voir [exemple 3.1.2](#)), donc C_1 est fermé sous f . Mais $1,5 \in C_2$ et $f(1,5) = 1,5^2 = 2,25 \notin C_2$, donc C_2 n'est pas fermé sous f .

Nous avons vu dans la partie 2 de [l'exemple 5.4.2](#) que \mathbb{N} n'est pas fermé sous la fonction $g: \mathbb{R} \rightarrow \mathbb{R}$ définie par la formule $g(x) = x - 1$. Supposons que nous voulions ajouter des éléments à \mathbb{N} pour obtenir un ensemble fermé par g . Puisque $0 \in \mathbb{N}$, il faudrait ajouter $g(0) = -1$. Mais si -1 était ajouté à l'ensemble, il devrait aussi contenir $g(-1) = -2$, et si on ajoutait -2 , il faudrait aussi ajouter $g(-2) = -3$. En continuant ainsi, il devrait être clair qu'il faudrait ajouter tous les entiers négatifs à \mathbb{N} , ce qui nous donnerait l'ensemble de tous les entiers, \mathbb{Z} . Mais notez que \mathbb{Z} est fermé par g , car pour tout entier n , $n - 1$ est aussi un entier.

Nous avons donc réussi notre tâche d'élargissement de \mathbb{N} pour obtenir un ensemble fermé par g .

Lorsque nous avons élargi \mathbb{N} à \mathbb{Z} , les nombres que nous avons ajoutés – les entiers négatifs – étaient des nombres qui *devaient* être ajoutés si nous voulions que l'ensemble résultant soit fermé par g . Il s'ensuit que \mathbb{Z} est le plus petit ensemble contenant \mathbb{N} qui soit fermé par g . Nous utilisons ici le mot *plus petit* exactement comme nous l'avons défini dans [la section 4.4](#). Si nous posons $\mathcal{F} = \{ C \subseteq \mathbb{R} \mid \mathbb{N} \subseteq C \text{ et que } C \text{ est fermé par } g \}$, alors \mathbb{Z} est le plus petit élément de \mathcal{F} , où comme d'habitude il est entendu que nous entendons plus petit au sens de l'ordre partiel des sous-ensembles. En d'autres termes, \mathbb{Z} est un élément de \mathcal{F} , et c'est un sous-ensemble de tout élément de \mathcal{F} . Nous dirons que \mathbb{Z} est la *fermeture* de \mathbb{N} par g .

Définition 5.4.3. Supposons $f: A \rightarrow A$ et $B \subseteq A$. Alors, la *fermeture* de B par f est le plus petit ensemble $C \subseteq A$ tel que $B \subseteq C$ et C soit fermé par f , s'il existe un tel plus petit ensemble. Autrement dit, un ensemble $C \subseteq A$ est la fermeture de B par f s'il possède les propriétés suivantes :

1. $B \subseteq C$.
2. C est fermé sous f .
3. Pour tout ensemble $D \subseteq A$, si $B \subseteq D$ et D est fermé sous f alors $C \subseteq D$.

D'après [le théorème 4.4.6](#), si un ensemble possède un plus petit élément, il ne peut en posséder qu'un seul. Ainsi, si un ensemble B possède une fermeture sous une fonction f , cette fermeture doit être unique ; il est donc logique de l'appeler *la* fermeture plutôt qu'*une* *fermeture*. Cependant, comme nous l'avons vu dans [l'exemple 4.4.7](#), certaines familles d'ensembles n'ont pas de plus petits éléments ; il n'est donc pas évident que les ensembles possèdent toujours des fermetures sous des fonctions. En fait, c'est le cas, comme nous le montrerons dans la preuve du [théorème 5.4.5](#) ci-dessous. Mais examinons d'abord quelques exemples supplémentaires de fermetures.

Exemple 5.4.4.

1. Dans la partie 1 de [l'exemple 5.4.2](#), l'ensemble $C_2 = \{a, b\}$ n'était pas fermé par f . Quelle est la fermeture de C_2 par f ?
2. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = x + 1$, et soit $B = \{0\}$. Quelle est la fermeture de B par f ?

Solutions

1. Puisque $a \in C_2$, pour obtenir un ensemble fermé par f , il faut ajouter $f(a) = c$. Mais il faut alors ajouter $f(c) = d$, ce qui nous donne l'ensemble $A = \{a, b, c, d\}$. Il est clair que A est fermé par f , donc la fermeture de C_2 par f est A .
2. Puisque $0 \in B$, la fermeture de B sous f doit contenir $f(0) = 1$. Mais alors elle doit aussi contenir $f(1) = 2, f(2) = 3, f(3) = 4$, et en fait tous les entiers positifs. En ajoutant tous les entiers positifs à B , on obtient l'ensemble \mathbb{N} , dont nous savons déjà, d'après la partie 2 de [l'exemple 5.4.2](#), qu'il est fermé sous f . Ainsi, la fermeture de $\{0\}$ sous f est \mathbb{N} .

Voici un exemple qui illustre l'utilité des concepts que nous avons discutés. Soit P un ensemble de personnes, et supposons que chaque personne de l'ensemble P ait un meilleur ami qui soit également dans P . Alors nous pouvons définir une fonction $f : P \rightarrow P$ par soit $f(p) =$ meilleur ami de p . *Supposons que chaque fois qu'une personne de l'ensemble P entend un ragots, elle le raconte à son meilleur ami (mais à personne d'autre).* Considérons maintenant un ensemble quelconque $C \subseteq P$, et supposons que C soit fermé par f . Alors pour toute personne $p \in C$, le meilleur ami de p est également dans C . Ainsi, si une personne dans C entend un ragots, la seule personne à qui elle le racontera est également dans C . Personne dans C ne transmettra jamais de ragots à une personne qui n'est pas dans C . Ainsi, si nous racontons un petit potin à certaines personnes de C , *il peut se propager à d'autres personnes de C* , mais il ne quittera jamais C . Si vous voulez suivre la propagation des potins dans cette population, vous devriez être intéressé à reconnaître quels sous-ensembles de P sont fermés sous f .

Supposons que nous racontions un commérage à tous les habitants d'un ensemble $B \subseteq P$. Comment ce commérage se propagera-t-il ? Les habitants de B en parleront à leurs meilleurs amis, qui en parleront à leur tour à leurs meilleurs amis, et ainsi de suite. D'après nos exemples précédents, on peut supposer que l'ensemble H des personnes qui entendront finalement le commérage constituera la fermeture de B sous f . Voyons si nous pouvons démontrer avec précision que H possède les trois propriétés énumérées dans [la définition 5.4.3](#).

Français Clairement $B \subseteq H$, puisque les gens de B entendent les ragots dès le début du processus. Ceci confirme la propriété 1 de [la Définition 5.4.3](#). Si p est un élément de H , alors p finit par entendre les ragots. Mais dès que p entend les ragots, il ou elle en parlera à $f(p)$, donc $f(p) \in H$ également. Ainsi H est fermé sous f , comme l'exige la propriété 2 de la définition. Finalement, supposons que $B \subseteq C \subseteq P$ et que C soit fermé sous f . Alors comme nous l'avons observé précédemment, tout ragots raconté aux gens de B peut se propager à d'autres dans C , mais il ne quittera jamais C . Ainsi, toute personne qui

entend les ragots doit appartenir à C , ce qui signifie que $H \subseteq C$. Ceci confirme la propriété 3, donc H est bien la fermeture de B sous f .

Nous passons maintenant à la preuve que les fermetures existent toujours. Supposons $f : A \rightarrow A$ et $B \subseteq A$. Une façon d'essayer de prouver l'existence de la fermeture de B sous f est d'ajouter à B les éléments qui doivent être ajoutés pour le rendre fermé sous f , comme nous l'avons fait dans les exemples précédents, puis de prouver que le résultat est fermé sous f . Bien que cela soit possible, un traitement minutieux des détails de cette preuve nécessiterait la méthode d'induction mathématique, que nous n'avons pas encore abordée. Nous présenterons cette preuve dans [la section 6.5](#), après avoir discuté de l'induction mathématique. Mais il existe une autre approche de la preuve qui utilise uniquement des idées que nous avons déjà étudiées. Nous savons que la fermeture de B sous f , si elle existe, doit être le plus petit élément de la famille $\mathcal{F} = \{C \subseteq A \mid B \subseteq C \text{ et } C \text{ est fermé sous } f\}$.

D'après [l'exercice 20 de la section 4.4](#), le plus petit élément d'un ensemble est aussi toujours la plus grande borne inférieure de l'ensemble, et d'après [le théorème 4.4.11](#), le glb de toute famille non vide d'ensembles \mathcal{F} est $\bigcap \mathcal{F}$. C'est la motivation de notre prochaine preuve.

Théorème 5.4.5. *Supposons que $f : A \rightarrow A$ et $B \subseteq A$. Alors B a une fermeture sous f .*

Preuve. Soit $\mathcal{F} = \{C \subseteq A \mid B \subseteq C \text{ et } C \text{ est fermé par } f\}$. On devrait pouvoir vérifier que $A \in \mathcal{F}$, et donc $\mathcal{F} \neq \emptyset$. Ainsi, on peut poser $C = \bigcap \mathcal{F}$ et par [l'exercice 9 de la section 3.3](#), $C \subseteq A$. On montrera que C est la fermeture de B par f en prouvant les trois propriétés de [la définition 5.4.3](#).

Pour prouver la première propriété, supposons $x \in B$. Soit D un élément arbitraire de \mathcal{F} . Alors par définition de \mathcal{F} , $B \subseteq D$, donc $x \in D$. Puisque D était arbitraire, cela montre que $\forall D \in \mathcal{F} (x \in D)$, donc $x \in \bigcap \mathcal{F} = C$. Ainsi, $B \subseteq C$.

Ensuite, supposons $x \in C$ et soit à nouveau D un élément arbitraire de \mathcal{F} . Alors puisque $x \in C = \bigcap \mathcal{F}, x \in D$. Mais puisque $D \in \mathcal{F}$, D est fermé par f , donc $f(x) \in D$. Puisque D était arbitraire, nous pouvons conclure que $\forall D \in \mathcal{F} (f(x) \in D)$, donc $f(x) \in \bigcap \mathcal{F} = C$. Ainsi, nous avons montré que C est fermé par f , ce qui est la deuxième propriété de [la définition 5.4.3](#).

Enfin, pour démontrer la troisième propriété, supposons que $B \subseteq D \subseteq A$ et que D soit fermé sous f . Alors $D \in \mathcal{F}$, et en appliquant à nouveau [l'exercice 9 de la section 3.3](#), nous pouvons conclure que $C = \bigcap \mathcal{F} \subseteq D$. \square

Commentaire. Notre objectif est $\exists C$ (C est la fermeture de B par f), nous devons donc commencer par définir C . Cependant, cette définition $C = \cap \mathcal{F}$ n'a de sens que si nous savons que $\mathcal{F} \neq \emptyset$; il faut donc d'abord le prouver. Puisque $\mathcal{F} \neq \emptyset$ signifie $\exists D$ ($D \in \mathcal{F}$), nous le prouvons en donnant un exemple d'élément de \mathcal{F} . L'exemple est A ; nous devons donc prouver que $A \in \mathcal{F}$. L'affirmation de la démonstration selon laquelle « vous devriez pouvoir vérifier » que $A \in \mathcal{F}$ signifie bien que vous devriez le faire. La vérification. Selon la définition de \mathcal{F} , dire que $A \in \mathcal{F}$ signifie que $A \subseteq A$, $B \subseteq A$ et A est fermé sous f . Assurez-vous de bien comprendre pourquoi ces trois affirmations sont vraies.

Après avoir défini C et vérifié que $C \subseteq A$, nous devons prouver que C a les trois propriétés de la définition de la fermeture de B par f . Pour prouver la première affirmation, $B \subseteq C$, nous posons x un élément arbitraire de B et prouvons $x \in C$. Puisque $C = \cap \mathcal{F}$, le but $x \in C$ signifie $\forall D \in \mathcal{F}(x \in D)$, donc pour le prouver nous posons D un élément arbitraire de \mathcal{F} et prouvons $x \in D$. Pour prouver que C est fermé par f , nous supposons que $x \in C$ et prouvons $f(x) \in C$. De nouveau, par la définition de C ce but signifie $\forall D \in \mathcal{F}(f(x) \in D)$, donc nous posons D un élément arbitraire de \mathcal{F} et prouvons $f(x) \in D$. Enfin, pour prouver le troisième objectif, nous supposons que $D \subseteq A$, $B \subseteq D$ et D est fermé sous f et prouvons $C \subseteq D$. Heureusement, un exercice d'une section précédente prend en charge cette preuve.

Les ensembles fermés et les fermetures apparaissent également dans l'étude des fonctions de plus d'une variable. Si $f: A \times A \rightarrow A$, alors f est dite une *fonction à deux variables*. Un élément du domaine de f serait une paire ordonnée (x, y) , où $x, y \in A$. Le résultat de l'application de f à cette paire devrait s'écrire $f((x, y))$, mais il est courant d'omettre une paire de parenthèses et d'écrire simplement $f(x, y)$.

Définition 5.4.6. Supposons $f: A \times A \rightarrow A$ et $C \subseteq A$. On dira que C est *fermé par f* si $\forall x \in C \forall y \in C (f(x, y) \in C)$.

Exemple 5.4.7.

- Soient $f: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ et $g: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ définis par les formules $f(x, y) = x/y$ et $g(x, y) = x^y \cdot \mathbb{Q}^+$ est-il fermé sous f ? Est-il fermé sous g ?

2. Soit $f: \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ et $g: \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ définis par les formules $f(X, Y) = X \cup Y$ et $g(X, Y) = X \cap Y$. Soit $\mathcal{I} = \{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ est infini}\}$. \mathcal{I} est-il fermé par f ? Est-il fermé par g ?

Solutions

1. Si $x, y \in \mathbb{Q}^+$, alors il existe des entiers positifs p, q, r et s tels que $x = p/q$ et $y = r/s$. Par conséquent

$$f(x, y) = \frac{x}{y} = \frac{p/q}{r/s} = \frac{p}{q} \cdot \frac{s}{r} = \frac{ps}{qr} \in \mathbb{Q}^+.$$

Ceci montre que \mathbb{Q}^+ est fermé sous f . Cependant, 2 et $1/2$ sont des éléments de \mathbb{Q}^+ et $g(2, 1/2) = 2^{1/2} = \sqrt{2} \notin \mathbb{Q}^+$ (voir [théorème 6.4.5](#)), donc \mathbb{Q}^+ n'est pas fermé sous g .

2. Si X et Y sont des ensembles infinis d'entiers naturels, alors $f(X, Y) = X \cup Y$ est aussi infini, donc \mathcal{I} est fermé par f . D'autre part, soit E l'ensemble des entiers naturels pairs et P l'ensemble des nombres premiers. Alors E et P sont tous deux infinis, mais $g(E, P) = E \cap P = \{2\}$, qui est fini. Par conséquent, \mathcal{I} n'est pas fermé par g .

Comme précédemment, nous pouvons définir la fermeture d'un ensemble sous une fonction de deux variables comme étant le plus petit ensemble fermé le contenant, et nous pouvons prouver que de telles fermetures existent toujours.

Définition 5.4.8. Supposons $f: A \times A \rightarrow A$ et $B \subseteq A$. Alors, la *fermeture de B par f* est le plus petit ensemble $C \subseteq A$ tel que $B \subseteq C$ et C soit fermé par f , s'il existe un tel plus petit ensemble. Autrement dit, un ensemble $C \subseteq A$ est la fermeture de B par f si il possède les propriétés suivantes :

1. $B \subseteq C$.
2. C est fermé sous f .
3. Pour tout ensemble $D \subseteq A$, si $B \subseteq D$ et D est fermé sous f alors $C \subseteq D$.

Théorème 5.4.9. Supposons que $f: A \times A \rightarrow A$ et $B \subseteq A$. Alors B a une fermeture sous f .

Preuve. Voir [exercice 11](#). \square

Une fonction de $A \times A$ vers A pourrait être considérée comme une opération qui peut être appliquée à une paire d'objets $(x, y) \in A \times A$

pour produire un autre élément de A . Souvent, en mathématiques, une opération à effectuer sur une paire d'objets mathématiques (x, y) est représentée par un symbole que nous écrivons entre x et y . Par exemple, si x et y sont des nombres réels alors $x + y$ désigne un autre nombre, et si x et y sont des ensembles alors $x \cup y$ est un autre ensemble. Imitant cette notation, lorsque les mathématiciens définissent une fonction de $A \times A$ vers A ils la représentent parfois avec un symbole plutôt qu'une lettre, et ils écrivent le résultat de l'application de la fonction à une paire (x, y) en plaçant le symbole entre x et y , plutôt qu'en mettant une lettre avant (x, y). Lorsqu'une fonction de $A \times A$ vers A est écrite de cette manière, elle est généralement appelée une *opération binaire sur A* .

Par exemple, dans la partie 2 de [l'exemple 5.4.7](#), nous avons défini $g : \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ par la formule $g(X, Y) = X \cap Y$. Au lieu d'introduire le nom g pour cette fonction, nous aurions pu parler de \cap comme d'une opération binaire sur $\mathcal{P}(\mathbb{N})$. Nous avons montré dans l'exemple que l'ensemble \mathcal{I} des sous-ensembles infinis de \mathbb{N} n'est pas fermé par g . Une autre façon de dire cela est que \mathcal{I} n'est pas fermé par l'opération binaire \cap . Quelle est la fermeture de \mathcal{I} par \cap ? Pour la réponse, voir [l'exercice 16](#).

Voici un autre exemple. On pourrait définir une opération binaire $*$ sur \mathbb{Z} en disant que pour tout entier x et y , $x * y = x^2 - y^2$. L'ensemble $\{0, 1\}$ est-il fermé par l'opération binaire $*$? La réponse est non, car $0 * 1 = 0^2 - 1^2 = -1 \notin \{0, 1\}$. Ainsi, la fermeture de $\{0, 1\}$ par $*$ doit inclure -1 . Mais comme on peut facilement le vérifier, $\{-1, 0, 1\}$ est fermé par $*$. Par conséquent, la fermeture de $\{0, 1\}$ par $*$ est $\{-1, 0, 1\}$.

Exercices

*1. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = (x + 1)/2$. Les ensembles suivants sont-ils fermés par f ?

- (a) \mathbb{Z} .
- (b) \mathbb{Q} .
- (c) $\{x \in \mathbb{R} \mid 0 \leq x < 4\}$.
- (d) $\{x \in \mathbb{R} \mid 2 \leq x < 4\}$.

2. Soit $f: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ défini par la formule $f(X) = X \cup \{17\}$. Les ensembles suivants sont-ils fermés par f ?

- (a) $\{X \subseteq \mathbb{N} \mid X \text{ est infini}\}$.
- (b) $\{X \subseteq \mathbb{N} \mid X \text{ est fini}\}$.
- (c) $\{X \subseteq \mathbb{N} \mid X \text{ a au plus } 100 \text{ éléments}\}$.
- (d) $\{X \subseteq \mathbb{N} \mid 17 \in X\}$.

*3. Soit $f: \mathbb{Z} \rightarrow \mathbb{Z}$ défini par la formule $f(n) = n^2 - n$. Trouver la fermeture de $\{-1, 1\}$ sous f .

4. Pour tout ensemble A , l'ensemble des relations sur A est $\mathcal{P}(A \times A)$.

Soit $f: \mathcal{P}(A \times A) \rightarrow \mathcal{P}(A \times A)$ défini par la formule $f(R) = R^{-1}$. L'ensemble des relations réflexives sur A est-il fermé par f ? Qu'en est-il de l'ensemble des relations symétriques et de l'ensemble des relations transitives? (Indice : Voir [l'exercice 12 de la section 4.3.](#))

5. Supposons $f: A \rightarrow A$. \emptyset est-il fermé sous f ?

6. Supposons $f: A \rightarrow A$.

- (a) Démontrer que si $\text{Ran}(f) \subseteq C \subseteq A$ alors C est fermé sous f .
- (b) Démontrer que pour tout ensemble $B \subseteq A$, la fermeture de B sous f est un sous-ensemble de $B \cup \text{Ran}(f)$.

*7. Supposons que $f: A \rightarrow A$ et que f soit bijectif et sur. Alors, par [le théorème 5.3.1](#), $f^{-1}: A \rightarrow A$. Démontrer que si $C \subseteq A$ et C est fermé par f , alors $A \setminus C$ est fermé par f^{-1} .

8. Supposons $f: A \rightarrow A$ et $C \subseteq A$. Démontrer que C est fermé par f ssi la fermeture de C par f est C .

*9. Supposons que $f: A \rightarrow A$ et C_1 et C_2 sont des sous-ensembles de A qui sont fermés sous f .

- (a) Démontrer que $C_1 \cup C_2$ est fermé sous f .
- (b) $C_1 \cap C_2$ doit-il être fermé sous f ? Justifiez votre réponse.
- (c) $C_1 \setminus C_2$ doit-il être fermé sous f ? Justifiez votre réponse.

10. Supposons $f: A \rightarrow A$, $B_1 \subseteq A$ et $B_2 \subseteq A$. Soit C_1 la fermeture de B_1 par f , et soit C_2 la fermeture de B_2 .

- (a) Démontrer que si $B_1 \subseteq B_2$ alors $C_1 \subseteq C_2$.
- (b) Démontrer que la fermeture de $B_1 \cup B_2$ sous f est $C_1 \cup C_2$.
- (c) La fermeture de $B_1 \cap B_2$ doit-elle être $C_1 \cap C_2$? Justifiez votre réponse.
- (d) La fermeture de $B_1 \setminus B_2$ doit-elle être $C_1 \setminus C_2$? Justifiez votre réponse.

11. Démontrer [le théorème 5.4.9](#).

12. Si \mathcal{F} est un ensemble de fonctions de A dans A et $C \subseteq A$, alors nous dirons que C est *fermé par \mathcal{F}* si $\forall f \in \mathcal{F} \forall x \in C (f(x) \in C)$. Autrement dit, C est fermé par \mathcal{F} si pour tout $f \in \mathcal{F}$, C est fermé par f . Si $B \subseteq A$, alors la *fermeture* de B par \mathcal{F} est le plus petit ensemble $C \subseteq A$ tel que $B \subseteq C$ et C soit fermé par \mathcal{F} . (L'exercice suivant vous demandera de prouver que la fermeture existe toujours.)

- (a) Soient f et g les fonctions de \mathbb{R} dans \mathbb{R} définies par les formules $f(x) = x + 1$ et $g(x) = x - 1$. Trouvez la fermeture de $\{0\}$ sous $\{f, g\}$.
- (b) Pour chaque entier naturel n , soit $f_n: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ défini par la formule $f_n(X) = X \cup \{n\}$, et soit $\mathcal{F} = \{f_n \mid n \in \mathbb{N}\}$. Trouvez la fermeture de $\{\emptyset\}$ sous \mathcal{F} .

13. Supposons que \mathcal{F} soit un ensemble de fonctions de A vers A et $B \subseteq A$.

Voir l'exercice précédent pour la définition de la fermeture de B sous \mathcal{F} .

- (a) Démontrer que B a une fermeture sous \mathcal{F} .

Pour chaque $f \in \mathcal{F}$, soit C_f la fermeture de B sous f , et soit C la fermeture de B sous \mathcal{F} .

- (b) Prouver que $\bigcup_{f \in \mathcal{F}} C_f \subseteq C$
- (c) Doit $\bigcup_{f \in \mathcal{F}} C_f$ être fermé sous \mathcal{F} ? Justifiez votre réponse avec une preuve ou un contre-exemple.

- (d) Vous devez justifier votre réponse avec une preuve ou un contre-exemple.

14. Soit $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x, y) = x - y$. Quelle est la fermeture de \mathbb{N} sous f ?

15. Soit $f: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ défini par la formule $f(x, y) = x / y$. Quelle est la fermeture de \mathbb{Z}^+ sous f ?

16. Comme dans la partie 2 de [l'exemple 5.4.7](#), soit $\mathcal{I} = \{X \in \mathcal{P}(\mathbb{N}) \mid X$ est infini $\}$.

(a) Démontrer que pour tout ensemble $X \subseteq \mathbb{N}$ il existe des ensembles $Y, Z \in \mathcal{I}$ tels que $Y \cap Z = X$.

(b) Quelle est la fermeture de \mathcal{I} sous l'opération binaire \cap ?

17. Soit $\mathcal{F} = \{f \mid f: \mathbb{R} \rightarrow \mathbb{R}\}$. Alors pour tout $f, g \in \mathcal{F}, f \circ g \in \mathcal{F}$, donc \circ est une opération binaire sur \mathcal{F} . Les ensembles suivants sont-ils fermés par \circ ?

(a) $\{f \in \mathcal{F} \mid f \text{ est bijectif}\}$. (Indice : voir [le théorème 5.2.5.](#))

(b) $\{f \in \mathcal{F} \mid f \text{ est sur}\}$.

(c) $\{f \in \mathcal{F} \mid f \text{ est strictement croissante}\}$. (Une fonction $f: \mathbb{R} \rightarrow \mathbb{R}$ est *strictement croissante* si $\forall x \in \mathbb{R} \forall y \in \mathbb{R} (x < y \rightarrow f(x) < f(y))$.)

(d) $\{f \in \mathcal{F} \mid f \text{ est strictement décroissante}\}$. (Une fonction $f: \mathbb{R} \rightarrow \mathbb{R}$ est *strictement décroissante* si $\forall x \in \mathbb{R} \forall y \in \mathbb{R} (x < y \rightarrow f(x) > f(y))$.)

18. Soit $\mathcal{F} = \{f \mid f: \mathbb{R} \rightarrow \mathbb{R}\}$. Si $f, g \in \mathcal{F}$, alors on définit la fonction $f + g: \mathbb{R} \rightarrow \mathbb{R}$ par la formule $(f + g)(x) = f(x) + g(x)$. Notons que $+$ est une opération binaire sur \mathcal{F} . Les ensembles suivants sont-ils fermés par $+$?

(a) $\{f \in \mathcal{F} \mid f \text{ est bijectif}\}$.

(b) $\{f \in \mathcal{F} \mid f \text{ est sur}\}$.

(c) $\{f \in \mathcal{F} \mid f \text{ est strictement croissante}\}$. (Voir l'exercice précédent pour la définition de strictement croissante.)

(d) $\{f \in \mathcal{F} \mid f \text{ est strictement décroissante}\}$. (Voir l'exercice précédent pour la définition de strictement décroissante.)

19. Pour tout ensemble A , l'ensemble des relations sur A est $\mathcal{P}(A \times A)$, et \circ est une opération binaire sur $\mathcal{P}(A \times A)$. L'ensemble des relations réflexives sur A est-il fermé par \circ ? Qu'en est-il de l'ensemble des relations symétriques et de l'ensemble des relations transitives ?

20. La division n'est pas une opération binaire sur \mathbb{R} , car on ne peut pas diviser par 0. Mais nous pouvons résoudre ce problème. Commençons par ajouter un nouvel élément à \mathbb{R} . Nous l'appellerons « NaN » (pour « Not a Number »). Soit $\bar{\mathbb{R}} = \mathbb{R} \cup \{\text{NaN}\}$ et définir $f: \bar{\mathbb{R}} \times \bar{\mathbb{R}} \rightarrow \bar{\mathbb{R}}$ comme suit :

$$f(x, y) = \begin{cases} x/y, & \text{if } x, y \in \mathbb{R} \text{ and } y \neq 0, \\ \text{NaN}, & \text{otherwise.} \end{cases}$$

Cette notation signifie que si $x, y \in \mathbb{R}$ et $y \neq 0$ alors $f(x, y) = x / y$, et sinon $f(x, y) = \text{NaN}$. Ainsi, par exemple, $f(3, 7) = 3/7$, $f(3, 0) = \text{NaN}$, et $f(\text{NaN}, 7) = \text{NaN}$. Lequel des ensembles suivants est fermé par f ?

- (a) \mathbb{R} .
- (b) \mathbb{R}^+ .
- (c) \mathbb{R}^- .
- (d) \mathbb{Q} .
- (e) $\mathbb{Q} \cup \{\text{NaN}\}$.

21. Si \mathcal{F} est un ensemble de fonctions de $A \times A$ dans A et $C \subseteq A$, alors nous dirons que C est *fermé par \mathcal{F}* si $\forall f \in \mathcal{F} \forall x \in C \forall y \in C (f(x, y) \in C)$. Autrement dit, C est fermé par \mathcal{F} ssi pour tout $f \in \mathcal{F}$, C est fermé par f . Si $B \subseteq A$, alors la *fermeture* de B par \mathcal{F} est le plus petit ensemble $C \subseteq A$ tel que $B \subseteq C$ et C est fermé par \mathcal{F} , s'il existe un tel plus petit ensemble. (Comparer ces définitions à celles de [l'exercice 12.](#))

- (a) Démontrer que la fermeture de B sous \mathcal{F} existe.
- (b) Soit $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ et $g: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ définis par les formules $f(x, y) = x + y$ et $g(x, y) = xy$. Démontrer que la fermeture de $\mathbb{Q} \cup \{\sqrt{2}\}$ avec $\sqrt{2}$ sous{ f joint „ g ”} est l'ensemble $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ et est noté $\mathbb{Q}(\sqrt{2})$. (Cet ensemble est appelé \mathbb{Q})
- (c) Avec f et g définis comme dans la partie (b), quelle est la fermeture de $\mathbb{Q} \cup \{\sqrt[3]{2}\}$ sous { f, g } ?

5.5. Images et images inversées : un projet de recherche

Supposons $f: A \rightarrow B$. Nous avons déjà vu que f peut être considéré comme faisant correspondre chaque élément de A à exactement un élément de B . Dans cette section, nous verrons que f peut également être considéré comme faisant correspondre *des sous-ensembles* de A à des sous-ensembles de B et vice-versa.

Définition 5.5.1. Supposons $f: A \rightarrow B$ et $X \subseteq A$. Alors l' *image* de X par f est l'ensemble $f(X)$ défini comme suit :

$$\begin{aligned} f(X) &= \{f(x) \mid x \in X\} \\ &= \{b \in B \mid \exists x \in X (f(x) = b)\}. \end{aligned}$$

(Notez que l'image de l'ensemble du domaine A sous f est $\{f(a) \mid a \in A\}$, et comme nous l'avons vu dans [la section 5.1](#), c'est la même chose que la plage de f .)

Si $Y \subseteq B$, alors l'*image inverse* de Y par f est l'ensemble $f^{-1}(Y)$ défini comme suit :

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

Notez que la fonction f de [la définition 5.5.1](#) peut ne pas être bijective ou sur-unitaire, et par conséquent f^{-1} peut ne pas être une fonction de B vers A , et pour $y \in B$, la notation « $f^{-1}(y)$ » peut être dénuée de sens. Cependant, même dans ce cas, [la définition 5.5.1](#) attribue toujours un sens à la notation « $f^{-1}(Y)$ » pour $Y \subseteq B$. Si cela vous surprend, revoyez la définition de $f^{-1}(Y)$ et constatez qu'elle ne l'est pas. Ne pas traiter f^{-1} comme une fonction. La définition se réfère uniquement aux résultats de l'application *de* f aux éléments de A , et non à ceux de l'application de f^{-1} aux éléments de B .

Par exemple, soit L la fonction définie dans la partie 3 de [l'exemple 5.1.2](#), qui attribue à chaque ville le pays où elle se situe. Comme dans [l'exemple 5.1.2](#), soit C l'ensemble de toutes les villes et N l'ensemble de tous les pays. Si B est l'ensemble de toutes les villes d'au moins un million d'habitants, alors B est un sous-ensemble de C , et l'image de B sous L serait l'ensemble.

$$\begin{aligned} L(B) &= \{L(b) \mid b \in B\} \\ &= \{n \in N \mid \exists b \in B (L(b) = n)\} \\ &= \{n \in N \mid \text{there is some city with population at least one million that is located in the country } n\}. \end{aligned}$$

Ainsi, $L(B)$ est l'ensemble de tous les pays qui contiennent une ville d'au moins un million d'habitants. Soit maintenant A le sous-ensemble de N constitué de tous les pays d'Afrique. Alors, l'image inverse de A sous L est l'ensemble

$$\begin{aligned} L^{-1}(A) &= \{c \in C \mid L(c) \in A\} \\ &= \{c \in C \mid \text{the country in which } c \text{ is located is in Africa}\}. \end{aligned}$$

Ainsi, $L^{-1}(A)$ est l'ensemble de toutes les villes des pays africains.

Prenons un autre exemple. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = x^2$, et soit $X = \{x \in \mathbb{R} \mid 0 \leq x < 2\}$. Alors

$$f(X) = \{f(x) \mid x \in X\} = \{x^2 \mid 0 \leq x < 2\}.$$

Ainsi, $f(X)$ est l'ensemble des carrés des nombres réels compris entre 0 et 2 (incluant 0 mais non 2). Un instant de réflexion devrait vous convaincre que cet ensemble est $\{x \in \mathbb{R} \mid 0 \leq x < 4\}$. Soit maintenant $Y =$

$\{x \in \mathbb{R} \mid 0 \leq x < 4\}$ et calculons $f^{-1}(Y)$. D'après la définition de l'image inverse,

$$\begin{aligned} f^{-1}(Y) &= \{x \in \mathbb{R} \mid f(x) \in Y\} \\ &= \{x \in \mathbb{R} \mid 0 \leq f(x) < 4\} \\ &= \{x \in \mathbb{R} \mid 0 \leq x^2 < 4\} \\ &= \{x \in \mathbb{R} \mid -2 < x < 2\}. \end{aligned}$$

Vous avez maintenant acquis suffisamment d'expérience en rédaction de preuves pour être prêt à mettre vos compétences en rédaction de preuves au service de questions mathématiques. Ainsi, la majeure partie de cette section sera consacrée à un projet de recherche au cours duquel vous découvrirez par vous-même les réponses à des questions mathématiques fondamentales sur les images et les images inverses. Pour commencer, nous allons trouver la réponse à la première question.

Supposons que $f: A \rightarrow B$, et que W et X soient des sous-ensembles de A . Une question naturelle que vous pourriez vous poser est de savoir si $f(W \cap X)$ doit ou non être le même que $f(W) \cap f(X)$. Il semble plausible que la réponse soit oui, alors voyons si nous pouvons le prouver. Ainsi, notre objectif sera de prouver que $f(W \cap X) = f(W) \cap f(X)$. Comme il s'agit d'une équation entre deux ensembles, nous procédons en prenant un élément arbitraire de chaque ensemble et en essayant de prouver qu'il est un élément de l'autre.

Supposons d'abord que y est un élément arbitraire de $f(W \cap X)$. Par définition de $f(W \cap X)$, cela signifie que $y = f(x)$ pour un certain $x \in W \cap X$. Puisque $x \in W \cap X$, il s'ensuit que $x \in W$ et $x \in X$. Mais maintenant nous avons $y = f(x)$ et $x \in W$, nous pouvons donc conclure que $y \in f(W)$. De même, puisque $y = f(x)$ et $x \in X$, il s'ensuit que $y \in f(X)$. Ainsi, $y \in f(W) \cap f(X)$. Ceci termine la première moitié de la preuve.

Supposons maintenant que $y \in f(W) \cap f(X)$. Alors $y \in f(W)$, donc il existe un $w \in W$ tel que $f(w) = y$, et aussi $y \in f(X)$, donc il existe un $x \in X$ tel que $y = f(x)$. Si seulement nous savions que w et x étaient égaux, nous pourrions conclure que $w = x \in W \cap X$, donc $y = f(x) \in f(W \cap X)$. Mais le mieux que nous puissions faire est de dire que $f(w) = y = f(x)$. Cela devrait vous rappeler la définition de l'injectif. Si nous savions que f était injectif, nous pourrions conclure du fait que $f(w) = f(x)$ que $w = x$, et la preuve serait faite. Mais sans cette information, nous semblons être coincés.

Résumons ce que nous avons découvert. Tout d'abord, la première moitié de la preuve a bien fonctionné, nous pouvons donc certainement dire qu'en général $f(W \cap X) \subseteq f(W) \cap f(X)$. La seconde moitié a fonctionné si nous savions que f était exact, nous pouvons donc aussi dire que si f est exact, alors $f(W \cap X) = f(W) \cap f(X)$. Mais que se passe-t-il si f n'est pas exact ? Il existe peut-être un moyen de corriger

la preuve pour montrer que l'équation $f(W \cap X) = f(W) \cap f(X)$ est toujours vraie même si f n'est pas injective. Mais à présent, vous avez probablement commencé à soupçonner que $f(W \cap X)$ et $f(W) \cap f(X)$ ne sont peut-être pas toujours égales, nous devrions donc peut-être consacrer un peu de temps à essayer de montrer que le théorème proposé est incorrect. En d'autres termes, voyons si nous pouvons trouver un contre-exemple - un exemple d'une fonction f et d'ensembles W et X pour lesquels $f(W \cap X) \neq f(W) \cap f(X)$.

utiliser une fonction non bijective, mais l'examen de notre tentative de preuve nous permet d'en savoir plus. La tentative de preuve que $f(W \cap X) = f(W) \cap f(X)$ a rencontré des difficultés uniquement lorsque W et X contenaient des éléments w et x tels que $w \neq x$ mais $f(w) = f(x)$. Nous devons donc choisir un exemple où cela se produit. Autrement dit, nous devons non seulement nous assurer que f n'est pas bijective, mais aussi que W et X contiennent des éléments qui montrent que f n'est pas bijective.

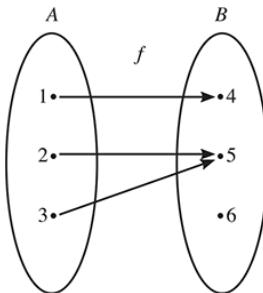


Figure 5.6.

Le graphique de [la figure 5.6](#) illustre une fonction simple qui n'est pas bijective. En l'écrivant comme un ensemble de paires ordonnées, on pourrait dire que $f = \{(1, 4), (2, 5), (3, 5)\}$ et $f: A \rightarrow B$, où $A = \{1, 2, 3\}$ et $B = \{4, 5, 6\}$. Les deux éléments de A qui montrent que f n'est pas bijective sont 2 et 3, donc ils devraient être des éléments de W et X , respectivement. Pourquoi ne pas simplement essayer de poser $W = \{2\}$ et $X = \{3\}$? Avec ces choix, on obtient $f(W) = \{f(2)\} = \{5\}$ et $f(X) = \{f(3)\} = \{5\}$, donc $f(W) \cap f(X) = \{5\} \cap \{5\} = \{5\}$. Mais $f(W \cap X) = f(\emptyset) = \emptyset$, donc $f(W \cap X) \neq f(W) \cap f(X)$. (Si vous ne savez pas pourquoi $f(\emptyset) = \emptyset$, résolvez-le en utilisant [la définition 5.5.1](#) !) Si vous voulez voir un exemple dans lequel $W \cap X \neq \emptyset$, essayez $W = \{1, 2\}$ et $X = \{1, 3\}$.

Cet exemple montre qu'il serait incorrect d'énoncer un théorème affirmant que $f(W \cap X)$ et $f(W) \cap f(X)$ sont toujours égales. Cependant, notre démonstration montre que le théorème suivant est correct :

Théorème 5.5.2. *Supposons que $f: A \rightarrow B$, et que W et X soient des sous-ensembles de A . Alors $f(W \cap X) \subseteq f(W) \cap f(X)$. De plus, si f est bijectif,*

alors $f(W \cap X) = f(W) \cap f(X)$.

Voici maintenant quelques questions auxquelles vous pouvez répondre. Dans chaque cas, essayez de comprendre le plus possible. Justifiez vos réponses avec des preuves et des contre-exemples.

1. Supposons que $f: A \rightarrow B$ et W et X sont des sous-ensembles de A .

- (a) Sera-t-il toujours vrai que $f(W \cup X) = f(W) \cup f(X)$?
- (b) Sera-t-il toujours vrai que $f(W \setminus X) = f(W) \setminus f(X)$?
- (c) Sera-t-il toujours vrai que $W \subseteq X \leftrightarrow f(W) \subseteq f(X)$?

2. Supposons que $f: A \rightarrow B$ et Y et Z sont des sous-ensembles de B .

- (a) Sera-t-il toujours vrai que $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$?
- (b) Sera-t-il toujours vrai que $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$?
- (c) Sera-t-il toujours vrai que $f^{-1}(Y \setminus Z) = f^{-1}(Y) \setminus f^{-1}(Z)$?
- (d) Sera-t-il toujours vrai que $Y \subseteq Z \leftrightarrow f^{-1}(Y) \subseteq f^{-1}(Z)$?

3. Supposons $f: A \rightarrow B$ et $X \subseteq A$. Sera-t-il toujours vrai que $f^{-1}(f(X)) = X$?

4. Supposons $f: A \rightarrow B$ et $Y \subseteq B$. Sera-t-il toujours vrai que $f(f^{-1}(Y)) = Y$?

5. Supposons $f: A \rightarrow A$ et $C \subseteq A$. Démontrer que les affirmations suivantes sont équivalentes :

- (a) C est fermé sous f .
- (b) $f(C) \subseteq C$.
- (c) $C \subseteq f^{-1}(C)$.

6. Supposons $f: A \rightarrow B$ et $g: B \rightarrow C$. Pouvez-vous démontrer des théorèmes intéressants sur les images et les images inverses d'ensembles sous $g \circ f$?

Remarque : Un lecteur attentif aura peut-être remarqué une ambiguïté dans notre notation pour les images et les images inverses. Si $f: A \rightarrow B$ et $Y \subseteq B$, alors nous avons utilisé la notation $f^{-1}(Y)$ pour représenter l'image inverse de Y par f . Mais si f est bijective et sur, alors, comme nous l'avons vu dans [la section 5.3](#), f^{-1} est une fonction de B vers A . Ainsi, $f^{-1}(Y)$ pourrait aussi être interprétée comme l'image de Y par f^{-1} . Heureusement, cette ambiguïté est sans conséquence, comme le montre le problème suivant.

7. Supposons que $f: A \rightarrow B$, f soit bijectif et sur, et $Y \subseteq B$. Montrer que l'image réciproque de Y par f et l'image de Y par f^{-1} sont égales.
(Indice : écrivez d'abord soigneusement les définitions des deux ensembles !)

6

Induction mathématique

6.1. Preuve par induction mathématique

Au [chapitre 3](#), nous avons étudié les techniques de preuve applicables au raisonnement sur n'importe quel sujet mathématique. Dans ce chapitre, nous aborderons une autre technique de preuve, appelée *induction mathématique*, conçue pour prouver des affirmations concernant ce qui est peut-être la structure mathématique la plus fondamentale : les nombres naturels. Rappelons que l'ensemble des nombres naturels est $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Supposons que vous souhaitiez prouver que tout nombre naturel possède une propriété P . Autrement dit, vous souhaitez montrer que 0, 1, 2, etc. possèdent tous la propriété P . Bien sûr, cette liste étant infinie, il est impossible de vérifier individuellement qu'ils possèdent tous la propriété P . L'idée clé de l'induction mathématique est que pour lister tous les nombres naturels, il suffit de commencer par 0 et d'y ajouter 1 à plusieurs reprises. Ainsi, vous pouvez démontrer que tout nombre naturel possède la propriété P en montrant que 0 possède la propriété P , et que chaque fois que vous ajoutez 1 à un nombre possédant la propriété P , le nombre résultant possède également la propriété P . Cela garantirait que, lorsque vous parcourez la liste de tous les nombres naturels, en commençant par 0 et en y ajoutant 1 à plusieurs reprises, chaque nombre rencontré possède nécessairement la propriété P . Autrement dit, tous les nombres naturels possèdent la propriété P . Voici donc comment fonctionne la méthode d'induction mathématique.

Pour prouver un but de la forme $\forall n \in \mathbb{N} P(n)$:

Commencez par prouver $P(0)$, puis prouvez $\forall n \in \mathbb{N} (P(n) \rightarrow P(n+1))$. La première de ces preuves est parfois appelée le *cas de base* et la seconde l'*étape d'induction*.

Forme de l'épreuve finale :

Cas de base : [La preuve de $P(0)$ va ici.]

Étape d'induction : [La preuve de $\forall n \in \mathbb{N} (P(n) \rightarrow P(n+1))$ va ici.]

Nous reviendrons plus tard sur la justification de la méthode d'induction mathématique, mais examinons d'abord un exemple de preuve utilisant l'induction mathématique. La liste de calculs suivante suggère une tendance surprenante :

$$\begin{aligned} 2^0 &= 1 = 2^1 - 1 \\ 2^0 + 2^1 &= 1 + 2 = 3 = 2^2 - 1 \\ 2^0 + 2^1 + 2^2 &= 1 + 2 + 4 = 7 = 2^3 - 1 \\ 2^0 + 2^1 + 2^2 + 2^3 &= 1 + 2 + 4 + 8 = 15 = 2^4 - 1 \end{aligned}$$

Le schéma général semble être le suivant :

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1.$$

Ce modèle est-il valable pour toutes les valeurs de n ? Voyons si nous pouvons le prouver.

Exemple 6.1.1. Démontrer que pour tout nombre naturel n , $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$.

Travail à partir de zéro

Notre objectif est de prouver l'affirmation $\forall n \in \mathbb{N} P(n)$, où $P(n)$ est l'énoncé $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$. Selon notre stratégie, nous pouvons le faire en prouvant deux autres énoncés, $P(0)$ et $\forall n \in \mathbb{N} (P(n) \rightarrow P(n+1))$.

Si $n = 0$, on constate que $P(0)$ est simplement l'énoncé $2^0 = 2^1 - 1$, le premier de nos calculs. La preuve est simple : il suffit de faire le calcul pour vérifier que les deux côtés sont égaux à 1. Le cas de base d'une preuve par induction est souvent très simple, et la seule difficulté pour comprendre la preuve réside dans l'étape d'induction.

Pour l'étape d'induction, nous devons prouver $\forall n \in \mathbb{N} (P(n) \rightarrow P(n+1))$. Bien entendu, toutes les techniques de preuve présentées au [chapitre 3](#) sont applicables aux preuves par induction mathématique. Nous pouvons donc le faire en posant n comme un entier naturel arbitraire, en supposant que $P(n)$ est vraie, puis en prouvant que $P(n+1)$ est vraie. Autrement dit, nous poserons n comme un entier naturel arbitraire, supposerons que $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$, puis prouverons que $2^0 + 2^1 + \cdots + 2^{n+1} = 2^{n+2} - 1$. Ceci nous donne les données et l'objectif suivants :

	<i>Givens</i>	<i>Goal</i>
$n \in \mathbb{N}$	$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$	$2^0 + 2^1 + \cdots + 2^{n+1} = 2^{n+2} - 1$

De toute évidence, la seconde donnée est similaire à l'objectif. Existe-t-il un moyen de partir de la seconde donnée et de déduire l'objectif par des étapes algébriques ? La clé de la preuve consiste à reconnaître que le membre de gauche de l'équation dans le but est exactement le même que le membre de gauche de la seconde donnée, mais avec l'ajout du terme supplémentaire 2^{n+1} . Essayons donc d'ajouter 2^{n+1} aux deux membres de la seconde donnée. Cela nous donne

$$(2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1},$$

ou en d'autres termes,

$$2^0 + 2^1 + \cdots + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1.$$

C'est le but, donc on a fini !

Solution

Théorème. Pour tout nombre naturel n , $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$.

Preuve. Nous utilisons l'induction mathématique.

Cas de base : en définissant $n = 0$, nous obtenons $2^0 = 1 = 2^1 - 1$ comme requis.

Étape d'induction : Soit n un nombre naturel arbitraire et supposons que $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$. Alors

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^{n+1} &= (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} \\ &= (2^{n+1} - 1) + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \\ &= 2^{n+2} - 1. \end{aligned}$$

□

La preuve de [l'exemple 6.1.1](#) vous convainc-elle que l'équation $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$, que nous avons appelée $P(n)$ dans notre travail de base, est vraie pour tous les entiers naturels n ? Eh bien, $P(0)$ est certainement vraie, puisque nous l'avons vérifié explicitement dans le cas de base de la preuve. Dans l'étape d'induction, nous avons montré que $\forall n \in \mathbb{N} (P(n) \rightarrow P(n+1))$, nous savons donc que pour tout entier naturel n , $P(n) \rightarrow P(n+1)$. Par exemple, en remplaçant $n = 0$, nous pouvons conclure que $P(0) \rightarrow P(1)$. Mais maintenant nous savons que $P(0)$ et $P(0) \rightarrow P(1)$ sont tous deux vrais, donc en appliquant le modus ponens, nous pouvons conclure que $P(1)$ est également vrai. De même, en posant $n = 1$ par induction, on obtient $P(1) \rightarrow P(2)$. Ainsi, en appliquant le modus ponens aux affirmations $P(1)$ et $P(1) \rightarrow P(2)$, on peut conclure que $P(2)$ est vraie. En posant $n = 2$ par induction, on

obtient $P(2) \rightarrow P(3)$. Par modus ponens, $P(3)$ est donc vraie. En poursuivant ainsi, vous devriez constater qu'en appliquant plusieurs fois l'induction, vous pouvez démontrer que $P(n)$ doit être vraie pour tout entier naturel n . Autrement dit, la $\text{r}\backslash\text{e}\approx\approx\text{e}$ montre bien que $\forall n \in \mathbb{N} P(n)$.

Comme nous l'avons vu dans le dernier exemple, la partie la plus difficile d'une preuve par induction mathématique est généralement l'étape d'induction, dans laquelle vous devez prouver l'énoncé $\forall n \in \mathbb{N} (P(n) \rightarrow P(n+1))$. Il est généralement préférable de le faire en posant n comme un nombre naturel arbitraire, en supposant que $P(n)$ est vrai, puis en prouvant que $P(n+1)$ est vrai. L'hypothèse que $P(n)$ est vraie est parfois appelée *hypothèse inductive*, et la clé de la preuve est généralement de déterminer une relation entre l'hypothèse inductive $P(n)$ et l'objectif $P(n+1)$.

Voici un autre exemple de preuve par induction mathématique.

Exemple 6.1.2. Démontrer que $\forall n \in \mathbb{N} (3 \mid (n^3 - n))$.

Travail à partir de zéro

Comme d'habitude, le cas de base est facile à vérifier. Les détails sont donnés dans la preuve suivante. Pour l'étape d'induction, soit n un entier naturel arbitraire et supposons que $3 \mid (n^3 - n)$, et nous devons prouver que $3 \mid ((n+1)^3 - (n+1))$. En complétant la définition des *divisions*, nous pouvons résumer notre situation ainsi :

$$\begin{array}{ccc} & \text{Given} & \text{Goal} \\ n \in \mathbb{N} & & \exists j \in \mathbb{Z} (3j = (n+1)^3 - (n+1)) \\ \exists k \in \mathbb{Z} (3k = n^3 - n) & & \end{array}$$

La deuxième hypothèse donnée est l'hypothèse inductive, et nous devons déterminer comment elle peut être utilisée pour établir l'objectif.

Selon nos techniques de traitement des quantificateurs existentiels dans les preuves, la meilleure solution consiste à utiliser la seconde donnée et à considérer k comme un entier tel que $3k = n^3 - n$. Pour achever la preuve, nous devons trouver un entier j (probablement lié à k) tel que $3j = (n+1)^3 - (n+1)$. Nous développons le membre de droite de cette équation afin de trouver un moyen de la relier à l'équation $3k = n^3 - n$:

$$\begin{aligned} (n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= (n^3 - n) + 3n^2 + 3n \\ &= 3k + 3n^2 + 3n \\ &= 3(k + n^2 + n). \end{aligned}$$

Il devrait maintenant être clair que nous pouvons compléter la preuve en posant $j = k + n^2 + n$. Comme dans les preuves précédentes, nous ne prenons pas la peine de mentionner j dans la preuve.

Solution

Théorème. Pour tout nombre naturel n , $3 \mid (n^3 - n)$.

Preuve. Nous utilisons l'induction mathématique.

Cas de base : si $n = 0$, alors $n^3 - n = 0 = 3 \cdot 0$, donc $3 \mid (n^3 - n)$.

Étape d'induction : Soit n un entier naturel arbitraire et supposons $3 \mid (n^3 - n)$. On peut alors choisir un entier k tel que $3k = n^3 - n$. Ainsi,

$$\begin{aligned} (n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= (n^3 - n) + 3n^2 + 3n \\ &= 3k + 3n^2 + 3n \\ &= 3(k + n^2 + n). \end{aligned}$$

Par conséquent $3 \mid ((n+1)^3 - (n+1))$, comme requis.

□

Une fois que vous aurez compris le fonctionnement de l'induction mathématique, vous serez capable de comprendre des démonstrations impliquant de légères variations de la méthode d'induction. L'exemple suivant illustre une telle variation. Dans cet exemple, nous allons essayer de déterminer lequel est le plus grand, n^2 ou 2^n . Examinons quelques valeurs de n :

n	n^2	2^n	Which is larger?
0	0	1	2^n
1	1	2	2^n
2	4	4	tie
3	9	8	n^2
4	16	16	tie
5	25	32	2^n
6	36	64	2^n

La course est serrée au début, mais à partir de $n = 5$, il semble que 2^n *prenne* une avance décisive sur n^2 . Pouvons-nous prouver qu'il conservera l'avantage pour des valeurs de n plus élevées ?

Exemple 6.1.3. Démontrer que $\forall n \geq 5 (2^n > n^2)$.

Travail à partir de zéro

Nous souhaitons uniquement démontrer l'inégalité $2^n > n^2$ pour $n \geq 5$. Par conséquent, utiliser $n = 0$ comme cas de base de notre preuve par induction n'aurait aucun sens. Nous prendrons $n = 5$ comme cas de

base pour notre induction plutôt que $n = 0$. Une fois que nous aurons vérifié que l'inégalité est vraie lorsque $n = 5$, l'étape d'induction montrera que l'inégalité doit rester vraie si, en commençant par $n = 5$, nous ajoutons 1 à n de manière répétée. Ainsi, elle doit également être vraie pour $n = 6, 7, 8$, etc. Autrement dit, nous pourrons conclure que l'inégalité est vraie pour tout $n \geq 5$.

Le cas de base $n = 5$ a déjà été vérifié dans le tableau. Pour l'étape d'induction, nous posons $n \geq 5$ arbitraire, supposons $2^n > n^2$, et essayons de prouver que $2^{n+1} > (n+1)^2$. Comment pouvons-nous relier l'hypothèse inductive au but ? La relation la plus simple implique peut-être les côtés gauches des deux inégalités : $2^{n+1} = 2 \cdot 2^n$. Ainsi, en multipliant les deux côtés de l'hypothèse inductive $2^n > n^2$ par 2, nous pouvons conclure que $2^{n+1} > 2n^2$. Comparons maintenant cette inégalité au but, $2^{n+1} > (n+1)^2$. Si nous pouvions prouver que $2n^2 \geq (n+1)^2$, alors le but suivrait facilement. Oublions donc le but initial et voyons si nous pouvons prouver que $2n^2 \geq (n+1)^2$.

En multipliant le côté droit du nouvel objectif, nous constatons que nous devons prouver que $2n^2 \geq n^2 + 2n + 1$, autrement dit $n^2 \geq 2n + 1$. La preuve est simple : puisque nous avons supposé que $n \geq 5$, il s'ensuit que $n^2 \geq 5n = 2n + 3n > 2n + 1$.

Solution

Théorème. Pour tout nombre naturel $n \geq 5$, $2^n > n^2$.

Preuve. Par induction mathématique.

Cas de base : lorsque $n = 5$ nous avons $2^5 = 32 > 25 = n^2$.

Étape d'induction : Soit $n \geq 5$ arbitraire, et supposons que $2^n > n^2$. Alors

$$\begin{aligned}
 2^{n+1} &= 2 \cdot 2^n \\
 &> 2n^2 && \text{(inductive hypothesis)} \\
 &= n^2 + n^2 \\
 &\geq n^2 + 5n && \text{(since } n \geq 5\text{)} \\
 &= n^2 + 2n + 3n \\
 &> n^2 + 2n + 1 = (n+1)^2.
 \end{aligned}$$

□

Exercices

- *1. Démontrer que pour tout $n \in \mathbb{N}$, $0 + 1 + 2 + \cdots + n = n(n + 1)/2$.
2. Démontrer que pour tout $n \in \mathbb{N}$, $0^2 + 1^2 + 2^2 + \cdots + n^2 = n(n + 1)(2n + 1)/6$.
- *3. Démontrer que pour tout $n \in \mathbb{N}$, $0^3 + 1^3 + 2^3 + \cdots + n^3 = [n(n + 1)/2]^2$.
4. Trouvez une formule pour $1 + 3 + 5 + \cdots + (2n - 1)$, pour $n \geq 1$, et prouvez que votre formule est correcte. (Conseil : essayez d'abord quelques valeurs particulières de n et recherchez une tendance.)
5. Démontrer que pour tout $n \in \mathbb{N}$, $0 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 + \cdots + n(n + 1) = n(n + 1)(n + 2)/3$.
6. Trouvez une formule pour $0 \cdot 1 \cdot 2 + 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n + 1)(n + 2)$, pour $n \in \mathbb{N}$, et prouvez que votre formule est correcte. (Indice : comparez cet exercice aux [exercices 1](#) et [5](#) et essayez de deviner la formule.)
- *7. Trouvez une formule pour $3^0 + 3^1 + 3^2 + \cdots + 3^n$, pour $n \geq 0$, et prouvez que votre formule est correcte. (Indice : essayez de deviner la formule en vous basant sur [l'exemple 6.1.1](#). Testez ensuite quelques valeurs de n et ajustez votre estimation si nécessaire.)
8. Démontrer que pour tout $n \geq 1$,
- $$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2n-1} - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} + \cdots + \frac{1}{2n}.$$
9. (a) Démontrer que pour tout $n \in \mathbb{N}$, $2 | (n^2 + n)$.
 (b) Démontrer que pour tout $n \in \mathbb{N}$, $6 | (n^3 - n)$.
10. Démontrer que pour tout $n \in \mathbb{N}$, $64 | (9^n - 8n - 1)$.
11. Démontrer que pour tout $n \in \mathbb{N}$, $9 | (4^n + 6n - 1)$.
12. (a) Démontrer que pour tout $n \in \mathbb{N}$, $7^n - 5^n$ est pair.
 (b) Démontrer que pour tout $n \in \mathbb{N}$, $24 | (2 \cdot 7^n - 3 \cdot 5^n + 1)$.
13. Démontrer que pour tous les entiers a et b et tout $n \in \mathbb{N}$, $(a - b) | (a^n - b^n)$.
 (Indice : Soient a et b des entiers arbitraires, puis prouvons par récurrence que $\forall n \in \mathbb{N} [(a - b) | (a^n - b^n)]$. Pour l'étape d'induction, vous devez relier $a^{n+1} - b^{n+1}$ à $a^n - b^n$. Il peut être utile de commencer par compléter l'équation suivante : $a^{n+1} - b^{n+1} = a(a^n - b^n) + \underline{\hspace{2cm}}$.)
14. Démontrer que pour tous les entiers a et b et tout $n \in \mathbb{N}$, $(a + b) | (a^{2n+1} + b^{2n+1})$.
15. Démontrer que pour tout $n \geq 10$, $2^n > n^3$.

16. (a) Démontrer que pour tout $n \in \mathbb{N}$, soit n est pair, soit n est impair, mais pas les deux.
- (b) Démontrer que, comme indiqué dans [la section 3.4](#), tout entier est pair ou impair, mais pas les deux. (Indice : pour prouver qu'un entier négatif n est pair ou impair, mais pas les deux, appliquer la partie (a) à $-n$.)
17. Démontrer que pour tout $n \geq 1$, $2 \cdot 2^1 + 3 \cdot 2^2 + 4 \cdot 2^3 + \cdots + (n+1)2^n = n2^{n+1}$.
18. (a) Quel est le problème avec la preuve suivante selon laquelle pour tout $n \in \mathbb{N}$, $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2n+1)3^n = n3^{n+1}$?

Preuve. Nous utilisons l'induction mathématique. Soit n un nombre naturel arbitraire, et supposons $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2n+1)3^n = n3^{n+1}$.

Alors

$$\begin{aligned} & 1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2n+1)3^n + (2n+3)3^{n+1} \\ &= n3^{n+1} + (2n+3)3^{n+1} \\ &= (3n+3)3^{n+1} \\ &= (n+1)3^{n+2}, \end{aligned}$$

selon les besoins. □

- (b) Trouvez une formule pour $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2n+1)3^n$ et prouvez que votre formule est correcte.
19. Supposons que a est un nombre réel et $a < 0$. Démontrer que pour tout $n \in \mathbb{N}$, si n est pair alors $a^n > 0$, et si n est impair alors $a^n < 0$.
20. Supposons que a et b soient des nombres réels et que $0 < a < b$.
- (a) Démontrer que pour tout $n \geq 1$, $0 < a^n < b^n$. (Remarquez que ceci généralise [l'exemple 3.1.2.](#))
- (b) Démontrer que pour tout $n \geq 2$, $0 < \sqrt[n]{a} < \sqrt[n]{b}$.
- (c) Démontrer que pour tout $n \geq 1$, $ab^n + ba^n < a^{n+1} + b^{n+1}$.
- (d) Démontrer que pour tout $n \geq 2$,

$$\left(\frac{a+b}{2}\right)^n < \frac{a^n + b^n}{2}.$$

6.2. Autres exemples

Nous avons présenté l'induction mathématique dans la section précédente comme une méthode permettant de démontrer que tous les entiers naturels possèdent une propriété. Cependant, les applications de l'induction mathématique vont bien au-delà de l'étude des entiers

naturels. Dans cette section, nous examinerons quelques exemples de démonstrations par induction mathématique illustrant le large éventail d'applications de l'induction.

Exemple 6.2.1. Supposons que R soit un ordre partiel sur un ensemble A . Démontrer que tout ensemble fini non vide $B \subseteq A$ possède un élément R -minimal.

Travail à partir de zéro

On pourrait penser au premier abord que l'induction mathématique n'est pas appropriée pour cette preuve, car le but ne semble pas avoir la forme $\forall n \in \mathbb{N} P(n)$. En fait, l'objectif ne mentionne pas explicitement les entiers naturels ! Mais on voit que les entiers naturels entrent en jeu lorsque l'on reconnaît que dire que B est fini et non vide signifie qu'il a n éléments, pour un certain $n \in \mathbb{N}$, $n \geq 1$. (Nous donnerons une définition plus précise du nombre d'éléments dans un ensemble fini au [chapitre 8](#). Pour le moment, une compréhension intuitive de ce concept suffira.) Ainsi, le but signifie $\forall n \geq 1 \forall B \subseteq A (B \text{ a } n \text{ éléments} \rightarrow B \text{ a un élément minimal})$. Nous pouvons maintenant utiliser l'induction pour prouver cette affirmation.

Dans le cas de base, $n = 1$; il faut donc prouver que si B possède un élément, alors il possède un élément minimal. Il est facile de vérifier que, dans ce cas, l'élément minimal de B doit être minimal.

Pour l'étape d'induction, nous laissons $n \geq 1$ arbitraire, supposons que $\forall B \subseteq A (B \text{ a } n \text{ éléments} \rightarrow B \text{ a un élément minimal})$, et essayons de prouver que $\forall B \subseteq A (B \text{ a } n + 1 \text{ éléments} \rightarrow B \text{ a un élément minimal})$. Guidés par la forme de l'objectif, nous laissons B être un sous-ensemble arbitraire de A , supposons que B a $n + 1$ éléments, et essayons de prouver que B a un élément minimal.

Comment utiliser l'hypothèse inductive pour atteindre notre objectif ? L'hypothèse inductive nous dit que si nous avions un sous-ensemble de A à n éléments, alors il aurait un élément minimal. Pour l'appliquer, nous devons trouver un sous-ensemble de A à n éléments. Notre ensemble arbitraire B est un sous-ensemble de A , et nous avons supposé qu'il avait $n + 1$ éléments. Ainsi, une façon simple de produire un sous-ensemble de A à n éléments serait de retirer un élément de B . On ne sait pas exactement où ce raisonnement mènera, mais cela semble être la façon la plus simple d'utiliser l'hypothèse inductive. Essayons.

Soit b un élément quelconque de B , et soit $B' = B \setminus \{b\}$. Alors B' est un sous-ensemble de A à n éléments ; par conséquent, par hypothèse inductive, B' possède un élément minimal. Ceci étant une affirmation

existentielle, nous introduisons immédiatement une nouvelle variable, disons c , pour représenter un élément minimal de B' .

Notre objectif est de prouver que B possède un élément minimal, ce qui est également une affirmation existentielle. Nous devrions donc essayer de trouver un élément minimal de B . Nous ne connaissons que deux éléments de B à ce stade, b et c , nous devrions donc probablement essayer de prouver que l'un d'eux est un élément minimal de B . Lequel ? Eh bien, cela pourrait dépendre de la plus petite taille de l'un d'eux selon l'ordre partiel R . Cela suggère que nous pourrions avoir besoin d'utiliser la preuve par cas. Dans notre preuve, nous utilisons les cas bRc et $\neg bRc$. Dans le premier cas, nous prouvons que b est un élément minimal de B , et dans le second cas, nous prouvons que c est un élément minimal de B . Notez que dire que quelque chose est un élément minimal de B est une affirmation négative, donc dans les deux cas, nous utilisons la preuve par contradiction.

Solution

Théorème. *Supposons que R soit un ordre partiel sur un ensemble A . Alors tout ensemble fini non vide $B \subseteq A$ possède un élément R -minimal.*

Preuve. Nous montrerons par récurrence que pour tout entier naturel $n \geq 1$, tout sous-ensemble de A à n éléments possède un élément minimal.

Cas de base : $n = 1$. Supposons que $B \subseteq A$ et que B possède un élément. Alors $B = \{b\}$ pour un certain $b \in A$. Clairement $\neg \exists x \in B (x \neq b)$, donc certainement $\neg \exists x \in B (xRb \wedge x \neq b)$. Ainsi, b est minimal.

Étape d'induction : Supposons que $n \geq 1$, et que tout sous-ensemble de A à n éléments possède un élément minimal. Soit maintenant B un sous-ensemble quelconque de A à $n + 1$ éléments. Soit b un élément quelconque de B , et soit $B' = B \setminus \{b\}$, un sous-ensemble de A à n éléments. Par hypothèse inductive, on peut choisir un élément minimal $c \in B'$.

Cas 1. bRc . On affirme que b est un élément minimal de B . Pour comprendre pourquoi, supposons que ce ne soit pas le cas. On peut alors choisir un $x \in B$ tel que xRb et $x \neq b$. Puisque $x \neq b$, $x \in B'$. De plus, puisque xRb et bRc , par transitivité de R il s'ensuit que xRc . Ainsi, puisque c est un élément minimal de B' , on doit avoir $x = c$. Mais alors puisque xRb on a cRb , et on connaît aussi bRc , donc par antisymétrie de R il s'ensuit que $b = c$. C'est clairement impossible, puisque $c \in B' = B \setminus \{b\}$. Ainsi, b doit être un élément minimal de B .

Cas 2. $\neg bRc$. Dans ce cas, on affirme que c est un élément minimal de B . Pour comprendre pourquoi, supposons que ce ne soit pas le cas. On peut alors choisir un $x \in B$ tel que xRc et $x \neq c$. Puisque c est un élément minimal de B' , on ne peut pas avoir $x \in B'$; la seule autre possibilité est

donc $x = b$. Mais comme xRc nous devons alors avoir bRc , ce qui contredit notre hypothèse $\neg bRc$. Ainsi, c est un élément minimal de B .

□

Il est à noter qu'un sous-ensemble infini d'un ensemble partiellement ordonné n'a pas nécessairement d'élément minimal, comme nous l'avons vu dans la première partie de [l'exemple 4.4.5](#). Ainsi, l'hypothèse de finesse de B était nécessaire dans notre dernier théorème. Ce théorème peut servir à démontrer un autre fait intéressant concernant les ordres partiels, toujours par induction mathématique :

Exemple 6.2.2. Supposons que A soit un ensemble fini et que R soit un ordre partiel sur A . Démontrer que R peut être étendu à un ordre total sur A . Autrement dit, démontrer qu'il existe un ordre total T sur A tel que $R \subseteq T$.

Travail à partir de zéro

Nous nous contenterons d'esquisser la démonstration, laissant de nombreux détails en exercices. L'idée est de prouver par récurrence que $\forall n \in \mathbb{N} \forall A \forall R [(\text{A a } n \text{ éléments et } R \text{ est un ordre partiel sur } A) \rightarrow \exists T (\text{T est un ordre total sur } A \text{ et } R \subseteq T)]$. L'étape de récurrence est similaire à celle du dernier exemple. Si R est un ordre partiel sur un ensemble A à $n + 1$ éléments, alors on retire un élément, appelé a , de A , et Appliquer l'hypothèse inductive à l'ensemble restant $A' = A \setminus \{a\}$. Cela nous donnera un ordre total T' sur A' , et pour compléter la preuve, nous devons d'une manière ou d'une autre le transformer en un ordre total T sur A tel que $R \subseteq T$. La relation T' nous indique déjà comment comparer deux éléments quelconques de A' , mais elle ne nous dit pas comment comparer a aux éléments de A' . C'est ce que nous devons décider pour définir T , et la principale difficulté de cette étape de la preuve est que nous devons prendre cette décision de telle manière que nous nous retrouvions avec $R \subseteq T$. Notre résolution de cette difficulté dans la preuve suivante consiste à choisir a avec soin en premier lieu. Nous choisissons a comme étant un élément R -minimal de A , puis lorsque nous définissons T , nous rendons a plus petit dans l'ordre T que tout élément de A' . Nous utilisons le théorème du dernier exemple, avec $B = A$, pour garantir que A possède un élément R -minimal.

Solution

Théorème. Supposons que A soit un ensemble fini et R un ordre partiel sur A . Alors il existe un ordre total T sur A tel que $R \subseteq T$.

Preuve. Nous montrerons par récurrence sur n que tout ordre partiel sur un ensemble à n éléments peut être étendu à un ordre total. Ceci

suffit évidemment à démontrer le théorème.

Cas de base : $n = 0$. Supposons que R soit un ordre partiel sur A et que A comporte 0 élément. Alors, clairement, $A = R = \emptyset$. Il est facile de vérifier que \emptyset est un ordre total sur A (toutes les propriétés requises sont vérifiées indéfiniment), nous avons donc terminé.

Étape d'induction : Soit n un entier naturel arbitraire, et supposons que tout ordre partiel sur un ensemble à n éléments puisse être étendu à un ordre total. Supposons maintenant que A possède $n + 1$ éléments et que R soit un ordre partiel sur A . D'après le théorème du dernier exemple, il doit exister un $a \in A$ tel que a soit un élément *R-minimal* de A . Soit $A' = A \setminus \{a\}$ et soit $R' = R \cap (A' \times A')$. On vous demande de montrer dans [l'exercice 1](#) que R' est un ordre partiel sur A' . Par l'hypothèse inductive, on peut poser T' un ordre total sur A' tel que $R' \subseteq T'$. Soit maintenant $T = T' \cup (\{a\} \times A)$. Il vous est également demandé de montrer dans [l'exercice 1](#) que T est un ordre total sur A et $R \subseteq T$, comme requis.

□

Le théorème du dernier exemple peut être étendu aux ordres partiels sur des ensembles infinis. Pour une approche dans ce sens, voir [l'exercice 19 de la section 8.1](#).

Exemple 6.2.3. Démontrer que pour tout $n \geq 3$, si n points distincts sur un cercle sont reliés consécutivement par des droites, alors la somme des angles intérieurs du polygone résultant est $(n - 2)180^\circ$.

Solution

[La figure 6.1](#) montre un exemple avec $n = 4$. Nous ne donnerons pas le travail de base séparément pour cette preuve.

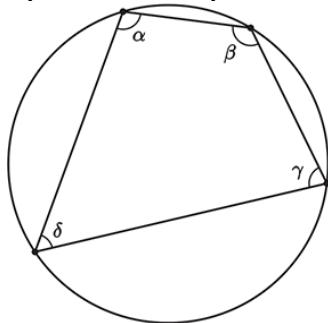


Figure 6.1. $\alpha + \beta + \gamma + \delta = (4 - 2)180^\circ = 360^\circ$.

Théorème. Pour tout $n \geq 3$, si n points distincts sur un cercle sont reliés dans l'ordre consécutif par des lignes droites, alors les angles intérieurs du polygone résultant s'additionnent à $(n - 2)180^\circ$.

Preuve. On utilise l'induction sur n .

Cas de base : Supposons que $n = 3$. Le polygone est alors un triangle, et il est bien connu que la somme des angles intérieurs d'un triangle est de 180° .

Étape d'induction : Soit n un entier naturel arbitraire, $n \geq 3$, et supposons que l'affirmation soit vraie pour n . Considérons maintenant le polygone P formé en reliant $n + 1$ points distincts A_1, A_2, \dots, A_{n+1} sur un cercle. Si l'on ignore le dernier point A_{n+1} , on obtient un polygone P' à n sommets seulement, et par hypothèse d'induction, la somme des angles intérieurs de ce polygone est égale à $(n - 2)180^\circ$. Mais comme le montre [la figure 6.2](#), la somme des angles intérieurs de P est égale à la somme des angles intérieurs de P' plus la somme des angles intérieurs du triangle $A_1 A_n A_{n+1}$. Puisque la somme des angles intérieurs du triangle est de 180° , nous pouvons conclure que la somme des angles intérieurs de P est

$$(n - 2)180^\circ + 180^\circ = ((n + 1) - 2)180^\circ,$$

selon les besoins. □

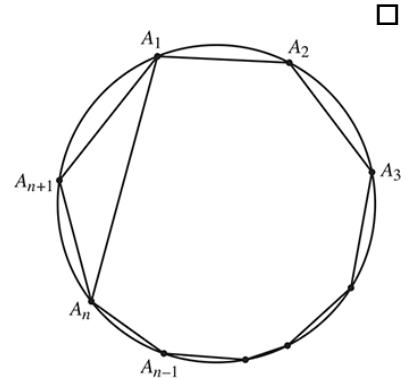
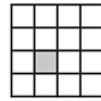


Figure 6.2.

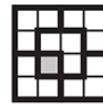
Exemple 6.2.4. Démontrer que pour tout entier positif n , une grille carrée de $2^n \times 2^n$ dont une case est supprimée peut être recouverte de tuiles en L ressemblant à ceci :

Travail à partir de zéro

[La figure 6.3](#) montre un exemple pour le cas $n = 2$. Dans ce cas, $2^n = 4$, nous avons donc une grille 4×4 , et la case supprimée est grisée. Les lignes épaisses indiquent comment les cases restantes peuvent être recouvertes de cinq tuiles en L.



(a) 4×4 grid with one square removed.



(b) Grid covered with L-shaped tiles.

Figure 6.3.

Nous utiliserons l'induction dans notre preuve, et comme nous ne nous intéressons qu'à n positif, le cas de base sera $n = 1$. Dans ce cas, nous avons une grille 2×2 avec un carré supprimé, et celle-ci peut clairement être recouverte d'une tuile en forme de L. (Dessine une image !)

Pour l'étape d'induction, nous laissons n être un entier positif arbitraire et supposons qu'une grille $2^n \times 2^n$ avec un carré supprimé peut être recouverte de grilles en forme de L. Tuiles. Supposons maintenant que nous ayons une grille $2^{n+1} \times 2^{n+1}$ dont une case a été supprimée. Pour appliquer notre hypothèse inductive, nous devons la relier d'une manière ou d'une autre à la grille $2^n \times 2^n$.

Puisque $2^{n+1} = 2^n \cdot 2$, la grille $2^{n+1} \times 2^{n+1}$ est deux fois plus large et deux fois plus haute que la grille $2^n \times 2^n$. Autrement dit, en divisant la grille $2^{n+1} \times 2^{n+1}$ en deux horizontalement et verticalement, nous pouvons la diviser en quatre « sous-grilles » $2^n \times 2^n$. Ceci est illustré à [la figure 6.4](#). La case supprimée se trouvera dans l'une des quatre sous-grilles ; dans [la figure 6.4](#), elle se trouve en haut à droite.

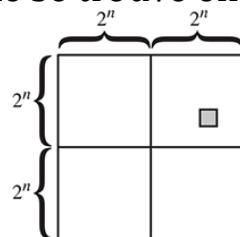


Figure 6.4.

L'hypothèse inductive nous indique qu'il est possible de recouvrir la sous-grille supérieure droite de [la figure 6.4](#) avec des tuiles en L. Mais qu'en est-il des trois autres sous-grilles ? Il existe une méthode astucieuse pour placer une tuile sur la grille, ce qui permet ensuite, grâce à l'hypothèse inductive, de démontrer que les sous-grilles restantes peuvent être recouvertes. Voyez si vous pouvez le comprendre avant de lire la réponse dans la démonstration suivante.

Solution

Théorème. Pour tout entier positif n , une grille carrée de $2^n \times 2^n$ dont un carré est supprimé peut être recouverte de tuiles en forme de L.

Preuve. On utilise l'induction sur n .

Cas de base : supposons que $n = 1$. La grille est alors une grille 2×2 avec un carré supprimé, qui peut clairement être recouvert d'une tuile en forme de L.

Étape d'induction : Soit n un entier positif arbitraire, et supposons qu'une grille $2^n \times 2^n$, dont une case a été supprimée, puisse être recouverte de tuiles en L. Considérons maintenant une grille $2^{n+1} \times 2^{n+1}$, dont une case a été supprimée. Coupez la grille en deux verticalement et horizontalement, en quatre sous-grilles $2^n \times 2^n$. La case supprimée provient de l'une de ces sous-grilles ; par hypothèse inductive, le reste de cette sous-grille peut donc être recouvert de tuiles en L. Tuiles de forme. Pour couvrir les trois autres sous-grilles, placez d'abord une tuile en L au centre, de manière à couvrir un carré de chacune des trois sous-grilles restantes, comme illustré à [la figure 6.5](#). La zone restant à couvrir contient désormais tous les carrés sauf un de chaque sous-grille. En appliquant l'hypothèse inductive à chaque sous-grille, nous pouvons donc constater que cette zone peut être couverte par des tuiles.

□

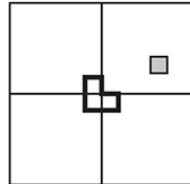


Figure 6.5.

Il est intéressant de noter que cette preuve peut servir à déterminer comment placer des tuiles sur une grille particulière. Prenons par exemple la grille 8×8 avec une case supprimée, illustrée à la [figure 6.6](#).

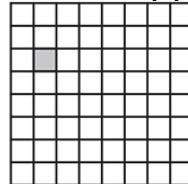


Figure 6.6.

D'après la démonstration précédente, la première étape pour recouvrir cette grille de tuiles consiste à la diviser en quatre sous-grilles 4×4 et à placer une tuile au centre, en recouvrant un carré de chaque sous-grille, sauf en haut à gauche. Ceci est illustré à [la figure 6.7](#). La zone restant à couvrir est maintenant constituée de quatre sous-grilles 4×4 , dont un carré a été retiré à chacune.

Comment recouvrir les sous-grilles 4×4 restantes ? Par la même méthode, bien sûr ! Par exemple, recouvrons la sous-grille en haut à droite de [la figure 6.7](#). Nous devons recouvrir chaque carré de cette sous-grille, sauf le coin inférieur gauche, qui a déjà été recouvert. Nous commençons par la découper en quatre sous-grilles 2×2 , et placez une tuile au milieu, comme dans [la figure 6.8](#). La zone restante à couvrir est maintenant constituée de quatre sous-grilles 2×2 , dont un carré a été retiré de chacune. Chacune d'elles peut être recouverte d'une tuile, complétant ainsi la sous-grille supérieure droite de [la figure 6.7](#).

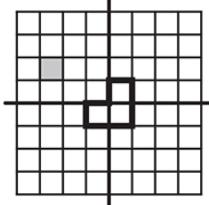


Figure 6.7.

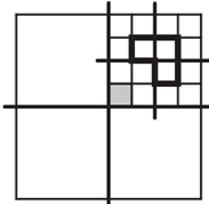


Figure 6.8.

Les trois quarts restants de [la figure 6.7](#) sont complétés par une procédure similaire. La solution finale est présentée à [la figure 6.9](#).

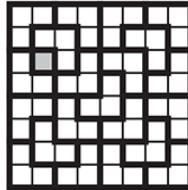


Figure 6.9.

La méthode utilisée pour résoudre ce problème est un exemple de procédure *récursive*. Nous avons résolu le problème pour une grille 8×8 en la divisant en quatre problèmes de grille 4×4 . Pour résoudre chacun d'eux, nous l'avons scindé en quatre problèmes 2×2 , tous faciles à résoudre. Si nous avions commencé avec une grille plus grande, nous aurions peut-être dû répéter le découpage plusieurs fois avant d'atteindre des problèmes 2×2 faciles. La récursivité et sa relation avec l'induction mathématique font l'objet de la section suivante.

Exercices

- *1. Complétez la preuve de [l'exemple 6.2.2](#) en effectuant les démonstrations suivantes. (Nous utilisons ici la même notation que dans l'exemple.)
- Démontrer que R' est un ordre partiel sur A' .
 - Démontrer que T est un ordre total sur A et $R \subseteq T$.
2. Supposons que R soit un ordre partiel sur un ensemble A , $B \subseteq A$ et B est fini. Démontrer qu'il existe un ordre partiel T sur A tel que $R \subseteq T$ et $\forall x \in B \forall y \in A (xT y \vee yT x)$. Notons que, en particulier, si A est fini, on peut poser $B = A$, et la conclusion signifie alors que T est un ordre total sur A . Ceci donne donc une approche alternative à la démonstration du théorème de [l'exemple 6.2.2](#). (Indice : utiliser l'induction sur le nombre d'éléments dans B . Pour l'étape d'induction, supposer que la conclusion est vraie pour tout ensemble $B \subseteq A$ de n éléments, et supposer que B est un sous-ensemble de A de $n + 1$ éléments. Soit b un élément quelconque de B et soit $B' = B \setminus \{b\}$, un sous-ensemble de A de n éléments. Par l'hypothèse inductive, soit T' un ordre partiel sur A tel que $R \subseteq T'$ et $\forall x \in B' \forall y \in A (xT' y \vee yT' x)$. Maintenant, soit $A_1 = \{x \in A \mid (x, b) \in T'\}$ et $A_2 = A \setminus A_1$, et soit $T = T' \cup (A_1 \times A_2)$. Démontrer que T a toutes les propriétés requises.)
3. Supposons que R soit un ordre total sur un ensemble A . Démontrer que tout ensemble fini non vide $B \subseteq A$ possède un R -plus petit élément et un R -plus grand élément.
- *4. (a) Supposons que R soit une relation sur A , et $\forall x \in A \forall y \in A (xRy \vee yRx)$. (Notez que cela implique que R est réflexif.) Démontrer que pour tout ensemble fini non vide $B \subseteq A$, il existe un $x \in B$ tel que $\forall y \in B ((x, y) \in R \circ R)$. (Indice : imiter [l'exemple 6.2.1](#).)
- (b) Considérons un tournoi où chaque concurrent affronte tous les autres concurrents une seule fois, et l'un d'eux gagne. On dira qu'un concurrent x est *excellent* si, pour chaque autre concurrent y , soit x bat y , soit il existe un troisième concurrent z tel que x bat z et z bat y . Démontrer qu'il existe au moins un excellent concurrent.
5. Pour chaque $n \in \mathbb{N}$, soit $F_n = 2^{(2^n)} + 1$. (Ces nombres sont appelés nombres de Fermat, du nom du mathématicien français Pierre de Fermat (1601-1665). Fermat a démontré que F_0, F_1, F_2, F_3 et F_4 sont premiers et a conjecturé que tous les nombres de Fermat sont premiers. Cependant, plus de cent ans plus tard, Euler a démontré que F_5 n'est pas premier. On ignore s'il existe un nombre $n > 4$ pour lequel F_n est premier.)

Démontrer que pour tout $n \geq 1$, $F_n = (F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1}) + 2$.

6. Démontrer que si $n \geq 1$ et a_1, a_2, \dots, a_n sont des nombres réels, alors $|a_1 + a_2 + \cdots + a_n| \leq |a_1| + |a_2| + \cdots + |a_n|$. (Notez que ceci généralise l'inégalité triangulaire ; voir [l'exercice 13\(c\)](#) de la section [3.5.](#))
7. (a) Démontrer que si a et b sont des nombres réels positifs, alors $a/b + b/a \geq 2$. (Indice : Commencez par le fait que $(a - b)^2 \geq 0$.)
(b) Supposons que a, b et c soient des nombres réels et que $0 < a \leq b \leq c$. Démontrer que $b/c + c/a - b/a \geq 1$. (Indice : Commençons par le fait que $(c-a)(c-b) \geq 0$.)
(c) Démontrer que si $n \geq 2$ et a_1, a_2, \dots, a_n sont des nombres réels tels que $0 < a_1 \leq a_2 \leq \cdots \leq a_n$, alors $a_1/a_2 + a_2/a_3 + \cdots + a_{n-1}/a_n + a_n/a_1 \geq n$.
- *8. Si $n \geq 2$ et a_1, a_2, \dots, a_n est une liste de nombres réels positifs, alors le nombre $(a_1 + a_2 + \cdots + a_n)/n$ est appelé *moyenne arithmétique* des nombres a_1, a_2, \dots, a_n , et ce nombre $\sqrt[n]{a_1 a_2 \cdots a_n}$ est appelé *moyenne géométrique*. Dans cet exercice, vous démontrerez l'*inégalité moyenne arithmétique-moyenne géométrique*, qui stipule que la moyenne arithmétique est toujours au moins aussi grande que la moyenne géométrique.
(a) Démontrer que l'inégalité moyenne arithmétique-moyenne géométrique est vraie pour les listes de nombres de longueur 2. En d'autres termes, prouver que pour tous les nombres réels positifs a et b , $(a + b)/2 \geq \sqrt{ab}$.
(b) Démontrer que l'inégalité moyenne arithmétique-moyenne géométrique est vraie pour toute liste de nombres dont la longueur est une puissance de 2. En d'autres termes, démontrer que pour tout $n \geq 1$, si a_1, a_2, \dots, a_{2^n} est une liste de nombres réels positifs, alors

$$\frac{a_1 + a_2 + \cdots + a_{2^n}}{2^n} \geq \sqrt[2^n]{a_1 a_2 \cdots a_{2^n}}.$$

- (c) Supposons que $n_0 \geq 2$ et que l'inégalité moyenne arithmétique-moyenne géométrique soit invalide pour une liste de longueur n_0 . Autrement dit, il existe des nombres réels positifs a_1, a_2, \dots, a_{n_0} tels que

$$\frac{a_1 + a_2 + \cdots + a_{n_0}}{n_0} < \sqrt[n_0]{a_1 a_2 \cdots a_{n_0}}.$$

Démontrer que pour tout $n \geq n_0$, l'inégalité moyenne arithmétique-moyenne géométrique échoue pour une liste de longueur n .

- (d) Démontrer que l'inégalité moyenne arithmétique-moyenne géométrique est toujours vraie.

9. Démontrer que si $n \geq 2$ et a_1, a_2, \dots, a_n est une liste de nombres réels positifs, alors

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 a_2 \cdots a_n}.$$

(Indice : Appliquez [l'exercice 8](#). Le nombre à gauche de l'inégalité ci-dessus est appelé la *moyenne harmonique* des nombres a_1, a_2, \dots, a_n .)

10. (a) Démontrer que si a_1, a_2, b_1 et b_2 sont des nombres réels, avec $a_1 \leq a_2$ et $b_1 \leq b_2$, alors $a_1 b_2 + a_2 b_1 \leq a_1 b_1 + a_2 b_2$.

- (b) Supposons que n soit un entier positif, a_1, a_2, \dots, a_n et b_1, b_2, \dots, b_n soient des nombres réels, $a_1 \leq a_2 \leq \dots \leq a_n$, $b_1 \leq b_2 \leq \dots \leq b_n$, et f soit une fonction bijective de $\{1, 2, \dots, n\}$ à $\{1, 2, \dots, n\}$. Démontrer que $a_1 b_{f(1)} + a_2 b_{f(2)} + \dots + a_n b_{f(n)} \leq a_1 b_1 + a_2 b_2 + \dots + a_n b_n$. (Ce fait est connu sous le nom d' *inégalité de réarrangement*.)

11. Démontrer que pour tout ensemble A , si A a n éléments alors $\mathcal{P}(A)$ a 2^n éléments.

12. Si A est un ensemble, soit $\mathcal{P}_2(A)$ l'ensemble de tous les sous-ensembles de A ayant exactement deux éléments. Démontrer que pour tout ensemble A , si A a n éléments, alors $\mathcal{P}_2(A)$ a $n(n-1)/2$ éléments. (Indice : Voir le corrigé de [l'exercice 11](#).)

13. Supposons que n soit un entier positif. Un triangle équilatéral est découpé en 4^n triangles équilatéraux congruents par des segments de droite équidistants parallèles aux côtés du triangle, et un coin est supprimé. ([La figure 6.10](#) montre un exemple pour le cas $n = 2$.) Montrer que l'aire restante peut être recouverte par des tuiles trapézoïdales comme ceci : 

Figure 6.10.

14. Soit n un entier positif. Supposons que n cordes soient tracées dans un cercle de telle sorte que chaque corde intersecte toutes les

autres, mais qu'aucune ne se coupe en un point. Démontrer que les cordes coupent le cercle en régions $(n^2 + n + 2)/2$. ([La figure 6.11](#) montre un exemple pour $n = 4$. Noter qu'il y a $(4^2 + 4 + 2)/2 = 11$ régions sur cette figure.)

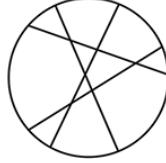


Figure 6.11.

15. Soit n un entier positif, et supposons que n cordes soient tracées dans un cercle, de quelque manière que ce soit, découpant le cercle en un nombre a de régions. Démontrer que ces régions peuvent être colorées de deux couleurs de telle sorte que les régions adjacentes (c'est-à-dire les régions qui partagent un bord) sont de couleurs différentes. ([La figure 6.12](#) montre un exemple dans le cas $n = 4$.)

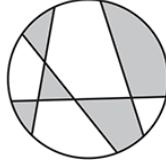


Figure 6.12.

16. Démontrer que pour tout ensemble fini A et toute fonction $f: A \rightarrow A$, si f est indicielle alors f est sur. (Indice : utiliser l'induction sur le nombre d'éléments de A . Pour l'induction, supposer que la conclusion est vraie pour tout ensemble A à n éléments, et supposer que A a $n + 1$ éléments et $f: A \rightarrow A$. Supposer que f est indicielle mais n'est pas sur. Alors il existe un $a \in A$ tel que $a \notin \text{Ran}(f)$. Soient $A' = A \setminus \{a\}$ et $f' = f \cap (A' \times A')$. Montrer que $f': A' \rightarrow A'$, f' est indicielle et f' n'est pas sur, ce qui contredit l'hypothèse inductive.)
17. Quel est le problème avec la preuve suivante selon laquelle si $A \subseteq \mathbb{N}$ et $0 \in A$ alors $A = \mathbb{N}$?

Preuve. Nous prouverons par récurrence que $\forall n \in \mathbb{N} (n \in A)$.

Cas de base : si $n = 0$, alors $n \in A$ par hypothèse.

Étape d'induction : Soit $n \in \mathbb{N}$ arbitraire, et supposons que $n \in A$. Puisque n est arbitraire, il s'ensuit que tout nombre naturel est un élément de A , et donc en particulier $n + 1 \in A$.

□

18. Supposons $f: \mathbb{R} \rightarrow \mathbb{R}$. Quel est le problème avec la preuve suivante selon laquelle pour tout ensemble fini non vide $A \subseteq \mathbb{R}$ il existe un

nombre réel c tel que $\forall x \in A (f(x) = c)$?

Preuve. Nous allons prouver par récurrence que pour tout $n \geq 1$, si A est un sous-ensemble de \mathbb{R} à n éléments alors $\exists c \in \mathbb{R} \forall x \in A (f(x) = c)$.

Cas de base : $n = 1$. Supposons que $A \subseteq \mathbb{R}$ et que A possède un élément. Alors $A = \{a\}$, pour un certain $a \in \mathbb{R}$. Soit $c = f(a)$. Alors clairement $\forall x \in A (f(x) = c)$.

Étape d'induction : Supposons $n \geq 1$, et pour tout $A \subseteq \mathbb{R}$, si A a n éléments alors $\exists c \in \mathbb{R} \forall x \in A (f(x) = c)$. Supposons maintenant que $A \subseteq \mathbb{R}$ et que A ait $n + 1$ éléments. Soit a_1 un élément quelconque de A , et soit $A_1 = A \setminus \{a_1\}$. Alors A_1 a n éléments, donc par hypothèse inductive il existe un $c_1 \in \mathbb{R}$ tel que $\forall x \in A_1 (f(x) = c_1)$. Si nous pouvons montrer que $f(a_1) = c_1$ alors nous aurons terminé, puisqu'il s'ensuivra alors que $\forall x \in A (f(x) = c_1)$.

Soit a_2 un élément de A différent de a_1 , et soit $A_2 = A \setminus \{a_2\}$. En appliquant à nouveau l'hypothèse inductive, nous pouvons choisir un nombre $c_2 \in \mathbb{R}$ tel que $\forall x \in A_2 (f(x) = c_2)$. Remarquez que puisque $a_1 \neq a_2$, $a_1 \in A_2$, donc $f(a_1) = c_2$. Maintenant, soit a_3 un élément de A différent à la fois de a_1 et de a_2 . Alors $a_3 \in A_1$ et $a_3 \in A_2$, donc $f(a_3) = c_1$ et $f(a_3) = c_2$. Par conséquent $c_1 = c_2$, donc $f(a_1) = c_1$, comme requis.

□

6.3. Récursivité

Au [chapitre 3](#), nous avons appris à prouver des affirmations de la forme $\forall n P(n)$ en posant n comme arbitraire et en prouvant $P(n)$. Dans ce chapitre, nous avons découvert une autre méthode pour prouver de telles affirmations, lorsque n est compris entre les entiers naturels : prouver $P(0)$, puis prouver que pour tout entier naturel n , si $P(n)$ est vrai, alors $P(n+1)$ l'est aussi. Une fois ces affirmations prouvées, nous pouvons parcourir tous les entiers naturels dans l'ordre et constater que P doit être vrai pour chacun d'eux.

On peut utiliser une idée similaire pour introduire une nouvelle façon de définir les fonctions. Au [chapitre 5](#), nous avons généralement défini une fonction f en expliquant comment calculer $f(n)$ pour tout n dans le domaine de définition de f . Si le domaine de définition de f est l'ensemble de tous les entiers naturels, une méthode alternative pour définir f serait d'indiquer ce qu'est $f(0)$ puis, pour tout entier naturel n , d'expliquer comment calculer $f(n+1)$ si nous connaissons déjà la valeur de $f(n)$. Une telle définition nous permettrait de parcourir tous les entiers naturels afin de calculer l'image de chacun sous f .

Par exemple, nous pourrions utiliser les équations suivantes pour définir une fonction f de domaine \mathbb{N} :

$$\begin{aligned} f(0) &= 1; \\ \text{for every } n \in \mathbb{N}, \quad f(n+1) &= (n+1) \cdot f(n). \end{aligned}$$

La deuxième équation nous indique comment calculer $f(n+1)$, mais seulement si nous connaissons déjà la valeur de $f(n)$. Ainsi, bien que cette équation ne puisse pas nous indiquer directement l'image d'un nombre quelconque par f , elle nous permet de parcourir tous les nombres naturels dans l'ordre et de calculer leurs images.

Commençons par $f(0)$, dont la première équation indique qu'elle est égale à 1. En remplaçant $n = 0$ dans la seconde équation, nous obtenons que $f(1) = 1 \cdot f(0) = 1 \cdot 1 = 1$, ce qui nous a permis de déterminer la valeur de $f(1)$. Maintenant que nous savons que $f(1) = 1$, nous pouvons utiliser à nouveau la seconde équation pour calculer $f(2)$. En remplaçant $n = 1$ dans la seconde équation, nous obtenons que $f(2) = 2 \cdot f(1) = 2 \cdot 1 = 2$. De même, en posant $n = 2$ dans la seconde équation, nous obtenons $f(3) = 3 \cdot f(2) = 3 \cdot 2 = 6$. En continuant ainsi, nous pouvons calculer $f(n)$ pour tout entier naturel n . Ainsi, les deux équations fournissent bien une règle déterminant une valeur unique. $f(n)$ pour chaque entier naturel n , ils définissent donc une fonction f de domaine \mathbb{N} . Les définitions de ce type sont appelées définitions récursives.

Il arrive que l'on procède à rebours lorsqu'on utilise une définition récursive pour évaluer une fonction. Par exemple, supposons que l'on veuille calculer $f(6)$, où f est la fonction qui vient d'être définie. Selon la deuxième équation de la définition de f , $f(6) = 6 \cdot f(5)$, pour terminer le calcul, il faut donc calculer $f(5)$. En utilisant à nouveau la deuxième équation, on trouve $f(5) = 5 \cdot f(4)$, il faut donc calculer $f(4)$. En poursuivant ainsi, on obtient le calcul suivant :

$$\begin{aligned}f(6) &= 6 \cdot f(5) \\&= 6 \cdot 5 \cdot f(4) \\&= 6 \cdot 5 \cdot 4 \cdot f(3) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot f(2) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot f(1) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot f(0) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 \\&= 720.\end{aligned}$$

Peut-être reconnaissiez-vous maintenant la fonction f . Pour tout entier positif n , $f(n) = n \cdot (n-1) \cdot (n-2) \cdots 1$, et $f(0) = 1$. Le nombre $f(n)$ est appelé *factorielle n*, et est noté $n!$. (Rappelons que nous avons utilisé cette notation dans notre preuve du [théorème 3.7.3](#).) Par exemple, $6! = 720$. Souvent, si une fonction peut être écrite comme une formule avec des points de suspension (\dots), alors l'utilisation des points de suspension peut être évitée en donnant une définition récursive pour la fonction. Une telle définition est généralement plus facile à utiliser.

De nombreuses fonctions courantes sont plus facilement définies par des définitions récursives. Par exemple, pour tout nombre a , on pourrait définir a^n avec la définition récursive suivante :

$$\begin{aligned}a^0 &= 1; \\ \text{for every } n \in \mathbb{N}, a^{n+1} &= a^n \cdot a.\end{aligned}$$

En utilisant cette définition, nous calculerions a^4 comme ceci :

$$\begin{aligned}a^4 &= a^3 \cdot a \\&= a^2 \cdot a \cdot a \\&= a^1 \cdot a \cdot a \cdot a \\&= a^0 \cdot a \cdot a \cdot a \cdot a \\&= 1 \cdot a \cdot a \cdot a \cdot a.\end{aligned}$$

Prenons un autre exemple : la somme $2^0 + 2^1 + 2^2 + \cdots + 2^n$, présentée dans le premier exemple de ce chapitre. Les points de suspension suggèrent une définition récursive. Si l'on pose $f(n) = 2^0 + 2^1 + 2^2 + \cdots + 2^n$, on remarque que pour tout $n \in \mathbb{N}$, $f(n+1) = 2^0 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} = f(n) + 2^{n+1}$. On pourrait ainsi définir f récursivement comme suit :

$$f(0) = 2^0 = 1; \\ \text{for every } n \in \mathbb{N}, f(n+1) = f(n) + 2^{n+1}.$$

Pour vérifier que cette définition est correcte, essayons-la dans le cas $n = 3$:

$$\begin{aligned} f(3) &= f(2) + 2^3 \\ &= f(1) + 2^2 + 2^3 \\ &= f(0) + 2^1 + 2^2 + 2^3 \\ &= 2^0 + 2^1 + 2^2 + 2^3 \\ &= 15. \end{aligned}$$

Des sommes comme celle du dernier exemple sont assez fréquentes pour qu'il existe une notation spécifique. Si a_0, a_1, \dots, a_n est une liste de nombres, alors la somme de ces nombres s'écrit $\sum_{i=0}^n a_i$. « la somme lorsque i va de 0 à n de a_i ». Par exemple, nous pouvons utiliser cette notation pour écrire la somme du dernier exemple :

$$\sum_{i=0}^n 2^i = 2^0 + 2^1 + 2^2 + \dots + 2^n.$$

Plus généralement, si $n \geq m$, alors

$$\sum_{i=m}^n a_i = a_m + a_{m+1} + a_{m+2} + \dots + a_n.$$

Par exemple,

$$\sum_{i=3}^6 i^2 = 3^2 + 4^2 + 5^2 + 6^2 = 9 + 16 + 25 + 36 = 86.$$

La lettre i dans ces formules est une variable liée et peut donc être remplacée par une nouvelle variable sans changer le sens de la formule.

Essayons maintenant de donner une définition récursive de cette notation. Soit m un entier arbitraire, puis procédons par récursivité sur n . De même que le cas de base d'une preuve par induction n'a pas besoin d'être $n = 0$, la base d'une définition récursive peut l'être. Il peut également être un nombre différent de 0. Dans ce cas, nous ne sommes intéressés que par $n \geq m$, nous prenons donc $n = m$ comme base pour notre récursivité :

$$\begin{aligned} \sum_{i=m}^m a_i &= a_m; \\ \text{for every } n \geq m, \sum_{i=m}^{n+1} a_i &= \sum_{i=m}^n a_i + a_{n+1}. \end{aligned}$$

En essayant cette définition sur l'exemple précédent, nous obtenons

$$\begin{aligned}
\sum_{i=3}^6 i^2 &= \sum_{i=3}^5 i^2 + 6^2 \\
&= \sum_{i=3}^4 i^2 + 5^2 + 6^2 \\
&= \sum_{i=3}^3 i^2 + 4^2 + 5^2 + 6^2 \\
&= 3^2 + 4^2 + 5^2 + 6^2,
\end{aligned}$$

exactement comme nous le voulions.

Il est clair que l'induction et la récursivité sont étroitement liées. Il n'est donc pas surprenant que, si un concept a été défini par récursivité, les preuves impliquant ce concept soient souvent mieux réalisées par induction. Par exemple, à [la section 6.1](#), nous avons vu des preuves par induction impliquant des sommes et des exponentiations, et nous avons maintenant vu que ces deux méthodes peuvent être définies de manière récursive. Comme la fonction factorielle peut également être définie de manière récursive, les preuves impliquant des factorielles utilisent souvent l'induction.

Exemple 6.3.1. Démontrer que pour tout $n \geq 4$, $n! > 2^n$.

Travail à partir de zéro

Comme le problème implique la factorielle et l'exponentiation, toutes deux définies de manière récursive, l'induction semble être une bonne méthode à utiliser. Le cas de base sera $n = 4$, et il suffit d'une simple question d'arithmétique pour vérifier que l'inégalité est vraie dans ce cas. Pour l'étape d'induction, notre hypothèse inductive sera $n! > 2^n$, et nous devons prouver que $(n+1)! > 2^{n+1}$. Bien sûr, la façon de relier l'hypothèse inductive à l'objectif est d'utiliser les définitions récursives de la factorielle et de l'exponentiation, qui nous disent que $(n+1)! = (n+1) \cdot n!$ et $2^{n+1} = 2^n \cdot 2$. Une fois ces équations insérées, le reste est assez simple.

Solution

Théorème. Pour chaque $n \geq 4$, $n! > 2^n$.

Preuve. Par induction mathématique.

Cas de base : lorsque $n = 4$ nous avons $n! = 24 > 16 = 2^4$.

Étape d'induction : Soit $n \geq 4$ arbitraire et supposons que $n! > 2^n$. Alors

$$\begin{aligned}
 (n+1)! &= (n+1) \cdot n! \\
 &> (n+1) \cdot 2^n && \text{(inductive hypothesis)} \\
 &> 2 \cdot 2^n = 2^{n+1}.
 \end{aligned}$$

□

Exemple 6.3.2. Démontrer que pour tout nombre réel a et tous les nombres naturels m et n , $a^{m+n} = a^m \cdot a^n$.

Travail à partir de zéro

Il existe ici trois quantificateurs universels, et nous traiterons les deux premiers différemment du troisième. Soit a et m arbitraires, puis nous utilisons l'induction mathématique pour prouver que $\forall n \in \mathbb{N} (a^{m+n} = a^m \cdot a^n)$. Le fait algébrique clé de l'étape d'induction sera la formule $a^{n+1} = a^n \cdot a$ issue de la définition récursive de l'exponentiation.

Solution

Théorème. Pour tout nombre réel a et tous les nombres naturels m et n , $a^{m+n} = a^m \cdot a^n$.

Preuve. Soit a un nombre réel quelconque et m un nombre naturel quelconque. Procédons maintenant par récurrence sur n .

Cas de base : lorsque $n = 0$, nous avons $a^{m+n} = a^{m+0} = a^m = a^m \cdot 1 = a^m \cdot a^0 = a^m \cdot a^n$.

Étape d'induction. Supposons que $a^{m+n} = a^m \cdot a^n$. Alors

$$\begin{aligned}
 a^{m+(n+1)} &= a^{(m+n)+1} \\
 &= a^{m+n} \cdot a && \text{(definition of exponentiation)} \\
 &= a^m \cdot a^n \cdot a && \text{(inductive hypothesis)} \\
 &= a^m \cdot a^{n+1} && \text{(definition of exponentiation).}
 \end{aligned}$$

□

Exemple 6.3.3. Une séquence de nombres a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$\begin{aligned}
 a_0 &= 0; \\
 \text{for every } n \in \mathbb{N}, a_{n+1} &= 2a_n + 1.
 \end{aligned}$$

Trouvez une formule pour a_n et prouvez que votre formule est correcte.

Travail à partir de zéro

Il est probablement judicieux de commencer par calculer les premiers termes de la suite. Nous savons déjà que $a_0 = 0$; en remplaçant $n = 0$

dans la deuxième équation, nous obtenons $a_1 = 2a_0 + 1 = 0 + 1 = 1$. Ainsi, en remplaçant $n = 1$, nous obtenons $a_2 = 2a_1 + 1 = 2 + 1 = 3$. En poursuivant ainsi, nous obtenons le tableau de valeurs suivant :

n	0	1	2	3	4	5	6	...
a_n	0	1	3	7	15	31	63	...

Ah ! Les nombres obtenus sont inférieurs de un aux puissances de 2. Il semble que la formule soit probablement $n = 2^{n-1}$, mais on ne peut en être sûr que si on la prouve. Heureusement, il est assez facile de prouver la formule par récurrence.

Solution

Théorème. Si la séquence a_0, a_1, a_2, \dots est définie par la définition récursive donnée précédemment, alors pour tout nombre naturel n , $a_n = 2^{n-1}$.

Preuve. Par induction.

Cas de base : $a_0 = 0 = 2^0 - 1$.

Étape d'induction : Supposons que $a_n = 2^{n-1}$. Alors

$$\begin{aligned} a_{n+1} &= 2a_n + 1 && \text{(definition of } a_{n+1}) \\ &= 2(2^{n-1}) + 1 && \text{(inductive hypothesis)} \\ &= 2^{n+1} - 2 + 1 = 2^{n+1} - 1. \end{aligned}$$

□

Nous terminons cette section par un exemple plutôt inhabituel. Nous allons démontrer que pour tout nombre réel $x > -1$ et tout entier naturel n , $(1+x)^n > nx$. Une méthode naturelle consisterait à poser $x > -1$ comme arbitraire, puis à utiliser l'induction sur n . Dans cette étape, nous supposerons que $(1+x)^n > nx$, puis nous tenterons de démontrer que $(1+x)^{n+1} > (n+1)x$. Puisque nous avons supposé $x > -1$, nous avons $1+x > 0$, nous pouvons donc multiplier les deux côtés de l'hypothèse inductive $(1+x)^n > nx$ par $1+x$ pour obtenir

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &> (1+x)nx \\ &= nx + nx^2. \end{aligned}$$

Mais la conclusion dont nous avons besoin pour l'étape d'induction est $(1+x)^{n+1} > (n+1)x$, et il n'est pas clair comment obtenir cette conclusion à partir de l'inégalité que nous avons dérivée.

Notre solution à cette difficulté sera de remplacer notre problème initial par un problème apparemment plus difficile, mais en réalité plus simple. Au lieu de prouver directement l'inégalité $(1+x)^n > nx$, nous

prouverons $(1 + x)^n \geq 1 + nx$, puis observerons que puisque $1 + nx > nx$, il en résulte immédiatement que $(1 + x)^n > nx$. On pourrait penser que si nous avons eu des difficultés à prouver $(1 + x)^n > nx$, nous aurons sûrement plus de difficultés à prouver l'affirmation plus forte $(1 + x)^n \geq 1 + nx$. Mais il s'avère que l'approche que nous avons essayée sans succès sur le problème initial fonctionne parfaitement sur le nouveau problème !

Théorème 6.3.4. Pour tout $x > -1$ et tout nombre naturel n , $(1 + x)^n > nx$.

Preuve. Soit $x > -1$ quelconque. On va démontrer par récurrence que pour tout entier naturel n , $(1 + x)^n \geq 1 + nx$, d'où il résulte clairement que $(1 + x)^n > nx$.

Cas de base : si $n = 0$, alors $(1 + x)^0 = (1 + x)^0 = 1 = 1 + 0 = 1 + nx$.

Étape d'induction : Supposons que $(1 + x)^n \geq 1 + nx$. Alors

$$\begin{aligned} (1 + x)^{n+1} &= (1 + x)(1 + x)^n \\ &\geq (1 + x)(1 + nx) && \text{(inductive hypothesis)} \\ &= 1 + x + nx + nx^2 \\ &\geq 1 + (n + 1)x && \text{(since } nx^2 \geq 0\text{).} \end{aligned}$$

□

Exercices

*1. Trouvez une formule pour $\sum_{i=1}^n \frac{1}{i(i+1)}$ et prouvez que votre formule est correcte.

2. Démontrer que pour tout $n \geq 1$,

$$\sum_{i=1}^n \frac{1}{i(i+1)(i+2)} = \frac{n^2 + 3n}{4(n+1)(n+2)}.$$

3. Démontrer que pour tout $n \geq 2$,

$$\sum_{i=2}^n \frac{1}{(i-1)(i+1)} = \frac{3n^2 - n - 2}{4n(n+1)}.$$

4. Démontrer que pour tout $n \in \mathbb{N}$,

$$\sum_{i=0}^n (2i+1)^2 = \frac{(n+1)(2n+1)(2n+3)}{3}.$$

5. Supposons que r est un nombre réel et que $r \neq 1$. Démontrer que pour tout $n \in \mathbb{N}$,

$$\sum_{i=0}^n r^i = \frac{r^{n+1} - 1}{r - 1}.$$

(Notez que cet exercice généralise [l'exemple 6.1.1](#) et [l'exercice 7](#) de [la section 6.1](#).)

*6. Démontrer que pour tout $n \geq 1$,

$$\sum_{i=1}^n \frac{1}{i^2} \leq 2 - \frac{1}{n}.$$

7. (a) Supposons que $a_0, a_1, a_2, \dots, a_n$ et $b_0, b_1, b_2, \dots, b_n$ soient deux suites de nombres réels. Démontrer que

$$\sum_{i=0}^n (a_i + b_i) = \sum_{i=0}^n a_i + \sum_{i=0}^n b_i.$$

(b) Supposons que c soit un nombre réel et que a_0, a_1, \dots, a_n soit une suite de nombres réels. Démontrer que

$$c \cdot \sum_{i=0}^n a_i = \sum_{i=0}^n (c \cdot a_i).$$

*8. Les *nombres harmoniques* sont les nombres H_n pour $n \geq 1$ définis par la formule

$$H_n = \sum_{i=1}^n \frac{1}{i}.$$

(a) Démontrer que pour tous les nombres naturels n et m , si $n \geq m \geq 1$ alors $H_n - H_m \geq (n - m)/n$. (Indice : Soit m un nombre naturel arbitraire avec $m \geq 1$, puis procéder par induction sur n , avec $n = m$ comme cas de base de l'induction.)

(b) Démontrer que pour tout $n \geq 0$, $H_2^n \geq 1 + n/2$.

(c) (Pour ceux qui ont étudié le calcul.) Montrer que $\lim_{n \rightarrow \infty} H_n = \infty$, donc $\sum_{i=1}^{\infty} (1/i)$ diverge.

9. Soit H_n défini comme dans [l'exercice 8](#). Démontrer que pour tout $n \geq 2$,

$$\sum_{k=1}^{n-1} H_k = nH_n - n.$$

10. Trouvez une formule pour $\sum_{i=1}^n (i \cdot (i!))$ et prouvez que votre formule est correcte.

11. Trouvez une formule pour $\sum_{i=0}^n (i/(i+1)!)$ et prouvez que votre formule est correcte.

12. (a) Démontrer que pour tout $n \in \mathbb{N}$, $2^n > n$.

- (b) Démontrer que pour tout $n \geq 9$, $n! \geq (2^n)^2$.
(c) Démontrer que pour tout $n \in \mathbb{N}$, $n! \leq 2^{(n^2)}$.

13. Supposons que k soit un entier positif.

- (a) Démontrer que pour tout $n \in \mathbb{N}$, $(k^2 + n)! \geq k^{2n}$.
(b) Démontrer que pour tout $n \geq 2$, $k^n \geq k^n$. (Indice : utiliser l'induction, et pour le cas de base utiliser la partie (a). Notons que dans le langage de [l'exercice 19 de la section 5.1](#), cela montre que si $f(n) = k^n$ et $g(n) = n!$, alors $f \in O(g)$.)

14. Démontrer que pour tout nombre réel a et tous les nombres naturels m et n , $(a^m)^n = a^{mn}$.

15. Une séquence a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$a_0 = 0; \\ \text{for every } n \in \mathbb{N}, a_{n+1} = 2a_n + n.$$

Démontrer que pour tout $n \in \mathbb{N}$, $a_n = 2^n - n - 1$.

16. Une séquence a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$a_0 = 2; \\ \text{for every } n \in \mathbb{N}, a_{n+1} = (a_n)^2.$$

Trouvez une formule pour a_n et prouvez que votre formule est correcte.

17. Une séquence a_1, a_2, a_3, \dots est définie récursivement comme suit :

$$a_1 = 1; \\ \text{for every } n \geq 1, a_{n+1} = \frac{a_n}{a_n + 1}.$$

Trouvez une formule pour a_n et prouvez que votre formule est correcte.

18. Pour $n \geq k \geq 0$, la quantité $\binom{n}{k}$ est définie comme suit :

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

- (a) Démontrer que pour tout $n \in \mathbb{N}$, $\binom{n}{0} = \binom{n}{n} = 1$.
(b) Démontrer que pour tous les nombres naturels n et k , si $n \geq k > 0$ alors $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.
(c) Si A est un ensemble et $k \in \mathbb{N}$, soit $\mathcal{P}_k(A)$ l'ensemble de tous les sous-ensembles de A qui ont k éléments. Démontrer que si A a n éléments et $n \geq k \geq 0$, alors $\mathcal{P}_k(A)$ a $\binom{n}{k}$ des éléments. (Indice : Démontrer par récurrence que $\forall n \in \mathbb{N} \forall A [A \text{ est un ensemble de } n \text{ éléments} \rightarrow \forall k (n \geq k \geq 0 \rightarrow \mathcal{P}_k(A) \text{ a } \binom{n}{k} \text{ des éléments})]$. Reproduire [les exercices 11 et 12 de la section 6.2](#). En fait, cet exercice

généralise l'exercice 12 de la section 6.2. Cet exercice montre que $\binom{n}{k}$ est le nombre de façons de choisir k éléments dans un ensemble de taille n , on dit donc parfois n choisir k .)

- (d) Démontrer que pour tous les nombres réels x et y et tout nombre naturel n ,

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

(C'est ce qu'on appelle le *théorème binomial*, c'est pourquoi les nombres $\binom{n}{k}$ sont parfois appelés *coefficients binomiaux*.)

Remarque : Les parties (a) et (b) montrent que l'on peut calculer $\binom{n}{k}$ facilement les nombres en utilisant un tableau triangulaire comme celui de la figure 6.13. Ce tableau est appelé *triangle de Pascal*, du nom du mathématicien français Blaise Pascal (1623-1662). Chaque ligne du triangle correspond à une valeur particulière de n et répertorie les valeurs de $\binom{n}{k}$ pour tout k de 0 à n . La partie (a) montre que le premier et le dernier nombre de chaque ligne sont 1. La partie (b) montre que tout autre nombre est la somme des deux nombres qui le précédent. Par exemple, les lignes de la figure 6.13 illustrent que $\binom{3}{2} = 3$ est la somme de $\binom{2}{1} = 2$ et $\binom{2}{2} = 1$.

$n = 0:$	1
$n = 1:$	1 1
$n = 2:$	1 2 1
$n = 3:$	1 3 3 1
$n = 4:$	1 4 6 4 1
	⋮

Figure 6.13. Triangle de Pascal.

19. Pour la signification de la notation utilisée dans cet exercice, voir l'exercice 18.
- (a) Démontrer que pour tout $n \in \mathbb{N}$, $\sum_{k=0}^n \binom{n}{k} = 2^n$. (Indice : vous pouvez le faire par récurrence en utilisant les parties (a) et (b) de l'exercice 18, ou vous pouvez combiner partie (c) de l'exercice 18 avec l'exercice 11 de la section 6.2, ou vous pouvez brancher quelque chose pour x et y dans la partie (d) de l'exercice 18.)
- (b) Démontrer que pour tout $n \geq 1$, $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.
20. Une séquence a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$\begin{aligned} a_0 &= 0; \\ \text{for every } n \in \mathbb{N}, \quad a_{n+1} &= (a_n)^2 + \frac{1}{4}. \end{aligned}$$

Démontrer que pour tout $n \geq 1$, $0 < a_n < 1$.

21. Dans ce problème, nous définirons, pour tout entier naturel n , une fonction $f_n: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$. La suite de fonctions f_0, f_1, f_2, \dots est définie récursivement comme suit :

for every $x \in \mathbb{Z}^+$, $f_0(x) = x$;
for every $n \in \mathbb{N}$ and every $x \in \mathbb{Z}^+$, $f_{n+1}(x) = 2^{f_n(x)}$.

- (a) La première équation de cette définition récursive donne une formule pour $f_0(x)$, à savoir $f_0(x) = x$. Trouvez les formules pour $f_1(x)$, $f_2(x)$ et $f_3(x)$.
 - (b) Démontrer que pour tous les nombres naturels n et tous les entiers positifs x et y , si $x < y$ alors $f_n(x) < f_n(y)$.
 - (c) Démontrer que pour tous les nombres naturels m et n et tous les entiers positifs x , si $m < n$ alors $f_m(x) < f_n(x)$.
 - (d) Démontrer que pour tout entier naturel n , $f_n \in O(f_{n+1})$ mais $f_{n+1} \notin O(f_n)$. (Voir [l'exercice 19 de la section 5.1](#) pour la signification de la notation utilisée ici.)
Définissez maintenant $g : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ par la formule $g(x) = f_x(x)$.
 - (e) Calculez $g(1)$, $g(2)$ et $g(3)$. (N'essayez pas de calculer $g(4)$; la réponse serait un nombre de plus de 6×10^{19727} chiffres.)
 - (f) Démontrer que pour tout nombre naturel n , $f_n \in O(g)$ mais $g \notin O(f_n)$.
22. Expliquez le paradoxe dans la preuve du [théorème 6.3.4](#), dans lequel nous avons facilité la preuve en changeant l'objectif en une déclaration qui semblait plus difficile à prouver.

6.4. Forte induction

Lors de l'étape d'induction d'une preuve par induction mathématique, nous prouvons qu'un entier naturel possède une propriété en supposant que le nombre précédent possède la même propriété. Dans certains cas, cette hypothèse n'est pas suffisamment solide pour que la preuve soit valide, et nous devons supposer que *tous* les entiers naturels plus petits Les nombres possèdent la propriété suivante. C'est l'idée qui sous-tend une variante de l'induction mathématique, parfois appelée *induction forte* :

Pour prouver un but de la forme $\forall n \in \mathbb{N} P(n)$:

Démontrer que $\forall n [(\forall k < n P(k)) \rightarrow P(n)]$, où n et k sont compris entre les entiers naturels de cette affirmation. Bien sûr, la manière la plus directe de le prouver est de poser n comme entier naturel arbitraire, de supposer que $\forall k < n P(k)$, puis de démontrer $P(n)$.

Notez qu'aucun cas de base n'est nécessaire dans une preuve par induction forte. Il suffit d'une forme modifiée de l'étape d'induction,

prouvant que si tout entier naturel inférieur à n possède la propriété P , alors n possède la propriété P . Dans une preuve par induction forte, on appelle *hypothèse inductive* l' hypothèse selon laquelle tout entier naturel inférieur à n possède la propriété P .

Pour comprendre pourquoi l'induction forte fonctionne, il peut être utile de commencer par rappeler brièvement pourquoi l'induction ordinaire fonctionne. Rappelons qu'une preuve par induction ordinaire nous permet de passer en revue tous les entiers naturels dans l'ordre et de constater que chacun d'eux possède une propriété P . Le cas de base lance le processus, et l'étape d'induction montre que le processus peut toujours être poursuivi d'un nombre à l'autre. Mais notez que dans ce processus, au moment où nous vérifions qu'un entier naturel n possède la propriété P , nous avons déjà vérifié que *tous les nombres plus petits* possèdent cette propriété. Autrement dit, nous savons déjà que $\forall k < n P(k)$. L'idée derrière l'induction forte est que nous devrions pouvoir utiliser cette information dans notre preuve de $P(n)$.

Français Travaillons plus attentivement les détails de cette idée. Supposons que nous ayons suivi la stratégie de preuve par induction forte et que nous ayons prouvé l'énoncé $\forall n [(\forall k < n P(k)) \rightarrow P(n)]$. Ensuite, en remplaçant n par 0 , nous pouvons conclure que $(\forall k < 0 P(k)) \rightarrow P(0)$. Mais comme il n'y a pas de nombres naturels plus petits que 0 , l'énoncé $\forall k < 0 P(k)$ est vide de sens. Par conséquent, par modus ponens, $P(0)$ est vrai. (Ceci explique pourquoi le cas de base n'a pas besoin d'être vérifié séparément dans une preuve par induction forte ; le cas de base $P(0)$ découle en fait de la forme modifiée de l'étape d'induction utilisée dans l'induction forte.) De même, en remplaçant n par 1 , nous pouvons conclure que $(\forall k < 1 P(k)) \rightarrow P(1)$. Le seul entier naturel inférieur à 1 est 0 , et nous venons de montrer que $P(0)$ est vrai, donc l'affirmation $\forall k < 1 P(k)$ est vraie. Par conséquent, par modus ponens, $P(1)$ est également vraie. Maintenant, remplacez n par 2 pour obtenir l'affirmation $(\forall k < 2 P(k)) \rightarrow P(2)$. Puisque $P(0)$ et $P(1)$ sont tous deux vrais, l'affirmation $\forall k < 2 P(k)$ est vraie, et donc par modus ponens, $P(2)$ est vraie. En continuant de cette manière, nous pouvons montrer que $P(n)$ est vrai pour tout entier naturel n , comme requis. Pour une justification alternative de la méthode d'induction forte, voir [l'exercice 1](#).

Comme premier exemple de la méthode d'induction forte, nous prouvons un fait important de la théorie des nombres connu sous le nom d'*algorithme de division* .[1](#)

Théorème 6.4.1. (Algorithme de division) *Pour tout entier naturel n et m , si $m > 0$, alors il existe des entiers naturels q et r tels que $n = qm + r$ et $r < m$. (Les nombres q et r sont appelés quotient et reste lorsque n est divisé par m .)*

Travail à partir de zéro

Soit m un entier positif arbitraire, puis nous utilisons l'induction forte pour prouver que $\forall n \exists q \exists r (n = qm + r \wedge r < m)$. Selon la description de l'induction forte, cela signifie que nous devrions soit n un nombre naturel arbitraire, supposer que $\forall k < n \exists q \exists r (k = qm + r \wedge r < m)$, et prouver que $\exists q \exists r (n = qm + r \wedge r < m)$.

Notre objectif est une affirmation existentielle, nous devrions donc essayer de trouver des valeurs de q et r avec les propriétés requises. Si $n < m$ alors c'est facile car nous pouvons simplement poser $q = 0$ et $r = n$. Mais si $n \geq m$, alors cela ne fonctionnera pas, car nous devons avoir $r < m$, nous devons donc procéder différemment dans ce cas. Comme d'habitude dans les preuves par induction, nous nous intéressons à l'hypothèse inductive. L'hypothèse inductive commence par $\forall k < n$, donc pour l'appliquer nous devrions remplacer k par un entier naturel plus petit que n , mais que remplacer ? La référence à la division dans l'énoncé du théorème fournit un indice. Si nous considérons la division comme une soustraction répétée, alors diviser n par m revient à soustraire m de n à plusieurs reprises. La première étape de ce processus serait de calculer $n - m$, qui est un entier naturel plus petit que n . Peut-être devrions-nous remplacer k par $n - m$. On ne sait pas exactement où cela mènera, mais cela vaut la peine d'essayer. En fait, comme vous le verrez dans la démonstration, une fois cette étape franchie, la conclusion souhaitée découle presque immédiatement.

Notez que nous utilisons l'existence d'un quotient et d'un reste pour un nombre naturel inférieur à n afin de prouver leur existence pour n , mais ce nombre $n - 1$ n'est pas $n - 1$, mais $n - m$. C'est pourquoi nous utilisons l'induction forte plutôt que l'induction ordinaire pour cette démonstration.

Preuve. Soit m un entier positif arbitraire et procérons ensuite par induction forte sur n .

Supposons que n soit un nombre naturel et que pour chaque $k < n$ il existe des nombres naturels q et r tels que $k = qm + r$ et $r < m$.

Cas 1. $n < m$. Soit $q = 0$ et $r = n$. Alors clairement $n = qm + r$ et $r < m$.

Cas 2. $n \geq m$. Soit $k = n - m < n$ et notons que puisque $n \geq m$, k est un entier naturel. Par l'hypothèse inductive on peut choisir q' et r' tels que $k = q'm + r'$ et $r' < m$. Alors $n - m = q'm + r'$, donc $n = q'm + r' + m = (q' + 1)m + r'$. Ainsi, si on pose $q = q' + 1$ et $r = r'$, alors on a $n = qm + r$ et $r < m$, comme requis.

□

L'algorithme de division peut également être étendu aux entiers négatifs n , et il est possible de démontrer que pour tout nombre m et n ,

le quotient et le reste q et r sont uniques. Pour plus d'informations, voir [l'exercice 14](#).

L'exemple suivant est un autre théorème important de la théorie des nombres. Nous l'avons utilisé dans notre démonstration, en introduction, de l'existence d'une infinité de nombres premiers. Nous reviendrons sur ce théorème au [chapitre 7](#).

Théorème 6.4.2. *Tout entier $n > 1$ est soit premier, soit un produit de deux ou plusieurs nombres premiers.*

Travail à partir de zéro

Français Nous écrivons le but sous la forme $\forall n \in \mathbb{N} [n > 1 \rightarrow (n \text{ est premier} \vee n \text{ est un produit de nombres premiers})]$ puis utilisons l'induction forte. Ainsi, notre hypothèse inductive est $\forall k < n [k > 1 \rightarrow (k \text{ est premier} \vee k \text{ est un produit de nombres premiers})]$, et nous devons prouver que $n > 1 \rightarrow (n \text{ est premier} \vee n \text{ est un produit de nombres premiers})$. Bien sûr, nous commençons par supposer $n > 1$, et selon nos stratégies pour prouver les disjonctions, une bonne façon de compléter la preuve serait de supposer que n n'est pas premier et de prouver qu'il doit être un produit de nombres premiers. Puisque l'hypothèse que n n'est pas premier signifie $\exists a \exists b (n = ab \wedge a < n \wedge b < n)$, nous utilisons immédiatement l'instanciation existentielle pour introduire les nouvelles variables a et b dans la preuve. L'application de l'hypothèse inductive à a et b conduit maintenant à la conclusion souhaitée.

Preuve. On utilise l'induction forte. Supposons que $n > 1$, et que pour tout entier k , si $1 < k < n$ alors k est soit premier, soit un produit de nombres premiers. Bien sûr, si n est premier, il n'y a rien à prouver ; supposons donc que n ne soit pas premier. On peut alors choisir des entiers strictement positifs a et b tels que $n = ab$, $a < n$ et $b < n$. Notons que puisque $a < n = ab$, il s'ensuit que $b > 1$, et de même, $a > 1$. Ainsi, par l'hypothèse inductive, a et b sont soit premiers, soit un produit de nombres premiers. Mais puisque $n = ab$, n est un produit de nombres premiers.

□

La méthode de récursivité étudiée dans la section précédente possède également une forme forte. À titre d'exemple, considérons la définition suivante d'une suite de nombres, appelée *nombres de Fibonacci*. Ces nombres ont été étudiés pour la première fois par le mathématicien italien Léonard de Pise (vers 1170-vers 1250), plus connu sous le surnom de Fibonacci.

$$\begin{aligned}F_0 &= 0; \\F_1 &= 1; \\ \text{for every } n \geq 2, F_n &= F_{n-2} + F_{n-1}.\end{aligned}$$

Par exemple, en remplaçant $n = 2$ dans la dernière équation, nous trouvons que $F_2 = F_0 + F_1 = 0 + 1 = 1$. De même, $F_3 = F_1 + F_2 = 1 + 1 = 2$ et $F_4 = F_2 + F_3 = 1 + 2 = 3$. En continuant de cette manière, nous obtenons les valeurs suivantes :

n	0	1	2	3	4	5	6	7	8	\dots
F_n	0	1	1	2	3	5	8	13	21	\dots

Notez qu'à partir de F_2 , chaque nombre de Fibonacci est calculé en utilisant non seulement le nombre précédent de la séquence, mais aussi celui qui le précède. C'est en ce sens que la récursivité est forte. Il n'est donc pas surprenant que les preuves impliquant les nombres de Fibonacci nécessitent souvent une induction forte plutôt qu'une induction ordinaire.

Pour illustrer cela, nous allons prouver la formule remarquable suivante pour les nombres de Fibonacci :

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

Il est difficile de croire, au premier abord, que cette formule soit correcte. Après tout, les nombres de Fibonacci sont des entiers, et il n'est pas du tout évident que cette formule donne une valeur entière. Et quel est le rapport entre les nombres de Fibonacci et... ? $\sqrt{5}$? Néanmoins, une preuve par induction forte montre que la formule est correcte. (Pour voir comment cette formule pourrait être dérivée, voir [l'exercice 9.](#))

Théorème 6.4.3. Si F_n est le n -ième nombre de Fibonacci, alors

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

Travail à partir de zéro

Puisque F_0 et F_1 sont définies séparément de F_n pour $n \geq 2$, nous vérifions la formule pour ces cas séparément. Pour $n \geq 2$, la définition de F_n suggère de partir de l'hypothèse que la formule est correcte pour F_{n-2} et F_{n-1} afin de prouver qu'elle est correcte pour F_n . Puisque nous devons vérifier que la formule fonctionne pour *les deux cas précédents*, nous devons utiliser l'induction forte plutôt que l'induction forte . que

l'induction ordinaire. Le reste de la preuve est simple, même si l'algèbre devient un peu confuse.

Preuve. On utilise l'induction forte. Soit n un nombre naturel arbitraire, et supposons que pour tout $k < n$,

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

Cas 1. $n = 0$. Alors

$$\begin{aligned} \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^0 - \left(\frac{1-\sqrt{5}}{2}\right)^0}{\sqrt{5}} \\ &= \frac{1 - 1}{\sqrt{5}} = 0 = F_0. \end{aligned}$$

Cas 2. $n = 1$. Alors

$$\begin{aligned} \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1}{\sqrt{5}} \\ &= \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_1. \end{aligned}$$

Cas 3. $n \geq 2$. En appliquant ensuite l'hypothèse inductive à $n - 2$ et $n - 1$, nous obtenons

$$\begin{aligned} F_n &= F_{n-2} + F_{n-1} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\ &= \frac{\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\right] - \left[\left(\frac{1-\sqrt{5}}{2}\right)^{n-2} + \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right]}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} \left[1 + \frac{1+\sqrt{5}}{2}\right] - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2} \left[1 + \frac{1-\sqrt{5}}{2}\right]}{\sqrt{5}}. \end{aligned}$$

Notez maintenant que

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2},$$

et de même

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

En remplaçant F_n dans la formule, nous obtenons

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

□

Notez que dans la preuve du [théorème 6.4.3.](#), nous avons dû traiter séparément les cas $n = 0$ et $n = 1$. Le rôle de ces cas dans la preuve est similaire à celui du cas de base dans une preuve par induction mathématique ordinaire. Bien que nous ayons indiqué que les preuves par induction forte ne nécessitent pas de cas de base, il n'est pas rare de trouver certains cas initiaux traités séparément dans ces preuves.

Une propriété importante des entiers naturels, liée à l'induction mathématique, est le fait que tout ensemble non vide d'entiers naturels possède un plus petit élément. Ce principe, parfois appelé *principe de bon ordre*, peut être démontré par induction forte.

Théorème 6.4.4. (Principe de bon ordre) *Tout ensemble non vide de nombres naturels possède un plus petit élément.*

Travail à partir de zéro

Notre objectif est $\forall S \subseteq \mathbb{N} (\ S \neq \emptyset \rightarrow S \text{ a un plus petit élément})$. Après avoir posé S comme un sous-ensemble arbitraire de \mathbb{N} , nous prouverons la contraposée de l'énoncé conditionnel. Autrement dit, nous supposerons que S n'a pas de plus petit élément et prouverons que $S = \emptyset$. L'induction intervient : pour un ensemble $S \subseteq \mathbb{N}$, dire que $S = \emptyset$ revient à dire que $\forall n \in \mathbb{N} (\ n / \in S)$. Nous prouverons cette dernière affirmation par induction forte.

Preuve. Supposons que $S \subseteq \mathbb{N}$ et que S n'ait pas de plus petit élément. Nous allons démontrer que $\forall n \in \mathbb{N} (\ n / \in S)$, donc $S = \emptyset$. Ainsi, si $S \neq \emptyset$ alors S doit avoir un plus petit élément.

Pour prouver que $\forall n \in \mathbb{N} (\ n / \in S)$, on utilise l'induction forte. Supposons que $n \in \mathbb{N}$ et $\forall k < n (\ k / \in S)$. Clairement, si $n \in S$ alors n serait le plus petit élément de S , et cela contredirait l'hypothèse que S n'a pas de plus petit élément. Donc $n / \in S$.

□

Parfois, des preuves qui pourraient être réalisées par induction sont plutôt présentées comme des applications du principe de bon ordre. À titre d'exemple d'utilisation du principe de bon ordre dans une preuve, nous présentons une preuve $\sqrt{2}$ irrationnelle. Voir [l'exercice 2](#) pour une approche alternative de cette preuve par induction forte.

Théorème 6.4.5. $\sqrt{2}$ est irrationnel.

Travail à partir de zéro

Puisque *irrationnel* signifie « non rationnel », notre objectif est une affirmation négative. La preuve par l'absurde est donc une méthode logique. Ainsi, nous supposons $\sqrt{2}$ que est rationnel et cherchons à trouver une contradiction. L'hypothèse « $\sqrt{2}$ rationnel » signifie qu'il existe des entiers p et q tels que, $\frac{p}{q} = \sqrt{2}$.et puisque $\sqrt{2}$ est positif, nous pouvons tout aussi bien nous concentrer sur les entiers p et q *positifs*. Puisqu'il s'agit d'une affirmation existentielle, notre prochaine étape devrait probablement consister à considérer p et q comme des entiers positifs tels que. $\frac{p}{q} = \sqrt{2}$.Comme vous le verrez dans la démonstration, de simples manipulations algébriques de l'équation $\frac{p}{q} = \sqrt{2}$ ne conduisent pas à des contradictions évidentes, mais elles conduisent à la conclusion que p et q doivent être pairs. Ainsi, dans la fraction p / q , nous pouvons annuler un 2 au numérateur et au dénominateur, obtenant une nouvelle fraction avec un numérateur et un dénominateur plus petits, égale à $\sqrt{2}$.

Comment pouvons-nous déduire une contradiction de cette conclusion ? L'idée clé est de noter que notre raisonnement s'appliquerait à *toute* fraction égale à . $\sqrt{2}$.Ainsi, dans toute fraction de ce type, on peut annuler un facteur 2 du numérateur et du dénominateur, et il ne peut donc y avoir de plus petit numérateur ou dénominateur possible pour une telle fraction. Mais cela violerait le principe de bon ordre ! D'où notre contradiction.

Cette idée est explicitée plus en détail dans la preuve suivante, où nous avons appliqué le principe de bon ordre à l'ensemble de tous les dénominateurs possibles des fractions égales à . $\sqrt{2}$.Nous avons choisi de placer cette application du principe de bon ordre au début de la preuve, car cela semble donner la preuve la plus courte et la plus directe. Les lecteurs de la preuve pourraient être perplexes au premier abord quant à l'utilisation du principe de bon ordre (à moins qu'ils n'aient lu ce travail de base !), mais une fois les manipulations algébriques de l'équation $\frac{p}{q} = \sqrt{2}$ terminées, la contradiction apparaît presque immédiatement. C'est un bon exemple de la façon dont une étape astucieuse et soigneusement planifiée en début de preuve peut mener à une excellente chute à la fin de la preuve.

Preuve. Supposons que cela $\sqrt{2}$ soit rationnel. Cela signifie que $\exists q \in \mathbb{Z}^+ \exists p \in \mathbb{Z}^+ (p/q = \sqrt{2})$.L'ensemble $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+ (p/q = \sqrt{2})\}$ est donc non vide. Par le principe de bon ordre, nous pouvons définir q comme le plus petit élément de S . Puisque $q \in S$, nous pouvons choisir un $p \in \mathbb{Z}^+$ tel que, $\frac{p}{q} = \sqrt{2}$.donc $p^2 / q^2 = 2$, donc $p^2 = 2q^2$ et donc p^2 est pair. Appliquons maintenant le théorème de [l'exemple 3.4.3](#) , qui stipule que pour tout entier x , x est pair ssi x^2 est pair. Puisque p^2 est pair, p doit être pair, nous pouvons donc choisir un $\bar{p} \in \mathbb{Z}^+$ tel que, $p = 2\bar{p}$.donc, $p^2 = 4\bar{p}^2$.en

remplaçant cela dans l'équation $p^2 = 2q^2$, nous obtenons $4\bar{p}^2 = 2q^2$, so $2\bar{p}^2 = q^2$ et donc q^2 est pair. En faisant à nouveau appel à [l'exemple 3.4.3](#), cela signifie que q doit être pair, donc nous pouvons en choisir un $\bar{q} \in \mathbb{Z}^+$ tel que $q = 2\bar{q}$. Mais alors $\sqrt{2} = p/q = (2\bar{p})/(2\bar{q}) = \bar{p}/\bar{q}$, so $\bar{q} \in S$. Clairement $\bar{q} < q$, cela contredit le fait que q a été choisi pour être le *plus petit* élément de S . Par conséquent, $\sqrt{2}$ est irrationnel.

□

Exercices

- *1. Cet exercice propose une autre façon de justifier la méthode d'induction forte. Toutes les variables de cet exercice sont supérieures à \mathbb{N} . Supposons que $P(n)$ soit un énoncé portant sur un entier naturel n , et supposons qu'en suivant la stratégie d'induction forte, nous ayons prouvé que $\forall n [(\forall k < n P(k)) \rightarrow P(n)]$. Soit $Q(n)$ l'énoncé $\forall k < n P(k)$.
- Démontrer que $\forall n Q(n) \leftrightarrow \forall n P(n)$ sans utiliser l'induction.
 - Démontrer $\forall n Q(n)$ par induction *ordinaire*. Ainsi, d'après la partie (a), $\forall n P(n)$ est vrai.
2. Réécrivez la preuve du [théorème 6.4.5](#) comme une preuve par induction forte que $\forall q \in \mathbb{N} [q > 0 \rightarrow \neg \exists p \in \mathbb{Z}^+ (p/q = \sqrt{2})]$.
3. Dans cet exercice, vous donnerez une autre preuve $\sqrt{2}$ irrationnelle. Supposons $\sqrt{2}$ que soit rationnel. Comme dans la preuve du [théorème 6.4.5](#), sois $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+ (p/q = \sqrt{2})\} \neq \emptyset$, soit q le plus petit élément de S , et soit p un entier positif tel que $p/q = \sqrt{2}$. Maintenant, obtenons une contradiction en montrant que $p - q \in S$ et $p - q < q$.
- *4. (a) Démontrer que $\sqrt{6}$ c'est irrationnel.
(b) Prouver que $\sqrt{2} + \sqrt{3}$ c'est irrationnel.
5. Le système monétaire martien utilise des perles colorées au lieu de pièces. Une perle bleue vaut 3 crédits martiens et une perle rouge 7 crédits martiens. Ainsi, trois perles bleues valent 9 crédits, et une perle bleue et une perle rouge ensemble valent 10 crédits, mais aucune combinaison de perles bleues et rouges ne vaut 11 crédits. Démontrer que pour tout $n \geq 12$, il existe une combinaison de perles bleues et rouges valant n crédits.
6. Supposons que x soit un nombre réel, $x \neq 0$ et $x + 1/x$ un entier. Démontrer que pour tout $n \geq 1$, $x^n + 1/x^n$ est un entier.
- *7. Soit F_n le n -ième *nombre de Fibonacci*. Toutes les variables de cet exercice sont supérieures à \mathbb{N} .
- Démontrer que pour tout n , $\sum_{i=0}^n F_i = F_{n+2} - 1$.
 - Démontrer que pour tout n , $\sum_{i=0}^n (F_i)^2 = F_n F_{n+1}$.
 - Démontrer que pour tout n , $\sum_{i=0}^n F_{2i+1} = F_{2n+2}$.
 - Trouvez une formule pour $\sum_{i=0}^n F_{2i}$ et prouvez que votre formule est correcte.
8. Soit F_n le n -ième *nombre de Fibonacci*. Toutes les variables de cet exercice sont supérieures à \mathbb{N} .
- Démontrer que pour tout $m \geq 1$ et tout n , $F_{m+n} = F_{m-1} F_n + F_m F_{n+1}$.

(b) Démontrer que pour tout $m \geq 1$ et tout $n \geq 1$, $F_{m+n} = F_{m+1}F_{n+1} - F_{m-1}F_{n-1}$.

(c) Démontrer que pour tout n , $(F_n)^2 + (F_{n+1})^2 = F_{2n+1}$ et $(F_{n+2})^2 - (F_n)^2 = F_{2n+2}$.

(d) Démontrer que pour tout m et n , si $m \mid n$ alors $F_m \mid F_n$.

(e) Voir [l'exercice 18](#) de [la section 6.3](#) pour la signification de la notation utilisée dans cet exercice. Démontrer que pour tout $n \geq 1$,

$$\begin{aligned} F_{2n-1} &= \binom{2n-2}{0} + \binom{2n-3}{1} + \binom{2n-4}{2} + \cdots + \binom{n-1}{n-1} \\ &= \sum_{i=0}^{n-1} \binom{2n-i-2}{i} \end{aligned}$$

et

$$\begin{aligned} F_{2n} &= \binom{2n-1}{0} + \binom{2n-2}{1} + \binom{2n-3}{2} + \cdots + \binom{n}{n-1} \\ &= \sum_{i=0}^{n-1} \binom{2n-i-1}{i}. \end{aligned}$$

*9. Une suite de nombres a_0, a_1, a_2, \dots est appelée *suite de Fibonacci généralisée*, ou *suite de Gibonacci* en abrégé, si pour tout $n \geq 2$, $a_n = a_{n-2} + a_{n-1}$. Ainsi, une suite de Gibonacci satisfait la même *relation de récurrence* que les nombres de Fibonacci, mais son origine peut être différente.

(a) Supposons que c soit un nombre réel et $\forall n \in \mathbb{N}$ ($a_n = c^n$). Démontrer que a_0, a_1, a_2, \dots est une suite de Gibonacci ssi $c = (1 + \sqrt{5})/2$ ou $c = (1 - \sqrt{5})/2$.

(b) Supposons que s et t soient des nombres réels, et pour tout $n \in \mathbb{N}$,

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

Démontrer que a_0, a_1, a_2, \dots est une suite de Gibonacci.

(c) Supposons que a_0, a_1, a_2, \dots soit une suite de Gibonacci. Démontrer qu'il existe des nombres réels s et t tels que pour tout $n \in \mathbb{N}$,

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

(Indice : montrez d'abord qu'il existe des nombres réels s et t tels que la formule ci-dessus est correcte pour a_0 et a_1 . Montrez ensuite qu'avec ce choix de s et t , la formule est correcte pour tout n .)

10. Les *nombres de Lucas* (du nom du mathématicien français Édouard Lucas (1842–1891)) sont les nombres L_0, L_1, L_2, \dots définis comme suit :

$$\begin{aligned}L_0 &= 2; \\L_1 &= 1; \\ \text{for every } n \geq 2, L_n &= L_{n-2} + L_{n-1}.\end{aligned}$$

Trouvez une formule pour L_n et prouvez que votre formule est correcte. (Indice : appliquez [l'exercice 9.](#))

11. Une séquence a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$\begin{aligned}a_0 &= -1; \\a_1 &= 0; \\ \text{for every } n \geq 2, a_n &= 5a_{n-1} - 6a_{n-2}.\end{aligned}$$

Trouvez une formule pour a_n et prouvez que votre formule est correcte. (Indice : imitez [l'exercice 9.](#))

12. Une séquence a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$\begin{aligned}a_0 &= 0; \\a_1 &= 1; \\a_2 &= 1; \\ \text{for every } n \geq 3, a_n &= \frac{1}{2}a_{n-3} + \frac{3}{2}a_{n-2} + \frac{1}{2}a_{n-1}.\end{aligned}$$

Démontrer que pour tout $n \in \mathbb{N}$, $a_n = F_n$, le n ième nombre de Fibonacci.

13. Pour tout entier positif n , soit $A_n = \{1, 2, \dots, n\}$, et soit $P_n = \{X \in \mathcal{P}(A_n) \mid X \text{ ne contient pas deux entiers consécutifs}\}$. Par exemple, $P_3 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 3\}\}$; P_3 ne contient pas les ensembles $\{1, 2\}$, $\{2, 3\}$ et $\{1, 2, 3\}$ car chacun contient au moins une paire d'entiers consécutifs. Démontrer que pour tout n , le nombre d'éléments de P_n est F_{n+2} , le $(n+2)$ -ième nombre de Fibonacci. (Par exemple, le nombre d'éléments de P_3 est $5 = F_5$. Indice : Quels éléments de P_n contiennent n ? Lesquels n'en contiennent pas? Les réponses aux deux questions sont liées aux éléments de P_m , pour un certain $m < n$.)

14. Supposons que n et m soient des entiers et que $m > 0$.

(a) Démontrer qu'il existe des entiers q et r tels que $n = qm + r$ et $0 \leq r < m$. (Indice : Si $n \geq 0$, cela découle du [théorème 6.4.1](#). Si $n < 0$, commencer par appliquer [le théorème 6.4.1](#) à $-n$ et m . Une autre possibilité est d'appliquer [le théorème 6.4.1](#) à $-n-1$ et m .)

(b) Démontrer que les entiers q et r de la partie (a) sont uniques. Autrement dit, montrer que si q' et r' sont des entiers tels que $n =$

- $q' m + r'$ et $0 \leq r' < m$, alors $q = q'$ et $r = r'$.
- (c) Démontrer que pour tout entier n , une seule des affirmations suivantes est vraie : $n \equiv 0 \pmod{3}$, $n \equiv 1 \pmod{3}$, $n \equiv 2 \pmod{3}$. (Rappelons que cette notation a été introduite dans [la définition 4.5.9](#).)
15. Supposons que k soit un entier strictement positif. Démontrer qu'il existe un entier strictement positif a tel que pour tout $n > a$, $2^n \geq n^k$. (Dans le langage de [l'exercice 19](#) de [la section 5.1](#), cela implique que si $f(n) = n^k$ et $g(n) = 2^n$ alors $f \in O(g)$. Indice : Par l'algorithme de division, pour tout entier naturel n , il existe des entiers naturels q et r tels que $n = qk + r$ et $0 \leq r < k$. Par conséquent, $2^n \geq 2^{qk} = (2^q)^k$. Pour choisir a , déterminer la valeur de q nécessaire pour garantir que $2^q \geq n$. [L'exemple 6.1.3 peut vous être utile.](#))
16. (a) Supposons que k soit un entier positif, que a_1, a_2, \dots, a_k soient des nombres réels, et que f_1, f_2, \dots, f_k et g soient des fonctions de \mathbb{Z}^+ dans \mathbb{R} . Supposons également que f_1, f_2, \dots, f_k soient des éléments de $O(g)$. (Voir [l'exercice 19](#) de [la section 5.1](#) pour la signification de la notation utilisée ici.) Définissons $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ par la formule $f(n) = a_1 f_1(n) + a_2 f_2(n) + \dots + a_k f_k(n)$. Démontrer que $f \in O(g)$. (Indice : utiliser l'induction sur k et [l'exercice 19\(c\)](#) de [la section 5.1](#).)
- (b) Soit $g: \mathbb{Z}^+ \rightarrow \mathbb{R}$ défini par la formule $g(n) = 2^n$. Supposons que $a_0, a_1, a_2, \dots, a_k$ soient des nombres réels, et définissons $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ par la formule $f(n) = a_0 + a_1 n + a_2 n^2 + \dots + a_k n^k$. (Une telle fonction est appelée un *polynôme*.) Démontrer que $f \in O(g)$. (Indice : utilisez [l'exercice 15](#) et la partie (a).)
17. Une séquence a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$a_0 = 1;$$

$$\text{for every } n \in \mathbb{N}, a_{n+1} = 1 + \sum_{i=0}^n a_i.$$

Trouvez une formule pour a_n et prouvez que votre formule est correcte.

18. Une séquence a_0, a_1, a_2, \dots est définie récursivement comme suit :

$$a_0 = 1;$$

$$\text{for every } n \in \mathbb{N}, a_{n+1} = 1 + \frac{1}{a_n}.$$

Trouvez une formule pour un_n et prouvez qu'elle est correcte.
(Indice : ces nombres sont liés aux nombres de Fibonacci.)

19. Dans ce problème, vous prouverez qu'il n'existe aucun entier positif a, b, c et d tel que

$$a^2 + 2b^2 = c^2 \quad \text{and} \quad 2a^2 + b^2 = d^2. \quad (*)$$

- (a) Démontrer que pour tout entier m et n , si $3 \mid (m^2 + n^2)$ alors $3 \mid m$ et $3 \mid n$. (Indice : D'après [l'exercice 14\(c\)](#), soit $m \equiv 0 \pmod{3}$, soit $m \equiv 1 \pmod{3}$, soit $m \equiv 2 \pmod{3}$, et aussi soit $n \equiv 0 \pmod{3}$, soit $n \equiv 1 \pmod{3}$, soit $n \equiv 2 \pmod{3}$. Cela donne neuf possibilités. Déterminer lesquelles sont compatibles avec l'hypothèse $3 \mid (m^2 + n^2)$.)

Supposons maintenant qu'il existe des entiers positifs satisfaisant (*). Soit

$$S = \{d \in \mathbb{Z}^+ \mid \exists a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+ \exists c \in \mathbb{Z}^+ (a^2 + 2b^2 = c^2 \wedge 2a^2 + b^2 = d^2)\}.$$

Alors $S \neq \emptyset$, donc par le principe de bon ordre, nous pouvons laisser d être le plus petit élément de S . Soient a, b et c des entiers positifs satisfaisant (*).

- (b) Démontrer que $3 \mid c$ et $3 \mid d$. (Indice : additionnez les deux équations dans (*) puis appliquez la partie (a).)
- (c) Démontrer que $3 \mid a$ et $3 \mid b$. (Indice : additionnez les deux équations dans (*) puis appliquez la partie (b).)
- (d) Montrez qu'il existe un élément de S qui est plus petit que d , ce qui contredit notre choix de d . (Indice : Combinez les parties (b) et (c).)
20. Le nombre $\frac{1+\sqrt{5}}{2}$ qui apparaît dans la formule des nombres de Fibonacci du [théorème 6.4.3](#) est appelé le *nombre d'or*. Il est généralement noté φ et apparaît dans de nombreux contextes en mathématiques, en art et dans le monde naturel. Dans cet exercice, vous étudierez quelques contextes mathématiques dans lesquels φ apparaît.
- (a) Dans [la figure 6.14](#), $AEDF$ est un carré. Montrer que si le rapport entre la longueur du côté le plus long du rectangle $BCFE$ et celle de son côté le plus court est égal au rapport entre la longueur du côté le plus long du rectangle $ABCD$ et celle de son côté le plus court, alors ce rapport est φ .
- (b) Montrer que $\cos(36^\circ) = \varphi/2$. (Indice : Soit $x = \cos(36^\circ)$. Montrer d'abord que $\cos(108^\circ) = -\cos(72^\circ)$. Utiliser ensuite des identités trigonométriques pour exprimer $\cos(108^\circ)$ et $\cos(72^\circ)$ en fonction de x . Remplacer dans l'équation par $\cos(108^\circ) = -\cos(72^\circ)$

•) pour obtenir une équation impliquant x , puis résoudre l'équation.)

- (c) Dans [la figure 6.15](#) , $ABCDE$ est un pentagone régulier de côté 1. Montrez que la diagonale AC a pour longueur φ . (Indice : Commencez par trouver les angles du triangle ABC ; [l'exemple 6.2.3 peut vous être utile](#). Utilisez ensuite la partie (b).)

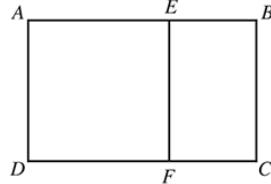


Figure 6.14.

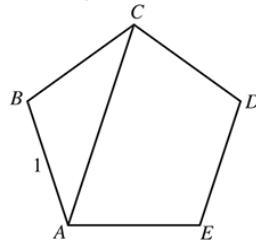


Figure 6.15.

21. La loi commutative de la multiplication stipule que pour tout nombre a et b , $ab = ba$. La loi associative stipule que pour tout nombre a , b et c , $(ab) c = a (bc)$. Dans ce problème, vous montrerez que, bien que ces lois soient énoncées pour des produits de deux ou trois nombres, elles peuvent servir à justifier le réordonnancement et le regroupement des termes d'un produit de n'importe quelle liste de nombres, de n'importe quelle manière.

- (a) Utilisez les lois commutatives et associatives pour montrer que pour tous les nombres a , b , c et d , $(ab)(cd) = c ((ad) b)$.
 (b) Disons que le *produit groupé à gauche* d'une liste de nombres a_1 , a_2 , ..., a_n est le produit dans lequel les termes sont groupés comme suit :

$$(\cdots (((a_1 a_2) a_3) a_4) \cdots a_{n-1}) a_n.$$

Plus précisément, nous pouvons définir le produit groupé à gauche de manière récursive comme suit : pour une liste constituée d'un seul nombre a_1 , le produit groupé à gauche est a_1 . Si le produit groupé à gauche de a_1 , a_2 , ..., a_n est p , alors le produit groupé à gauche de a_1 , a_2 , ..., a_n , a_{n+1} est $p a_{n+1}$. Utilisez la loi associative pour montrer que tout produit d'une liste de nombres a_1 , a_2 , ..., a_n (avec les termes dans cet ordre, mais avec des parenthèses

insérées pour regrouper les termes de n'importe quelle manière) est égal au produit groupé à gauche.

- (c) Utilisez les lois commutatives et associatives pour montrer que deux produits quelconques des nombres a_1, a_2, \dots, a_n , avec les termes dans n'importe quel ordre et groupés de n'importe quelle manière, sont égaux.

6.5. Fermetures à nouveau

Dans [la section 5.4](#), nous avons promis d'utiliser l'induction mathématique pour proposer un traitement alternatif des fermetures d'ensembles sous des fonctions. Dans cette section, nous tenons cette promesse.

Rappelons que si $f: A \rightarrow A$ et $B \subseteq A$, alors la fermeture de B par f est le plus petit ensemble $C \subseteq A$ tel que $B \subseteq C$ et C soit fermé par f . Dans cette section, nous trouverons cet ensemble C en commençant par B puis en ajoutant uniquement les éléments de A qui doivent être ajoutés pour obtenir un ensemble fermé par f . Nous commençons par une description sommaire de la manière dont nous allons procéder, motivée par les exemples de [la section 5.4](#). Ensuite, nous utiliserons la récursivité et l'induction pour préciser cette idée sommaire et prouver qu'elle fonctionne.

Français Comme nous l'avons vu dans les exemples de [la Section 5.4](#), si nous voulons trouver un ensemble $C \subseteq A$ tel que $B \subseteq C$ et C soit fermé par f , alors pour tout $x \in B$, nous devons avoir $f(x) \in C$. Autrement dit, $\{f(x) \mid x \in B\} \subseteq C$. Rappelons de [la Section 5.5](#) que $\{f(x) \mid x \in B\}$ est appelée l'image de B par f , et est notée $f(B)$. Nous aurons donc besoin d'avoir $f(B) \subseteq C$. Mais alors un raisonnement similaire implique que l'image de $f(B)$ par f doit aussi être un sous-ensemble de C ; autrement dit, $f(f(B)) \subseteq C$.

Continuer de cette façon conduit à une suite d'ensembles qui doivent être contenus dans C : $B, f(B), f(f(B)),$ et ainsi de suite. Nous allons prouver que rassembler ces ensembles en prenant leur union nous donnera la fermeture de B sous f . En d'autres termes, si nous posons $B_0 = B, B_1 = f(B), B_2 = f(f(B)), \dots$, alors la fermeture de B sous f est $B_0 \cup B_1 \cup B_2 \cup \dots$. L'utilisation d'ellipses dans notre description de ce processus suggère que pour le rendre précis, nous devrions utiliser l'induction et la récursivité. C'est ce que nous faisons dans l'énoncé et la preuve de notre prochain théorème.

Théorème 6.5.1. Supposons $f : A \rightarrow A$ et $B \subseteq A$. Soient les ensembles B_0, B_1, B_2, \dots être défini récursivement comme suit :

$$B_0 = B; \\ \text{for all } n \in \mathbb{N}, B_{n+1} = f(B_n).$$

Alors la fermeture de B sous f est l'ensemble $\bigcup_{n \in \mathbb{N}} B_n$.

Preuve. Soit $C = \bigcup_{n \in \mathbb{N}} B_n$. Puisque $f : A \rightarrow A$, il n'est pas difficile de voir que tout ensemble B_n est un sous-ensemble de A , et donc $C \subseteq A$. D'après la définition de la fermeture, il faut vérifier que $B \subseteq C$, C est fermé par f , et pour tout ensemble $D \subseteq A$, si $B \subseteq D$ et D est fermé par f alors $C \subseteq D$.

La première de ces hypothèses est vraie car $B = B_0 \subseteq \bigcup_{n \in \mathbb{N}} B_n = C$ pour la seconde, supposons que $x \in C$. Alors, par définition de C , nous pouvons choisir un $m \in \mathbb{N}$ tel que $x \in B_m$. Mais alors $f(x) \in f(B_m) = B_{m+1}$, donc $f(x) \in \bigcup_{n \in \mathbb{N}} B_n = C$. Puisque x est un élément arbitraire de C , cela montre que C est fermé sous f .

Supposons enfin que $B \subseteq D \subseteq A$ et que D soit fermé par f . Il faut montrer que $C \subseteq D$, et par définition de C il suffit de montrer que $\forall n \in \mathbb{N} (B_n \subseteq D)$. On le prouve par récurrence sur n .

Français Le cas de base est vérifié car nous avons $B_0 = B \subseteq D$ par hypothèse. Pour l'étape d'induction, supposons que $n \in \mathbb{N}$ et $B_n \subseteq D$. Supposons maintenant $x \in B_{n+1}$. Par définition de B_{n+1} cela signifie $x \in f(B_n)$, donc il existe un $b \in B_n$ tel que $x = f(b)$. Mais par l'hypothèse inductive, $B_n \subseteq D$, donc $b \in D$, et comme D est fermé par f il s'ensuit que $x = f(b) \in D$. Puisque x était un élément arbitraire de B_{n+1} , cela montre que $B_{n+1} \subseteq D$.

□

Commentaire. Comme la preuve doit souvent faire référence à l'ensemble $\bigcup_{n \in \mathbb{N}} B_n$, il est pratique de lui donner le nom C dès le début de la preuve. La preuve affirme qu'il n'est pas difficile de voir que pour tout $n \in \mathbb{N}$, $B_n \subseteq A$, et donc $C \subseteq A$. Comme d'habitude, si vous ne comprenez pas pourquoi cela est vrai, vous devriez travailler vous-même les détails de la preuve. (Vous pourriez essayer de prouver $\forall n \in \mathbb{N} (B_n \subseteq A)$ par induction mathématique.) La définition de la clôture nous dit alors que nous devons prouver trois affirmations : $B \subseteq C$, C est fermé par f , et pour tout $D \subseteq A$, si $B \subseteq D$ et D est fermé par f alors $C \subseteq D$. Bien sûr, nous les prouvons une par une.

Français La preuve de la première de ces affirmations, $B \subseteq C$, n'est pas non plus élaborée en détail. Si vous avez du mal à la suivre,

consultez [l'exercice 8 de la section 3.3](#). La deuxième affirmation que nous devons prouver dit que C est fermé par f , et la preuve est basée sur la définition de fermé : nous posons x arbitraire, supposons $x \in C$, et prouvons que $f(x) \in C$. Selon la définition de C , l'affirmation $x \in C$ signifie $\exists n \in \mathbb{N} (x \in B_n)$, nous introduisons donc immédiatement la variable m pour représenter un entier naturel tel que $x \in B_m$. L'objectif $f(x) \in C$ est également une affirmation existentielle, donc pour la prouver nous devons trouver un entier naturel k tel que $f(x) \in B_k$. La preuve montre que $k = m + 1$ fonctionne.

Enfin, pour prouver la troisième affirmation, nous utilisons la stratégie naturelle qui consiste à poser D comme un ensemble arbitraire, en supposant que $B \subseteq D \subseteq A$ et que D est fermé par f , puis en prouvant que $C \subseteq D$. Encore une fois, si vous ne voyez pas pourquoi la conclusion $C \subseteq D$ découle de $\forall n \in \mathbb{N} (B_n \subseteq D)$, comme indiqué dans la preuve, vous devriez travailler les détails de la preuve vous-même. Cette dernière affirmation est prouvée par induction, comme on pourrait s'y attendre d'après la nature récursive de la définition de B_n . Pour l'étape d'induction, nous posons n comme un nombre naturel arbitraire, supposons que $B_n \subseteq D$, et prouvons que $B_{n+1} \subseteq D$. Pour prouver que $B_{n+1} \subseteq D$ nous prenons un élément arbitraire de B_{n+1} et prouvons qu'il doit être un élément de D . L'écriture de la définition récursive de B_{n+1} nous donne un moyen d'utiliser l'hypothèse inductive, qui, comme d'habitude, est la clé pour terminer l'étape d'induction.

Nous terminons ce chapitre en revenant une fois de plus à l'une des démonstrations de l'introduction. Rappelons que, dans notre première démonstration, nous avons utilisé la formule

$$(2^b - 1) \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) = 2^{ab} - 1.$$

Nous avons de nouveau discuté de cette démonstration à [la section 3.7](#) et promis de fournir une démonstration plus détaillée de cette formule après avoir abordé l'induction mathématique. Nous sommes maintenant prêts à la présenter. Bien entendu, nous pouvons maintenant énoncer la formule plus précisément en utilisant la notation sommative.

Théorème 6.5.2. *Pour tous les entiers positifs a et b ,*

$$(2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} = 2^{ab} - 1.$$

Preuve. Soit b un entier positif arbitraire et procérons ensuite par récurrence sur a .

Cas de base : Lorsque $a = 1$, nous avons

$$\begin{aligned}(2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} &= (2^b - 1) \cdot \sum_{k=0}^0 2^{kb} \\ &= (2^b - 1) \cdot 1 \\ &= 2^{ab} - 1.\end{aligned}$$

Étape d'induction : Supposons que $a \geq 1$ et $(2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} = 2^{ab} - 1$ alors

$$\begin{aligned}(2^b - 1) \cdot \sum_{k=0}^a 2^{kb} &= (2^b - 1) \cdot \left(\sum_{k=0}^{a-1} 2^{kb} + 2^{ab} \right) \\ &= (2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} + 2^b \cdot 2^{ab} - 2^{ab} \\ &= 2^{ab} - 1 + 2^{b+ab} - 2^{ab} \quad (\text{inductive hypothesis}) \\ &= 2^{(a+1)b} - 1.\end{aligned}$$

□

Exercices

- *1. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = x + 1$, et soit $B = \{0\}$. Nous avons vu dans la partie 2 de [l'exemple 5.4.4](#) que la fermeture de B par f est \mathbb{N} . Quels sont les ensembles B_0, B_1, B_2, \dots définis dans [le théorème 6.5.1](#) ?
2. Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x) = x - 1$, et soit $B = \mathbb{N}$. Nous avons vu après [l'exemple 5.4.2](#) que la fermeture de B par f est \mathbb{Z} . Quels sont les ensembles B_0, B_1, B_2, \dots définis dans [le théorème 6.5.1](#) ?
3. Supposons que \mathcal{F} soit un ensemble de fonctions de A dans A et que $B \subseteq A$. Dans [l'exercice 12 de la section 5.4](#), nous avons défini la fermeture de B par \mathcal{F} comme étant le plus petit ensemble $C \subseteq A$ tel que $B \subseteq C$ et que pour tout $f \in \mathcal{F}$, C soit fermé par f . Soient les ensembles B_0, B_1, B_2, \dots définis récursivement comme suit :

$$\begin{aligned}B_0 &= B; \\ \text{for all } n \in \mathbb{N}, B_{n+1} &= \bigcup_{f \in \mathcal{F}} f(B_n).\end{aligned}$$

Démontrer que $\bigcup_{n \in \mathbb{N}} B_n$ c'est la fermeture de B sous \mathcal{F} .

- *4. Pour tout entier naturel n , soit $f_n : \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ défini par la formule $f_n(X) = X \cup \{n\}$, et soit $\mathcal{F} = \{f_n \mid n \in \mathbb{N}\}$. Soit $B = \{\emptyset\}$. Dans la partie (b) de [l'exercice 12](#) de [la section 5.4](#), vous avez montré que la clôture de B par \mathcal{F} est l'ensemble de tous les sous-ensembles finis de \mathbb{N} . Quels sont les ensembles B_0, B_1, B_2, \dots définis dans [l'exercice 3](#) ?
- *5. Soit $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ défini par la formule $f(x, y) = xy$. Soit P l'ensemble de tous les nombres premiers. Quelle est la clôture de P par f ?
6. Considérez le théorème incorrect suivant :

Théorème incorrect. Supposons $f : A \times A \rightarrow A$ et $B \subseteq A$. Soient les ensembles B_0, B_1, B_2, \dots définis récursivement comme suit :

$$\begin{aligned} B_0 &= B; \\ \text{for all } n \in \mathbb{N}, \quad B_{n+1} &= f(B_n \times B_n). \end{aligned}$$

Alors la fermeture de B sous f est l'ensemble $\bigcup_{n \in \mathbb{N}} B_n$.

Quel est le problème avec la preuve suivante du théorème ?

Preuve $C = \bigcup_{n \in \mathbb{N}} B_n$. Il n'est pas difficile de voir que chaque ensemble B_n est un sous-ensemble de A , donc $C \subseteq A$, et $B = B_0 \subseteq C$.

Pour voir que C est fermé sous f , supposons $x, y \in C$. Alors par définition de C , il existe un $m \in \mathbb{N}$ tel que $x, y \in B_m$. Par conséquent

$$f(x, y) \in f(B_m \times B_m) = B_{m+1}, \text{ so } f(x, y) \in \bigcup_{n \in \mathbb{N}} B_n = C.$$

Finalement, supposons que $B \subseteq D \subseteq A$ et que D soit fermé par f . Pour prouver que $C \subseteq D$, il suffira de prouver que $\forall n \in \mathbb{N} (B_n \subseteq D)$. Nous le prouvons par récurrence. Le cas de base est vérifié car $B_0 = B \subseteq D$ par hypothèse. Pour l'étape de récurrence, supposons $B_n \subseteq D$ et soit $x \in B_{n+1}$ arbitraire. Par définition de B_{n+1} cela signifie que $x = f(a, b)$ pour certains $a, b \in B_n$. Par l'hypothèse inductive, $B_n \subseteq D$, donc $a, b \in D$, et puisque D est fermé par f , il s'ensuit que $x = f(a, b) \in D$. Par conséquent $B_{n+1} \subseteq D$.

-
- *7. Soit $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ défini par la formule $f(x, y) = xy$, et soit $B = \{x \in \mathbb{R} \mid -2 \leq x \leq 0\}$. Dans ce problème, vous montrerez que f et B sont un contre-exemple au théorème incorrect de [l'exercice 6](#).
- (a) Quels sont les ensembles B_0, B_1, B_2, \dots définis dans le théorème incorrect ?

(b) Montrez que $\bigcup_{n \in \mathbb{N}} B_n$ n'est pas la fermeture de B sous f . Laquelle des trois propriétés de la définition de fermeture ([Définition 5.4.8](#)) n'est pas vérifiée ?

(c) Quelle est la fermeture de B sous f ?

8. Supposons $f: A \times A \rightarrow A$ et $B \subseteq A$. Soient les ensembles B_0, B_1, B_2, \dots définis récursivement comme suit :

$$B_0 = B; \\ \text{for all } n \in \mathbb{N}, B_{n+1} = B_n \cup f(B_n \times B_n).$$

(a) Démontrer que pour tous les nombres naturels m et n , si $m \leq n$ alors $B_m \subseteq B_n$. (Indice : Soit m arbitraire, puis utiliser l'induction sur n .)

(b) Démontrer que $\bigcup_{n \in \mathbb{N}} B_n$ est la fermeture de B sous f .

9. Supposons que $f: A \rightarrow A$ et que f soit une fonction constante ; autrement dit, il existe un $c \in A$ tel que pour tout $x \in A$, $f(x) = c$. Supposons que $B \subseteq A$. Quels sont les ensembles B_0, B_1, B_2, \dots définis dans [le théorème 6.5.1](#) ? Quelle est la fermeture de B par f ?

10. L'introduction contient une autre preuve qui pourrait être formulée plus rigoureusement par récurrence. Rappelons que, pour la démonstration du théorème 4 de l'introduction, nous avons utilisé le principe suivant : si n est un entier strictement positif, $x = (n+1)! + 2$, et $0 \leq i \leq n-1$, alors $(i+2) \mid (x+i)$. Utilisez la récurrence pour le démontrer. (Nous avons utilisé ce principe pour montrer que $x+i$ n'est pas premier.)

Les exercices suivants de cette section utiliseront la définition suivante. Supposons que $R \subseteq A \times A$. Soient R^1, R^2, R^3, \dots définis récursivement comme suit :

$$R^1 = R; \\ \text{for all } n \in \mathbb{Z}^+, R^{n+1} = R^n \circ R.$$

, pour tout entier positif n , R^n est une relation sur A .

11. Supposons que $R \subseteq A \times A$. Démontrer que pour tous les entiers positifs m et n , $R^{m+n} = R^m \circ R^n$.

12. Supposons $f: A \rightarrow A$.

(a) Démontrer que pour tout entier positif n , $f^n: A \rightarrow A$.

(b) Supposons que $B \subseteq A$, et que les ensembles B_0, B_1, B_2, \dots soient définis comme dans [le théorème 6.5.1](#). Démontrer que pour tout entier positif n , $f^n(B) = B_n$.

13. Supposons $f: A \rightarrow A$ et $a \in A$. On dit que a est un *point périodique* pour f s'il existe un entier positif n tel que $f^n(a) = a$.

- (a) Montrer que si a est un point périodique pour f alors la fermeture de $\{a\}$ sous f est un ensemble fini.
- (b) Supposons que la fermeture de $\{a\}$ sous f soit un ensemble fini. a doit-il être un point périodique pour f ?
14. Supposons $R \subseteq A \times A$ et $T = \bigcup_{n \in \mathbb{Z}^+} R^n$. démontrons que T est la clôture transitive de R . (Voir [l'exercice 25](#) de [la section 4.4](#) pour la définition de la clôture transitive.)
15. Supposons que R et S soient des relations sur A et $R \subseteq S$. Démontrer que pour tout entier positif n , $R^n \subseteq S^n$.
16. Supposons que R et S soient des relations sur A et n est un entier positif.
- (a) Quelle est la relation entre $R^n \cap S^n$ et $(R \cap S)^n$? Justifiez vos conclusions par des preuves ou des contre-exemples.
- (b) Quelle est la relation entre $R^n \cup S^n$ et $(R \cup S)^n$? Justifiez vos conclusions avec des preuves ou des contre-exemples.
17. Supposons que R soit une relation sur A et que T soit la clôture transitive de R . Si $(a, b) \in T$, alors, d'après [l'exercice 14](#), il existe un entier positif n tel que $(a, b) \in R^n$, et donc, d'après le principe de bon ordre ([théorème 6.4.4](#)), il doit exister un plus petit tel n . On définit la *distance* de a à b comme étant le plus petit entier positif n tel que $(a, b) \in R^n$, et on note $d(a, b)$ pour désigner cette distance.
- (a) Supposons que $(a, b) \in T$ et $(b, c) \in T$ (et donc $(a, c) \in T$, puisque T est transitif). Démontrer que $d(a, c) \leq d(a, b) + d(b, c)$.
- (b) Supposons que $(a, c) \in T$ et $0 < m < d(a, c)$. Démontrer qu'il existe un $b \in A$ tel que $d(a, b) = m$ et $d(b, c) = d(a, c) - m$.
18. Supposons que R soit une relation sur A . Pour tout entier positif n , soit $J_n = \{0, 1, 2, \dots, n\}$. Si $a \in A$ et $b \in A$, on dira qu'une fonction $f: J_n \rightarrow A$ est un *R-chemin de a vers b de longueur n* si $f(0) = a$, $f(n) = b$, et pour tout $i < n$, $(f(i), f(i+1)) \in R$.
- (a) Démontrer que pour tout $n \in \mathbb{Z}^+$, $R^n = \{(a, b) \in A \times A \mid$ il existe un *R*-chemin de a à b de longueur $n\}$.
- (b) Démontrer que la fermeture transitive de R est $\{(a, b) \in A \times A \mid$ il existe un *R*-chemin de a à b (de n'importe quelle longueur)\}.
19. Supposons que R soit une relation sur A . Dans ce problème, nous trouvons une relation entre la distance, telle que définie dans [l'exercice 17](#), et les *R*-chemins, qui ont été discutés dans [l'exercice 18](#).
- (a) Supposons que $d(a, b) = n$ et $a \neq b$. Démontrer que si f est un *R*-chemin de a à b de longueur n , alors f est bijectif.

(b) Supposons que $d(a, a) = n$. Démontrer que si f est un R -chemin de a vers a de longueur n , alors $\forall i < n \forall j < n (f(i) = f(j) \rightarrow i = j)$.
(En d'autres termes, f est bijectif, à l'exception de $f(0) = f(n) = a$.)

20. Supposons que R soit une relation sur A , que T soit la clôture transitive de R et que A ait m éléments. Démontrer que

$$T = R \cup R^2 \cup \dots \cup R^m = \bigcup \{R^n \mid 1 \leq n \leq m\}.$$

(Indice : utilisez [l'exercice 19.](#))

¹ La terminologie utilisée ici est quelque peu regrettable, car ce que nous appelons l'algorithme de division est en réalité un théorème et non un algorithme. Néanmoins, cette terminologie est courante.

Théorie des nombres

7.1. Plus grands diviseurs communs

Dans ce chapitre, nous présenterons une introduction à la théorie des nombres : l'étude des entiers strictement positifs 1, 2, 3, Il peut sembler que ces nombres soient si faciles à comprendre que leur étude ne mènera à aucune découverte intéressante. Mais nous verrons dans ce chapitre que des questions simples sur les entiers strictement positifs peuvent être étonnamment difficiles à résoudre, et que les réponses révèlent parfois des schémas subtils et inattendus. Bien sûr, la seule façon d'être sûr des réponses à nos questions sera de fournir des preuves, en utilisant les méthodes développées dans les chapitres précédents de ce livre. Vous devriez maintenant maîtriser la lecture et l'écriture de preuves ; nous aborderons donc moins la stratégie des preuves et nous en donnerons davantage sous forme d'exercices.

Nous commençons par un concept fondamental pour toute la théorie des nombres, le *plus grand diviseur commun* d'une paire d'entiers positifs.

Définition 7.1.1. Supposons que a soit un entier strictement positif. Les *diviseurs* de a sont les entiers strictement positifs qui divisent a . On notera l'ensemble des diviseurs de a par $D(a)$. Ainsi,

$$D(a) = \{d \in \mathbb{Z}^+ \mid d \text{ divides } a\} = \{d \in \mathbb{Z}^+ \mid \exists k \in \mathbb{Z} (a = kd)\}.$$

Si a et b sont deux entiers strictement positifs, alors $D(a) \cap D(b)$ est l'ensemble des entiers strictement positifs qui divisent a et b , c'est-à-dire leurs diviseurs communs. Le plus grand élément de cet ensemble est appelé le *plus grand commun diviseur* de a et b , et est noté $\text{pgcd}(a, b)$.

Par exemple, $D(18) = \{1, 2, 3, 6, 9, 18\}$ et $D(12) = \{1, 2, 3, 4, 6, 12\}$, donc l'ensemble des diviseurs communs de 18 et 12 est $D(18) \cap D(12) = \{1, 2, 3, 6\}$. Le plus grand de ces diviseurs communs est 6, donc $\text{pgcd}(18, 12) = 6$.

Notez que 1 et a sont toujours des éléments de $D(a)$, et $D(a)$ est un ensemble fini, puisque $D(a) \subseteq \{1, 2, \dots, a\}$. Ainsi, pour deux entiers positifs quelconques a et b , $D(a) \cap D(b)$ est un ensemble fini qui est non vide (puisque il contient 1), il a donc un plus grand élément (voir [l'exercice 3 de la section 6.2](#)). En d'autres termes, $\gcd(a, b)$ est toujours défini.

Étant donnés deux entiers positifs a et b , comment calculer $\gcd(a, b)$? Une solution consiste à commencer par lister tous les éléments de $D(a)$ et $D(b)$, comme nous l'avons fait pour calculer $\gcd(18, 12)$. Cependant, si a et b sont grands, cela peut s'avérer peu pratique. Heureusement, il existe une meilleure méthode.

Puisque $D(a) \cap D(b) = D(b) \cap D(a)$, $\gcd(a, b) = \gcd(b, a)$. Autrement dit, dans notre notation du plus grand commun diviseur de deux entiers positifs, le premier entier indiqué n'a pas d'importance. Il est souvent plus pratique d'indiquer le plus grand entier en premier ; en particulier, pour calculer $\gcd(a, b)$, nous supposerons que $a \geq b$.

Une observation utile est que si $b | a$ alors $\gcd(a, b) = b$. Ceci est dû au fait que b est le plus grand élément de $D(b)$. Si $b | a$ alors b est aussi un élément de $D(a)$, il doit donc être le plus grand élément de $D(a) \cap D(b)$. Cela suggère que pour calculer $\gcd(a, b)$, où $a \geq b$, nous pourrions commencer par diviser a par b . Selon l'algorithme de division ([Théorème 6.4.1](#)), si nous divisons a par b nous trouverons des nombres naturels q et r (le quotient et le reste) tels que $a = qb + r$ et $r < b$. Si $r = 0$, alors $a = qb$, donc $b | a$ et donc $\gcd(a, b) = b$.

Mais que se passe-t-il si $r > 0$? Comment pouvons-nous calculer $\gcd(a, b)$ dans ce cas? Nous affirmons que dans ce cas, $D(a) \cap D(b) = D(b) \cap D(r)$. Démontrons ce fait. Supposons d'abord que $d \in D(a) \cap D(b)$. Alors $d | a$ et $d | b$, il existe donc des entiers j et k tels que $a = jd$ et $b = kd$. Mais alors, à partir de l'équation $a = qb + r$, nous obtenons $r = a - qb = jd - qkd = (j - qk)d$, donc $d | r$. Par conséquent $d \in D(r)$, et comme nous avons aussi $d \in D(b)$, $d \in D(b) \cap D(r)$. Un argument similaire montre que si $d \in D(b) \cap D(r)$ alors $d \in D(a) \cap D(b)$, donc $D(a) \cap D(b) = D(b) \cap D(r)$. Par définition du plus grand commun diviseur, il s'ensuit que $\gcd(a, b) = \gcd(b, r)$.

Résumons ce que nous avons appris avec un théorème.

Théorème 7.1.2. *Supposons que a et b soient des entiers positifs avec $a \geq b$. Soit r le reste lorsque l'on divise a par b . Si $r = 0$ alors $\gcd(a, b) = b$, et si $r > 0$ alors $\gcd(a, b) = \gcd(b, r)$.*

Si $r > 0$, ce théorème permet-il de calculer $\gcd(a, b)$? Une raison de le penser est que $b \leq a$ et $r < b$; il est donc probablement plus facile de calculer $\gcd(b, r)$ que $\gcd(a, b)$. Ce théorème permet donc de

remplacer notre problème initial de calcul de $\text{pgcd}(a, b)$ par celui, potentiellement plus simple, de calculer $\text{pgcd}(b, r)$.

Cela devrait vous rappeler notre étude de la récursivité au [chapitre 6](#). Une définition récursive d'une fonction f de domaine \mathbb{Z}^+ nous donne une méthode pour trouver $f(n)$ en utilisant les valeurs de $f(k)$ pour $k < n$. En utilisant cette méthode de manière répétée, nous sommes capables de calculer $f(n)$ pour tout n . Peut-être qu'en appliquant notre méthode de division de manière répétée, nous pourrons calculer $\text{gcd}(a, b)$.

Avant de généraliser cette idée, essayons-la avec un exemple. Supposons que nous cherchions à trouver le $\text{pgcd}(672, 161)$. Nous commençons par diviser $a = 672$ par $b = 161$, ce qui nous donne un quotient $q = 4$ et un reste $r = 28$:

$$672 = 4 \cdot 161 + 28.$$

D'après [le théorème 7.1.2](#), nous concluons que $\text{pgcd}(672, 161) = \text{pgcd}(a, b) = \text{pgcd}(b, r) = \text{pgcd}(161, 28)$. Essayons donc de calculer $\text{pgcd}(161, 28)$, ce qui semble plus simple.

Comment résoudre ce problème ? Par la même méthode, bien sûr ! On commence par diviser 161 par 28, ce qui donne un quotient de 5 et un reste de 21 :

$$161 = 5 \cdot 28 + 21.$$

En appliquant à nouveau [le théorème 7.1.2](#), on constate que $\text{pgcd}(161, 28) = \text{pgcd}(28, 21)$. Pour calculer $\text{pgcd}(28, 21)$, on divise 28 par 21 :

$$28 = 1 \cdot 21 + 7.$$

Ainsi, $\text{pgcd}(28, 21) = \text{pgcd}(21, 7)$. Or, $21 = 3 \cdot 7 + 0$, donc $7 \mid 21$, et donc $\text{pgcd}(21, 7) = 7$. Nous concluons que c'est la réponse à notre problème initial : $\text{pgcd}(672, 161) = 7$.

Nous pouvons résumer nos calculs avec la liste d'équations suivante :

$$\begin{aligned} 672 &= 4 \cdot 161 + 28, \\ 161 &= 5 \cdot 28 + 21, \\ 28 &= 1 \cdot 21 + 7, \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

Ces calculs produisent une liste décroissante d'entiers naturels : 672, 161, 28, 21, 7, 0. Les deux premiers nombres sont nos entiers positifs initiaux a et b ; ensuite, chaque nombre est le reste de la division du nombre précédent par celui qui le précède. Les plus grands diviseurs communs de toutes les paires adjacentes d'entiers positifs de la liste sont identiques. Le calcul s'est terminé lorsque nous avons obtenu un

reste de 0, et le dernier nombre non nul de la liste est $7 = \gcd(21, 7) = \gcd(672, 161)$.

Généralisons maintenant. Supposons que nous cherchions à trouver le $\text{pgcd}(a, b)$, où a et b sont des entiers strictement positifs et $a \geq b$. Nous définissons une suite d'entiers naturels. r_0, r_1, r_2, \dots récursivement comme suit. Pour commencer la suite, posons $r_0 = a$ et $r_1 = b$, notons que $r_0 \geq r_1$. Soit alors q_2 et r_2 le quotient et le reste de la division de r_0 par r_1 :

$$r_0 = q_2 \cdot r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

Si $r_2 \neq 0$, on divise r_1 par r_2 pour obtenir le quotient q_3 et le reste r_3 . En général, après avoir calculé r_2, r_1, \dots, r_n , si $r_2 \neq 0$, on divise r_{n-1} par r_n pour obtenir le quotient et le reste de q_{n+1} et r_{n+1} :

$$r_{n-1} = q_{n+1} \cdot r_n + r_{n+1}, \quad 0 \leq r_{n+1} < r_n.$$

Le calcul s'arrête lorsque nous atteignons un reste de 0.

Sommes-nous sûrs d'avoir finalement un reste nul ? Si ce n'est pas le cas, la suite de divisions se poursuivra indéfiniment et nous aboutirons à une suite infinie d'entiers strictement positifs r_0, r_1, r_2, \dots avec $r_0 \geq r_1 > r_2 > \dots$. Ceci est impossible, car $\{r_0, r_1, r_2, \dots\}$ serait un ensemble non vide d'entiers naturels sans plus petit élément, ce qui contredit le principe de bon ordre (théorème 6.4.4). Ainsi, nous devons finalement avoir un reste nul.

Supposons que m soit le plus grand indice pour lequel $r_m \neq 0$. Alors $r_{m+1} = 0$, et il y a m divisions, qui peuvent être résumées comme suit :

$$\begin{aligned} r_0 &= q_2 \cdot r_1 + r_2, \\ r_1 &= q_3 \cdot r_2 + r_3, \\ &\vdots \\ r_{m-1} &= q_{m+1} \cdot r_m + 0. \end{aligned}$$

En appliquant le théorème 7.1.2 à chaque division, nous concluons que

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{m-1}, r_m) = r_m.$$

Ainsi, $\gcd(a, b)$ est la dernière valeur non nulle de la séquence r_0, r_1, r_2, \dots

Cette méthode de calcul du plus grand commun diviseur de deux entiers positifs est appelée *algorithme d'Euclide*. Son nom vient d'Euclide, qui l'a décrit dans le livre VII de ses *Éléments*.

Exemple 7.1.3. Trouver le plus grand commun diviseur de 444 et 1392.

Solution

Nous appliquons l'algorithme d'Euclide avec $a = 1392$ et $b = 444$. Les calculs sont présentés dans [la figure 7.1](#). Chaque équation de la colonne « Division » montre le calcul de division qui conduit au quotient et au reste dans la ligne suivante. Le dernier reste non nul étant 12, nous concluons que $\text{pgcd}(1392, 444) = 12$.

n	q_n	r_n	Division
0		1392	
1		444	$1392 = 3 \cdot 444 + 60$
2	3	60	$444 = 7 \cdot 60 + 24$
3	7	24	$60 = 2 \cdot 24 + 12$
4	2	12	$24 = 2 \cdot 12 + 0$
5	2	0	

Figure 7.1. Calcul du $\text{pgcd}(1392, 444)$ par l'algorithme euclidien.

Dans le dernier exemple, les entrées de l'algorithme d'Euclide étaient $a = 1392$ et $b = 444$. Il est intéressant de voir comment les restes calculés sont liés à ces entrées. En réorganisant la première équation de la colonne « Division » de [la figure 7.1](#), on constate que

$$r_2 = 60 = 1392 - 3 \cdot 444 = a - 3b.$$

De même, à partir de l'équation suivante, nous obtenons

$$r_3 = 24 = 444 - 7 \cdot 60 = b - 7r_2 = b - 7(a - 3b) = -7a + 22b,$$

et la troisième équation nous donne

$$r_4 = 12 = 60 - 2 \cdot 24 = r_2 - 2r_3 = (a - 3b) - 2(-7a + 22b) = 15a - 47b.$$

On voit que chaque reste peut s'écrire sous la forme $sa + tb$, pour certains entiers s et t . On dit que chaque reste est une *combinaison linéaire* de a et b . Mais le dernier reste non nul est le plus grand commun diviseur de a et b , on conclut donc que $\text{pgcd}(a, b)$ est une combinaison linéaire de a et b : $\text{pgcd}(a, b) = r_4 = 15a - 47b$. L'application générale de ce raisonnement prouve notre prochain théorème.

Théorème 7.1.4. *Pour tous les entiers positifs a et b , il existe des entiers s et t tels que $\text{pgcd}(a, b) = sa + tb$.*

Preuve. Comme d'habitude, on peut supposer que $a \geq b$; sinon, on peut simplement inverser les valeurs de a et b . Soit r_0, r_1, \dots, r_{m+1} la suite de nombres produite par l'algorithme d'Euclide, où $r_m \neq 0$ et $r_{m+1} = 0$. On affirme que pour tout entier naturel $n \leq m$, r_n est une combinaison linéaire de a et b . Autrement dit, pour tout entier naturel

n , si $n \leq m$ alors il existe des entiers s_n et t_n tels que $r_n = s_n a + t_n b$. On démontre cette affirmation par induction forte.

Supposons que n soit un nombre naturel et $n \leq m$, et supposons également que pour tout $k < n$, r_k soit une combinaison linéaire de a et b . Nous considérons maintenant trois cas.

Cas 1 : $n = 0$. Alors $r_n = r_0 = a = s_0 a + t_0 b$, où $s_0 = 1$ et $t_0 = 0$.

Cas 2 : $n = 1$. Alors $r_n = r_1 = b = s_1 a + t_1 b$, où $s_1 = 0$ et $t_1 = 1$.

Cas 3 : $n \geq 2$. Alors r_n est le reste lorsque r_{n-2} est divisé par r_{n-1} :

$$r_{n-2} = q_n \cdot r_{n-1} + r_n.$$

Par l'hypothèse inductive, il existe des entiers s_{n-1} , s_{n-2} , t_{n-1} et t_{n-2} tels que

$$r_{n-1} = s_{n-1}a + t_{n-1}b, \quad r_{n-2} = s_{n-2}a + t_{n-2}b.$$

Donc

$$\begin{aligned} r_n &= r_{n-2} - q_n \cdot r_{n-1} = (s_{n-2}a + t_{n-2}b) - q_n(s_{n-1}a + t_{n-1}b) \\ &= (s_{n-2} - q_n s_{n-1})a + (t_{n-2} - q_n t_{n-1})b, \end{aligned}$$

donc $r_n = s_n a + t_n b$, où $s_n = s_{n-2} - q_n s_{n-1}$ et $t_n = t_{n-2} - q_n t_{n-1}$.

Ceci complète la preuve inductive selon laquelle, pour tout $n \leq m$, r_n est une combinaison linéaire de a et b . En appliquant cette affirmation au cas $n = m$, nous concluons que $\text{pgcd}(a, b) = r_m$ est une combinaison linéaire de a et b . \square

Pour une autre démonstration du [théorème 7.1.4](#), voir [l'exercice 4](#). L'un des avantages de cette démonstration est qu'elle permet de trouver les entiers s et t tels que $\text{pgcd}(a, b) = sa + tb$. En appliquant l'algorithme d'Euclide, on peut calculer les nombres s_n et t_n de manière récursive en utilisant les formules suivantes :

$$\begin{array}{ll} s_0 = 1, & t_0 = 0, \\ s_1 = 0, & t_1 = 1, \\ \text{for } n \geq 2, s_n = s_{n-2} - q_n s_{n-1}, & t_n = t_{n-2} - q_n t_{n-1}. \end{array}$$

Si m est le plus grand indice pour lequel $r_m \neq 0$, alors $\text{gcd}(a, b) = r_m = s_m a + t_m b$. La version de l'algorithme d'Euclide dans laquelle nous gardons une trace de ces nombres supplémentaires s_n et t_n est appelée *l'algorithme d'Euclide étendu*.

Exemple 7.1.5. Utilisez l'algorithme d'Euclide étendu pour trouver le $\text{pgcd}(574, 168)$ et l'exprimer comme une combinaison linéaire de 574 et 168.

Solution

Les calculs sont présentés dans [la figure 7.2](#). Nous concluons que $\text{pgcd}(574, 168) = 14 = 5 \cdot 574 - 17 \cdot 168$.

n	q_n	r_n	s_n	t_n	Division
0		574	1	0	
1		168	0	1	$574 = 3 \cdot 168 + 70$
2	3	70	$1 - 3 \cdot 0 = 1$	0	$168 = 2 \cdot 70 + 28$
3	2	28	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot (-3) = 7$	$70 = 2 \cdot 28 + 14$
4	2	14	$1 - 2 \cdot (-2) = 5$	$-3 - 2 \cdot 7 = -17$	$28 = 2 \cdot 14 + 0$
5	2	0			

Figure 7.2. Calcul de $\text{pgcd}(574, 168)$ par algorithme euclidien étendu.

En conséquence immédiate du [théorème 7.1.4](#), nous avons le fait surprenant suivant.

Théorème 7.1.6. Pour tous les entiers positifs a , b et d , si $d \mid a$ et $d \mid b$ alors $d \mid \text{pgcd}(a, b)$.

Preuve. Soient a , b et d des entiers strictement positifs, et supposons que $d \mid a$ et $d \mid b$. Il existe alors des entiers j et k tels que $a = jd$ et $b = kd$. Or, d'après [le théorème 7.1.4](#), soit s et t des entiers tels que $\text{pgcd}(a, b) = sa + tb$. Alors

$$\text{gcd}(a, b) = sa + tb = sjd + tkd = (sj + tk)d,$$

donc $d \mid \text{pgcd}(a, b)$. \square

Rappelons, comme le montre la partie 3 de [l'exemple 4.4.3](#), que la relation de divisibilité est un ordre partiel sur \mathbb{Z}^+ . On pourrait interpréter [le théorème 7.1.6](#) comme indiquant que $\text{pgcd}(a, b)$ est le plus grand élément de $D(a) \cap D(b)$ non seulement par rapport à l'ordre usuel des entiers positifs, mais aussi par rapport à l'ordre partiel de divisibilité.

Exercices

1. Soit $a = 57$ et $b = 36$.

(a) Trouvez $D(a)$, $D(b)$ et $D(a) \cap D(b)$.

(b) Utilisez l'algorithme d'Euclide pour trouver $\text{pgcd}(a, b)$.

*2. Trouvez le $\text{pgcd}(a, b)$ et exprimez-le comme une combinaison linéaire de a et b .

(a) $a = 775, b = 682$.

(b) $a = 562, b = 243$.

3. Trouvez le $\text{pgcd}(a, b)$ et exprimez-le comme une combinaison linéaire de a et b .

(a) $a = 2790, b = 1206$.

(b) $a = 191, b = 156$.

4. Complétez la démonstration alternative suivante du [théorème 7.1.4](#).

Supposons que a et b soient des entiers strictement positifs. Soit $L = \{n \in \mathbb{Z}^+ \mid \exists s \in \mathbb{Z} \ \exists t \in \mathbb{Z} (n = sa + tb)\}$. Montrez que L possède un plus petit élément. Soit d le plus petit élément de L . Montrez maintenant que $d = \text{pgcd}(a, b)$. (Indice : Montrez que lorsque l'on divise a ou b par d , le reste ne peut pas être positif.)

*5. Supposons que a et b soient des entiers positifs, et soit $d = \text{pgcd}(a, b)$. Montrer que pour tout entier n , n est une combinaison linéaire de a et b ssi $d \mid n$.

6. Démontrer que pour tous les entiers positifs a, b et c , $\text{gcd}(a, b) = \text{gcd}(a + bc, b)$.

*7. Supposons que a, a', b et b' soient des entiers positifs.

(a) Si $a \leq a'$ et $b \leq b'$, est-il vrai que $\text{pgcd}(a, b) \leq \text{pgcd}(a', b')$? Justifiez votre réponse par une preuve ou un contre-exemple.

(b) Si $a \mid a'$ et $b \mid b'$, doit-il être vrai que $\text{pgcd}(a, b) \mid \text{pgcd}(a', b')$? Justifiez votre réponse par une preuve ou un contre-exemple.

8. Démontrer que pour tout entier positif a , $\text{pgcd}(5a + 2, 13a + 5) = 1$.

*9. Démontrer que pour tous les entiers positifs a et b , $\text{pgcd}(2^a - 1, 2^b - 1) = 2^{\text{pgcd}(a, b)} - 1$.

10. Démontrer que pour tous les entiers positifs a, b et n , $\text{gcd}(na, nb) = n \text{gcd}(a, b)$.

11. Supposons que a, b et c soient des entiers positifs.

(a) Démontrer que $D(\text{gcd}(a, b)) = D(a) \cap D(b)$.

(b) Démontrer que $\text{pgcd}(\text{pgcd}(a, b), c)$ est le plus grand élément de $D(a) \cap D(b) \cap D(c)$.

12. (a) Utilisez l'algorithme d'Euclide pour trouver le $\text{pgcd}(55, 34)$. Reconnaissez-vous les nombres de la suite r_0, r_1, \dots ? (Indice : reportez-vous à [la section 6.4](#).) Combien y a-t-il d'étapes de division?

(b) Supposons que $n \geq 2$. Quel est le $\text{pgcd}(F_{n+1}, F_n)$? Combien d'étapes de division faut-il pour trouver $\text{pgcd}(F_{n+1}, F_n)$ avec l'algorithme d'Euclide? (F est le n -ième nombre de Fibonacci.)

13. Supposons que a et b soient des entiers positifs avec $a \geq b$. Soit r_0, r_1, \dots, r_{m+1} la suite de nombres produite par l'algorithme d'Euclide

pour calculer $\text{pgcd}(a, b)$, où $r_m \neq 0$ et $r_{m+1} = 0$. Ceci signifie que l'algorithme nécessite m divisions.

- (a) Démontrer que $\forall k \in \mathbb{N} (k < m \rightarrow r_{m-k} \geq F_{k+2})$, où F_{k+2} est le ($k+2$)ème nombre de Fibonacci.
- (b) Soit $\varphi = \frac{1+\sqrt{5}}{2}$. Démontrer que pour tout φ est positif rapport des entiers d'or ; voir l'exercice 20 dans la section (Conseil : utilisez [le théorème 6.4.3](#).)
- (c) Montrer que

$$m < \frac{\log(b+1)}{\log \varphi} + \frac{\log 5}{2 \log \varphi} - 1.$$

(Vous pouvez utiliser des logarithmes en base 10 ou des logarithmes naturels dans cette formule.)

- (d) Montrez que si b comporte au plus 100 chiffres, alors le nombre de divisions lors de l'utilisation de l'algorithme euclidien pour calculer $\text{gcd}(a, b)$ sera au plus de 479.
14. (a) Démontrez la version alternative suivante de l'algorithme de division : Pour tout entier positif a et b , il existe des nombres naturels q et r tels que $r \leq b/2$ et soit $a = qb + r$ soit $a = qb - r$.
- (b) Supposons que a, b et r soient des entiers positifs, que q soit un nombre naturel et que $a = qb + r$ ou $a = qb - r$. Démontrer que $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.
 - (c) Supposons que a et b soient des entiers positifs avec $a \geq b$. Définissons une suite r_0, r_1, \dots récursivement comme suit : $r_0 = a$, $r_1 = b$, et pour tout $n \geq 1$, si $r_n \neq 0$ alors nous utilisons la partie (a) pour trouver les entiers naturels q_{n+1} et r_{n+1} tels que $r_{n+1} \leq r_n/2$ et soit $r_{n-1} = q_{n+1}r_n + r_{n+1}$ ou $r_{n-1} = q_{n+1}r_n - r_{n+1}$. Démontrer qu'il existe un m tel que $r_m \neq 0$ et $r_{m+1} = 0$, et $\text{pgcd}(a, b) = r_m$. Cela nous donne une nouvelle méthode de calcul des plus grands diviseurs communs ; elle est appelée *algorithme euclidien du plus petit reste absolu*.
 - (d) Calculer $\text{pgcd}(1515, 555)$ par l'algorithme d'Euclide et par l'algorithme du plus petit reste absolu. Lequel nécessite le moins d'étapes ?

7.2. Factorisation en nombres premiers

Dans [la section 6.4](#), nous avons vu que tout entier $n > 1$ est soit premier, soit peut s'écrire comme un produit de nombres premiers ; on dit que n possède une *factorisation première*. Dans cette section, nous montrerons que cette factorisation première est, en un certain sens,

unique. Un outil important de cette étude sera le plus grand commun diviseur. En particulier, nous nous intéresserons aux paires d'entiers strictement positifs dont le plus grand commun diviseur a la plus petite valeur possible, 1.

Définition 7.2.1. Si a et b sont des entiers positifs et que $\text{pgcd}(a, b) = 1$, alors on dit que a et b sont *premiers entre eux*.

De manière équivalente, on peut dire que a et b sont premiers entre eux si leur seul diviseur commun est 1. Par exemple, $D(50) = \{1, 2, 5, 10, 25, 50\}$ et $D(63) = \{1, 3, 7, 9, 21, 63\}$, donc $D(50) \cap D(63) = \{1\}$. Par conséquent, $\text{pgcd}(50, 63) = 1$, donc 50 et 63 sont premiers entre eux.

L'une des raisons pour lesquelles les entiers premiers entre eux sont importants est donnée par notre théorème suivant. La clé de sa démonstration réside dans l'utilisation de l'instanciation existentielle pour introduire des noms pour les entiers dont nous savons qu'ils existent.

Théorème 7.2.2. Pour tous les entiers positifs a , b et c , si $c \mid ab$ et $\text{gcd}(a, c) = 1$ alors $c \mid b$.

Preuve. Supposons que $c \mid ab$ et $\text{pgcd}(a, c) = 1$. Alors il existe un entier j tel que $ab = jc$, et d'après [le théorème 7.1.4](#), il existe des entiers s et t tels que $sa + tc = 1$. Par conséquent

$$b = b \cdot 1 = b \cdot (sa + tc) = sab + tbc = sjc + tbc = (sj + tb)c,$$

donc $c \mid b$. \square

Remarquez que si p est un nombre premier alors $D(p) = \{1, p\}$. Ainsi, pour tout entier positif a , les seules valeurs possibles de $\text{pgcd}(a, p)$ sont 1 et p . Si $p \mid a$ alors $\text{pgcd}(a, p) = p$, et sinon, le seul diviseur commun de a et p est 1 et donc a et p sont premiers entre eux. En combinant cette observation avec [le théorème 7.2.2](#), nous obtenons le fait important suivant concernant les diviseurs premiers.

Théorème 7.2.3. Pour tous les entiers positifs a , b et p , si p est premier et $p \mid ab$ alors soit $p \mid a$ soit $p \mid b$.

Preuve. Supposons que p soit premier et $p \mid ab$. Comme observé précédemment, si $p \nmid a$ alors a et p sont premiers entre eux, et donc, d'après [le théorème 7.2.2](#), $p \mid b$. Ainsi, soit $p \mid a$, soit $p \mid b$. \square

Commentaire. Notez que pour prouver la disjonction $(p \mid a) \vee (p \mid b)$, nous avons utilisé la stratégie consistant à supposer $p \nmid a$ puis à prouver $p \mid b$.

En utilisant l'induction mathématique, nous pouvons étendre ce théorème au cas d'un nombre premier divisant un produit d'une liste d'entiers positifs.

Théorème 7.2.4. *Supposons que p soit un nombre premier et que a_1, a_2, \dots, a_k soient des entiers positifs. Si $p \mid (a_1 a_2 \cdots a_k)$, alors pour un certain $i \in \{1, 2, \dots, k\}$, $p \mid a_i$.*

Preuve. Nous démontrons ce théorème par récurrence sur k . Autrement dit, nous utiliserons l'induction pour démontrer l'affirmation suivante : pour tout $k \geq 1$, si p divise le produit d'une liste quelconque de k entiers positifs, alors il divise l'un des entiers de la liste.

Notre cas de base est $k = 1$, et dans ce cas l'énoncé est clairement vrai : si $p \mid a_1$, alors il existe un $i \in \{1\}$ tel que $p \mid a_i$, à savoir, $i = 1$.

Supposons maintenant que l'énoncé soit valable pour toute liste de k entiers positifs, et soit a_1, a_2, \dots, a_{k+1} une liste d'entiers positifs tels que $p \mid (a_1 a_2 \cdots a_k a_{k+1})$. Puisque $a_1 a_2 \cdots a_k a_{k+1} = (a_1 a_2 \cdots a_k) a_{k+1}$, par [le théorème 7.2.3](#) soit $p \mid (a_1 a_2 \cdots a_k)$ ou $p \mid a_{k+1}$. Dans le premier cas, par hypothèse inductive, on a $p \mid a_i$ pour un $i \in \{1, 2, \dots, k\}$, et dans le second, on a $p \mid a_i$ où $i = k + 1$. \square

Nous sommes maintenant prêts à aborder la question de l'unicité des factorisations premières. Prenons par exemple l'écriture de 12 comme produit de nombres premiers. Il existe en réalité trois façons d'écrire 12 comme produit de nombres premiers : $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$. Mais bien sûr, dans les trois cas, nous multiplions les mêmes trois nombres premiers, mais dans un ordre différent. Pour éviter de les compter comme trois factorisations premières différentes de 12, nous ne considérerons que les factorisations où les nombres premiers sont classés du plus petit au plus grand. Une seule factorisation première de 12 satisfait à cette exigence supplémentaire : $12 = 2 \cdot 2 \cdot 3$.

Plus généralement, on s'intéressera aux expressions de la forme $p_1 p_2 \cdots p_k$, où p_1, p_2, \dots, p_k sont des nombres premiers et $p_1 \leq p_2 \leq \cdots \leq p_k$. On dira qu'une telle expression est le produit d'une *liste non décroissante de nombres premiers*. On montrera que tout entier supérieur à 1 peut s'écrire comme le produit d'une liste non décroissante de nombres premiers de manière unique.

Rappelons que, pour démontrer l'unicité d'un objet possédant une propriété, il faut démontrer que deux objets possédant cette propriété

doivent être égaux. Ainsi, la clé pour démontrer l'unicité des factorisations en nombres premiers réside dans le fait suivant.

Théorème 7.2.5. *Supposons que p_1, p_2, \dots, p_k et q_1, q_2, \dots, q_m soient des nombres premiers, $p_1 \leq p_2 \leq \dots \leq p_k$, $q_1 \leq q_2 \leq \dots \leq q_m$, et $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$. Alors $k = m$ et pour tout $i \in \{1, \dots, k\}$, $p_i = q_i$.*

Preuve. La preuve se fera par induction sur k . Autrement dit, on utilise l'induction pour prouver que pour tout $k \geq 1$, si le produit d'une liste non décroissante de k nombres premiers est égal au produit d'une autre liste non décroissante de nombres premiers, alors les deux listes doivent être identiques.

Lorsque $k = 1$, nous avons $p_1 = q_1 q_2 \cdots q_m$. Si $m > 1$ alors cela contredit le fait que p_1 est premier. Par conséquent $m = 1$ et $p_1 = q_1$.

Pour l'étape d'induction, supposons que l'énoncé soit vrai pour les produits de listes non décroissantes de k nombres premiers, et supposons que p_1, p_2, \dots, p_{k+1} et q_1, q_2, \dots, q_m sont des nombres premiers, $p_1 \leq p_2 \leq \dots \leq p_{k+1}$, $q_1 \leq q_2 \leq \dots \leq q_m$, et $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_m$. Notez que si $m = 1$, alors cette équation dit $p_1 p_2 \cdots p_{k+1} = q_1$, et comme dans le cas de base, cela contredit le fait que q_1 est premier, donc $m > 1$.

Clairement $p_{k+1} \mid (p_1 p_2 \cdots p_{k+1})$, donc $p_{k+1} \mid (q_1 q_2 \cdots q_m)$, et d'après [le théorème 7.2.4](#), il résulte que $p_{k+1} \mid q_i$ pour un certain i . Par conséquent, $p_{k+1} \leq q_i \leq q_m$. Un argument similaire montre que $q_m \mid p_j$ pour un certain j , donc $q_m \leq p_j \leq p_{k+1}$. On conclut que $p_{k+1} = q_m$. En annulant ces facteurs de l'équation $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_m$ nous donne $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_{m-1}$, et maintenant l'hypothèse inducive nous dit que les facteurs restants des deux côtés de l'équation sont les mêmes, comme requis. \square

Nous disposons désormais de tout le nécessaire pour établir l'existence et l'unicité des factorisations en nombres premiers. Ce théorème est si important qu'il est appelé le théorème fondamental de l'arithmétique.

Théorème 7.2.6. (Théorème fondamental de l'arithmétique) *Pour tout entier $n > 1$, il existe des nombres premiers uniques p_1, p_2, \dots, p_k tels que $p_1 \leq p_2 \leq \dots \leq p_k$ et $n = p_1 p_2 \cdots p_k$.*

Preuve. D'après [le théorème 6.4.2](#), tout entier supérieur à 1 est soit premier, soit un produit de nombres premiers. En classant les nombres premiers du plus petit au plus grand, on obtient la factorisation en nombres premiers non décroissants requise. L'unicité de la factorisation découle du [théorème 7.2.5](#).

Si nous écrivons le produit de la liste des nombres premiers p_1, p_2, \dots, p_k sous la forme $1 \cdot p_1 p_2 \cdots p_k$, alors il est naturel d'introduire la convention selon laquelle le produit de la liste vide est 1. Avec cette convention, nous pouvons étendre le théorème fondamental de l'arithmétique pour dire que chaque entier positif a une factorisation première unique, où la factorisation du nombre 1 est le produit de la liste vide de nombres premiers.

Exemple 7.2.7. Déterminer les décompositions en facteurs premiers des entiers suivants :

275, 276, 277.

Solution

La manière la plus simple de trouver la factorisation première d'un entier positif est de rechercher son plus petit diviseur premier, de le factoriser et de répéter jusqu'à ce que tous les facteurs soient premiers. Ceci donne les résultats suivants. (Notez que 277 est premier ; la factorisation de 277 s'arrête donc immédiatement.)

$$\begin{aligned} 275 &= 5 \cdot 55 = 5 \cdot 5 \cdot 11, \\ 276 &= 2 \cdot 138 = 2 \cdot 2 \cdot 69 = 2 \cdot 2 \cdot 3 \cdot 23, \\ 277 &= 277. \end{aligned}$$

Lorsqu'il y a des nombres premiers répétés dans la factorisation première d'un entier, on utilise souvent la notation exposant pour écrire la factorisation première. Par exemple, les factorisations de 275 et 276 dans le dernier exemple pourraient s'écrire sous la forme $275 = 5^2 \cdot 11$ et $276 = 2^2 \cdot 3 \cdot 23$. Plus généralement, on peut écrire la factorisation première d'un entier positif n sous la forme $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ où p_1, p_2, \dots, p_k sont des nombres premiers, $p_1 < p_2 < \cdots < p_k$, et e_1, e_2, \dots, e_k sont des entiers positifs. Là encore, d'après le théorème fondamental de l'arithmétique, cette représentation de n est unique.

Le théorème fondamental de l'arithmétique peut éclairer plusieurs concepts de la théorie des nombres. Par exemple, supposons que n et d soient des entiers strictement positifs et que $d \mid n$. Il existe alors un entier strictement positif c tel que $cd = n$. Soit maintenant les

factorisations premières de c et d : $c = p_1 \cdot p_2 \cdots p_k$ et $d = q_1 \cdot q_2 \cdots q_m$. Alors $n = cd = p_1 \cdot p_2 \cdots p_k \cdot q_1 \cdot q_2 \cdots q_m$. Si nous réorganisons les nombres premiers de ce produit dans l'ordre non décroissant, alors cela doit être l'unique factorisation première de n . Par conséquent, d doit être le produit d'une sous-collection des nombres premiers de la factorisation première de n . Notez que nous incluons ici la possibilité que la sous-collection soit la sous-collection vide (de sorte que $d = 1$ et $c = n$) ou qu'elle inclue tous les nombres premiers de la factorisation de n (de sorte que $d = n$ et $c = 1$).

En reformulant cette conclusion en utilisant la notation des exposants, supposons que la factorisation première de n soit... $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Alors les diviseurs de n sont précisément les nombres de la forme $p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, où pour tout $i \in \{1, 2, \dots, k\}$, $0 \leq f_i \leq e_i$. Par exemple, nous avons vu dans [l'exemple 7.2.7](#) que la factorisation première de 276 est $276 = 2^2 \cdot 3 \cdot 23$. Par conséquent

$$\begin{aligned} D(276) &= \{1, 2, 2^2, 3, 2 \cdot 3, 2^2 \cdot 3, 23, 2 \cdot 23, 2^2 \cdot 23, 3 \cdot 23, 2 \cdot 3 \cdot 23, 2^2 \cdot 3 \cdot 23\} \\ &= \{1, 2, 4, 3, 6, 12, 23, 46, 92, 69, 138, 276\}. \end{aligned}$$

La factorisation en nombres premiers peut également nous aider à comprendre les plus grands diviseurs communs. Supposons que a et b soient des entiers strictement positifs. Soient p_1, p_2, \dots, p_k la liste de tous les nombres premiers présents dans la factorisation en nombres premiers de a ou de b . On peut alors écrire a et b sous la forme

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k},$$

où certains des exposants e_i et f_i pourraient être nuls, car certains nombres premiers pourraient n'apparaître que dans une seule factorisation. D'après la discussion sur la divisibilité et la factorisation en nombres premiers présentée au paragraphe précédent, les diviseurs communs de a et b sont tous des nombres de la forme $p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$, où, pour tout $i \in \{1, \dots, k\}$, $g_i \leq e_i$ et $g_i \leq f_i$. Le plus grand diviseur commun peut être trouvé en attribuant à chaque g_i la plus grande valeur possible, soit $\min(e_i, f_i) =$ le minimum de e_i et f_i . Autrement dit,

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}.$$

Par exemple, dans [l'exemple 7.1.3](#), nous avons utilisé l'algorithme d'Euclide pour trouver que $\text{pgcd}(1392, 444) = 12$. Nous aurions pu factoriser 1392 et 444 en nombres premiers :

$$1392 = 2^4 \cdot 3 \cdot 29 = 2^4 \cdot 3^1 \cdot 29^1 \cdot 37^0,$$

$$444 = 2^2 \cdot 3 \cdot 37 = 2^2 \cdot 3^1 \cdot 29^0 \cdot 37^1.$$

Ces factorisations nous donnent une autre façon de trouver le plus grand diviseur commun de 1392 et 444 :

$$\begin{aligned}\gcd(1392, 444) &= 2^{\min(4,2)} \cdot 3^{\min(1,1)} \cdot 29^{\min(1,0)} \cdot 37^{\min(0,1)} \\ &= 2^2 \cdot 3^1 \cdot 29^0 \cdot 37^0 = 12.\end{aligned}$$

En général, l'algorithme d'Euclide est plus efficace que la factorisation en nombres premiers pour trouver le plus grand commun diviseur de deux entiers positifs. Cependant, si vous connaissez les factorisations en nombres premiers de deux entiers positifs, vous pouvez calculer leur plus grand commun diviseur très facilement.

Un autre concept éclairci par la factorisation en nombres premiers est celui des plus petits communs multiples. Pour tout entier positif a et b , le *plus petit commun multiple* de a et b , noté $\text{ppcm}(a, b)$, est le plus petit entier positif m tel que $a \mid m$ et $b \mid m$. Les plus petits communs multiples apparaissent lors de l'addition de fractions : pour additionner deux fractions de dénominateurs a et b , on commence par les réécrire avec le dénominateur commun $\text{ppcm}(a, b)$.

Supposons que, comme auparavant,

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}.$$

Pour chaque $i \in \{1, \dots, k\}$, tout multiple commun de a et b doit inclure un facteur $p_i^{g_i}$ dans sa décomposition en facteurs premiers, où $g_i \geq e_i$ et $g_i \geq f_i$. La plus petite valeur possible de g_i est le maximum de e_i et f_i , que nous noterons $\max(e_i, f_i)$, donc

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}.$$

Il n'est pas difficile de montrer que pour tous les nombres e et f , $\min(e, f) + \max(e, f) = e + f$ (voir [exercice 4](#)), donc

$$\begin{aligned}\gcd(a, b) \cdot \text{lcm}(a, b) &= (p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)}) \cdot (p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)}) \\ &= p_1^{\min(e_1, f_1) + \max(e_1, f_1)} \cdots p_k^{\min(e_k, f_k) + \max(e_k, f_k)} \\ &= p_1^{e_1 + f_1} \cdots p_k^{e_k + f_k} \\ &= (p_1^{e_1} \cdots p_k^{e_k}) \cdot (p_1^{f_1} \cdots p_k^{f_k}) = ab.\end{aligned}$$

Cela nous donne une autre façon de calculer $\text{lcm}(a, b)$:

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

Pour une preuve alternative de cette formule, voir [l'exercice 8](#).

Par exemple, nous avons maintenant deux façons de calculer $\text{lcm}(1392, 444)$:

$$\begin{aligned}\text{lcm}(1392, 444) &= 2^{\max(4,2)} \cdot 3^{\max(1,1)} \cdot 29^{\max(1,0)} \cdot 37^{\max(0,1)} \\ &= 2^4 \cdot 3^1 \cdot 29^1 \cdot 37^1 = 51504,\end{aligned}$$

et

$$\text{lcm}(1392, 444) = \frac{1392 \cdot 444}{\text{gcd}(1392, 444)} = \frac{618048}{12} = 51504.$$

Cela montre que si nous voulons additionner deux fractions avec des dénominateurs 1392 et 444, nous devons utiliser le dénominateur commun 51504.

Exemple 7.2.8. Trouver le plus petit commun multiple de 1386 et 1029.

Solution

Nous commençons par utiliser l'algorithme d'Euclide pour trouver $\text{pgcd}(1386, 1029)$. Les calculs de [la figure 7.3](#) montrent que $\text{pgcd}(1386, 1029) = 21$. Par conséquent

$$\text{lcm}(1386, 1029) = \frac{1386 \cdot 1029}{\text{gcd}(1386, 1029)} = \frac{1386 \cdot 1029}{21} = 67914.$$

n	q_n	r_n	Division
0		1386	
1		1029	$1386 = 1 \cdot 1029 + 357$
2	1	357	$1029 = 2 \cdot 357 + 315$
3	2	315	$357 = 1 \cdot 315 + 42$
4	1	42	$315 = 7 \cdot 42 + 21$
5	7	21	$42 = 2 \cdot 21 + 0$
6	2	0	

Figure 7.3. Calcul du $\text{pgcd}(1386, 1029)$ par l'algorithme euclidien.

Alternativement, nous pourrions utiliser des factorisations premières : $1386 = 2 \cdot 3^2 \cdot 7 \cdot 11$ et $1029 = 3 \cdot 7^3$, donc $\text{lcm}(1386, 1029) = 2 \cdot 3^2 \cdot 7^3 \cdot 11 = 67914$.

Exercices

- Trouvez les factorisations premières des entiers positifs suivants : 650, 756, 1067.
- * Trouvez $\text{lcm}(1495, 650)$.
- Trouvez $\text{lcm}(1953, 868)$.

4. Démontrer que pour tous les nombres e et f , $\min(e, f) + \max(e, f) = e + f$.
- *5. Supposons que a et b soient des entiers strictement positifs. Démontrer que a et b sont premiers entre eux si et seulement si leurs décompositions en facteurs premiers n'ont aucun nombre premier en commun.
6. Supposons que a et b soient des entiers strictement positifs. Démontrer que a et b sont premiers entre eux ssi il existe des entiers s et t tels que $sa + tb = 1$.
7. Supposons que a, b, a' et b' soient des entiers positifs, que a et b soient premiers entre eux, que $a' | a$ et $b' | b$. Démontrer que a' et b' sont premiers entre eux.
- *8. Supposons que a et b soient des entiers strictement positifs. Dans cet exercice, vous donnerez une autre preuve de la formule $\text{lcm}(a, b) = ab / \gcd(a, b)$. Soit $m = \text{lcm}(a, b)$.
- (a) Démontrer que $ab / \gcd(a, b)$ est un entier et que $a | (ab / \gcd(a, b))$ et $b | (ab / \gcd(a, b))$. Utiliser ceci pour conclure que $m \leq ab / \gcd(a, b)$.
 Soient q et r le quotient et le reste lorsque ab est divisé par m . Ainsi, $ab = qm + r$ et $0 \leq r < m$.
- (b) Démontrer que $r = 0$.
- (c) Par la partie (b), $ab = qm$. Démontrer que $q | a$ et $q | b$.
- (d) Utiliser la partie (c) pour conclure que $m \geq ab / \gcd(a, b)$. Avec la partie (a), cela montre que $m = ab / \gcd(a, b)$.
9. Supposons que a et b soient des entiers strictement positifs, et soit $d = \text{pgcd}(a, b)$. Alors $d | a$ et $d | b$, il existe donc des entiers strictement positifs j et k tels que $a = jd$ et $b = kd$. Démontrer que j et k sont premiers entre eux.
10. Démontrer que pour tous les entiers positifs a, b et d , si $d | ab$ alors il existe des entiers positifs d_1 et d_2 tels que $d = d_1 d_2$, $d_1 | a$ et $d_2 | b$.
11. Démontrer que pour tous les entiers positifs a, b et m , si $a | m$ et $b | m$ alors $\text{lcm}(a, b) | m$.
12. Supposons que a, b et c soient des entiers strictement positifs. Soit m le plus petit entier strictement positif tel que $a | m$, $b | m$ et $c | m$. Démontrer que $m = \text{lcm}(\text{lcm}(a, b), c)$.
13. Démontrer que pour tous les entiers positifs a et b , si $a^2 | b^2$ alors $a | b$.
14. (a) Trouvez tous les nombres premiers p tels que $5p + 9 \in \{n^2 \mid n \in \mathbb{N}\}$.
 (b) Trouvez tous les nombres premiers p tels que $15p + 4 \in \{n^2 \mid n \in \mathbb{N}\}$.

- (c) Trouvez tous les nombres premiers p tels que $5p + 8 \in \{n^3 \mid n \in \mathbb{N}\}$.
15. Soit $H = \{4n + 1 \mid n \in \mathbb{N}\} = \{1, 5, 9, 13, \dots\}$. Les éléments de H sont appelés *nombres de Hilbert* (du nom de David Hilbert (1862–1943)). Un nombre de Hilbert supérieur à 1, qui ne peut être écrit comme le produit de deux nombres de Hilbert plus petits, est appelé *nombre premier de Hilbert*. Par exemple, 9 est un nombre premier de Hilbert. (Bien sûr, 9 n'est pas un nombre premier, puisque $9 = 3 \cdot 3$, mais $3 \notin H$.)
- (a) Montrer que H est fermé par multiplication, c'est-à-dire $\forall x \in H \forall y \in H (xy \in H)$.
 - (b) Montrez que tout nombre de Hilbert supérieur à 1 est soit un nombre premier de Hilbert, soit un produit de deux ou plusieurs nombres premiers de Hilbert.
 - (c) Montrer que 441 est un nombre de Hilbert qui peut s'écrire comme le produit d'une liste non décroissante de nombres premiers de Hilbert de deux manières différentes. Ainsi, la factorisation en nombres premiers de Hilbert n'est pas unique.
16. Supposons que a et b soient des entiers strictement positifs. Démontrer qu'il existe des entiers strictement positifs c et d tels que $c \mid a, d \mid b$, et $cd = \text{ppcm}(a, b)$.
17. Supposons que a, b et c soient des entiers positifs.
- (a) Démontrer que $\text{pgcd}(a, bc) \mid (\text{pgcd}(a, b) \cdot \text{pgcd}(a, c))$.
 - (b) Démontrer que $\text{lcm}(\text{pgcd}(a, b), \text{pgcd}(a, c)) \mid \text{pgcd}(a, bc)$. (Indice : utilisez [l'exercice 11.](#))
 - (c) Supposons que b et c soient premiers entre eux. Démontrer que $\text{pgcd}(a, bc) = \text{pgcd}(a, b) \cdot \text{pgcd}(a, c)$.
18. Rappelons, comme [l'exercice 5 de la section 6.2](#), que les nombres $F_n = 2^{(2^n)} + 1$ sont appelés nombres de Fermat. Fermat a montré que F_n est premier pour $0 \leq n \leq 4$, et Euler a montré que F_5 n'est pas premier. On ignore s'il existe un nombre $n > 4$ pour lequel F_n est premier. Cet exercice vous permettra de comprendre une raison pour laquelle on pourrait s'intéresser aux nombres premiers de cette forme. Montrer que si m est un entier strictement positif et que $2^m + 1$ est premier, alors m est une puissance de 2. (Indice : si m n'est pas une puissance de 2, alors m a un nombre premier impair p dans sa décomposition en facteurs premiers. Il existe donc un entier strictement positif r tel que $m = pr$. Appliquez maintenant [l'exercice 14 de la section 6.1](#) pour conclure que $(2^r + 1) \mid (2^m + 1)$.)
19. Supposons que x soit un nombre rationnel positif.
- (a) Démontrer qu'il existe des entiers positifs a et b tels que $x = a/b$ et $\text{pgcd}(a, b) = 1$.

(b) Supposons que a, b, c et d soient des entiers positifs, $x = a / b = c / d$ et $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. Démontrer que $a = c$ et $b = d$.

(c) Démontrer qu'il existe des nombres premiers p_1, p_2, \dots, p_k et des entiers non nuls e_1, e_2, \dots, e_k tels que $p_1 < p_2 < \dots < p_k$ et

$$x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Notez que certains des exposants e_i peuvent être négatifs.

(d) Démontrer que la représentation de x dans la partie (c) est unique. Autrement dit, si p_1, p_2, \dots, p_k et q_1, q_2, \dots, q_m sont des nombres premiers, e_1, e_2, \dots, e_k et f_1, f_2, \dots, f_m sont des entiers non nuls, $p_1 < p_2 < \dots < p_k, q_1 < q_2 < \dots < q_m$, et

$$x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m},$$

alors $k = m$ et pour tout $i \in \{1, 2, \dots, k\}$, $p_i = q_i$ et $e_i = f_i$.

20. Complétez la preuve irrationnelle suivante : supposons que $\sqrt{2}a / b = \sqrt{2}$ où a et b sont des entiers positifs. Alors $a^2 = 2b^2$. Déduisez maintenant une contradiction en considérant l'exposant de 2 dans les factorisations premières de a et b .

7.3. Arithmétique modulaire

Supposons que m soit un entier strictement positif. Rappelons, d'après [la définition 4.5.9](#), que pour tout entier a et b , on dit que a est *congru à b modulo m* si $m \mid (a - b)$. On note $a \equiv b \pmod{m}$, ou plus brièvement $a \equiv_m b$, pour indiquer que a est congru à b modulo m . Nous avons vu dans [le théorème 4.5.10](#) que \equiv_m est une relation d'équivalence sur \mathbb{Z} . Pour tout entier a , soit $[a]_m$ la classe d'équivalence de a par rapport à la relation d'équivalence \equiv_m . L'ensemble de ces classes d'équivalence est noté \mathbb{Z}/\equiv_m . Ainsi,

$$[a]_m = \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\}, \quad \mathbb{Z}/\equiv_m = \{[a]_m \mid a \in \mathbb{Z}\}.$$

Comme nous le savons grâce [au théorème 4.5.4](#), \mathbb{Z}/\equiv_m est une partition de \mathbb{Z} .

Par exemple, dans le cas $m = 3$, nous avons

$$\begin{aligned}[0]_3 &= \{b \in \mathbb{Z} \mid b \equiv 0 \pmod{3}\} = \{0, 3, 6, 9, \dots, -3, -6, -9, \dots\}, \\ [1]_3 &= \{b \in \mathbb{Z} \mid b \equiv 1 \pmod{3}\} = \{1, 4, 7, 10, \dots, -2, -5, -8, \dots\}, \\ [2]_3 &= \{b \in \mathbb{Z} \mid b \equiv 2 \pmod{3}\} = \{2, 5, 8, 11, \dots, -1, -4, -7, \dots\}.\end{aligned}$$

Notez que chaque entier est un élément d'une seule de ces classes d'équivalence. Il en résulte que chaque entier est congru modulo 3 à l'un des nombres 0, 1 et 2. Ceci illustre le théorème général suivant.

Théorème 7.3.1. *Supposons que m soit un entier positif. Alors, pour tout entier a , il existe exactement un entier r tel que $0 \leq r < m$ et $a \equiv r \pmod{m}$.*

Preuve. Soit a un entier arbitraire. Soient q et r le quotient et le reste de a divisé par m (voir [exercice 14](#) de [la section 6.4](#)). Cela signifie que $a = qm + r$ et $0 \leq r < m$. Alors $a - r = qm$, donc $m \mid (a - r)$, et donc $a \equiv r \pmod{m}$. Ceci prouve l'existence de l'entier r requis.

Pour prouver l'unicité, supposons que r_1 et r_2 soient des entiers tels que $0 \leq r_1 < m$, $0 \leq r_2 < m$, $a \equiv r_1 \pmod{m}$ et $a \equiv r_2 \pmod{m}$. Alors, par la symétrie et la transitivité de la relation d'équivalence \equiv_m , $r_1 \equiv r_2 \pmod{m}$, il existe donc un entier d tel que $r_1 - r_2 = dm$. Mais à partir de $0 \leq r_1 < m$ et $0 \leq r_2 < m$ nous voyons que $-m < r_1 - r_2 < m$. Ainsi $-m < dm < m$, ce qui implique que $-1 < d < 1$. Le seul entier strictement

compris entre -1 et 1 est 0 , donc $d = 0$ et donc $r_1 - r_2 = dm = 0$. En d'autres termes, $r_1 = r_2$. \square

Commentaire. Bien entendu, l'^{existence} et l'unicité du nombre r sont prouvées séparément, et la preuve d'unicité utilise la stratégie habituelle consistant à supposer que r_1 et r_2 sont *deux* entiers possédant les propriétés requises, puis à prouver que $r_1 = r_2$.

Le théorème 7.3.1 affirme que tout entier est congru modulo m à exactement un élément de l'ensemble $\{0, 1, \dots, m - 1\}$. On dit que cet ensemble est un *système résiduel complet modulo m* .

Notez que par le lemme 4.5.5,

$$a \equiv r \pmod{m} \quad \text{iff} \quad a \in [r]_m \quad \text{iff} \quad [a]_m = [r]_m.$$

Ainsi, le théorème 7.3.1 montre que chaque classe d'équivalence dans \mathbb{Z}/\equiv_m est égale à exactement une des classes d'équivalence dans la liste $[0]_m, [1]_m, \dots, [m - 1]_m$. Ainsi, ces m classes d'équivalence sont distinctes, et $\mathbb{Z}/\equiv_m = \{[0]_m, [1]_m, \dots, [m - 1]_m\}$.

Considérons deux classes d'équivalence X et Y dans \mathbb{Z}/\equiv_m . Un phénomène surprenant se produit si l'on additionne ou multiplie des éléments de X et Y . Il s'avère que toutes les sommes de la forme $x + y$, où $x \in X$ et $y \in Y$, appartiennent à la même classe d'équivalence, et que tous les produits xy appartiennent également à la même classe d'équivalence. Autrement dit, nous avons le théorème suivant.

Théorème 7.3.2. *Supposons que m soit un entier positif et que X et Y soient des éléments de \mathbb{Z}/\equiv_m . Alors :*

1. *Il existe un unique $S \in \mathbb{Z}/\equiv_m$ tel que $\forall x \in X \forall y \in Y (x + y \in S)$.*
2. *Il existe un unique $P \in \mathbb{Z}/\equiv_m$ tel que $\forall x \in X \forall y \in Y (xy \in P)$.*

Nous allons démontrer ce théorème sous peu, mais nous l'utilisons d'abord pour introduire deux opérations binaires sur \mathbb{Z}/\equiv_m .

Définition 7.3.3. Supposons que X et Y soient des éléments de \mathbb{Z}/\equiv_m . On définit alors la somme et le produit de X et Y , notés $X + Y$ et $X \cdot Y$, comme suit :

$$\begin{aligned} X + Y &= \text{the unique } S \in \mathbb{Z}/\equiv_m \text{ such that } \forall x \in X \forall y \in Y (x + y \in S), \\ X \cdot Y &= \text{the unique } P \in \mathbb{Z}/\equiv_m \text{ such that } \forall x \in X \forall y \in Y (xy \in P). \end{aligned}$$

La clé de notre preuve du théorème 7.3.2 sera le lemme suivant.

Lemme 7.3.4. Supposons que m soit un entier positif. Alors pour tous les entiers a, a', b et b' , si $a' \equiv a \pmod{m}$ et $b' \equiv b \pmod{m}$ alors $a' + b' \equiv a + b \pmod{m}$ et $a' b' \equiv ab \pmod{m}$.

Preuve. Supposons que $a' \equiv a \pmod{m}$ et $b' \equiv b \pmod{m}$. Alors $m | (a' - a)$ et $m | (b' - b)$, donc on peut choisir des entiers c et d tels que $a' - a = cm$ et $b' - b = dm$, ou en d'autres termes $a' = a + cm$ et $b' = b + dm$. Donc $(a' + b') - (a + b) = (a + cm + b + dm) - (a + b) = cm + dm = (c + d)m$, donc $m | ((a' + b') - (a + b))$, ce qui signifie $a' + b' \equiv a + b \pmod{m}$. De même, $a' b' - ab = (a + cm)(b + dm) - ab = adm + bcm + cdm^2 = (ad + bc + cdm)m$, donc $m | (a' b' - ab)$, et donc $a' b' \equiv ab \pmod{m}$. \square

Preuve du théorème 7.3.2. Puisque X et Y sont des éléments de \mathbb{Z} / \equiv_m , on peut poser a et b comme entiers $X = [a]_m$ et $Y = [b]_m$. Pour prouver la première partie du théorème, soit $S = [a + b]_m$. Soient maintenant $x \in X$ et $y \in Y$ arbitraires. Alors $x \in [a]_m$ et $y \in [b]_m$, donc $x \equiv a \pmod{m}$ et $y \equiv b \pmod{m}$. D'après le lemme 7.3.4, il s'ensuit que $x + y \equiv a + b \pmod{m}$, donc $x + y \in [a + b]_m = S$. Puisque x et y sont arbitraires, on conclut que $\forall x \in X \forall y \in Y (x + y \in S)$.

Pour prouver que S est unique, supposons que S' soit une autre classe d'équivalence telle que $\forall x \in X \forall y \in Y (x + y \in S')$. Puisque $a \in X$ et $b \in Y$, $a + b \in S$ et $a + b \in S'$. Par conséquent, S et S' ne sont pas disjoints, et puisque \mathbb{Z} / \equiv_m est deux à deux disjoint, cela implique que $S = S'$.

La preuve de la partie 2 est similaire, en utilisant $P = [ab]_m$; voir exercice 2. \square

La preuve du théorème 7.3.2 montre que si $X = [a]_m$ et $Y = [b]_m$, alors la somme de X et Y est la classe d'équivalence $S = [a + b]_m$ et le produit est $P = [ab]_m$. Ainsi, nous avons le théorème suivant.

Théorème 7.3.5. Pour tout entier positif m et tout entier a et b ,

$$[a]_m + [b]_m = [a + b]_m \quad \text{and} \quad [a]_m \cdot [b]_m = [ab]_m.$$

Français Essayons ces idées. Considérons le cas $m = 5$. Nous savons que chaque élément de \mathbb{Z} / \equiv_5 est égal à $[0]_5, [1]_5, [2]_5, [3]_5$ ou $[4]_5$, et nous choisirons souvent d'écrire les classes d'équivalence sous l'une de ces formes. Par exemple, $[2]_5 + [4]_5 = [6]_5$, mais aussi $6 \equiv 1 \pmod{5}$, donc $[6]_5 = [1]_5$. Ainsi, nous pouvons dire que $[2]_5 + [4]_5 = [1]_5$. De

même, $[2]_5 \cdot [4]_5 = [8]_5 = [3]_5$. [La figure 7.4](#) montre les tables d'addition et de multiplication complètes pour \mathbb{Z}/\equiv_5 .

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	\cdot	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Figure 7.4. Tables d'addition et de multiplication pour \mathbb{Z}/\equiv_5 .

Comment l'addition et la multiplication dans \mathbb{Z}/\equiv_m compareraient-elles à l'addition et à la multiplication dans \mathbb{Z} ? De nombreuses propriétés de l'addition et de la multiplication dans \mathbb{Z} s'appliquent facilement à \mathbb{Z}/\equiv_m .

Théorème 7.3.6. *Supposons que m soit un entier positif. Alors, pour toutes les classes d'équivalence X, Y et Z dans \mathbb{Z}/\equiv_m :*

1. $X + Y = Y + X$. (*L'addition est commutative.*)
2. $(X + Y) + Z = X + (Y + Z)$. (*L'addition est associative.*)
3. $X + [0]_m = X$. (*[0]_m est un élément d'identité pour l'addition.*)
4. Il existe un $X' \in \mathbb{Z}/\equiv_m$ tel que $X + X' = [0]_m$. (*X a un inverse additif.*)
5. $X \cdot Y = Y \cdot X$. (*La multiplication est commutative.*)
6. $(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$. (*La multiplication est associative.*)
7. $X \cdot [1]_m = X$. (*[1]_m est un élément neutre pour la multiplication.*)
8. $X \cdot [0]_m = [0]_m$.
9. $X \cdot (Y + Z) = (X \cdot Y) + (X \cdot Z)$. (*La multiplication se répartit sur l'addition.*)

Preuve. Puisque $X, Y, Z \in \mathbb{Z}/\equiv_m$, il existe des entiers a, b et c tels que $X = [a]_m$, $Y = [b]_m$ et $Z = [c]_m$. Pour la première partie, on utilise la commutativité de l'addition dans \mathbb{Z} :

$$X + Y = [a]_m + [b]_m = [a + b]_m = [b + a]_m = [b]_m + [a]_m = Y + X.$$

La preuve de la partie 2 est similaire. Pour prouver la partie 3, nous calculons

$$X + [0]_m = [a]_m + [0]_m = [a + 0]_m = [a]_m = X.$$

Pour la partie 4, soit $X' = [-a]_m$. Alors

$$X + X' = [a]_m + [-a]_m = [a + (-a)]_m = [0]_m.$$

Les preuves des parties restantes sont similaires (voir [exercice 3](#)). \square

On vous demande de montrer dans [l'exercice 4](#) que les éléments neutres et les inverses du [théorème 7.3.6](#) sont uniques. Ainsi, dans la partie 3 du théorème, nous pouvons dire que $[0]_m$ n'est pas seulement *un* élément neutre pour l'addition, mais *l'* élément neutre, et de même $[1]_m$ est *l'* élément neutre pour la multiplication. Dans la partie 4, nous pouvons dire que X' est *l'* inverse additif de X ; nous noterons l'inverse additif de X par $-X$. Par exemple, d'après la table d'addition pour \mathbb{Z}/\equiv_5 de [la figure 7.4](#), $[4]_5 + [1]_5 = [0]_5$, donc $-[4]_5 = [1]_5$.

Qu'en est-il des inverses multiplicatifs ? Si $X \in \mathbb{Z}/\equiv_m$, $X' \in \mathbb{Z}/\equiv_m$, et $X \cdot X' = [1]_m$, alors nous disons que X' est un inverse multiplicatif de X . Par exemple, selon la table de multiplication pour \mathbb{Z}/\equiv_5 dans [la Figure 7.4](#), $[3]_5 \cdot [2]_5 = [1]_5$, donc $[2]_5$ est un inverse multiplicatif de $[3]_5$. En fait, dans \mathbb{Z}/\equiv_5 , chaque élément sauf $[0]_5$ a un inverse multiplicatif. Les inverses multiplicatifs, lorsqu'ils existent, sont également uniques (voir [exercice 4](#)), donc nous pouvons dire que $[2]_5$ est *l'* inverse multiplicatif de $[3]_5$. En général, si $X \in \mathbb{Z}/\equiv_m$, alors l'inverse multiplicatif de X , s'il existe, est noté X^{-1} . Ainsi $[3]_5^{-1} = [2]_5$.

Quelques expérimentations révèlent que les inverses multiplicatifs sont souvent inexistant. Par exemple, nous vous laissons vérifier que dans \mathbb{Z}/\equiv_6 , seuls $[1]_6$ et $[5]_6$ ont des inverses multiplicatifs (voir [exercice 1](#)). Quand une classe d'équivalence possède-t-elle un inverse multiplicatif ? La réponse est donnée par notre théorème suivant.

Théorème 7.3.7. *Supposons que a et m soient des entiers strictement positifs. Alors $[a]_m$ possède une inverse multiplicative si et seulement si m et a sont premiers entre eux.*

Preuve. Supposons d'abord que $[a]_m$ possède un inverse multiplicatif ; disons $[a]_m^{-1} = [a']_m$. Alors $[a]_m \cdot [a']_m = [aa']_m = [1]_m$, et donc $aa' \equiv 1 \pmod{m}$. Cela signifie que $m | (aa' - 1)$, donc nous pouvons choisir un entier c tel que $aa' - 1 = cm$, ou de manière équivalente $-cm + a'a = 1$. Ainsi 1 est une combinaison linéaire de m et a , et par [l'exercice 6](#) de la dernière section, il s'ensuit que m et a sont premiers entre eux.

Dans l'autre sens, supposons que m et a soient premiers entre eux. Alors, d'après [le théorème 7.1.4](#), il existe des entiers strictement positifs s et t tels que $sm + ta = 1$. Par conséquent, $ta - 1 = -sm$, donc $ta \equiv 1 \pmod{m}$. On conclut que $[a]_m \cdot [t]_m = [ta]_m = [1]_m$, donc $[t]_m$ est l'inverse multiplicatif de $[a]_m$. \square

Commentaire. Notez que la conclusion du théorème est une affirmation biconditionnelle, et que la démonstration utilise la stratégie habituelle consistant à prouver séparément les deux directions de la bicondition.

La preuve du [théorème 7.3.7](#) montre que pour tout entier positif m et a , nous pouvons utiliser l'algorithme d'Euclide étendu pour trouver $[a]_m^{-1}$. Si l'algorithme montre que $\gcd(m, a) \neq 1$ alors $[a]_m^{-1}$ n'existe pas, et si nous trouvons que $\gcd(m, a) = 1 = sm + ta$ alors $[a]_m^{-1} = [t]_m$.

Exemple 7.3.8. Trouvez, si possible, les inverses multiplicatifs de $[34]_{847}$ et $[35]_{847}$ dans \mathbb{Z}/\equiv_{847} .

Solution

[La figure 7.5](#) montre le calcul de $\text{pgcd}(847, 34)$ par l'algorithme d'Euclide étendu. Nous concluons que $\text{pgcd}(847, 34) = 1 = 11 \cdot 847 - 274 \cdot 34$, et donc $[34]_{847}^{-1} = [-274]_{847} = [573]_{847}$. Comme vous pouvez facilement le vérifier, $34 \cdot 573 = 19482 \equiv 1 \pmod{847}$, donc $[34]_{847} \cdot [573]_{847} = [19482]_{847} = [1]_{847}$.

n	q_n	r_n	s_n	t_n	Division
0		847	1	0	
1		34	0	1	$847 = 24 \cdot 34 + 31$
2	24	31	1	-24	$34 = 1 \cdot 31 + 3$
3	1	3	-1	25	$31 = 10 \cdot 3 + 1$
4	10	1	11	-274	$3 = 3 \cdot 1 + 0$
5	3	0			

Figure 7.5. Calcul de $\text{pgcd}(847, 34)$ par algorithme euclidien étendu.

Nous vous laissons calculer que $\gcd(847, 35) = 7$. Par conséquent $[35]_{847}$ n'a pas d'inverse multiplicatif.

Exemple 7.3.9. Une classe compte 25 élèves. Pour Pâques, l'enseignante a acheté plusieurs cartons d'œufs, contenant chacun une douzaine d'œufs, puis les a distribués aux élèves pour qu'ils les décorent. Après avoir distribué un nombre égal d'œufs à chaque élève, il lui en restait 7. Quel est le plus petit nombre de cartons d'œufs qu'elle aurait pu acheter ?

Solution

Soit x le nombre de cartons d'œufs achetés par l'enseignante. Elle avait alors $12x$ œufs, et en mettant de côté les 7 restants à la fin, les œufs restants ont été répartis équitablement entre 25 élèves. Par conséquent, $25 \mid (12x - 7)$, donc $12x \equiv 7 \pmod{25}$. Il faut trouver le plus petit entier positif x satisfaisant cette congruence.

Si nous devions résoudre l'équation $12x = 7$ pour un nombre réel x , nous saurions comment procéder. Si $12x = 7$, alors en multipliant les deux côtés de l'équation par $1/12$, nous concluons que $x = 7/12$. En fait, ce raisonnement peut être inversé : si $x = 7/12$, alors en multipliant par 12, nous obtenons $12x = 7$. Ainsi, les équations $12x = 7$ et $x = 7/12$ sont équivalentes, ce qui signifie que $x = 7/12$ est l'unique solution de l'équation $12x = 7$.

Malheureusement, nous travaillons avec la congruence $12x \equiv 7 \pmod{25}$, qui n'est pas une équation. Cependant, nous pouvons la transformer en équation en utilisant des classes d'équivalence. Notre congruence est équivalente à l'équation $[12]_{25} \cdot [x]_{25} = [7]_{25}$, et nous pouvons résoudre cette équation en imitant notre solution à l'équation $12x = 7$. Nous commençons par trouver l'inverse multiplicatif de $[12]_{25}$. En appliquant l'algorithme d'Euclide étendu, nous trouvons que $\text{pgcd}(25, 12) = 1 = 1 \cdot 25 - 2 \cdot 12$, donc $[\text{pgcd}(25, 12)]^{-1} = [12]_{25}^{-1} = [-2]_{25} = [23]_{25}$.

Pour résoudre l'équation $[12]_{25} \cdot [x]_{25} = [7]_{25}$, nous multiplions les deux côtés par $[\text{pgcd}(25, 12)]^{-1} = [23]_{25}$. Nous détaillons toutes les étapes, pour clarifier comment les propriétés du [théorème 7.3.6](#) sont utilisées :

$$\begin{aligned} [12]_{25} \cdot [x]_{25} &= [7]_{25}, \\ [12]_{25}^{-1} \cdot ([12]_{25} \cdot [x]_{25}) &= [12]_{25}^{-1} \cdot [7]_{25}, \\ ([12]_{25}^{-1} \cdot [12]_{25}) \cdot [x]_{25} &= [23]_{25} \cdot [7]_{25}, \\ [1]_{25} \cdot [x]_{25} &= [161]_{25} = [11]_{25}, \\ [x]_{25} &= [11]_{25}. \end{aligned}$$

Comme précédemment, ces étapes peuvent être inversées : en multipliant les deux côtés de l'équation $[x]_{25} = [11]_{25}$ par $[12]_{25}$, on obtient $[12]_{25} \cdot [x]_{25} = [7]_{25}$. Par conséquent

$$12x \equiv 7 \pmod{25} \text{ iff } [12]_{25} \cdot [x]_{25} = [7]_{25} \text{ iff } [x]_{25} = [11]_{25} \text{ iff } x \in [11]_{25}.$$

En d'autres termes, les solutions à la congruence $12x \equiv 7 \pmod{25}$ sont précisément les éléments de la classe d'équivalence $[11]_{25}$, et la plus petite solution positive est $x = 11$. Si l'enseignante achetait 11 cartons d'œufs, elle avait alors 132 œufs, et après en avoir donné 5 à chaque élève, il lui en restait 7.

Dans cet exemple, nous avons eu la chance que 25 et 12 soient premiers entre eux, de sorte que $[12]_{25}$ possédait une inverse multiplicative. Cette inverse multiplicative a joué un rôle crucial dans notre résolution de la congruence $12x \equiv 7 \pmod{25}$. Comment résoudre une congruence $ax \equiv b \pmod{m}$ si m et a ne sont pas premiers entre eux ? Nous n'analyserons pas ces congruences en détail, mais nous donnerons quelques exemples illustrant comment de telles congruences peuvent être résolues en utilisant les deux théorèmes suivants.

Théorème 7.3.10. *Supposons que m et a soient des entiers strictement positifs, et que $d = \text{pgcd}(m, a)$. Alors, pour tout entier b , si $d \nmid b$ alors il n'existe pas d'entier x tel que $ax \equiv b \pmod{m}$.*

Preuve. Voir [exercice 7.](#) □

Théorème 7.3.11. *Supposons que n et m soient des entiers positifs. Alors, pour tous les entiers a et b ,*

$$na \equiv nb \pmod{nm} \quad \text{iff} \quad a \equiv b \pmod{m}.$$

Preuve. Voir [exercice 8.](#) □

Exemple 7.3.12. Résolvez les congruences suivantes :

$$77x \equiv 120 \pmod{374}, \quad 77x \equiv 121 \pmod{374}.$$

Solution

Nous commençons par calculer que $\text{gcd}(374, 77) = 11$. Puisque $11 \nmid 120$, [Le théorème 7.3.10](#) indique que la première congruence, $77x \equiv 120 \pmod{374}$, n'a pas de solution. Pour résoudre la seconde congruence, on l'écrit d'abord $11 \cdot 7x \equiv 11 \cdot 11 \pmod{11 \cdot 34}$, puis on observe que, d'après [le théorème 7.3.11](#), cela équivaut à $7x \equiv 11 \pmod{34}$. Pour résoudre cette congruence, on calcule que $\text{pgcd}(34, 7) = 1 = -1 \cdot 34 + 5 \cdot 7$, donc $[7]_{34}^{-1} = [5]_{34}$.

$$\begin{aligned} 7x \equiv 11 \pmod{34} &\text{ iff } [7]_{34} \cdot [x]_{34} = [11]_{34} \\ &\text{ iff } [x]_{34} = [7]_{34}^{-1} \cdot [11]_{34} = [5]_{34} \cdot [11]_{34} = [55]_{34} = [21]_{34} \\ &\text{ iff } x \in [21]_{34}. \end{aligned}$$

Ainsi, les solutions à la deuxième congruence sont les éléments de $[21]$

Exercices

1. Faites des tables d'addition et de multiplication pour \mathbb{Z} / \equiv_6 .
 2. Complétez la preuve du [théorème 7.3.2](#).
 3. Démontrer les parties 5 à 9 du [théorème 7.3.6](#).
- *4. Supposons que m soit un entier positif.
- (a) Supposons que Z_1 et Z_2 soient tous deux des éléments additifs neutres pour \mathbb{Z} / \equiv_m ; autrement dit, pour tout $X \in \mathbb{Z} / \equiv_m$, $X + Z_1 = X$ et $X + Z_2 = X$. Démontrer que $Z_1 = Z_2$. Ceci montre que l'élément additif neutre dans \mathbb{Z} / \equiv_m est unique. (Indice : calculer $Z_1 + Z_2$ de deux manières différentes.)
 - (b) Supposons que $X \in \mathbb{Z} / \equiv_m$ et x'_1 et x'_2 soient tous deux des inverses additifs pour X ; en d'autres termes, $X + x'_1 = X + x'_2 = [0]_m$. Prouvez que $x'_1 = x'_2$. Cela montre que l'inverse additif de X est unique. (Indice : calculez $x'_1 + X + x'_2$ de deux manières différentes.)
 - (c) Démontrer que l'élément d'identité multiplicatif dans \mathbb{Z} / \equiv_m est unique.
 - (d) Démontrer que si une classe d'équivalence $X \in \mathbb{Z} / \equiv_m$ possède un inverse multiplicatif, alors cet inverse est unique.
5. Montrez que si p est un nombre premier, alors chaque élément de \mathbb{Z} / \equiv_p sauf $[0]_p$ a un inverse multiplicatif.
 6. Si $ab \equiv 0 \pmod{m}$, est-il nécessairement vrai que $a \equiv 0 \pmod{m}$ ou $b \equiv 0 \pmod{m}$? Justifiez votre réponse par une preuve ou un contre-exemple.
7. Démontrer [le théorème 7.3.10](#).
- *8. Démontrer [le théorème 7.3.11](#).
9. Une classe compte 26 élèves. L'enseignant a acheté des paquets de fiches, chacun contenant 20 fiches. En les distribuant aux élèves, il a constaté qu'il devait ajouter deux fiches supplémentaires de son bureau pour pouvoir distribuer le même nombre de fiches à chaque élève. Si chaque élève a reçu entre 10 et 20 fiches, combien de paquets a-t-il acheté?
- *10. Résolvez les congruences suivantes.
- (a) $40x \equiv 8 \pmod{237}$.
 - (b) $40x \equiv 8 \pmod{236}$.
11. Résolvez les congruences suivantes.
- (a) $31x \equiv 24 \pmod{384}$.
 - (b) $32x \equiv 24 \pmod{384}$.
12. Dans cet exercice, vous résoudrez le problème suivant : supposons qu'une chaise sans accoudoirs coûte 35 \$ et qu'une chaise avec

accoudoirs coûte 50 \$. Si Alice a dépensé 720 \$ en chaises, combien de chaises de chaque type a-t-elle achetées ?

- (a) Montrez que si x est le nombre de chaises sans accoudoirs qu'elle a achetées, alors $35x \equiv 20 \pmod{50}$.
 - (b) Résolvez la congruence dans la partie (a).
 - (c) Toutes les solutions à la congruence de la partie (a) ne mènent pas à une réponse possible au problème. Lesquelles le font ? (Remarque : il existe plusieurs réponses possibles au problème.)
13. Supposons que m et n soient des entiers positifs premiers entre eux. Démontrer que pour tous les entiers a et b , $a \equiv b \pmod{m}$ ssi $na \equiv nb \pmod{m}$.
14. Supposons que m_1 et m_2 soient des entiers strictement positifs. Démontrer que pour tous les entiers a et b , si $a \equiv b \pmod{m_1}$ et $a \equiv b \pmod{m_2}$ alors $a \equiv b \pmod{\text{lcm}(m_1, m_2)}$. (Indice : Utiliser [l'exercice 11 de la section 7.2.](#))
15. Démontrer que pour tous les entiers positifs m , a et b , si $a \equiv b \pmod{m}$ alors $\gcd(m, a) = \gcd(m, b)$.
16. Supposons que $a \equiv b \pmod{m}$. Démontrer que pour tout entier naturel n , $a^n \equiv b^n \pmod{m}$.

Dans [les exercices 17 à 19](#), nous utilisons la notation suivante. Si $d_0, d_1, \dots, d_k \in \{0, 1, \dots, 9\}$, alors $(d_k \cdots d_1 d_0)_{10}$ est le nombre dont la représentation en notation décimale est $d_k \cdots d_1 d_0$. En d'autres termes,

$$(d_k \cdots d_1 d_0)_{10} = d_0 + 10d_1 + \cdots + 10^k d_k.$$

17. Supposons que $n = (d \cdots dd)_{10}$.
- (a) Montrer que $n \equiv (d_0 + d_1 + \cdots + d_k) \pmod{3}$.
 - (b) Montrer que $3 | n$ ssi $3 | (d_0 + d_1 + \cdots + d_k)$. (Ceci constitue un moyen pratique de tester la divisibilité d'un nombre naturel par 3 : additionner les chiffres et vérifier si la somme des chiffres est divisible par 3.)
18. Supposons que $n = (d_k \cdots d_1 d_0)_{10}$.
- (a) Montrer que $n \equiv (d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k) \pmod{11}$.
 - (b) Montrer que $11 | n$ ssi $11 | (d_0 - d_1 + \cdots + (-1)^k d_k)$.
 - (c) 535172 est-il divisible par 11 ?
19. Définissez une fonction f de domaine $\{n \in \mathbb{Z} \mid n \geq 10\}$ comme suit : si $n = (d_k \cdots d_1 d_0)_{10}$ alors $f(n) = (d_k \cdots d_1)_{10} + 5d_0$. Par exemple, $f(1743) = 174 + 5 \cdot 3 = 189$.

- (a) Montrer que pour tout $n \geq 10$, $f(n) \equiv 5n \pmod{7}$ et $n \equiv 3f(n) \pmod{7}$.
- (b) Montrer que pour tout $n \geq 10$, $7 \mid n$ ssi $7 \mid f(n)$. (Ceci donne un moyen pratique de tester la divisibilité par 7 d'un grand entier n : appliquer f de manière répétée jusqu'à obtenir un nombre dont la divisibilité par 7 est facile à déterminer.)
- (c) 627334 est-il divisible par 7 ?
20. (a) Trouvez un exemple d'entiers positifs m, a, a', b et b' tels que $a' \equiv a \pmod{m}$ et $b' \equiv b \pmod{m}$ mais $([a]_m)^{[b]_m} = [a^{b'}]_m$.
- (b) Montrer qu'il est impossible de définir une opération d'exponentiation sur les classes d'équivalence de telle manière que pour tous les entiers positifs m, a et $(a')^{b'} \not\equiv a^b \pmod{m}$.
21. Supposons que m soit un entier positif. Définissez $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}/\equiv_m$ par la formule $f(a, b) = [a + b]_m$, et définissez $h: (\mathbb{Z}/\equiv_m) \times (\mathbb{Z}/\equiv_m) \rightarrow \mathbb{Z}/\equiv_m$ par la formule $h(X, Y) = X + Y$. Vous pouvez comparer cet exercice à [l'exercice 21 de la section 5.1](#).
- (a) Montrer que pour tous les entiers x_1, x_2, y_1 et y_2 , si $x_1 \equiv_m y_1$ et $x_2 \equiv_m y_2$ alors $f(x_1, x_2) = f(y_1, y_2)$. (En étendant la terminologie de [l'exercice 21 de la section 5.1](#), nous pourrions dire que f est compatible avec \equiv_m .)
- (b) Montrez que pour tous les entiers x_1 et x_2 , $h([x_1]_m, [x_2]_m) = f(x_1, x_2)$.

7.4. Théorème d'Euler

Dans la section précédente, nous avons vu que certains éléments de \mathbb{Z}/\equiv_m possèdent des inverses multiplicatifs, tandis que d'autres n'en possèdent pas. Dans cette section, nous nous intéressons à ceux qui en possèdent. Soit $(\mathbb{Z}/\equiv_m)^*$ l'ensemble des éléments de \mathbb{Z}/\equiv_m possédant des inverses multiplicatifs. Autrement dit,

$$(\mathbb{Z}/\equiv_m)^* = \{X \in \mathbb{Z}/\equiv_m \mid \text{for some } X' \in \mathbb{Z}/\equiv_m, X \cdot X' = [1]_m\}.$$

Le nombre d'éléments de $(\mathbb{Z}/\equiv_m)^*$ est noté $\varphi(m)$. La fonction φ est appelée *fonction phi d'Euler*, ou *fonction indicatrice d'Euler*; elle a été introduite par Euler en 1763. Pour tout entier positif m , $(\mathbb{Z}/\equiv_m)^* \subseteq \mathbb{Z}/\equiv_m$ et \mathbb{Z}/\equiv_m a m éléments, donc $\varphi(m) \leq m$. Et $[1]_m \cdot [1]_m = [1]_m$, donc $[1]_m \in (\mathbb{Z}/\equiv_m)^*$ et donc $\varphi(m) \geq 1$. Par exemple,

$$(\mathbb{Z}/\equiv_{10})^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\},$$

donc $\varphi(10) = 4$.

Pour notre propos, la propriété la plus importante de $(\mathbb{Z} / \equiv_m)^*$ est sa fermeture par les inverses et la multiplication. Autrement dit :

Théorème 7.4.1. *Supposons que m soit un entier positif.*

1. Pour tout X dans $(\mathbb{Z} / \equiv_m)^*$, $X^{-1} \in (\mathbb{Z} / \equiv_m)^*$.
2. Pour chaque X et Y dans $(\mathbb{Z} / \equiv_m)^*$, $X \cdot Y \in (\mathbb{Z} / \equiv_m)^*$.

Preuve.

1. Supposons que $X \in (\mathbb{Z} / \equiv_m)^*$. Alors X possède une réciproque multiplicative X^{-1} , et $X \cdot X^{-1} = [1]_m$. Mais cette équation nous indique aussi que X est la réciproque multiplicative de X^{-1} ; autrement dit, $(X^{-1})^{-1} = X$. Par conséquent, $X^{-1} \in (\mathbb{Z} / \equiv_m)^*$.
2. Supposons que $X \in (\mathbb{Z} / \equiv_m)^*$ et $Y \in (\mathbb{Z} / \equiv_m)^*$. Alors X et Y ont des inverses multiplicatifs X^{-1} et Y^{-1} . Par conséquent

$$(X \cdot Y) \cdot (X^{-1} \cdot Y^{-1}) = (X \cdot X^{-1}) \cdot (Y \cdot Y^{-1}) = [1]_m \cdot [1]_m = [1]_m.$$

Cela signifie que $X^{-1} \cdot Y^{-1}$ est l'inverse multiplicatif de $X \cdot Y$, donc $(X \cdot Y)^{-1} = X^{-1} \cdot Y^{-1}$ et $X \cdot Y \in (\mathbb{Z} / \equiv_m)^*$. \square

Supposons $X \in (\mathbb{Z} / \equiv_m)^*$. D'après [le théorème 7.4.1](#), pour tout $Y \in (\mathbb{Z} / \equiv_m)^*$, $X \cdot Y \in (\mathbb{Z} / \equiv_m)^*$, nous pouvons donc définir une fonction $f_X : (\mathbb{Z} / \equiv_m)^* \rightarrow (\mathbb{Z} / \equiv_m)^*$ par la formule $f_X(Y) = X \cdot Y$. Étudions les propriétés de cette fonction.

Nous affirmons d'abord que f_X est bijectif. Pour comprendre, supposons $Y_1 \in (\mathbb{Z} / \equiv_m)^*$, $Y_2 \in (\mathbb{Z} / \equiv_m)^*$, et $f_X(Y_1) = f_X(Y_2)$. Alors $X \cdot Y_1 = X \cdot Y_2$, et donc

$$Y_1 = [1]_m \cdot Y_1 = X^{-1} \cdot X \cdot Y_1 = X^{-1} \cdot X \cdot Y_2 = [1]_m \cdot Y_2 = Y_2.$$

Ceci prouve que f_X est bijectif. On affirme ensuite que f_X est sur. Pour le prouver, supposons $Y \in (\mathbb{Z} / \equiv_m)^*$. Alors, comme $(\mathbb{Z} / \equiv_m)^*$ est fermé par les inverses et la multiplication, $X^{-1} \cdot Y \in (\mathbb{Z} / \equiv_m)^*$, et

$$f_X(X^{-1} \cdot Y) = X \cdot X^{-1} \cdot Y = [1]_m \cdot Y = Y.$$

Ainsi, f_X est activé.

Français Par exemple, considérons à nouveau le cas $m = 10$, et soit $X = [3]_{10}$. L'application de f_X aux quatre éléments de $(\mathbb{Z} / \equiv_{10})^*$ donne les valeurs présentées dans [la Figure 7.6](#). Notez que, puisque f_X est bijectif et sur, chacun des quatre éléments de $(\mathbb{Z} / \equiv_{10})^*$ apparaît exactement une fois dans la colonne sous $f_X(Y)$; chaque élément apparaît au moins une fois parce que f_X est sur, et il n'apparaît qu'une seule fois parce que f_X est bijectif. Ainsi, les entrées de la deuxième colonne de [la Figure 7.6](#) sont exactement les mêmes que les entrées de la première colonne, mais listées dans un ordre différent.

Y	$f_X(Y)$
$[1]_{10}$	$[3]_{10} \cdot [1]_{10} = [3]_{10}$
$[3]_{10}$	$[3]_{10} \cdot [3]_{10} = [9]_{10}$
$[7]_{10}$	$[3]_{10} \cdot [7]_{10} = [1]_{10}$
$[9]_{10}$	$[3]_{10} \cdot [9]_{10} = [7]_{10}$

Figure 7.6. Valeurs de f_X lorsque $X = [3]_{10}$.

Français Plus généralement, supposons que m soit un entier positif et que $X \in (\mathbb{Z} / \equiv_m)^*$. Par définition de la fonction phi d'Euler, il y a $\varphi(m)$ éléments dans $(\mathbb{Z} / \equiv_m)^*$. Soit $Y_1, Y_2, \dots, Y_{\varphi(m)}$ une liste de ces éléments. Alors, comme f_X est bijectif et sur, chacun de ces éléments apparaît exactement une fois dans la liste $f_X(Y_1), f_X(Y_2), \dots, f_X(Y_{\varphi(m)})$. En d'autres termes, les deux listes $Y_1, Y_2, \dots, Y_{\varphi(m)}$ et $f_X(Y_1), f_X(Y_2), \dots, f_X(Y_{\varphi(m)})$ contiennent exactement les mêmes entrées, mais listées dans des ordres différents – tout comme les deux colonnes de [la Figure 7.6](#). Il s'ensuit, par les lois commutatives et associatives de la multiplication, que si nous multiplions tous les les entrées dans chacune des deux listes, les produits seront les mêmes (voir [exercice 21](#) dans [la section 6.4](#)):

$$\begin{aligned} Y_1 \cdot Y_2 \cdots Y_{\varphi(m)} &= f_X(Y_1) \cdot f_X(Y_2) \cdots f_X(Y_{\varphi(m)}) \\ &= (X \cdot Y_1) \cdot (X \cdot Y_2) \cdots (X \cdot Y_{\varphi(m)}) \\ &= X^{\varphi(m)} \cdot (Y_1 \cdot Y_2 \cdots Y_{\varphi(m)}), \end{aligned}$$

Où, bien sûr, par $X^{\varphi(m)}$ on entend X multiplié par lui-même $\varphi(m)$ fois. Pour simplifier cette équation, soit $Z = Y_1 \cdot Y_2 \cdots Y_{\varphi(m)}$. L'équation est alors $Z = X^{\varphi(m)} \cdot Z$. Puisque $(\mathbb{Z} / \equiv_m)^*$ est fermé par multiplication, $Z \in (\mathbb{Z} / \equiv_m)^*$, il possède donc une inverse. En multipliant les deux côtés de l'équation $Z = X^{\varphi(m)} \cdot Z$ par Z^{-1} , on obtient

$$[1]_m = Z \cdot Z^{-1} = X^{\varphi(m)} \cdot Z \cdot Z^{-1} = X^{\varphi(m)} \cdot [1]_m = X^{\varphi(m)}.$$

Ainsi, nous avons prouvé le théorème suivant.

Théorème 7.4.2. Supposons que m soit un entier positif et $X \in (\mathbb{Z} / \equiv_m)^*$. Alors $X^{\varphi(m)} = [1]_m$.

Pour comprendre la signification de ce théorème, il peut être utile de le reformuler en termes de nombres.

Théorème 7.4.3. (Théorème d'Euler) Supposons que m soit un entier positif. Alors, pour tout entier positif a , si $\text{pgcd}(m, a) = 1$ alors $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Preuve. Supposons que a soit un entier positif et que $\text{pgcd}(m, a) = 1$. Alors, d'après [le théorème 7.3.7](#), $[a]_m \in (\mathbb{Z} / \equiv_m)^*$, donc d'après [le théorème 7.4.2](#), $[a]_m^{\varphi(m)} = [1]_m$, où $[a]_m^{\varphi(m)}$ désigne $[a]_m$ multiplié par lui-même $\varphi(m)$ fois. Mais

$$[a]_m^{\varphi(m)} = \underbrace{[a]_m \cdot [a]_m \cdots [a]_m}_{\varphi(m) \text{ terms}} = \underbrace{[a \cdot a \cdots a]}_{\varphi(m) \text{ terms}}_m = [a^{\varphi(m)}]_m.$$

(Pour une preuve plus précise de cette équation, voir [l'exercice 5.](#)) Ainsi, $[a^{\varphi(m)}]_m = [a]_m^{\varphi(m)} = [1]_m$, et donc $a^{\varphi(m)} \equiv 1 \pmod{m}$. \square

Par exemple, 10 et 7 sont premiers entre eux, donc selon le théorème d'Euler, $7^{\varphi(10)} \equiv 1 \pmod{10}$ devrait être congru à 1 modulo 10. Pour vérifier cela, nous calculons

$$7^{\varphi(10)} = 7^4 = 2401 \equiv 1 \pmod{10}.$$

Pour appliquer le théorème d'Euler, nous devons être capables de calculer $\varphi(m)$. Bien sûr, nous pouvons vérifier tous les éléments de \mathbb{Z} / \equiv_m un par un et compter combien ont des inverses multiplicatifs, comme nous l'avons fait dans le cas $m = 10$, mais pour un grand m , cela sera être peu pratique. Nous consacrons le reste de cette section à la recherche d'un moyen plus efficace de calculer $\varphi(m)$.

Commençons par reformuler la définition de $\varphi(m)$. Nous savons que $\{0, 1, \dots, m-1\}$ est un système résiduel complet modulo m , mais comme $0 \equiv m \pmod{m}$, nous pouvons aussi dire que $\{1, 2, \dots, m\}$ est un système résiduel complet. Ainsi, $\mathbb{Z} / \equiv_m = \{[1]_m, [2]_m, \dots, [m-1]_m, [m]_m\} = \{[a]_m \mid 1 \leq a \leq m\}$, où chaque élément de \mathbb{Z} / \equiv_m apparaît exactement une fois dans cette liste d'éléments. Pour identifier lesquels de ces éléments sont dans $(\mathbb{Z} / \equiv_m)^*$, nous utilisons [le théorème 7.3.7](#), qui nous dit que pour tout entier positif a , $[a]_m$ a un inverse multiplicatif ssi m et a sont premiers entre eux. Ainsi,

$$(\mathbb{Z}/\equiv_m)^* = \{[a]_m \mid 1 \leq a \leq m \text{ and } \gcd(m, a) = 1\}.$$

Cela nous donne une autre façon de comprendre la fonction phi d'Euler :

$\varphi(m)$ = le nombre d'éléments dans l'ensemble { $a \mid 1 \leq a \leq m$ et $\gcd(m, a) = 1$ }.

En utilisant cette caractérisation de la fonction phi, il est facile de calculer $\varphi(p)$ lorsque p est premier : Si $1 \leq a \leq p - 1$ alors $p \nmid a$, et donc $\gcd(p, a) = 1$, mais $\gcd(p, p) = p > 1$. Par conséquent

$$\{a \mid 1 \leq a \leq p \text{ and } \gcd(p, a) = 1\} = \{1, 2, \dots, p - 1\},$$

Donc $\varphi(p) = p - 1$. En fait, il est presque aussi simple de calculer $\varphi(p^k)$ pour tout entier positif k . Si a est un entier positif et $p \mid a$ alors $\gcd(p^k, a) \geq p > 1$, mais si $p \nmid a$ alors le seul diviseur commun de p^k et a est 1, donc $\gcd(p^k, a) = 1$. Ainsi, les éléments de l'ensemble { $a \mid 1 \leq a \leq p^k$ } qui ne sont pas premiers entre eux avec p^k sont précisément ceux qui sont divisibles par p , et ces éléments sont $p, 2p, 3p, \dots, p^k = p^{k-1}p$. En d'autres termes,

$$\{a \mid 1 \leq a \leq p^k \text{ and } \gcd(p^k, a) = 1\} = \{1, 2, \dots, p^k\} \setminus \{p, 2p, \dots, p^{k-1}p\},$$

et le nombre d'éléments dans cet ensemble est $p^k - p^{k-1} = p^{k-1}(p - 1)$. Ainsi $\varphi(p^k) = p^{k-1}(p - 1)$.

Pour calculer $\varphi(m)$ pour d'autres valeurs de m , nous utilisons le théorème suivant, que nous prouverons plus tard dans cette section.

Théorème 7.4.4. *Supposons que m et n soient des entiers positifs premiers entre eux. Alors $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.*

Une fonction f des entiers positifs vers les nombres réels est dite *multiplicative* si elle possède la propriété que, pour tous les entiers positifs m et n premiers entre eux, $f(mn) = f(m) \cdot f(n)$. Ainsi, [le théorème 7.4.4](#) indique que la fonction phi d'Euler est une fonction multiplicative. Un certain nombre d'autres fonctions importantes de la théorie des nombres sont également multiplicatives, mais φ est la seule que nous étudierons dans ce livre. (Pour deux autres exemples, voir [les exercices 16 et 17.](#))

Le [théorème 7.4.4](#) nous permet d'utiliser la décomposition en facteurs premiers de tout entier positif m pour trouver $\varphi(m)$. Supposons que la décomposition en facteurs premiers de m soit $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ telle que p_1, p_2, \dots, p_k soient des nombres premiers et $p_1 < p_2 < \cdots < p_k$. Alors $p_i^{e_i}$ et $p_j^{e_j}$ sont premiers entre eux, car ils $p_2^{e_2} \cdots p_k^{e_k}$ n'ont pas de facteurs premiers en commun (voir

exercice 5 de la section 7.2). $\varphi(m) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2} \cdots p_k^{e_k})$. En répétant ce raisonnement, nous concluons que

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1 - 1) \cdot p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1).\end{aligned}$$

Par exemple, $600 = 2^3 \cdot 3 \cdot 5^2$, donc

$$\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = 2^2(2 - 1) \cdot 3^0(3 - 1) \cdot 5^1(5 - 1) = 160.$$

C'était beaucoup plus simple que d'énumérer explicitement les 160 éléments de $(\mathbb{Z}/600\mathbb{Z})^*$!

Notre preuve du théorème 7.4.4 dépendra de trois lemmes.

Lemme 7.4.5. *Supposons que m et n soient des entiers positifs premiers entre eux. Alors, pour tous les entiers a et b , $a \equiv b \pmod{mn}$ ssi $a \equiv b \pmod{m}$ et $a \equiv b \pmod{n}$.*

Preuve. Voir exercice 6. □

Lemme 7.4.6. *Pour tous les entiers positifs a , b et c , $\gcd(ab, c) = 1$ ssi $\gcd(a, c) = 1$ et $\gcd(b, c) = 1$.*

Preuve. Voir exercice 7. □

Lemme 7.4.7. *Supposons que m et n soient des entiers positifs premiers entre eux. Alors, pour tous les entiers a et b , il existe un entier r tel que $1 \leq r \leq mn$, $r \equiv a \pmod{m}$ et $r \equiv b \pmod{n}$.*

Preuve. Soient a et b des entiers arbitraires. Puisque m et n sont premiers entre eux, il existe des entiers s et t tels que $sm + tn = 1$. Par conséquent, $tn - 1 = -sm$ et $sm - 1 = -tn$.

Soit $x = tna + qn$. Alors

$$x - a = (tn - 1)a + smb = -sma + smb = sm(b - a),$$

donc $m | (x - a)$, et donc $x \equiv a \pmod{m}$. De même,

$$x - b = tna + (sm - 1)b = tna - tnb = tn(a - b),$$

donc $n | (x - b)$ et $x \equiv b \pmod{n}$.

Puisque $\{1, 2, \dots, mn\}$ est un système résiduel complet modulo mn , on peut trouver un entier r tel que $r \equiv x \pmod{mn}$ et $1 \leq r \leq mn$. D'après le lemme 7.4.5, $r \equiv x \pmod{m}$ et $r \equiv x \pmod{n}$, et par la transitivité de \equiv_m et \equiv_n , il s'ensuit que $r \equiv a \pmod{m}$ et $r \equiv b \pmod{n}$.

Commentaire. Après l'introduction des entiers arbitraires a et b , l'objectif est une affirmation existentielle. Comme c'est souvent le cas pour les démonstrations d'affirmations existentielles, la démonstration introduit un nombre x sans fournir de justification pour son choix. Ce nombre x possède la plupart des propriétés souhaitées, mais peut-être pas toutes, car il pourrait ne pas être compris entre 1 et mn . Il nous faut donc une étape supplémentaire pour obtenir le nombre r possédant toutes les propriétés requises.

Nous aurons besoin d'une idée supplémentaire pour notre preuve du [théorème 7.4.4](#). Supposons que A soit un ensemble à p éléments et que B soit un ensemble à q éléments ; disons que $A = \{a_1, a_2, \dots, a_p\}$ et $B = \{b_1, b_2, \dots, b_q\}$. Alors $A \times B$ a pq éléments. Pour comprendre pourquoi, imaginez disposer les éléments de $A \times B$ dans un tableau, avec la paire ordonnée (a_i, b_j) dans la ligne i , colonne j du tableau. Puisque le tableau aura p lignes et q colonnes, $A \times B$ doit avoir pq éléments. Pour une démonstration plus précise de ce fait, voir [l'exercice 22 de la section 8.1](#).

Nous sommes maintenant prêts à prouver que φ est une fonction multiplicative.

Preuve du théorème 7.4.4. Soit $R = \{a \mid 1 \leq a \leq mn \text{ et } \text{pgcd}(mn, a) = 1\}$. D'après [le lemme 7.4.6](#), si $a \in R$ alors $\text{pgcd}(m, a) = 1$ et $\text{pgcd}(n, a) = 1$, donc $[a]_m \in (\mathbb{Z}/\equiv_m)^*$ et $[a]_n \in (\mathbb{Z}/\equiv_n)^*$. On peut donc définir une fonction $f: R \rightarrow (\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$ par la formule $f(a) = ([a]_m, [a]_n)$. Notre objectif est de montrer que f est bijectif et sur, ce qui implique que les ensembles R et $(\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$ ont le même nombre d'éléments. Mais R a $\varphi(mn)$ éléments et $(\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$ a $\varphi(m) \cdot \varphi(n)$ éléments, ce qui établira que $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Français Pour montrer que f est inexact, supposons $a_1 \in R$, $a_2 \in R$ et $f(a_1) = f(a_2)$. Cela signifie que $([a_1]_m, [a_1]_n) = ([a_2]_m, [a_2]_n)$, donc $[a_1]_m = [a_2]_m$ et $[a_1]_n = [a_2]_n$, et donc $a_1 \equiv a_2 \pmod{m}$ et $a_1 \equiv a_2 \pmod{n}$. D'après [le lemme 7.4.5](#), il s'ensuit que $a_1 \equiv a_2 \pmod{mn}$. Mais puisque $\{a \mid 1 \leq a \leq mn\}$ est un système résiduel complet modulo mn , aucun élément distinct de R n'est congruent modulo mn , donc $a_1 = a_2$. Ceci complète la preuve que f est bijectif.

Enfin, pour montrer que f est sur, soit $([a]_m, [b]_n)$ un élément arbitraire de $(\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$. D'après [le lemme 7.4.7](#), il existe

un entier r tel que $1 \leq r \leq mn$, $r \equiv a \pmod{m}$ et $r \equiv b \pmod{n}$. Par conséquent, $[r]_m = [a]_m \in (\mathbb{Z}/\equiv_m)^*$ et $[r]_n = [b]_n \in (\mathbb{Z}/\equiv_n)^*$, donc d'après [le théorème 7.3.7](#), $\text{pgcd}(m, r) = \text{pgcd}(n, r) = 1$. En appliquant [le lemme 7.4.6](#), nous concluons que $\text{pgcd}(mn, r) = 1$. Par conséquent, $r \in R$ et $f(r) = ([r]_m, [r]_n) = ([a]_m, [b]_n)$, ce qui montre que f est sur. \square

Exercices

1. Énumérez les éléments de $(\mathbb{Z} / \equiv_{20})^*$.
- *2. Trouvez $\varphi(m)$:
(a) $m = 539$.
(b) $m = 540$.
(c) $m = 541$.
3. Vérifiez ces instances du théorème d'Euler en calculant $a^{\varphi(m)}$ et en vérifiant que $a^{\varphi(m)} \equiv 1 \pmod{m}$.
(a) $m = 18, a = 5$.
(b) $m = 19, a = 2$.
(c) $m = 20, a = 3$.
4. Vérifiez ces instances du [lemme 7.4.7](#) en trouvant un entier r tel que $1 \leq r \leq mn$, $r \equiv a \pmod{m}$ et $r \equiv b \pmod{n}$.
(a) $m = 5, n = 8, a = 4, b = 1$.
(b) $m = 7, n = 10, a = 6, b = 4$.
5. Supposons que m et a soient des entiers positifs. Démontrer par induction que pour tout entier positif n , $[a]^n_m = [a^n]_m$.
- *6. Démontrer [le lemme 7.4.5](#).
7. Démontrer [le lemme 7.4.6](#).
- *8. Montrez que si l'on abandonne l'hypothèse selon laquelle m et n sont premiers entre eux ([du lemme 7.4.5](#)), alors une direction de l'énoncé « ssi » est correcte et l'autre ne l'est pas. Justifiez votre réponse en fournissant une preuve pour une direction et un contre-exemple pour l'autre.
9. Si l'on abandonne l'hypothèse selon laquelle m et n sont premiers entre eux, issue [du lemme 7.4.7](#), ce lemme est-il toujours correct ? Justifiez votre réponse par une preuve ou un contre-exemple.
10. Démontrer le petit théorème de Fermat, qui dit que si p est un nombre premier, alors pour tout entier positif a , $a^p \equiv a \pmod{p}$.
11. Démontrer que si m et a sont des entiers positifs premiers entre eux, alors $[a]_m^{-1} = [a^{\varphi(m)-1}]_m$.
12. Démontrer que pour tous les entiers positifs m, a, p et q , si m et a sont premiers entre eux et $p \equiv q \pmod{\varphi(m)}$ alors $a^p \equiv a^q \pmod{m}$.
13. Démontrer que si a, b_1, b_2, \dots, b_k sont des entiers positifs et $\text{pgcd}(a, b_1) = \text{pgcd}(a, b_2) = \dots = \text{pgcd}(a, b_k) = 1$, alors $\text{pgcd}(a, b_1 b_2 \dots b_k) = 1$.

14. Supposons que m_1, m_2, \dots, m_k soient des entiers positifs deux à deux premiers entre eux ; c'est-à-dire que pour tout $i, j \in \{1, 2, \dots, k\}$, si $i \neq j$ alors $\text{pgcd}(m_i, m_j) = 1$. Soit $M = m_1 m_2 \cdots m_k$. Démontrer que pour tous les entiers a et b , $a \equiv b \pmod{M}$ ssi pour tout $i \in \{1, 2, \dots, k\}$, $a \equiv b \pmod{m_i}$.
15. Dans cet exercice, vous démontrerez le théorème du reste chinois.
(Ce théorème a été énoncé pour la première fois par le mathématicien chinois Sun Zi au IIIe siècle.)
- (a) Supposons que m_1, m_2, \dots, m_k soient des entiers positifs deux à deux premiers entre eux ; c'est-à-dire que pour tout $i, j \in \{1, 2, \dots, k\}$, si $i \neq j$ alors $\text{pgcd}(m_i, m_j) = 1$. Soit $M = m_1 m_2 \cdots m_k$. Démontrer que pour tout entier a_1, a_2, \dots, a_k il existe un entier r tel que $1 \leq r \leq M$ et que pour tout $i \in \{1, 2, \dots, k\}$, $r \equiv a_i \pmod{m_i}$. (Conseil : utiliser l'induction sur k . Dans l'étape d'induction, utiliser [le lemme 7.4.7](#). [Les exercices 13](#) et [14](#) vous seront également utiles.)
- (b) Démontrer que l'entier r dans la partie (a) est unique.
16. Pour tout entier positif n , soit $\tau(n)$ = le nombre d'éléments de $D(n)$. Par exemple, $D(6) = \{1, 2, 3, 6\}$, donc $\tau(6) = 4$. Dans cet exercice, vous démontrerez que τ est une fonction multiplicative. Supposons que m et n soient des entiers positifs premiers entre eux.
- (a) Démontrer que si $a \in D(m)$ et $b \in D(n)$ alors $ab \in D(mn)$.
- (b) Par la partie (a), nous pouvons définir une fonction $f: D(m) \times D(n) \rightarrow D(mn)$ par la formule $f(a, b) = ab$. Démontrer que f est bijective et sur.
- (c) Démontrer que $\tau(mn) = \tau(m) \cdot \tau(n)$, ce qui montre que τ est multiplicatif.
17. Pour tout entier positif n , soit $\sigma(n)$ = la somme de tous les éléments de $D(n)$. Par exemple, $D(6) = \{1, 2, 3, 6\}$, donc $\sigma(6) = 1 + 2 + 3 + 6 = 12$. Démontrer que σ est une fonction multiplicative. (Indice : Utiliser la fonction f de la partie (b) de [l'exercice 16](#).)
18. Dans cet exercice, vous démontrerez le théorème d'Euclide sur les nombres parfaits. Rappelons qu'un entier positif n est dit parfait si n est égal à la somme de tous les diviseurs de n inférieurs à n . De même, n est parfait si $\sigma(n) = 2n$, où σ est la fonction définie dans [l'exercice 17](#). Démontrer que si p est un entier positif et que $2p - 1$ est premier, alors $2p - 1$ est parfait. (Indice : [L'exercice 17](#) et [l'exemple 6.1.1](#) vous seront utiles.)
19. Dans cet exercice, vous démontrerez le théorème d'Euler sur les nombres parfaits. Supposons que n soit un nombre pair parfait. (Comme dans [l'exercice 18](#), dire que n est parfait signifie que $\sigma(n) = 2n$, où σ est la fonction définie dans [l'exercice 17](#).)

- (a) Démontrer qu'il existe des entiers positifs k et m tels que $n = 2^k m$ et m est impair.
- (b) Démontrer que $2^{k+1} m = (2^{k+1} - 1) \sigma(m)$.
- (c) Démontrer que $2^{k+1} | \sigma(m)$. Il existe donc un entier positif d tel que $\sigma(m) = 2^{k+1} d$.
- (d) Démontrer que $m = (2^{k+1} - 1) d$.
- (e) Démontrer que $d = 1$. (Indice : Supposons que $d > 1$. Alors 1, d et m sont des diviseurs distincts de m , donc $\sigma(m) \geq 1 + d + m$. Déduire une contradiction.)
- (f) Soit $p = k + 1$. Alors, par les parties (a), (d) et (e), $n = 2^{p-1} (2^p - 1)$. Démontrer que $2^p - 1$ est premier. Ainsi, n est un nombre parfait de la forme considérée dans [l'exercice 18](#).

7.5. Cryptographie à clé publique

Imaginez que vous souhaitez effectuer un achat en ligne. Vous vous rendez sur le site web du commerçant et passez commande. Le site vous demande ensuite de saisir votre numéro de carte bancaire. Vous saisissez ce numéro sur votre ordinateur, qui doit ensuite le transmettre par Internet à l'ordinateur du commerçant.

Les communications Internet transitent généralement par plusieurs ordinateurs entre l'expéditeur et le destinataire. Par conséquent, il est possible qu'une personne ayant accès à l'un de ces ordinateurs intermédiaires puisse espionner votre ordinateur lorsque celui-ci transmet votre numéro de carte de crédit au commerçant. Pour empêcher une telle personne de voler votre numéro de carte de crédit, votre ordinateur le *chiffre avant de l'envoyer*. *L'ordinateur du commerçant le déchiffre* ensuite et débite votre carte de crédit.

Par exemple, supposons que votre numéro de carte de crédit soit la séquence de 16 chiffres $m = m_1 m_2 \cdots m_{16}$. Chaque m_i est l'un des chiffres 0, 1, 2, ..., 9, mais nous le considérerons comme représentant la classe d'équivalence $[m_i]_{10} \in \mathbb{Z}/\equiv_{10}$. Si votre ordinateur et celui du commerçant pouvaient s'accorder sur une séquence aléatoire de chiffres $k = k_1 k_2 \cdots k_{16}$, alors ils pourraient procéder comme suit, en effectuant tous les calculs dans \mathbb{Z}/\equiv_{10} . Votre ordinateur pourrait remplacer le i -ème chiffre m_i de votre numéro de carte de crédit par le chiffre c_i tel que $[c_i]_{10} = [m_i]_{10} + [k_i]_{10}$. Votre ordinateur enverrait la séquence de 16 chiffres $c = c_1 c_2 \cdots c_{16}$ à l'ordinateur du commerçant, qui récupérerait alors la séquence originale m en utilisant la formule $[m_i]_{10} = [c_i]_{10} + (-[k_i]_{10})$. La séquence k est la *clé* que votre

ordinateur utilise pour crypter le numéro de carte de crédit et que l'ordinateur du commerçant utilise pour le décrypter. Un espion qui ne connaîtrait pas la clé k serait incapable de décrypter le message crypté c et d'apprendre votre numéro de carte de crédit m .

Mais comment votre ordinateur et celui du commerçant peuvent-ils s'accorder sur la clé k ? Si un ordinateur choisit la clé et l'envoie à l'autre, un espion pourrait la connaître et déchiffrer le message chiffré. Envoyer la clé en toute sécurité est aussi difficile que d'envoyer le numéro de carte de crédit ; nous ne semblons donc pas avoir progressé.

Le problème de ce système est qu'il utilise *une cryptographie symétrique*, où la même clé est utilisée pour le chiffrement et le déchiffrement. La solution consiste à utiliser *une cryptographie à clé publique*, où les clés de chiffrement et de déchiffrement sont différentes. L'ordinateur du commerçant crée deux clés, une pour le chiffrement et l'autre pour le déchiffrement. Il envoie la clé de chiffrement à votre ordinateur. Votre ordinateur utilise la clé de chiffrement pour chiffrer votre numéro de carte de crédit, puis envoie le numéro chiffré à l'ordinateur du commerçant, qui utilise la clé de déchiffrement pour le récupérer. Une personne mal intentionnée pourrait connaître la clé de chiffrement ; elle est donc considérée comme une *clé publique*. Mais cela n'aide pas l'internaute, car le déchiffrement nécessite la clé de déchiffrement, et cette clé n'est jamais transmise et reste secrète.

Il peut paraître surprenant qu'il soit possible d'utiliser des clés différentes pour le chiffrement et le déchiffrement, mais c'est possible. Dans cette section, nous abordons un système de chiffrement à clé publique bien connu appelé RSA. Il doit son nom à Ron Rivest (1947-), Adi Shamir (1952-) et Leonard Adleman (1945-), qui l'ont développé en 1977. Un système similaire a été développé en 1973 par Clifford Cocks (1950-), mathématicien travaillant pour les services de renseignement britanniques, mais il a été classifié et n'a été révélé qu'en 1997. Comme nous le verrons, le système RSA est basé sur le théorème d'Euler.

Français Nous avons introduit l'idée de la cryptographie à clé publique dans le contexte des achats sur Internet, mais elle peut être utilisée à chaque fois qu'une personne souhaite envoyer un message à une autre tout en empêchant une oreille indiscrète de lire le message. Supposons qu'Alice souhaite envoyer un message en toute sécurité à Bob. Pour utiliser le système de clé publique RSA, ils procéderaient comme suit. Tout d'abord, Bob choisit deux nombres premiers distincts p et q . Il calcule $n = pq$ et $\varphi(n) = (p - 1)(q - 1)$. Ensuite, il choisit un entier positif e tel que e et $\varphi(n)$ soient premiers entre eux et $e < \varphi(n)$. D'après [le théorème 7.3.7](#), $[e]_{\varphi(n)}$ a un inverse

multiplicatif dans $\mathbb{Z} / \equiv_{\varphi(n)}$, qui peut être calculé par l'algorithme d'Euclide étendu. Ainsi, Bob peut calculer un entier positif d tel que $d < \varphi(n)$ et $[e]_{\varphi(n)} \cdot [d]_{\varphi(n)} = [1]_{\varphi(n)}$, ce qui signifie que $ed \equiv 1 \pmod{\varphi(n)}$. Bob envoie la paire de nombres (n, e) à Alice ; c'est la clé de chiffrement qu'Alice utilisera pour chiffrer son message. Il garde les nombres p, q et d secrets ; il utilisera d pour déchiffrer le message d'Alice.

Nous supposerons que le message qu'Alice souhaite envoyer est un entier naturel $m < n$. Bien sûr, son message pourrait être un texte, et non un nombre, mais un texte peut être codé comme un entier naturel. Si le texte est long, il pourrait être nécessaire de le coder comme une suite d'entiers naturels, chacun étant inférieur à n , et chacun de ces entiers naturels devrait alors être chiffré séparément. Mais pour simplifier la discussion, nous supposerons que le message d'Alice est un seul entier naturel $m < n$.

Comme précédemment, nous pensons au message m comme représentant une classe d'équivalence $[m]_n \in \mathbb{Z} / \equiv_n$, et Alice et Bob feront tous leurs calculs en utilisant l'arithmétique dans \mathbb{Z} / \equiv_n . Pour crypter son message, Alice calcule $[m]_n^e$. En d'autres termes, elle calcule l'entier naturel unique $c < n$ tel que $[m]_n^e = [c]_n$. Le nombre c est le message crypté, qu'elle envoie à Bob.

Pour déchiffrer le message, Bob calcule $[c]_n^d$. Ce qui fait fonctionner le système RSA est le fait surprenant que, $[c]_n^d = [m]_n$, comme nous le démontrerons ci-dessous. Ainsi, en calculant, $[c]_n^d$, Bob peut récupérer le message original m . Notez que le chiffrement et le déchiffrement impliquent tous deux une exponentiation, mais l'exposant de chiffrement e et l'exposant de déchiffrement d sont différents. Ainsi, peu importe qu'un espion apprenne e ; tant que Bob garde d secret, l'espion ne saura pas quel exposant utiliser pour déchiffrer le message chiffré.

Pour montrer que RSA fonctionne, nous devons prouver le théorème suivant.

Théorème 7.5.1. *Supposons que p et q soient des nombres premiers distincts, $n = pq$, e et d sont des entiers positifs tels que $ed \equiv 1 \pmod{\varphi(n)}$, et m et c sont des nombres naturels tels que $[m]_n^e = [c]_n$. Alors $[c]_n^d = [m]_n$.*

Preuve. Si $e = d = 1$ alors $[m]_n = [c]_n$ et la conclusion est claire. Sinon, alors $ed > 1$, donc puisque $ed \equiv 1 \pmod{\varphi(n)}$, il existe un entier positif k tel que $ed - 1 = k\varphi(n)$, et donc $ed = k\varphi(n) + 1 = k(p-1)(q-1) + 1$. Et puisque $[m]_n^e = [c]_n$, $m^e \equiv c \pmod{n}$, donc $n \mid (m^e - c)$.

Bien que nous souhaitions finalement tirer une conclusion sur l'arithmétique dans \mathbb{Z} / \equiv_n , il nous sera utile d'effectuer d'abord quelques calculs dans \mathbb{Z} / \equiv_p et \mathbb{Z} / \equiv_q . Puisque $p \mid n$ et $n \mid (m^e - c)$, par la transitivité de la relation de divisibilité, $p \mid (m^e - c)$. Par conséquent, $m^e \equiv c \pmod{p}$, ou de manière équivalente $[m]^e_p = [c]_p$.

Notez que les règles habituelles d'exposant s'appliquent à l'exponentiation dans \mathbb{Z} / \equiv_p . Plus précisément, pour tout $X \in \mathbb{Z} / \equiv_p$ et tout entier positif a et b , nous avons

$$X^a \cdot X^b = \underbrace{X \cdots X}_{a \text{ terms}} \cdot \underbrace{X \cdots X}_{b \text{ terms}} = \underbrace{X \cdots X}_{a+b \text{ terms}} = X^{a+b}$$

et

$$(X^a)^b = \underbrace{(X \cdots X)}_{a \text{ terms}} \cdot \underbrace{(X \cdots X)}_{a \text{ terms}} \cdots \underbrace{(X \cdots X)}_{a \text{ terms}} = \underbrace{X \cdots X}_{b \text{ groups of terms}} = X^{ab}.$$

(Pour des preuves plus précises de ces équations, voir [l'exercice 8.](#)) En appliquant ces règles, nous voyons que

$$[c]^d_p = ([m]^e_p)^d = [m]^{ed}_p = [m]^k_p^{(p-1)(q-1)+1} = ([m]_p^{p-1})^{k(q-1)} \cdot [m]_p.$$

Nous affirmons maintenant que $[c]^d_p = [m]_p$. Pour le prouver, nous considérons deux cas.

Cas 1. $p \nmid m$. Alors p et m sont premiers entre eux, donc par le théorème d'Euler, $[m]_p^{p-1} = [1]_p$. Par conséquent

$$[c]^d_p = ([m]_p^{p-1})^{k(q-1)} \cdot [m]_p = [1]_p^{k(q-1)} \cdot [m]_p = [1]_p \cdot [m]_p = [m]_p.$$

Cas 2. $p \mid m$. Alors $[m]_p = [0]_p$, donc

$$[c]^d_p = [m]^{ed}_p = [0]^{ed}_p = [0]_p = [m]_p.$$

Dans les deux cas, nous sommes parvenus à la conclusion souhaitée : $[c]^d_p = [m]_p$. Par conséquent, $c^d \equiv m \pmod{p}$. Un raisonnement similaire montre que $c^d \equiv m \pmod{q}$, et puisque $pq = n$, il en résulte, d'après [le lemme 7.4.5](#), que $c^d \equiv m \pmod{n}$. Autrement dit, $[c]^d_n = [m]_n$, c'est ce que nous souhaitions démontrer.

Essayons cela avec un exemple simple. Supposons que Bob choisisse les nombres premiers $p = 3$ et $q = 11$, donc $n = pq = 33$ et $\varphi(n) = (p-1)(q-1) = 20$. Il choisit également $e = 7$, et il calcule ensuite $[e]_{\varphi(n)}^{-1} = [7]_{20}^{-1} = [3]_{20}$, donc $d = 3$. (Pour vérifier le travail de Bob, notez que $[7]_{20} \cdot [3]_{20} = [21]_{20} = [1]_{20}$.) Bob envoie les nombres $n = 33$ et $e = 7$ à Alice.

Supposons qu'Alice veuille envoyer le message $m = 5$ à Bob. Elle calcule

$$[m]_n^e = [5]_{33}^7 = [78125]_{33} = [14]_{33},$$

Son message chiffré est donc $c = 14$. Elle envoie ce nombre à Bob. Pour déchiffrer le message, Bob calcule

$$[c]_n^d = [14]_{33}^3 = [2744]_{33} = [5]_{33}.$$

Ainsi, Bob récupère avec succès le message d'origine $m = 5$.

Les communications d'Alice et Bob sont-elles sécurisées ? Supposons qu'un espion intercepte à la fois le message de Bob à Alice et celui d'Alice à Bob, apprenant ainsi les nombres $n = 33$, $e = 7$ et $c = 14$. En factorisant $n = 33 = 3 \cdot 11$, l'espion pourrait apprendre que $p = 3$ et $q = 11$ (ou vice-versa), et donc $\varphi(n) = (p - 1)(q - 1) = 20$. Mais alors, l'espion pourrait Calculez, comme Bob, que $[e]_{\varphi(n)}^{-1} = [7]_{20}^{-1} = [3]_{20}$. L'exposant de déchiffrement $d = 3$ est ainsi appris. L'espion peut alors déchiffrer le message d'Alice, exactement comme Bob. Les communications ne sont pas sécurisées !

Qu'est-ce qui s'est passé ? Le problème est que, dans cet exemple simple, nous avons utilisé de petits nombres. La première étape de l'écoute indiscrète a été de factoriser $n = 33$, qui est un produit de deux nombres premiers. Un petit nombre n peut être factorisé facilement en divisant simplement n par tous les plus petits nombres premiers jusqu'à trouver un facteur premier, mais si n est grand, cette procédure sera trop longue pour être pratique. Factoriser des nombres produits de deux grands nombres premiers est particulièrement difficile. En 2019, le plus grand nombre de ce type jamais factorisé est un produit de deux nombres premiers de 116 chiffres. Il a été factorisé en 2009 après deux ans de calcul par plusieurs centaines d'ordinateurs travaillant ensemble sur le problème, ce qui a nécessité près de 2 000 ans de calcul par un seul ordinateur. Factoriser un produit de nombres premiers nettement plus grand serait impossible avec les technologies informatiques actuelles. Aujourd'hui, la plupart des personnes qui utilisent RSA choisissent des nombres premiers de plusieurs centaines de chiffres. Si un espion découvre les nombres n et e , il dispose en principe de suffisamment d'informations pour trouver l'exposant de déchiffrement d , mais la seule méthode connue pour y parvenir est de factoriser n . La sécurité de RSA repose sur le fait qu'en pratique, les nombres utilisés sont si grands que la factorisation de n est impossible.

Mais attendez ! Qu'en est-il des calculs qu'Alice et Bob doivent effectuer avec ces nombres extrêmement grands ? Seront-ils également irréalisables ? Si oui, le système sera inutile. Heureusement, il existe des

moyens efficaces d'effectuer les calculs demandés à Alice et Bob. Bien qu'une discussion détaillée de la manière dont ces calculs sont effectués dépasse le cadre de ce livre, nous pouvons en commenter brièvement les points principaux.

Les calculs les plus difficiles qu'Alice et Bob doivent faire sont :

- Bob doit trouver deux grands nombres premiers p et q .
- Bob doit trouver $\varphi^{-1}(n)$.
- Alice doit calculer $[m]^e_n$ et Bob doit calculer $[c]^d_n$.

Pour trouver les nombres premiers p et q , Bob peut simplement choisir au hasard des nombres suffisamment grands et les tester pour voir s'ils sont premiers jusqu'à ce qu'il trouve deux nombres premiers. Le problème du test de primalité d'un grand nombre a été largement étudié. En 2019, grâce aux méthodes les plus connues, un ordinateur peut déterminer si un nombre de 1 000 chiffres est premier en quelques minutes. Cependant, cette rapidité est insuffisante pour convenir à RSA, car Bob peut devoir tester la primalité de centaines de nombres avant de trouver un nombre premier. La plupart des implémentations de RSA utilisent donc *des tests probabilistes de primalité*. Ces tests prennent une fraction de seconde, mais leur précision n'est pas garantie, notamment si un nombre ne l'est pas. Si le nombre est premier, il est possible que le test ne le détecte pas et indique que le nombre est premier. Cependant, en répétant le test plusieurs fois, la probabilité d'erreur peut être réduite au minimum. Pour en savoir plus sur les tests probabilistes de primalité, voir [les exercices 10 à 14](#).

Nous connaissons déjà une méthode permettant à Bob de calculer $\varphi^{-1}(n)$: l'algorithme d'Euclide étendu. Cet algorithme est très rapide, même avec de très grands nombres. Pour plus d'informations, voir [l'exercice 13 de la section 7.1](#).

Enfin, pour chiffrer et déchiffrer des messages, Alice et Bob doivent éléver les éléments de \mathbb{Z} / \equiv_n à des puissances élevées. Supposons que $X \in \mathbb{Z} / \equiv_n$ et que a soit un entier positif. La méthode la plus simple pour calculer X^a consiste à multiplier X par lui-même a , mais cela n'est pas réalisable si a est grand. Il existe une meilleure méthode, la récursivité. Si $a = 1$, alors $X^a = X$. Pour des valeurs plus grandes de a , on utilise les formules suivantes :

$$\begin{aligned} X^{2k} &= X^k \cdot X^k; \\ X^{2k+1} &= X^k \cdot X^k \cdot X. \end{aligned}$$

Exemple 7.5.2. Trouver $[347]^{172}_{582}$.

Solution

Soit $X = [347]_{582} \in \mathbb{Z} / \equiv_{582}$; nous devons trouver X^{172} . Puisque 172 est pair, nous commençons par

$$X^{172} = X^{2 \cdot 86} = X^{86} \cdot X^{86}.$$

Si nous trouvons X_2 , il suffit de le multiplier par lui-même pour obtenir X_2 . Pour trouver X_2 , nous utilisons la même méthode :

$$X^{86} = X^{2 \cdot 43} = X^{43} \cdot X^{43}.$$

Maintenant, nous devons trouver X^{43} , et comme 43 est impair, nous utilisons la formule

$$X^{43} = X^{2 \cdot 21 + 1} = X^{21} \cdot X^{21} \cdot X.$$

En continuant ainsi, nous obtenons la liste de formules suivante :

$$\begin{aligned} X^{172} &= X^{86} \cdot X^{86}, \\ X^{86} &= X^{43} \cdot X^{43}, \\ X^{43} &= X^{21} \cdot X^{21} \cdot X, \\ X^{21} &= X^{10} \cdot X^{10} \cdot X, \\ X^{10} &= X^5 \cdot X^5, \\ X^5 &= X^2 \cdot X^2 \cdot X, \end{aligned}$$

$$X^2 = X^1 \cdot X^1 = X \cdot X.$$

Nous pouvons maintenant parcourir cette liste dans l'ordre inverse et évaluer chaque formule :

$$\begin{aligned} X^2 &= X \cdot X = [347]_{582} \cdot [347]_{582} = [120409]_{582} = [517]_{582}, \\ X^5 &= X^2 \cdot X^2 \cdot X = [517]_{582} \cdot [517]_{582} \cdot [347]_{582} = [92749283]_{582} = [17]_{582}, \\ X^{10} &= X^5 \cdot X^5 = [17]_{582} \cdot [17]_{582} = [289]_{582}, \\ X^{21} &= X^{10} \cdot X^{10} \cdot X = [289]_{582} \cdot [289]_{582} \cdot [347]_{582} = [28981787]_{582} = [515]_{582}, \\ X^{43} &= X^{21} \cdot X^{21} \cdot X = [515]_{582} \cdot [515]_{582} \cdot [347]_{582} = [92033075]_{582} = [251]_{582}, \\ X^{86} &= X^{43} \cdot X^{43} = [251]_{582} \cdot [251]_{582} = [63001]_{582} = [145]_{582}, \\ X^{172} &= X^{86} \cdot X^{86} = [145]_{582} \cdot [145]_{582} = [21025]_{582} = [73]_{582}. \end{aligned}$$

Nous concluons que $[347]_{582}^{172} = [73]_{582}$. Si vous comptez, vous constaterez que nous n'avons effectué que 10 multiplications – bien moins que les 171 qui seraient nécessaires si nous multiplions simplement 172 X . Pour en savoir plus sur le nombre de multiplications nécessaires pour calculer X^a en général, voir [l'exercice 9](#).

Nous terminons cette section par un autre exemple d'utilisation de RSA. Cette fois, nous utiliserons des nombres suffisamment grands pour nous obliger à utiliser des méthodes de calcul efficaces, même s'ils ne sont pas aussi grands que ceux utilisés dans une application réelle de RSA.

Exemple 7.5.3. Supposons que Bob choisisse les nombres premiers $p = 48611$ et $q = 37813$. Il calcule $n = pq = 1838127743$ et $\varphi(n) = (p-1)(q-1) = 1838041320$. Il choisit ensuite l'exposant de chiffrement $e = 184270657$.

1. Trouvez l'exposant de déchiffrement d .
2. Supposons qu'Alice veuille envoyer le message $m = 357249732$. Trouvez le message chiffré c et vérifiez que Bob peut le déchiffrer.

Solutions

1. Pour calculer d , Bob utilise l'algorithme euclidien étendu pour trouver $[e]_{\varphi(n)}^{-1} = [184270657]_{1838041320}^{-1}$. Les étapes sont présentées dans [la figure 7.7](#). Bob conclut que $d = 88235833$.

n	q_n	r_n	s_n	t_n
0		1838041320	1	0
1		184270657	0	1
2	9	179605407	1	-9
3	1	4665250	-1	10
4	38	2325907	39	-389
5	2	13436	-79	788
6	173	1479	13706	-136713
7	9	125	-123433	1231205
8	11	104	1371469	-13679968
9	1	21	-1494902	14911173
10	4	20	7351077	-73324660
11	1	1	-8845979	88235833
12	20	0		

Figure 7.7. Calcul de l'exposant de déchiffrement d .

Pour vérifier, Bob peut calculer que

$$ed - 1 = 16259274917852280 = 8845979\varphi(n),$$

donc $ed \equiv 1 \pmod{\varphi(n)}$.

2. Soit $X = [m]_n = [357249732]_{1838127743}$. Pour chiffrer son message, Alice doit calculer $X^e = X^{184270657}$. Les étapes sont illustrées à [la figure 7.8](#); Alice planifie bien sûr ses calculs en commençant par la fin de ce tableau, mais les effectue depuis le début. Elle envoie le message chiffré $c = 1357673396$.

k	X^k	k	X^k
2	[413387288] _n	44987	[418397817] _n
5	[1105456936] _n	89975	[1597035021] _n
10	[1522283045] _n	179951	[1491451285] _n
21	[1773257888] _n	359903	[954701208] _n
43	[638596171] _n	719807	[1817497177] _n
87	[664005337] _n	1439614	[1774588706] _n
175	[661296271] _n	2879229	[1061291500] _n
351	[993223048] _n	5758458	[21397340] _n
702	[1294276724] _n	11516916	[1624593674] _n
1405	[1088781967] _n	23033832	[1474914774] _n
2811	[1010306117] _n	46067664	[1189097151] _n
5623	[1064784897] _n	92135328	[46825442] _n
11246	[1739950485] _n	184270657	[1357673396] _n
22493	[799178524] _n		

Figure 7.8. Calcul du message chiffré c .

Pour déchiffrer le message, Bob pose $Y = [c]_n$ et calcule $Y^d = Y^{88235833}$, comme illustré à [la figure 7.9](#). Comme prévu, il obtient $m = 357249732$.

k	Y^k	k	Y^k
2	[42593275] _n	21541	[120530669] _n
5	[1698473378] _n	43083	[189879402] _n
10	[1210371791] _n	86167	[781925623] _n
21	[1085519751] _n	172335	[1276315424] _n
42	[1335983514] _n	344671	[1511938429] _n
84	[1212154100] _n	689342	[1116941725] _n
168	[638363154] _n	1378684	[748516067] _n
336	[1695419879] _n	2757369	[590443992] _n
673	[250463254] _n	5514739	[1169450853] _n
1346	[1092090842] _n	11029479	[83459512] _n
2692	[149835148] _n	22058958	[643822280] _n
5385	[1009240318] _n	44117916	[1032113647] _n
10770	[1219871219] _n	88235833	[357249732] _n

Figure 7.9. Décryptage du message.

Exercices

1. Supposons que Bob choisisse $p = 5$, $q = 11$ et $e = 7$.
 - (a) Trouvez n , $\varphi(n)$ et d .
 - (b) Supposons qu'Alice veuille envoyer le message $m = 9$. Trouvez le message chiffré c et vérifiez que Bob peut le déchiffrer.
- *2. Supposons que Bob choisisse $p = 71$, $q = 83$ et $e = 1369$.
 - (a) Trouvez n , $\varphi(n)$ et d .
 - (b) Supposons qu'Alice veuille envoyer le message $m = 1001$. Trouvez le message chiffré c et vérifiez que Bob peut le déchiffrer.
3. Supposons que Bob choisisse $p = 71$ et $q = 83$. Pourquoi $e = 1368$ serait-il un mauvais choix ?
4. Supposons que Bob choisisse $p = 17389$, $q = 14947$ et $e = 35824631$.

- (a) Trouvez n , $\varphi(n)$ et d .
- (b) Supposons qu'Alice veuille envoyer le message $m = 123456789$. Trouvez le message chiffré c et vérifiez que Bob peut le déchiffrer.
- *5. Vous écoutez Alice et Bob. Vous interceptez le message $(n, e) = (493, 129)$ envoyé à Alice par Bob, puis le message $c = 149$ envoyé à Bob par Alice.
- (a) Facteur n .
- (b) Trouvez l'exposant de décryptage d .
- (c) Décryptez le message.
6. Supposons qu'Alice et Bob utilisent RSA. Comme d'habitude, Bob a généré les nombres n , e et d , et a envoyé n et e à Alice, mais a gardé d secret. Alice a un message m qui représente un contrat qu'elle veut faire signer à Bob. Le contrat n'est pas secret ; elle est heureuse de l'envoyer à Bob sans le chiffrer. Mais elle veut que Bob lui renvoie une *signature numérique*. Comme une signature ordinaire, ce message doit être infalsifiable, afin qu'Alice sache que c'est Bob, et non un imposteur, qui a écrit la signature, et que Bob ne puisse nier ultérieurement avoir signé le contrat. Pour créer sa signature, Bob calcule l'entier unique s tel que $0 \leq s < n$ et $[m]_n^d = [s]_n$. Il envoie s à Alice.
- (a) Montrer que $[s]_n^e = [m]_n$, et si s' est un entier tel que $0 \leq s' < n$ et $s' \neq s$, alors $[s']_n^e \neq [m]_n$. Ainsi, Alice peut authentifier la signature en calculant $[s]_n^e$ et en vérifiant qu'elle est égale à $[m]_n$.
- (b) Pourquoi un imposteur ne peut-il pas falsifier la signature de Bob ?
- *7. Dans cet exercice, nous verrons pourquoi il est important que p et q soient premiers. Supposons que Bob choisisse $p = 9$, $q = 35$ et $e = 95$, sans remarquer que 9 et 35 ne sont pas premiers. Il calcule $n = pq = 315$ et envoie $(n, e) = (315, 95)$ à Alice.
- (a) Supposons qu'Alice veuille envoyer le message $m = 123$. Quel message crypté c va-t-elle envoyer ?
- (b) Bob calcule $\varphi = (p - 1)(q - 1) = 272$; il pense que c'est $\varphi(n)$, mais il a tort. Pour trouver l'exposant de déchiffrement d , il calcule ensuite $[e]_{\varphi}^{-1} = [d]_{\varphi}$. Quelle valeur de d obtient-il ?
- (c) En utilisant l'exposant de déchiffrement d de la partie (b), qu'obtient Bob lorsqu'il essaie de déchiffrer le message d'Alice ?
- (d) Quelle est la valeur correcte de $\varphi(n)$? Quel exposant de déchiffrement d Bob aurait-il obtenu s'il avait utilisé la valeur correcte pour $\varphi(n)$ et calculé $[e]_{\varphi(n)}^{-1} = [d]_{\varphi(n)}$? En utilisant cet exposant de déchiffrement, qu'aurait obtenu Bob lorsqu'il a essayé de déchiffrer le message d'Alice ?
8. Supposons que m soit un entier positif et que $X \in \mathbb{Z} / \equiv_m$.
- (a) Donnez une définition récursive de X^a , pour les entiers positifs a .

- (b) Utilisez l'induction mathématique pour prouver que pour tous les entiers positifs a et b , $X^a \cdot X^b = X^{a+b}$.
- (c) Utilisez l'induction mathématique pour prouver que pour tous les entiers positifs a et b , $(X^a)^b = X^{ab}$.
- *9. Supposons que $X \in \mathbb{Z} / \equiv_n$. Démontrer que pour tout entier positif a , la méthode récursive de calcul de X^a illustrée dans [l'exemple 7.5.2](#) utilise au plus $2\log_2 a$ une multiplication.

[Les exercices 10 à 14](#) portent sur les tests probabilistes de primalité. Dans ces problèmes, nous cherchons un test de calcul réalisable sur un entier positif n , de sorte que si n est premier, alors n réussisse le test, et si n n'est pas premier, alors il échoue. Nous constaterons que certains tests fonctionnent dans de nombreux cas, mais pas dans tous.

10. D'après le théorème d'Euler, si n est premier et $2 \leq a \leq n - 1$, alors $a^{n-1} \equiv 1 \pmod{n}$. Ceci suggère le test de primalité suivant : pour tester si un entier $n > 2$ est premier, choisissez un nombre aléatoire $a \in \{2, 3, \dots, n - 1\}$ et vérifiez si $a^{n-1} \equiv 1 \pmod{n}$. Si oui, alors n réussit le test, et sinon, il échoue. Ce test est appelé *test de primalité de Fermat*, car l'instance du théorème d'Euler sur laquelle il est basé est étroitement liée au petit théorème de Fermat ; voir [l'exercice 10 de la section 7.4](#). Si n est premier, alors, d'après le théorème d'Euler, il est garanti de réussir le test. Malheureusement, les nombres composés réussissent parfois aussi le test. Si $2 \leq a \leq n - 1$ et $a^{n-1} \equiv 1 \pmod{n}$, mais que n n'est pas premier, alors on dit que n est un *pseudo-premier de Fermat de base a* ; il passe le test de primalité de Fermat en base a , même s'il n'est pas premier. Si $2 \leq a \leq n - 1$ et $a^{n-1} \not\equiv 1 \pmod{n}$ alors on dit que a est un *témoin de Fermat* pour n . S'il existe un témoin de Fermat pour n alors, d'après le théorème d'Euler, n n'est pas premier.

- (a) Montrez que 15 est un pseudo-premier de Fermat en base 4, mais que 3 est un témoin de Fermat pour 15.
 (b) Montrez que si n est un pseudo-premier de Fermat de base a , alors n et a sont premiers entre eux.

11. Rappelez-vous de [l'exercice 5 de la section 6.2](#) que les nombres $F_n = 2^{(2^n)} + 1$ sont appelés nombres de Fermat. Fermat a montré que F_n est premier pour $0 \leq n \leq 4$, et Euler a montré que F_5 n'est pas premier. On ignore s'il existe un nombre $n > 4$ pour lequel F_n est premier. Dans cet exercice, vous montrerez que pour tout nombre naturel n , $2^{F_n-1} \equiv 1 \pmod{F_n}$. Ainsi, si F_n n'est pas premier, alors, dans la terminologie de [l'exercice 10](#), il s'agit d'un nombre pseudo-premier de Fermat en

base 2. Autrement dit, le test de primalité de Fermat avec $a = 2$ ne sera pas utile pour tester si F_n est premier.

- (a) Montrer que $2^{(2^n)} \equiv -1 \pmod{F_n}$.
- (b) Montrer que $2^{(2^{n+1})} \equiv 1 \pmod{F_n}$.
- (c) Montrez que $2^{n+1} \mid (F_n - 1)$. (Indice : utilisez [l'exercice 12\(a\)](#) de la [section 6.3](#).)
- (d) Montrez que $2^{F_n-1} \equiv 1 \pmod{F_n}$. (Indice : utilisez les parties (b) et (c) et [l'exercice 16 de la section 7.3](#).)

12. Supposons que n soit un entier supérieur à 2 et soit $R = \{2, 3, \dots, n-1\}$. Soit

$$R_1 = \{a \in R \mid a^{n-1} \equiv 1 \pmod{n}\},$$

$$R_2 = R \setminus R_1 = \{a \in R \mid a^{n-1} \not\equiv 1 \pmod{n}\}.$$

Supposons que $a \in R_2$ et que $\text{pgcd}(n, a) = 1$. Alors a est un témoin de Fermat pour n , donc n n'est pas premier. (Voir [l'exercice 10](#) pour la signification des termes utilisés dans cet exercice.)

- (a) Montrer que pour chaque $x \in R_1$ il existe un unique $y \in R_2$ tel que $ax \equiv y \pmod{n}$.
- (b) Par la partie (a), nous pouvons définir une fonction $f: R_1 \rightarrow R_2$ par la formule

$$f(x) = \text{the unique } y \in R_2 \text{ such that } ax \equiv y \pmod{n}.$$

Montrer que f est bijectif.

- (c) Utiliser la partie (b) pour conclure qu'au moins la moitié des éléments de R sont des témoins de Fermat pour n . (Cela montre que, avec une probabilité d'au moins $1/2$, n échouera au test de primalité de Fermat. En répétant le test avec des choix différents pour a , la probabilité d'un résultat incorrect peut être réduite au minimum.)

13. L'exercice 12 montre que s'il existe au moins un témoin de Fermat pour n qui est premier entre eux avec n , alors le test de primalité de Fermat a de bonnes chances de détecter que n n'est pas premier. Malheureusement, il existe des nombres composés n pour lesquels aucun témoin de ce type n'existe. Un entier $n > 2$ est appelé *nombre de Carmichael* s'il n'est pas premier, mais il est un pseudo-premier de Fermat de base a pour tout entier $a \in \{2, 3, \dots, n-1\}$ tel que a et n soient premiers entre eux. Ils portent le nom de Robert Daniel Carmichael (1879-1967), qui les a étudiés le premier. Si n est un nombre de Carmichael, alors, bien que n ne soit pas premier, le test de primalité de Fermat a peu de chances de le détecter. En 1994, WR Alford (1937-2003), Andrew Granville (1962-) et Carl

Pomerance (1944–) ont prouvé qu'il existe une infinité de nombres de Carmichael. Dans ce problème, vous montrerez que 561 est un nombre de Carmichael. (En fait, c'est le plus petit nombre de Carmichael.) Nous vous laissons le soin de vérifier que $561 = 3 \cdot 11 \cdot 17$, donc 561 n'est pas premier. Supposons que $2 \leq a \leq n - 1$ et que $\text{pgcd}(561, a) = 1$.

- (a) Montrer que $a^{560} \equiv 1 \pmod{3}$.
- (b) Montrer que $a^{560} \equiv 1 \pmod{11}$.
- (c) Montrer que $a^{560} \equiv 1 \pmod{17}$.
- (d) Montrez que $a^{560} \equiv 1 \pmod{561}$. (Indice : utilisez [l'exercice 14 de la section 7.4.](#))

14. Dans cet exercice, vous étudierez les bases mathématiques du test de Miller-Rabin, un test probabiliste de primalité couramment utilisé. Il doit son nom à Gary L. Miller (1946–) et Michael O. Rabin (1931–). Supposons que n soit un entier impair et que $n > 1$.

- (a) Démontrer qu'il existe des entiers positifs s et d tels que $n - 1 = 2^s d$ et d est impair.
- (b) Démontrer que si n est premier et b est un entier positif tel que $b^2 \equiv 1 \pmod{n}$, alors soit $b \equiv 1 \pmod{n}$, soit $b \equiv -1 \pmod{n}$. Soient s et d comme dans la partie (a). Si $2 \leq a \leq n - 1$, $a^d \not\equiv 1 \pmod{n}$, et pour tout entier naturel $i < s$, $a^{2^i d} \not\equiv -1 \pmod{n}$. alors a est appelé un *témoin de Miller-Rabin* pour n .
- (c) Démontrer que s'il existe un témoin de Miller-Rabin pour n , alors n n'est pas premier. (Indice : Supposons que a soit un témoin de Miller-Rabin pour n et que n soit premier. Alors, d'après le théorème d'Euler, $a^{2^s d} = a^{n-1} \equiv 1 \pmod{n}$. on peut donc définir k comme le plus petit nombre naturel tel que... $a^{2^k d} \equiv 1 \pmod{n}$. Utilisons maintenant la partie (b) pour obtenir une contradiction.)

Le test de Miller-Rabin fonctionne comme suit : pour tester si un entier impair $n > 1$ est premier, choisissez un nombre aléatoire $a \in \{2, 3, \dots, n - 1\}$ et vérifiez si a est un témoin de Miller-Rabin pour n . Si c'est le cas, alors n échoue au test. Si ce n'est pas le cas, alors n le réussit. D'après la partie (c), si n est premier, il n'y a pas de témoin de Miller-Rabin, donc n est assuré de réussir le test. On peut prouver que si n n'est pas premier, alors au moins $3/4$ des nombres $a \in \{2, 3, \dots, n - 1\}$ sont des témoins de Miller-Rabin pour n , donc n échouera au test avec une probabilité d'au moins $3/4$. Comme dans [l'exercice 12](#), la probabilité d'un résultat incorrect peut être rendue aussi faible que souhaité en répétant le test avec différents choix de a .

- (d) Montrez que 13 n'est pas un témoin Miller-Rabin pour 85, mais que 14 l'est.

8

Ensembles infinis

8.1. Ensembles équinombreux

Dans ce chapitre, nous aborderons une méthode permettant de comparer les tailles d'ensembles infinis. Étonnamment, nous découvrirons que, d'une certaine manière, l'infini existe en différentes tailles !

Pour les ensembles finis, on détermine la taille d'un ensemble en comptant. Que signifie compter le nombre d'éléments d'un ensemble ? Lorsqu'on compte les éléments d'un ensemble A , on désigne tour à tour les éléments de A en prononçant *un*, *deux*, etc. On pourrait comparer ce processus à la définition d'une fonction f de l'ensemble $\{1, 2, \dots, n\}$ vers A , pour un entier naturel n . Pour tout $i \in \{1, 2, \dots, n\}$, on pose $f(i)$ comme l'élément de A désigné par « i ». Puisque chaque élément de A est désigné une seule fois, la fonction f est bijective et continue. Ainsi, compter les éléments de A revient simplement à établir une correspondance bijective entre l'ensemble $\{1, 2, \dots, n\}$ et A , pour un entier naturel n . La correspondance biunivoque est l'idée clé de la mesure de la taille des ensembles, et les ensembles de la forme $\{1, 2, \dots, n\}$ constituent les normes par rapport auxquelles nous mesurons la taille des ensembles finis. Ceci suggère la définition suivante.

Définition 8.1.1. Supposons que A et B soient des ensembles. On dira que A est *équinumère* à B s'il existe une fonction $f : A \rightarrow B$ bijective et sur. On notera $A \sim B$ pour indiquer que A est équinumère à B . Pour tout entier naturel n , soit $I_n = \{i \in \mathbb{Z}^+ \mid i \leq n\}$. Un ensemble A est dit *fini* s'il existe un entier naturel n tel que $I_n \sim A$. Sinon, A est *infini*.

[l'exercice 6](#), on vous demande de montrer que si A est fini, alors il existe *exactement un* n tel que $I_n \sim A$. Ainsi, il est logique de définir le *nombre d'éléments* d'un ensemble fini A comme étant l'*unique* n tel que $I_n \sim A$. Ce nombre est aussi parfois appelé *cardinal* de A , et il est noté $|A|$. Notons que selon cette définition, \emptyset est fini et $|\emptyset| = 0$.

La définition d'équinombre peut également s'appliquer aux ensembles infinis, avec des résultats parfois surprenants. Par exemple, on pourrait penser que \mathbb{Z}^+ ne pourrait pas être équinumère avec \mathbb{Z} car \mathbb{Z} inclut non seulement tous les entiers positifs, mais aussi tous les entiers négatifs et zéro. Mais considérons la fonction $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}$ définie comme suit :

$$f(n) = \begin{cases} n/2, & \text{if } n \text{ is even,} \\ (1-n)/2, & \text{if } n \text{ is odd.} \end{cases}$$

Cette notation signifie que pour tout entier positif n , si n est pair alors $f(n) = n/2$ et si n est impair alors $f(n) = (1-n)/2$. Le tableau des valeurs de f dans [la figure 8.1](#) révèle un modèle qui suggère que f pourrait être bijectif et sur.

n	1	2	3	4	5	6	7	\dots
$f(n)$	0	1	-1	2	-2	3	-3	\dots

Figure 8.1.

Pour vérifier cela plus attentivement, notons d'abord que pour tout entier positif n , si n est pair alors $f(n) = n/2 > 0$, et si n est impair alors $f(n) = (1-n)/2 \leq 0$. Supposons maintenant que n_1 et n_2 sont des entiers positifs et $f(n_1) = f(n_2)$. Si $f(n_1) = f(n_2) > 0$ alors n_1 et n_2 doivent tous deux être pairs, donc l'équation $f(n_1) = f(n_2)$ signifie $n_1/2 = n_2/2$, et donc $n_1 = n_2$. De même, si $f(n_1) = f(n_2) \leq 0$ alors n_1 et n_2 sont tous deux impairs, donc nous obtenons $(1-n_1)/2 = (1-n_2)/2$, et une fois de plus il s'ensuit que $n_1 = n_2$. Ainsi, f est bijectif.

Pour voir que f est sur, soit m un entier arbitraire. Si $m > 0$ alors soit $n = 2m$, un entier pair positif, et si $m \leq 0$ alors soit $n = 1 - 2m$, un entier impair positif. Dans les deux cas, il est facile de vérifier que $f(n) = m$. Ainsi, f est sur et bijective, donc selon [la définition 8.1.1](#), $\mathbb{Z}^+ \sim \mathbb{Z}$.

Notons que la fonction f a dû être choisie avec le plus grand soin. Il existe de nombreuses autres fonctions de \mathbb{Z}^+ à \mathbb{Z} qui sont bijectives mais non sur, sur mais non bijectives, ou ni bijectives ni sur, mais cela ne contredit pas notre affirmation selon laquelle $\mathbb{Z}^+ \sim \mathbb{Z}$. Selon [la définition 8.1.1](#), pour démontrer que $\mathbb{Z}^+ \sim \mathbb{Z}$ il suffit de démontrer qu'il existe au moins une fonction de \mathbb{Z}^+ à \mathbb{Z} qui est à la fois bijective et sur, et bien sûr, pour le démontrer, il suffit de donner un exemple d'une telle fonction.

Un exemple encore plus surprenant est peut-être celui de $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$. Pour le démontrer, nous devons trouver une fonction bijective $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$. Un élément du domaine de cette fonction serait un couple

ordonné (i, j), où i et j sont des entiers positifs. [L'exercice 12](#) vous demande de démontrer que la formule suivante définit une fonction de $\mathbb{Z}^+ \times \mathbb{Z}^+$ vers \mathbb{Z}^+ qui est bijective et sur :

$$f(i, j) = \frac{(i + j - 2)(i + j - 1)}{2} + i.$$

Une fois encore, le tableau de valeurs de [la figure 8.2](#) peut vous aider à comprendre cet exemple.

$f(i, j)$	1	2	3	4	5
1	1	2	4	7	11
2	3	5	8	12	
i	6	9	13		
3	10	14			
4					
5	15				

Figure 8.2.

Théorème 8.1.2. *Supposons que $A \sim B$ et $C \sim D$. Alors :*

1. $A \times C \sim B \times D$.
2. Si A et C sont disjoints et B et D sont disjoints, alors $A \cup C \sim B \cup D$.

Preuve. Puisque $A \sim B$ et $C \sim D$, nous pouvons choisir des fonctions $f : A \rightarrow B$ et $g : C \rightarrow D$ qui sont bijectives et sur.

1. Définissez $h : A \times C \rightarrow B \times D$ par la formule

$$h(a, c) = (f(a), g(c)).$$

Pour voir que h est bijectif, supposons que $h(a_1, c_1) = h(a_2, c_2)$. Cela signifie que $(f(a_1), g(c_1)) = (f(a_2), g(c_2))$, donc $f(a_1) = f(a_2)$ et $g(c_1) = g(c_2)$. Puisque f et g sont tous deux bijectifs, il s'ensuit que $a_1 = a_2$ et $c_1 = c_2$, donc $(a_1, c_1) = (a_2, c_2)$.

Pour voir que h est sur, supposons $(b, d) \in B \times D$. Alors, puisque f et g sont tous deux sur, nous pouvons choisir $a \in A$ et $c \in C$ tels que $f(a) = b$ et $g(c) = d$. Par conséquent, $h(a, c) = (f(a), g(c)) = (b, d)$, comme requis. Ainsi, h est bijectif et sur, donc $A \times C \sim B \times D$.

2. Supposons que A et C soient disjoints, et que B et D soient également disjoints. [L'exercice 14](#) vous demande de démontrer que $f \cup g$ est une fonction bijective et ononique de $A \cup C$ vers $B \cup D$, donc $A \cup C \sim B \cup D$. \square

Il n'est pas difficile de démontrer que \sim est réflexif, symétrique et transitif. Autrement dit, nous avons le théorème suivant :

Théorème 8.1.3. *Pour tous les ensembles A , B et C :*

1. $Un \sim A$.
2. Si $A \sim B$ alors $B \sim A$.
3. Si $A \sim B$ et $B \sim C$ alors $A \sim C$.

Preuve.

1. La fonction identité i_A est une fonction bijective de A vers A .
2. Supposons que $A \sim B$. On peut alors choisir une fonction $f : A \rightarrow B$ bijective et sur. D'après [le théorème 5.3.4](#), f^{-1} est une fonction de B vers A . Mais notons maintenant que $(f^{-1})^{-1} = f$, qui est une fonction de A vers B , donc, d'après [le théorème 5.3.4](#), f^{-1} est également bijective et sur. Par conséquent, $B \sim A$.
3. Supposons que $A \sim B$ et $B \sim C$. On peut alors choisir les fonctions bijectives $f : A \rightarrow B$ et $g : B \rightarrow C$. D'après [le théorème 5.2.5](#), $g \circ f : A \rightarrow C$ est bijective et sur, donc $A \sim C$. \square

[Les théorèmes 8.1.2](#) et [8.1.3](#) sont souvent utiles pour montrer que les ensembles sont équinombreux. Par exemple, nous avons montré précédemment que $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$ et $\mathbb{Z}^+ \sim \mathbb{Z}$, donc d'après la partie 3 du [théorème 8.1.3](#) il résulte que $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}$. La partie 2 nous indique qu'il n'est pas nécessaire de distinguer les affirmations « A est équinombre à B » et « B est équinombre à A », car elles sont équivalentes. Par exemple, nous savons déjà que $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$, donc nous pouvons aussi écrire $\mathbb{Z}^+ \sim \mathbb{Z}^+ \times \mathbb{Z}^+$. D'après la partie 1 du [théorème 8.1.2](#), $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}$, donc nous avons aussi $\mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}$.

Nous avons maintenant trouvé trois ensembles, \mathbb{Z} , $\mathbb{Z}^+ \times \mathbb{Z}^+$ et $\mathbb{Z} \times \mathbb{Z}$, équinombreux avec \mathbb{Z}^+ . Ces ensembles sont particulièrement importants et portent un nom spécifique.

Définition 8.1.4. Un ensemble A est dit *dénombrable* si $\mathbb{Z}^+ \sim A$. Il est dit *dénombrable* s'il est fini ou dénombrable. Sinon, il est *indénombrable*.

On pourrait considérer les ensembles dénombrables comme des ensembles dont les éléments peuvent être *comptés* en les désignant tous, un par un, tout en nommant les entiers positifs dans l'ordre. Si le dénombrement s'arrête à un moment donné, l'ensemble est fini ; et s'il ne s'arrête jamais, l'ensemble est dénombrable. Le théorème suivant propose deux autres façons de concevoir les ensembles dénombrables.

Théorème 8.1.5. Supposons que A soit un ensemble. Les affirmations suivantes sont équivalentes :

1. A est dénombrable.

2. Soit $A = \emptyset$, soit il existe une fonction $f: \mathbb{Z}^+ \rightarrow A$ qui est sur.

3. Il existe une fonction $f: A \rightarrow \mathbb{Z}^+$ c'est un à un.

Preuve. 1 → 2. Supposons que A soit dénombrable. Si A est dénombrable, alors il existe une fonction $f: \mathbb{Z}^+ \rightarrow A$ bijective et surunitaire ; l'énoncé 2 est donc vrai. Supposons maintenant que A soit fini. Si $A = \emptyset$, il n'y a plus rien à prouver ; supposons donc $A \neq \emptyset$. On peut alors choisir un élément $a_0 \in A$. Soit $g: I_n \rightarrow A$ une fonction surunitaire, où n est le nombre d'éléments de A . Définissons maintenant $f: \mathbb{Z}^+ \rightarrow A$ comme suit :

$$f(i) = \begin{cases} g(i), & \text{if } i \leq n, \\ a_0, & \text{if } i > n. \end{cases}$$

Il est facile de vérifier maintenant que f est activé, comme requis.

2 → 3. Supposons que $A = \emptyset$ ou qu'il existe une fonction onto de \mathbb{Z}^+ vers A . Examinons ces deux possibilités successivement. Si $A = \emptyset$, alors l'ensemble vide est une fonction bijective de A vers \mathbb{Z}^+ . Supposons maintenant que $g: \mathbb{Z}^+ \rightarrow A$ et que g soit sur. Alors, pour tout $a \in A$, l'ensemble $\{n \in \mathbb{Z}^+ \mid g(n) = a\}$ n'est pas vide ; par conséquent, selon le principe de bon ordre, il doit avoir un plus petit élément. Ainsi, on peut définir une fonction $f: A \rightarrow \mathbb{Z}^+$ par la formule

$$f(a) = \text{the smallest } n \in \mathbb{Z}^+ \text{ such that } g(n) = a.$$

Notez que pour chaque $a \in A$, $g(f(a)) = a$, donc $g \circ f = i_A$. Mais alors, d'après [le théorème 5.3.3](#), il s'ensuit que f est bijectif, comme requis.

3 → 1. Supposons que $g: A \rightarrow \mathbb{Z}^+$ et que g soit bijectif. Soit $B = \text{Ran}(g) \subseteq \mathbb{Z}^+$. Alors g est une fonction sur B . Cela signifie que si l'on considère g comme une fonction de A vers B , alors elle est bijective et sur, donc $A \sim B$. Il suffit donc de montrer que B est dénombrable, car d'après [le théorème 8.1.3](#) il en résulte que A est également dénombrable.

Supposons que B ne soit pas fini. Il faut montrer que B est dénombrable, ce que l'on peut faire en définissant une fonction bijective et sur $f: \mathbb{Z}^+ \rightarrow B$. L'idée derrière cette définition est simplement de poser $f(n)$ comme le n -ième élément de B , pour tout $n \in \mathbb{Z}^+$. (Rappelons que $B \subseteq \mathbb{Z}^+$, ce qui permet d'utiliser l'ordre des entiers positifs pour comprendre la notion de n -ième élément de B .) Pour une définition plus précise de f et la preuve que f est bijective et sur-f, voir [l'exercice 15](#).

Si A est dénombrable et $A \neq \emptyset$, alors d'après [le théorème 8.1.5](#) il existe une fonction $f: \mathbb{Z}^+ \rightarrow A$ qui est sur. Si, pour tout $n \in \mathbb{Z}^+$, on pose $a_n = f(n)$, alors le fait que f soit sur signifie que chaque élément de A apparaît au moins une fois dans la liste a_1, a_2, a_3, \dots . En d'autres termes, $A = \{a_1, a_2, a_3, \dots\}$. La dénombrabilité d'un ensemble A est souvent utilisée de cette façon pour nous permettre d'écrire les éléments de A dans une liste, indexée par les entiers positifs. En fait, vous pourriez vouloir penser à la dénombrabilité pour les ensembles non vides comme signifiant *la listabilité*. Bien sûr, si A est dénombrable, alors la fonction f peut être considérée comme bijective, ce qui signifie que chaque élément de A n'apparaîtra qu'une seule fois dans la liste a_1, a_2, a_3, \dots . Pour un exemple d'application de dénombrement dans lequel les éléments d'un ensemble dénombrable sont écrits dans une liste, voir [exercice 19](#).

[Le théorème 8.1.5](#) est également parfois utile pour prouver qu'un ensemble est dénombrable, comme le montre la preuve de notre prochain théorème.

Théorème 8.1.6. \mathbb{Q} est dénombrable.

Preuve. Soit $f: \mathbb{Z} \times \mathbb{Z}^+ \rightarrow \mathbb{Q}$ défini comme suit :

$$f(p, q) = p/q.$$

Il est clair que f est sur, puisque par définition tous les nombres rationnels peuvent s'écrire sous forme de fractions, mais il faut noter que f n'est pas bijectif. Par exemple, $f(1, 2) = f(2, 4) = 1/2$. Puisque $\mathbb{Z}^+ \sim \mathbb{Z}$, d'après [le théorème 8.1.2](#), nous avons $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}^+$, et comme nous savons déjà que $\mathbb{Z}^+ \times \mathbb{Z}^+$ est dénombrable, il s'ensuit que $\mathbb{Z} \times \mathbb{Z}^+$ est également dénombrable. Ainsi, nous pouvons choisir une fonction sur, bijective, $g: \mathbb{Z}^+ \rightarrow \mathbb{Z} \times \mathbb{Z}^+$. D'après [le théorème 5.2.5](#), $f \circ g: \mathbb{Z}^+ \rightarrow \mathbb{Q}$ est sur, donc d'après [le théorème 8.1.5](#), \mathbb{Q} est dénombrable. Il est clair que \mathbb{Q} n'est pas finie, elle doit donc être dénombrable. \square

Bien que ce chapitre porte sur les ensembles infinis, les méthodes présentées ici permettent de démontrer des théorèmes utiles au calcul des cardinalités des ensembles finis. Nous terminons cette section par un exemple d'un tel théorème, et en donnons plusieurs autres dans les exercices (voir [exercices 20 à 30](#)).

Théorème 8.1.7. *Supposons que A et B soient des ensembles finis disjoints. Alors $A \cup B$ est fini, et $|A \cup B| = |A| + |B|$.*

Preuve. Soit $n = |A|$ et $m = |B|$. Alors $A \sim I_n$ et $B \sim I_m$. Remarquons que si $x \in I_m$ alors $1 \leq x \leq m$, et donc $n + 1 \leq x + n \leq n + m$, donc $x + n \in I_{n+m} \setminus I_n$. On peut donc définir une fonction $f: I_m \rightarrow I_{n+m} \setminus I_n$ par la formule $f(x) = x + n$. Il est facile de vérifier que f est bijective et sur, donc $I_m \sim I_{n+m} \setminus I_n$. Puisque $B \sim I_m$, il s'ensuit que $B \sim I_{n+m} \setminus I_n$. En appliquant la deuxième partie du [théorème 8.1.2](#), nous pouvons conclure que $A \cup B \sim I_n \cup (I_{n+m} \setminus I_n) = I_{n+m}$. Par conséquent, $A \cup B$ est fini, et $|A \cup B| = n + m = |A| + |B|$. \square

Exercices

*1. Montrer que les ensembles suivants sont dénombrables.

(\approx).

(b) L'ensemble de tous les entiers pairs.

2. Montrer que les ensembles suivants sont dénombrables :

(a) $\mathbb{Q} \times \mathbb{Q}$.

(b) $\mathbb{Q}(\sqrt{2})$. (Voir [l'exercice 21\(b\)](#) de la section 5.4 pour la signification de la notation utilisée ici.)

3. Dans ce problème, nous utiliserons la notation suivante pour les intervalles de nombres réels. Si a et b sont des nombres réels et $a < b$, alors

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\},$$

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\},$$

$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\},$$

$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}.$$

(a) Montrez que $[0, 1] \sim [0, 2]$.

(b) Montrez que $(-\pi/2, \pi/2) \sim \mathbb{R}$. (Indice : utilisez une fonction trigonométrique.)

(c) Montrer que $(0, 1) \sim \mathbb{R}$.

(d) Montrez que $(0, 1] \sim (0, 1)$.

*4. Justifiez votre réponse à chaque question avec une preuve ou un contre-exemple.

(a) Supposons que $A \sim B$ et $A \times C \sim B \times D$. Doit-il être le cas que $C \sim D$?

(b) Supposons que $A \sim B$, A et C sont disjoints, B et D sont disjoints, et $A \cup C \sim B \cup D$. Doit-il être le cas que $C \sim D$?

5. Démontrer que si $A \sim B$ alors $\mathcal{P}(A) \sim \mathcal{P}(B)$.

*6. (a) Démontrer que pour tous les nombres naturels n et m , si $I_n \sim I_m$ alors $n = m$. (Indice : utiliser l'induction sur n .)

(b) Démontrer que si A est fini, alors il existe exactement un nombre naturel n tel que $I_n \sim A$.

7. Supposons que A et B soient des ensembles et que A soit fini. Démontrer que $A \sim B$ ssi B est également fini et $|A| = |B|$.

*8. (a) Démontrer que si $n \in \mathbb{N}$ et $A \subseteq I_n$, alors A est fini et $|A| \leq n$. De plus, si $A \neq I_n$, alors $|A| < n$.

(b) Démontrer que si A est fini et $B \subseteq A$, alors B est également fini, et $|B| \leq |A|$. De plus, si $B \neq A$, alors $|B| < |A|$.

9. Supposons que $B \subseteq A$, $B \neq A$ et $B \sim A$. Démontrer que A est infini.

10. Démontrer que si $n \in \mathbb{N}$, $f: I_n \rightarrow B$, et f est sur, alors B est fini et $|B| \leq n$.

11. Supposons que A et B soient des ensembles finis et $f: A \rightarrow B$.

(a) Démontrer que si $|A| < |B|$ alors f n'est pas sur.

(b) Démontrer que si $|A| > |B|$ alors f n'est pas bijectif. (Ceci est parfois appelé le *principe du casier*, car cela signifie que si n éléments sont mis dans m casiers, où $n > m$, alors un casier doit contenir plus d'un élément.)

(c) Démontrer que si $|A| = |B|$ alors f est bijectif ssi f est sur.

12. Montrer que la fonction $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ définie par la formule

$$f(i, j) = \frac{(i + j - 2)(i + j - 1)}{2} + i$$

est un à un et sur.

13. Dans cet exercice, vous donnerez une autre preuve que $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$. Soit $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ défini par la formule

$$f(m, n) = 2^{m-1}(2n - 1).$$

Démontrer que f est bijectif et sur.

14. Complétez la preuve de la partie 2 du [théorème 8.1.2](#) en montrant que si $f: A \rightarrow B$ et $g: C \rightarrow D$ sont des fonctions ondulatoires bijectives, A et C sont disjointes et B et D sont disjoint, alors $f \cup g$ est une fonction ondulatoire bijective de $A \cup C$ vers $B \cup D$.

15. Dans cet exercice, vous compléterez la démonstration de 3 → 1 du [théorème 8.1.5](#). Supposons que $B \subseteq \mathbb{Z}^+$ et que B soit infini. Nous définissons maintenant une fonction $f: \mathbb{Z}^+ \rightarrow B$ par récursivité comme suit :

Pour tout $n \in \mathbb{Z}^+$,

$$f(n) = \text{le plus petit élément de } B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\}.$$

Bien sûr, la définition est récursive car la spécification de $f(n)$ fait référence à $f(m)$ pour tout $m < n$.

- (a) Supposons que $n \in \mathbb{Z}^+$. La définition de $f(n)$ n'a de sens que si l'on est sûr que $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\} \neq \emptyset$, auquel cas le principe de bon ordre garantit qu'il possède un plus petit élément. Démontrer que $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\} \neq \emptyset$. (Indice : voir [exercices 8 et 10.](#))

(b) Démontrer que pour tout $n \in \mathbb{Z}^+, f(n) \geq n$.

(c) Démontrer que f est bijectif et sur.

16. Dans cet exercice, vous donnerez une preuve alternative du [théorème 8.1.6](#).

(a) Trouvez une fonction $f: \mathbb{Z}^+ \rightarrow \mathbb{Z} \setminus \{0\}$ qui est bijective et sur.

(b) Soit $g: \mathbb{Z}^+ \rightarrow \mathbb{Q}^+$ défini comme suit. Supposons que $n \in \mathbb{Z}^+$ et que la factorisation première de n soit $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, telle que p_1, p_2, \dots, p_k soient des nombres premiers, $p_1 < p_2 < \cdots < p_k$, et e_1, e_2, \dots, e_k soient des entiers positifs. Alors, on pose

$$g(n) = g(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = p_1^{f(e_1)} p_2^{f(e_2)} \cdots p_k^{f(e_k)},$$

Où f est la fonction de la partie (a). (Comme dans [la section 7.2](#), nous considérons que le produit vide est égal à 1, de sorte que $g(1) = 1$.) Démontrer que g est bijectif et sur. (Indice : [L'exercice 19 de la section 7.2 vous sera utile.](#))

(c) Utilisez g pour définir une fonction biunivoque $h: \mathbb{Z} \rightarrow \mathbb{Q}$ et concluez que \mathbb{Q} est dénombrable.

17. Démontrer que si $B \subseteq A$ et A est dénombrable, alors B est dénombrable.

18. Démontrer que si $B \subseteq A$, A est infini et B est fini, alors $A \setminus B$ est infini.

19. Supposons que A soit dénombrable et que R soit un ordre partiel sur A . Démontrer que R peut être étendu à un ordre total sur A . Autrement dit, démontrer qu'il existe un ordre total T sur A tel que $R \subseteq T$. Notons que nous avons démontré un théorème similaire pour A fini dans [l'exemple 6.2.2](#). (Indice : Puisque A est dénombrable, nous pouvons écrire les éléments de A dans une liste : $A = \{a_1, a_2, a_3, \dots\}$. Maintenant, en utilisant [l'exercice 2 de la section 6.2](#), définissez récursivement les ordres partiels R_n , pour $n \in \mathbb{N}$, de sorte que $R = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots$ et $\forall i \in I_n \forall j \in \mathbb{Z}^+ ((a_i, a_j) \in R_n \vee (a_j, a_i) \in R_n)$. Soit $T = \bigcup_{n \in \mathbb{N}} R_n$.

20. Supposons que A soit fini et que $B \subseteq A$. D'après [l'exercice 8](#), B et $A \setminus B$ sont tous deux finis. Démontrer que $|A \setminus B| = |A| - |B|$. (En particulier, si $a \in A$ alors $|A \setminus \{a\}| = |A| - 1$. Nous avons utilisé ce fait dans plusieurs démonstrations du [chapitre 6](#) ; par exemple, nous l'avons utilisé dans [les exemples 6.2.1 et 6.2.2](#).)
21. Supposons que n soit un entier positif et que pour tout $i \in I_n$, A_i soit un ensemble fini. Supposons également que $\forall i \in I_n \forall j \in I_n (i \neq j \rightarrow A_i \cap A_j = \emptyset)$. Démontrer que $\bigcup_{i \in I_n} A_i$ est fini et $|\bigcup_{i \in I_n} A_i| = \sum_{i=1}^n |A_i|$.
- *22. (a) Démontrer que si A et B sont des ensembles finis, alors $A \times B$ est fini et $|A \times B| = |A| \cdot |B|$. (Indice : utiliser l'induction sur $|B|$. Autrement dit, démontrer l'énoncé suivant par induction : $\forall n \in \mathbb{N} \forall A \forall B$ (si A et B sont finis et $|B| = n$, alors $A \times B$ est fini et $|A \times B| = |A| \cdot n$). [Le théorème 4.1.3](#) peut vous être utile.)
(b) Un repas au restaurant Alice's comprend un plat principal et un dessert. Le plat principal peut être un steak, du poulet, des côtelettes de porc, des crevettes ou des spaghettis, et le dessert peut être une glace, un gâteau ou une tarte. Combien de plats différents peut-on commander au restaurant Alice's ?
23. Pour tout ensemble A et B , l'ensemble de toutes les fonctions de A à B est noté ${}^A B$.
- (a) Démontrer que si $A \sim B$ et $C \sim D$ alors ${}^A C \sim {}^B D$.
 - (b) Démontrer que si A , B et C sont des ensembles et $A \cap B = \emptyset$, alors ${}^A \cup {}^B C \sim {}^A C \times {}^B C$.
 - (c) Démontrer que si A et B sont des ensembles finis, alors ${}^A B$ est fini et $|{}^A B| = |B|^{|A|}$. (Indice : utiliser l'induction sur $|A|$.)
 - (d) Un professeur a 20 étudiants dans sa classe et doit attribuer une note de A, B, C, D ou F à chacun d'eux. De combien de façons peuvent-on attribuer ces notes ?
24. Supposons que $|A| = n$, et soit $F = \{f \mid f \text{ est une fonction bijective de } I_n \text{ à } A\}$.
- (a) Démontrer que F est fini et $|F| = n!$. (Indice : utiliser l'induction sur n .)
 - (b) Soit $L = \{R \mid R \text{ est un ordre total sur } A\}$. Démontrer que $F \sim L$, et donc $|L| = n!$.
 - (c) Cinq personnes doivent s'asseoir sur une rangée de cinq sièges. De combien de façons peuvent-elles être assises ?
25. Supposons que A soit un ensemble fini et que R soit une relation d'équivalence sur A . Supposons également qu'il existe un entier strictement positif n tel que $\forall x \in A (|[x]_R| = n)$. Démontrer que A / R est fini et $|A / R| = |A| / n$. (Indice : Utiliser [l'exercice 21](#).)

26. (a) Supposons que A et B soient des ensembles finis. Démontrer que $A \cup B$ est fini, et $|A \cup B| = |A| + |B| - |A \cap B|$.
 (b) Supposons que A , B et C soient des ensembles finis. Démontrer que $A \cup B \cup C$ est fini, et

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

27. Dans ce problème, vous démontrerez le *principe d'inclusion-exclusion*, qui généralise les formules de [l'exercice 26](#). Supposons que A_1, A_2, \dots, A_n soient des ensembles finis. Soit $P = \mathcal{P}(I_n) \setminus \{\emptyset\}$, et pour tout $S \in P$ démontrons $A_S = \bigcap_{i \in S} A_i$. que $\bigcup_{i \in I_n} A_i$ est fini et

$$\left| \bigcup_{i \in I_n} A_i \right| = \sum_{S \in P} (-1)^{|S|+1} |A_S|.$$

(La notation du côté droit de cette équation désigne le résultat de l'exécution de tous les ensembles $S \in P$, du calcul du nombre $(-1)^{|S|+1} |A_S|$ pour chaque S , puis de l'addition de ces nombres. Astuce : utilisez l'induction sur n .)

28. Démontrer que si A et B sont des ensembles finis et $|A| = |B|$, alors $|A \Delta B|$ est pair.
 29. Chaque client d'une banque possède un code PIN, une séquence de quatre chiffres. Montrez que si la banque compte plus de 10 000 clients, deux clients doivent avoir le même code PIN. (Indice : voir [exercice 11](#).)
 30. Alice ouvrit son bulletin et s'exclama : « Je n'arrive pas à croire que le professeur Jones m'ait recalée en probabilités. » « Tu étais dans ce cours ? » demanda Bob. « C'est drôle, j'y étais aussi, et je ne me souviens pas t'y avoir jamais vu. » « Eh bien », admit Alice d'un air penaude, « je crois que j'ai séché beaucoup de cours. » « Oui, moi aussi », dit Bob. Prouve qu'Alice ou Bob a manqué au moins la moitié des cours.

8.2. Ensembles dénombrables et indénombrables

Souvent, lorsque nous effectuons une opération de théorie des ensembles avec des ensembles dénombrables, le résultat est à nouveau un ensemble dénombrable.

Théorème 8.2.1. *Supposons que A et B soient des ensembles dénombrables. Alors :*

1. *$A \times B$ est dénombrable.*
2. *$A \cup B$ est dénombrable.*

Preuve. Puisque A et B sont dénombrables, d'après [le théorème 8.1.5](#), nous pouvons choisir les fonctions bijectives $f : A \rightarrow \mathbb{Z}^+$ et $g : B \rightarrow \mathbb{Z}^+$.

1. Définir $h : A \times B \rightarrow \mathbb{Z}^+ \times \mathbb{Z}^+$ par la formule

$$h(a, b) = (f(a), g(b)).$$

Comme dans la preuve de la partie 1 du [théorème 8.1.2](#), il n'est pas difficile de montrer que h est injectif. Puisque $\mathbb{Z}^+ \times \mathbb{Z}^+$ est dénombrable, on peut poser $j : \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ une fonction onde injectif. Alors, d'après [le théorème 5.2.5](#), $j \circ h : A \times B \rightarrow \mathbb{Z}^+$ est injectif, donc d'après [le théorème 8.1.5](#), $A \times B$ est dénombrable.

2. Définissez $h : A \cup B \rightarrow \mathbb{Z}$ comme suit :

$$h(x) = \begin{cases} f(x), & \text{if } x \in A, \\ -g(x), & \text{if } x \notin A. \end{cases}$$

Français Nous affirmons maintenant que h est inexact. Pour comprendre pourquoi, supposons que $h(x_1) = h(x_2)$, pour certains x_1 et x_2 dans $A \cup B$. Si $h(x_1) = h(x_2) > 0$, alors selon la définition de h , nous devons avoir $x_1 \in A$, $x_2 \in A$, et $f(x_1) = h(x_1) = h(x_2) = f(x_2)$. Mais alors puisque f est inexact, $x_1 = x_2$. De même, si $h(x_1) = h(x_2) \leq 0$, alors nous devons avoir $g(x_1) = -h(x_1) = -h(x_2) = g(x_2)$, et alors puisque g est inexact, $x_1 = x_2$. Ainsi, h est bijectif.

Puisque \mathbb{Z} est dénombrable, on peut poser $j : \mathbb{Z} \rightarrow \mathbb{Z}^+$ comme une fonction on-line bijective. Comme dans la partie 1, on constate alors que $j \circ h : A \cup B \rightarrow \mathbb{Z}^+$ est bijective, donc $A \cup B$ est dénombrable.

Comme le montre notre prochain théorème, la partie 2 du [théorème 8.2.1](#) peut être étendue aux unions de plus de deux ensembles.

Théorème 8.2.2. *L'union d'un nombre dénombrable d'ensembles dénombrables est dénombrable. Autrement dit, si \mathcal{F} est une famille d'ensembles, \mathcal{F} est dénombrable, et aussi chaque élément de \mathcal{F} est dénombrable, alors $\cup \mathcal{F}$ est dénombrable.*

Preuve. On supposera d'abord que $\emptyset \notin \mathcal{F}$. À la fin de la preuve, on discutera du cas $\emptyset \in \mathcal{F}$.

Si $\mathcal{F} = \emptyset$, alors, bien sûr, $\cup \mathcal{F} = \emptyset$, lequel est dénombrable ? Supposons maintenant que $\mathcal{F} \neq \emptyset$. Alors, comme décrit après la démonstration du [théorème 8.1.5](#), puisque \mathcal{F} est dénombrable et non vide, nous pouvons écrire les éléments de \mathcal{F} dans une liste, indexée par les entiers positifs. Autrement dit, nous pouvons dire que $\mathcal{F} = \{A_1, A_2, A_3, \dots\}$. De même, tout élément de \mathcal{F} est dénombrable et non vide (puisque $\emptyset \notin \mathcal{F}$), donc pour tout entier positif i , les éléments de A_i peuvent être écrits dans une liste. Ainsi, nous pouvons écrire

$$\begin{aligned} A_1 &= \{a_1^1, a_2^1, a_3^1, \dots\}, \\ A_2 &= \{a_1^2, a_2^2, a_3^2, \dots\}, \end{aligned}$$

et, en général,

$$A_i = \{a_1^i, a_2^i, a_3^i, \dots\}.$$

Notez que, selon la définition de l'union, $\cup \mathcal{F} = \{a_j^i \mid i \in \mathbb{Z}^+, j \in \mathbb{Z}^+\}$.

Définissez maintenant une fonction $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \cup \mathcal{F}$ par la formule

$$f(i, j) = a_j^i.$$

Il est clair que f est sur. Puisque $\mathbb{Z}^+ \times \mathbb{Z}^+$ est dénombrable, on peut poser $g : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \times \mathbb{Z}^+$ comme une fonction sur. Alors $f \circ g : \mathbb{Z}^+ \rightarrow \cup \mathcal{F}$, étant sur, elle $\cup \mathcal{F}$ est dénombrable.

Supposons enfin que $\emptyset \in \mathcal{F}$. Soit $\mathcal{F}' = \mathcal{F} \setminus \{\emptyset\}$. Alors \mathcal{F}' est aussi une famille dénombrable d'ensembles dénombrables et $\emptyset \notin \mathcal{F}'$, selon le raisonnement précédent, $\cup \mathcal{F}'$ est dénombrable. Mais il est clair $\cup \mathcal{F} = \cup \mathcal{F}'$, qu'il $\cup \mathcal{F}$ l'est aussi. \square

Une autre opération qui préserve la dénombrabilité est la formation de suites finies. Supposons que A soit un ensemble et que a_1, a_2, \dots, a_n soit une liste d'éléments de A . On pourrait spécifier les termes de cette liste par une fonction $f: I_n \rightarrow A$, où pour chaque i , $f(i) = a_i$ = le i -ième terme de la liste. Une telle fonction est appelée *suite finie* d'éléments de A .

Définition 8.2.3. Supposons que A soit un ensemble. Une fonction $f: I_n \rightarrow A$, où n est un entier naturel, est appelée *suite finie* d'éléments de A , et n est appelée la *longueur* de la suite.

Théorème 8.2.4. Supposons que A soit un ensemble dénombrable. Alors l'ensemble de toutes les suites finies d'éléments de A est également dénombrable.

Preuve. Pour tout $n \in \mathbb{N}$, soit S_n l'ensemble des suites de longueur n d'éléments de A . On montre d'abord que pour tout $n \in \mathbb{N}$, S_n est dénombrable. On procède par récurrence sur n .

Dans le cas de base, nous supposons $n = 0$. Notez que $I_0 = \emptyset$, donc une séquence de longueur 0 est une fonction $f: \emptyset \rightarrow A$, et la seule fonction de ce type est \emptyset . Ainsi, $S_0 = \{\emptyset\}$, qui est clairement un ensemble dénombrable.

Pour l'étape d'induction, supposons que n soit un entier naturel et que S_n soit dénombrable. Il faut montrer que S_{n+1} est dénombrable. Considérons la fonction $F: S_n \times A \rightarrow S_{n+1}$ définie comme suit :

$$F(f, a) = f \cup \{(n+1, a)\}.$$

En d'autres termes, pour toute suite $f \in S_n$ et tout élément $a \in A$, $F(f, a)$ est la suite que vous obtenez en commençant par f , qui est une suite de longueur n , puis en ajoutant a comme terme numéro $n+1$. On vous demande dans [l'exercice 2](#) de vérifier que F est bijectif et continu. Ainsi, $S_n \times A \sim S_{n+1}$. Mais S_n et A sont tous deux dénombrables, donc par [le théorème 8.2.1](#), $S_n \times A$ est dénombrable, et donc S_{n+1} est dénombrable.

Ceci complète la preuve inductive que pour tout $n \in \mathbb{N}$, S_n est dénombrable. Enfin, notons que l'ensemble de toutes les suites finies d'éléments de A est $\bigcup_{n \in \mathbb{N}} S_n$, dénombrable d'après [le théorème 8.2.2](#). □

À titre d'exemple d'utilisation du [théorème 8.2.4](#), vous devriez être capable de montrer que l'ensemble de toutes les phrases

grammaticales de l'anglais est un ensemble dénombrable. (Voir [exercice 17.](#))

Vous vous demandez peut-être maintenant si *tous* les ensembles sont dénombrables ! Existe-t-il une opération ensembliste permettant de produire des ensembles indénombrables ? Nous verrons dans notre prochain théorème que la réponse est oui : l'opération des ensembles de puissances. Ce fait a été découvert par le mathématicien allemand Georg Cantor (1845–1918) grâce à une démonstration célèbre et ingénieuse. En fait, c'est Cantor qui a eu l'idée de comparer les tailles d'ensembles infinis. La démonstration de Cantor est un peu plus difficile que les précédentes de ce chapitre ; nous aborderons donc la stratégie de la démonstration avant de la présenter elle-même.

Théorème 8.2.5. (Théorème de Cantor) $\mathcal{P}(\mathbb{Z}^+)$ est indénombrable.

Travail à partir de zéro

La preuve repose sur l'énoncé 2 du [théorème 8.1.5](#). Nous allons montrer qu'il n'existe pas de fonction $f: \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$ qui soit sur. Il est clair que $\mathcal{P}(\mathbb{Z}^+) \neq \emptyset$, donc, d'après [le théorème 8.1.5](#), cela montre que $\mathcal{P}(\mathbb{Z}^+)$ n'est pas dénombrable.

Notre stratégie consiste à poser $f: \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$ une fonction arbitraire et à prouver que f n'est pas sur. En reformulant cet objectif négatif par une affirmation positive, nous devons montrer que $\exists D [D \in \mathcal{P}(\mathbb{Z}^+) \wedge \forall n \in \mathbb{Z}^+ (D \neq f(n))]$. Ceci suggère que nous devrions essayer de trouver un ensemble D particulier pour lequel nous pouvons prouver $D \in \mathcal{P}(\mathbb{Z}^+)$ et $\forall n \in \mathbb{Z}^+ (D \neq f(n))$. C'est l'étape la plus difficile pour établir la preuve. Il existe un ensemble D qui permet de la démontrer, mais il faudra une certaine ingéniosité pour le trouver.

Nous voulons nous assurer que $D \in \mathcal{P}(\mathbb{Z}^+)$, ou en d'autres termes $D \subseteq \mathbb{Z}^+$, nous savons donc que nous n'avons besoin de considérer que les entiers positifs pour décider quels devraient être les éléments de D . Mais cela nous laisse encore une infinité de décisions à prendre : pour chaque entier positif n , nous devons décider si nous voulons ou non que n soit un élément de D . Nous devons également nous assurer que $\forall n \in \mathbb{Z}^+ (D \neq f(n))$. Cela impose une infinité de restrictions sur notre choix de D : pour chaque entier positif n , nous devons nous assurer que $D \neq f(n)$. Pourquoi ne pas prendre chacune de nos infinies décisions de telle manière qu'elle garantisse que la restriction correspondante est satisfaite ? En d'autres termes, pour chaque entier positif n , nous prendrons notre décision sur le fait que n est ou non un élément de D de telle manière qu'elle garantisse que $D \neq f(n)$. Ce n'est pas difficile à

faire. On peut poser n comme élément de D si $n \in f(n)$, et exclure n de D si $n \notin f(n)$. Ceci garantit que $D \neq f(n)$, car l'un de ces ensembles contiendra n comme élément et l'autre non. Ceci suggère que l'on devrait poser $D = \{n \in \mathbb{Z}^+ \mid n \in f(n)\}$.

Français La figure 8.3 peut vous aider à comprendre la définition de l'ensemble D . Pour chaque $m \in \mathbb{Z}^+$, $f(m)$ est un sous-ensemble de \mathbb{Z}^+ , et il peut être spécifié en disant, pour chaque entier positif n , si $n \in f(m)$ ou non. Les réponses à ces questions peuvent être disposées dans un tableau comme le montre la figure 8.3. Chaque ligne du tableau donne les réponses nécessaires pour spécifier l'ensemble $f(m)$ pour une valeur particulière de m . L'ensemble D peut également être spécifié avec une ligne de oui et de non, comme le montre le bas de la figure 8.3. Pour chaque $n \in \mathbb{Z}^+$ nous avons décidé de déterminer si $n \in D$ ou non en demandant si $n \in f(n)$ ou non, et les réponses à ces questions sont celles entourées de cases dans la figure 8.3. Puisque $n \in D$ ssi $n \in f(n)$, la ligne de oui et de non spécifiant D peut être trouvée en lisant les réponses encadrées le long de la diagonale de la figure 8.3 et en inversant toutes les réponses. Il est garanti que cela sera différent de chaque ligne du tableau de la figure 8.3, car pour chaque $n \in \mathbb{Z}^+$ elle diffère de la ligne n en n -ième position.

Si vous avez trouvé ce raisonnement difficile à suivre, ne vous inquiétez pas. N'oubliez pas que le raisonnement utilisé pour choisir l'ensemble D ne fera de toute façon pas partie de la preuve ! Après avoir lu la preuve, vous pourrez revenir en arrière et relire les deux derniers paragraphes.

Is $n \in f(m)$?	n				
	1	2	3	4	5
1	yes	no	no	yes	yes
2	yes	yes	no	no	yes
m	no	no	no	yes	no
3	no	no	no	yes	no
4	yes	yes	no	yes	no
5	no	yes	yes	no	no
			⋮		
Is $n \in D$?	no	no	yes	no	yes
					...

Figure 8.3.

Il est clair que l'ensemble D que nous avons choisi est un sous-ensemble de \mathbb{Z}^+ , donc $D \in \mathcal{P}(\mathbb{Z}^+)$. Notre autre objectif est de prouver que $\forall n \in \mathbb{Z}^+ (D \neq f(n))$, donc soit n un entier positif arbitraire et prouvons que $D \neq f(n)$. Rappelons maintenant que nous avons soigneusement choisi D afin de pouvoir prouver que $D \neq f(n)$, et que le raisonnement derrière ce choix reposait sur la question de savoir si $n \in f(n)$. Peut-être la façon la plus simple d'écrire la preuve est de considérer séparément les deux cas $n \in f(n)$ et $n \notin f(n)$. Dans

chaque cas, l'application de la définition de D conduit facilement à la conclusion que $D \neq f(n)$.

Preuve. Supposons que $f : \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$. On montrera que f ne peut être sur en trouvant un ensemble $D \in \mathcal{P}(\mathbb{Z}^+)$ tel que $D \notin \text{Ran}(f)$. Soit $D = \{n \in \mathbb{Z}^+ \mid n \notin f(n)\}$. Clairement, $D \subseteq \mathbb{Z}^+$, donc $D \in \mathcal{P}(\mathbb{Z}^+)$. Soit maintenant n un entier positif arbitraire. On considère deux cas.

Cas 1. $n \in f(n)$. Puisque $D = \{n \in \mathbb{Z}^+ \mid n \notin f(n)\}$, on peut conclure que $n \notin D$. Mais alors puisque $n \in f(n)$ et $n \notin D$, il s'ensuit que $D \neq f(n)$.

Cas 2. $n \notin f(n)$. Alors par définition de D , $n \in D$. Puisque $n \in D$ et $n \notin f(n)$, $D \neq f(n)$.

Puisque ces cas sont exhaustifs, cela montre que $\forall n \in \mathbb{Z}^+ (D \neq f(n))$, donc $D \notin \text{Ran}(f)$. Puisque f est arbitraire, cela montre qu'il n'existe pas de fonction onto $-f : \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$. Clairement, $\mathcal{P}(\mathbb{Z}^+) \neq \emptyset$, donc, d'après [le théorème 8.1.5](#), $\mathcal{P}(\mathbb{Z}^+)$ est indénombrable. \square

La méthode utilisée pour la démonstration du [théorème 8.2.5](#) est appelée *diagonalisation* en raison de la disposition diagonale des réponses encadrées de [la figure 8.3](#). La diagonalisation est une technique puissante qui permet de démontrer de nombreux théorèmes, y compris notre théorème suivant. Cependant, plutôt que de recourir à un autre argument de diagonalisation, nous appliquerons simplement [le théorème 8.2.5](#) pour démontrer le théorème suivant.

Théorème 8.2.6. \mathbb{R} est indénombrable.

Preuve. Nous allons définir une fonction $f : \mathcal{P}(\mathbb{Z}^+) \rightarrow \mathbb{R}$ et montrer que f est bijective. Si \mathbb{R} était dénombrable, alors il existerait une fonction bijective $g : \mathbb{R} \rightarrow \mathbb{Z}^+$. Mais alors $g \circ f$ serait une fonction bijective de $\mathcal{P}(\mathbb{Z}^+)$ à \mathbb{Z}^+ et donc $\mathcal{P}(\mathbb{Z}^+)$ seraient dénombrables, ce qui contredit le théorème de Cantor. Ainsi, cela démontrera que \mathbb{R} est indénombrable.

Pour définir f , supposons $A \in \mathcal{P}(\mathbb{Z}^+)$. Alors $f(A)$ sera un nombre réel compris entre 0 et 1, que nous préciserons en donnant son développement décimal. Pour chaque entier positif n , le n -ième chiffre de $f(A)$ sera le nombre d_n *défini* comme suit :

$$d_n = \begin{cases} 3, & \text{if } n \notin A, \\ 7, & \text{if } n \in A. \end{cases}$$

En d'autres termes, en notation décimale, nous avons $f(A) = 0.d_1d_2d_3\dots$. Par exemple, si E est l'ensemble de tous les entiers pairs positifs, alors $f(E) = 0,37373737\dots$. Si P est l'ensemble de tous les nombres premiers, alors $f(P) = 0,37737373337\dots$.

Pour voir que f est bijectif, supposons que $A \in \mathcal{P}(\mathbb{Z}^+)$, $B \in \mathcal{P}(\mathbb{Z}^+)$ et $A \neq B$. Alors il existe un $n \in \mathbb{Z}^+$ tel que soit $n \in A$ et $n \notin B$, soit $n \in B$ et $n \notin A$. Mais alors $f(A)$ et $f(B)$ ne peuvent pas être égaux, car leurs développements décimaux diffèrent au n -ième chiffre. [1](#) Ainsi, f est bijectif. \square

Exercices

- *1. (a) Démontrer que l'ensemble de tous les nombres irrationnels, $\mathbb{R} \setminus \mathbb{Q}$, est indénombrable.
- (b) Démontrer que $\mathbb{R} \setminus \mathbb{Q} \sim \mathbb{R}$.
- 2. Soit $F : S_n \times A \rightarrow S_{n+1}$ la fonction définie dans la démonstration du [théorème 8.2.4](#). Montrer que F est bijective et sur.
- 3. Dans cet exercice, vous donnerez une autre preuve du [théorème 8.2.4](#). Supposons que A soit un ensemble dénombrable, et soit S l'ensemble de toutes les suites finies d'éléments de A . Puisque A est dénombrable, il existe une fonction bijective $g : A \rightarrow \mathbb{Z}^+$. Pour tout entier positif n , soit p_n le n -ième nombre premier ; ainsi, $p_1 = 2$, $p_2 = 3$, et ainsi de suite. Définissons $F : S \rightarrow \mathbb{Z}^+$ comme suit : Supposons que $f \in S$ et que f fait une longueur n . Alors

$$F(f) = p_1^{g(f(1))} p_2^{g(f(2))} \cdots p_n^{g(f(n))}.$$

Montrer que F est bijectif et donc que S est dénombrable.

- 4. Soit $P = \{X \in \mathcal{P}(\mathbb{Z}^+) \mid X \text{ est fini}\}$. Démontrer que P est dénombrable.
- *5. Démontrer la forme plus générale suivante du théorème de Cantor : Pour tout ensemble A , $A \not\sim \mathcal{P}(A)$. (Indice : imiter la preuve du [théorème 8.2.5](#).)
- 6. Pour la signification de la notation utilisée dans cet exercice, voir [l'exercice 23 de la section 8.1](#).
- (a) Démontrer que pour tous les ensembles A , B et C , ${}^A(B \times C) \sim {}^A B \times {}^A C$.
- (b) Démontrer que pour tous les ensembles A , B et C , ${}^{(A \times B)}C \sim {}^A({}^B C)$.

(c) Démontrer que pour tout ensemble A , $\mathcal{P}(A) \sim {}^A\{\text{oui, non}\}$.
 (Remarque : si A est fini et $|A| = n$ alors, d'après [l'exercice 23\(c\)](#) de la section 8.1, il s'ensuit que $|\mathcal{P}(A)| = |\{\text{oui, non}\}|^{|A|} = 2^n$. Bien sûr, vous avez déjà prouvé cela, par une méthode différente, dans [l'exercice 11 de la section 6.2.](#))

(d) Prouver que $\mathbb{Z}^+ \mathcal{P}(\mathbb{Z}^+) \sim \mathcal{P}(\mathbb{Z}^+)$.

7. Supposons que A soit dénombrable. Démontrer qu'il existe une partition P de A telle que P soit dénombrable et que pour tout $X \in P$, X soit dénombrable.
- *8. Démontrer que si A et B sont des ensembles disjoints, alors $\mathcal{P}(A \cup B) \sim \mathcal{P}(A) \times \mathcal{P}(B)$.
9. (a) Supposons que $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ et $\bigcup_{n \in \mathbb{Z}^+} A_n = \mathbb{R}$. Démontrer que pour tout ensemble indénombrable $B \subseteq \mathbb{R}$ il existe un entier positif n tel que $B \cap A_n$ soit indénombrable.
 (b) Supposons que $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ et $\bigcup_{n \in \mathbb{Z}^+} A_n = \mathbb{Z}^+$. Supposons également que pour tout ensemble infini $B \subseteq \mathbb{Z}^+$ il existe un entier positif n tel que $B \cap A_n$ soit infini. Démontrer que pour un certain n , $A = \mathbb{Z}^+$.
10. Supposons que $A \subseteq \mathbb{R}^+$, $b \in \mathbb{R}^+$, et que pour toute liste a_1, a_2, \dots, a_k d'un nombre fini d'éléments distincts de A , $a_1 + a_2 + \dots + a_k \leq b$. Démontrer que A est dénombrable. (Indice : Pour tout entier positif n , soit $A_n = \{x \in A \mid x \geq 1/n\}$. Que peut-on dire du nombre d'éléments dans A_n ?)
11. Supposons que E soit une relation d'équivalence sur \mathbb{R} et que pour tous les nombres réels x et y , $[x]_E \sim [y]_E$. Démontrer que soit \mathbb{R}/E est indénombrable, soit pour tout $x \in \mathbb{R}$, $[x]_E$ est indénombrable.
12. Un nombre réel x est dit *algébrique* s'il existe un entier positif n et des entiers a_0, a_1, \dots, a_n tels que $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = 0$ et $a_n \neq 0$. Soit A l'ensemble de tous les nombres algébriques.
 - (a) Démontrer que $\mathbb{Q} \subseteq A$.
 - (b) Prouver que $\sqrt{2} \in A$.
 - (c) Démontrer que A est dénombrable. Remarque : Vous pouvez utiliser le fait que si n est un entier positif, a_0, a_1, \dots, a_n sont des entiers et $a_n \neq 0$, alors $\{x \in \mathbb{R} \mid a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = 0\}$ est fini.
13. Supposons que $\mathcal{F} \subseteq \{f \mid f : \mathbb{Z}^+ \rightarrow \mathbb{R}\}$ et que \mathcal{F} soit dénombrable. Démontrer qu'il existe une fonction $g : \mathbb{Z}^+ \rightarrow \mathbb{R}$ telle que $\mathcal{F} \subseteq O(g)$. (Voir [l'exercice 19](#) de la section 5.1 pour la signification de la notation utilisée ici.)

14. Supposons que $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$ et que \mathcal{F} soit deux à deux disjoint.

Démontrer que \mathcal{F} est dénombrable.

*15. Si A et B sont des ensembles infinis, on dit que A et B sont *presque disjoints* si $A \cap B$ est fini. Si \mathcal{F} est une famille d'ensembles infinis, alors on dit que \mathcal{F} est *presque disjoint deux à deux* si, pour tout A et B dans \mathcal{F} , si $A \neq B$ alors A et B sont presque disjoints. Dans cet exercice, vous démontrerez qu'il existe un ensemble $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$ tel que tous les éléments de \mathcal{F} soient infinis, \mathcal{F} soit presque disjoint deux à deux et \mathcal{F} soit indénombrable. (Comparer cet exercice avec l'exercice précédent.)

Soit $P = \{X \in \mathcal{P}(\mathbb{Z}^+) \mid X \text{ est fini}\}$ et $Q = \{X \in \mathcal{P}(\mathbb{Z}^+) \mid X \text{ est infini}\}$. D'après [l'exercice 4](#), P est dénombrable, on peut donc choisir une fonction g bijective et sur-unitaire : $P \rightarrow \mathbb{Z}^+$.

- (a) Démontrer que Q est indénombrable. Pour tout $A \in Q$, soit $S_A = \{A \cap I_n \mid n \in \mathbb{Z}^+\}$. Par exemple, si A est l'ensemble de tous les nombres premiers, alors $S_A = \{\emptyset, \{2\}, \{2, 3\}, \{2, 3, 5\}, \dots\}$. (On pourrait décrire S_A comme l'ensemble de tous les segments initiaux de A .)
- (b) Démontrer que si $A \in Q$ alors $S_A \subseteq P$ et S_A est infini.
- (c) Démontrer que si $A, B \in Q$ et $A \neq B$ alors $S_A \cap S_B$ est fini.
- (d) Soit $\mathcal{F} = \{g(S_A) \mid A \in Q\}$. Démontrer que $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$, tout élément de \mathcal{F} est infini, \mathcal{F} est presque disjoint deux à deux et \mathcal{F} est indénombrable.
16. Démontrer qu'il existe une fonction $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ telle que pour tous les entiers positifs a, b et c il existe un entier positif n tel que $f(an + b) = c$.
17. Démontrer que l'ensemble des phrases grammaticales anglaises est dénombrable. (Indice : chaque phrase grammaticale anglaise est une suite finie de mots anglais. Démontrer d'abord que l'ensemble des phrases grammaticales est dénombrable, puis qu'il est infini.)
18. Certains nombres réels peuvent être définis par une expression anglaise. Par exemple, l'expression « le rapport de la circonférence d'un cercle à son diamètre » définit le nombre π .
- (a) Démontrer que l'ensemble des nombres définis par une expression anglaise est dénombrable. (Indice : voir [exercice 17](#).)
- (b) Démontrer qu'il existe des nombres réels qui ne peuvent pas être définis par des phrases anglaises.

8.3. Le théorème de Cantor-Schröder-Bernstein

Supposons que A et B soient des ensembles et que f soit une fonction bijective de A vers B . Alors f montre que $A \sim \text{Ran}(f) \subseteq B$; il est donc naturel de considérer B comme étant *au moins aussi grand que* A . Ceci suggère la notation suivante :

Définition 8.3.1. Si A et B sont des ensembles, alors on dira que B domine A et on notera $A \lesssim B$ s'il existe une fonction $f: A \rightarrow B$ bijective. Si $A \lesssim B$ et $A \not\sim B$, alors on dira que B domine strictement A et on notera $A < B$.

Par exemple, dans la preuve du [théorème 8.2.6](#), nous avons donné une fonction bijective $f: \mathcal{P}(\mathbb{Z}^+) \rightarrow \mathbb{R}$, donc $\mathcal{P}(\mathbb{Z}^+) \lesssim \mathbb{R}$. Bien sûr, pour tout ensemble A et B , si $A \sim B$ alors aussi $A \lesssim B$. Il devrait également être clair que si $A \subseteq B$ alors $A \lesssim B$. Par exemple, $\mathbb{Z}^+ \lesssim \mathbb{R}$. En fait, d'après [le théorème 8.2.6](#), nous savons aussi que $\mathbb{Z}^+ \not\sim \mathbb{R}$, donc nous pouvons dire que $\mathbb{Z}^+ < \mathbb{R}$.

On pourrait penser que \lesssim serait un ordre partiel, mais il s'avère que ce n'est pas le cas. Dans [l'exercice 1, on vous demande](#) de vérifier que \lesssim est réflexif et transitif, mais qu'il n'est pas antisymétrique. (Dans la terminologie de [l'exercice 25 de la section 4.5](#), \lesssim est un préordre.) Par exemple, $\mathbb{Z}^+ \sim \mathbb{Q}$, donc $\mathbb{Z}^+ \lesssim \mathbb{Q}$ et $\mathbb{Q} \lesssim \mathbb{Z}^+$, mais bien sûr $\mathbb{Z}^+ \neq \mathbb{Q}$. Mais cela soulève une question intéressante : si $A \lesssim B$ et $B \lesssim A$, alors A et B pourraient ne pas être égaux, mais doivent-ils être équinombres ?

Il s'avère que la réponse est oui, comme nous le démontrerons dans notre prochain théorème. Plusieurs noms de mathématiciens sont généralement associés à ce théorème. Cantor fut le premier à l'énoncer et en donna une preuve partielle. Plus tard, Ernst Schröder (1841-1902) et Felix Bernstein (1878-1956) découvrirent des preuves indépendamment.

Théorème 8.3.2. (Théorème de Cantor-Schröder-Bernstein) *Supposons que A et B soient des ensembles. Si $A \lesssim B$ et $B \lesssim A$, alors $A \sim B$.*

Travail à partir de zéro

Nous commençons par supposer que $A \lesssim B$ et $B \lesssim A$, ce qui signifie que nous pouvons choisir les fonctions bijectives $f: A \rightarrow B$ et $g: B \rightarrow A$. Pour prouver que $A \sim B$ nous devons trouver une fonction bijective $h: A \rightarrow B$.

À ce stade, nous ne savons pas grand-chose sur A et B . Les seuls outils dont nous disposons pour associer les éléments de A et B sont les fonctions f et g . Si f est sur, alors nous pouvons bien sûr poser $h = f$; et

si g est sur, alors nous pouvons poser $h = g^{-1}$. Mais il se peut que ni f ni g ne soient sur. Comment pouvons-nous obtenir la fonction h requise dans ce cas ?

Notre solution sera de combiner des parties de f et g^{-1} pour obtenir h . Pour ce faire, nous allons diviser A en deux parties X et Y , et B en deux parties W et Z , de telle manière que X et W puissent être appariés par f , et Y et Z puissent être appariés par g . Plus précisément, nous aurons $W = f(X) = \{f(x) \mid x \in X\}$ et $Y = g(Z) = \{g(z) \mid z \in Z\}$. La situation est illustrée dans [la Figure 8.4](#). Une fois cela fait, nous pourrons définir h en posant $h(a) = f(a)$ pour $a \in X$, et $h(a) = g^{-1}(a)$ pour $a \in Y$.

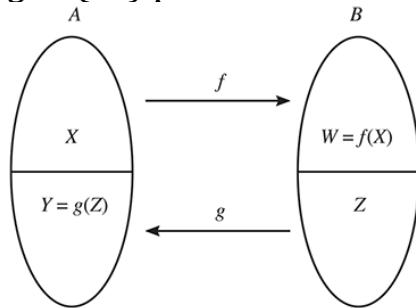


Figure 8.4.

Comment pouvons-nous choisir les ensembles X , Y , W et Z ? Tout d'abord, notons que chaque élément de Y doit être dans $\text{Ran}(g)$, donc tout élément de A qui n'est pas dans $\text{Ran}(g)$ doit être dans X . En d'autres termes, si nous posons $A_1 = A \setminus \text{Ran}(g)$, alors nous devons avoir $A_1 \subseteq X$. Mais considérons maintenant tout $a \in A_1$. Nous savons que nous devons avoir $a \in X$, et donc $f(a) \in W$. Mais notons maintenant que puisque g est inexact, $g(f(a))$ sera différent de $g(z)$ pour tout $z \in Z$, et donc $g(f(a)) \notin g(Z) = Y$. Ainsi, nous devons avoir $g(f(a)) \in X$. Puisque a est un élément arbitraire de A_1 , cela montre que si nous posons $A_2 = g(f(A_1)) = \{g(f(a)) \mid a \in A_1\}$, alors nous devons avoir $A_2 \subseteq X$. De même, si nous posons $A_3 = g(f(A_2))$, alors il s'avère que nous devons avoir $A_3 \subseteq X$. En continuant de cette manière, nous pouvons définir des ensembles A_n pour tout entier positif n , et pour tout n nous devons avoir $A_n \subseteq X$. Comme vous le verrez, laisser $X = \bigcup_{n \in \mathbb{Z}^+} A_n$ fonctionne. Dans la preuve suivante, nous ne mentionnons pas les ensembles W et Z .

Preuve. Supposons que $A \precsim B$ et $B \precsim A$. Alors nous pouvons choisir les fonctions bijectives $f: A \rightarrow B$ et $g: B \rightarrow A$. Soit $R = \text{Ran}(g) \subseteq A$. Alors g est appliqué à R , donc d'après [le théorème 5.3.4](#), $g^{-1}: R \rightarrow B$.

Nous définissons maintenant une suite d'ensembles A_1, A_2, A_3, \dots par récursivité comme suit :

$$A_1 = A \setminus R; \\ \text{for every } n \in \mathbb{Z}^+, A_{n+1} = g(f(A_n)) = \{g(f(a)) \mid a \in A_n\}.$$

Soit $X = \bigcup_{n \in \mathbb{Z}^+} A_n$. Bien sûr, chaque élément de A est dans X ou Y , mais pas les deux. Définissons maintenant $h : A \rightarrow B$ comme suit :

$$h(a) = \begin{cases} f(a), & \text{if } a \in X, \\ g^{-1}(a), & \text{if } a \in Y. \end{cases}$$

Notez que pour tout $a \in A$, si $a \notin R$ alors $a \in A_1 \subseteq X$. Ainsi, si $a \in Y$ alors $a \in R$, donc $g^{-1}(a)$ est défini. Par conséquent, cette définition est logique.

Nous allons montrer que h est bijectif et sur, ce qui établira que $A \sim B$. Pour voir que h est bijectif, supposons $a_1 \in A$, $a_2 \in A$ et $h(a_1) = h(a_2)$.

Cas 1. $a_1 \in X$. Supposons que $a_2 \in Y$. Alors, selon la définition de h , $h(a_1) = f(a_1)$ et $h(a_2) = g^{-1}(a_2)$. Ainsi, l'équation $h(a_1) = h(a_2)$ signifie que $f(a_1) = g^{-1}(a_2)$, donc $g(f(a_1)) = g(g^{-1}(a_2)) = a_2$. Puisque $a_1 \in X = \bigcup_{n \in \mathbb{Z}^+} A_n$, on peut choisir un $n \in \mathbb{Z}^+$ tel que $a_1 \in A_n$. Mais alors $a_2 = g(f(a_1)) \in g(f(A_n)) = A_{n+1}$, donc $a_2 \in X$, ce qui contredit notre hypothèse que $a_2 \in Y$.

Ainsi, $a_2 \notin Y$, donc $a_2 \in X$. Cela signifie que $h(a_2) = f(a_2)$, donc à partir de l'équation $h(a_1) = h(a_2)$ nous obtenons $f(a_1) = f(a_2)$. Mais f est bijectif, il s'ensuit donc que $a_1 = a_2$.

Cas 2. $a_1 \in Y$. Comme dans le cas 1, si $a_2 \in X$, alors nous pouvons en déduire une contradiction, nous devons donc avoir $a_2 \in Y$. Ainsi, l'équation $h(a_1) = h(a_2)$ signifie $g^{-1}(a_1) = g^{-1}(a_2)$. Par conséquent, $a_1 = g(g^{-1}(a_1)) = g(g^{-1}(a_2)) = a_2$.

Dans les deux cas, nous avons $a_1 = a_2$, donc h est bijectif.

Pour voir que h est sur, supposons $b \in B$. Alors $g(b) \in A$, donc soit $g(b) \in X$ soit $g(b) \in Y$.

Cas 1. $g(b) \in X$. Choisir n tel que $g(b) \in A_n$. Noter que $g(b) \in \text{Ran}(g) = R$ et $A_1 = A \setminus R$, donc $g(b) \notin A_1$. Ainsi, $n > 1$, donc $A_n = g(f(A_{n-1}))$, et donc on peut choisir un $a \in A_{n-1}$ tel que $g(f(a)) = g(b)$. Mais alors comme g est bijectif, $f(a) = b$. Puisque $a \in A_{n-1}$, $a \in X$, donc $h(a) = f(a) = b$. Ainsi, $b \in \text{Ran}(h)$.

Cas 2. $g(b) \in Y$. Alors $h(g(b)) = g^{-1}(g(b)) = b$, donc $b \in \text{Ran}(h)$.
 Dans les deux cas, nous avons $b \in \text{Ran}(h)$, donc h est sur. \square

Le théorème de Cantor-Schröder-Bernstein est souvent utile pour montrer que des ensembles sont équinombreux. Par exemple, dans [l'exercice 3](#) de [la section 8.1](#), on vous demandait de montrer que $(0, 1] \sim (0, 1)$, où

$$(0, 1] = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$$

et

$$(0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

Il est étonnamment difficile de trouver une correspondance bijective entre ces deux ensembles, mais il est facile de montrer qu'ils sont équinombreux en utilisant le théorème de Cantor-Schröder-Bernstein. Bien sûr, $(0, 1) \subseteq (0, 1]$, donc clairement $(0, 1) \lesssim (0, 1]$. Pour l'autre direction, définissons $f: (0, 1] \rightarrow (0, 1)$ par la formule $f(x) = x/2$. Il est facile de vérifier que cette fonction est bijective (bien qu'elle soit pas sur), donc $(0, 1] \lesssim (0, 1)$. Ainsi, par le théorème de Cantor-Schröder-Bernstein, $(0, 1] \sim (0, 1)$. Pour plus d'informations sur cet exemple, voir [l'exercice 9](#).

Notre prochain théorème donne une conséquence plus surprenante du théorème de Cantor-Schröder-Bernstein.

Théorème 8.3.3. $\mathbb{R} \sim \mathcal{P}(\mathbb{Z}^+)$.

Il est assez difficile de démontrer directement [le théorème 8.3.3](#) en donnant un exemple de fonction bijective de \mathbb{R} dans $\mathcal{P}(\mathbb{Z}^+)$. Dans notre démonstration, nous utiliserons le théorème de Cantor-Schröder-Bernstein et le lemme suivant.

Lemme 8.3.4. *Supposons que x et y soient des nombres réels et que $x < y$. Il existe alors un nombre rationnel q tel que $x < q < y$.*

Preuve. Soit k un entier strictement positif supérieur à $1/(y - x)$. Alors $1/k < y - x$. Nous allons montrer qu'il existe une fraction de dénominateur k comprise entre x et y .

Français Soient m et n des entiers tels que $m < x < n$, et soit $S = \{j \in \mathbb{N} \mid m + j/k > x\}$. Notons que $m + k(n - m)/k = n > x$, et donc $k(n - m) \in S$. Ainsi $S \neq \emptyset$, donc par le principe de bon ordre il a un plus petit élément. Soit j le plus petit élément de S . Notons aussi que $m + 0/k = m < x$, donc $0 \notin S$, et donc $j > 0$. Ainsi, $j - 1$ est un entier naturel, mais

comme j est le plus petit élément de S , $j - 1 / \in S$. Il s'ensuit que $m + (j - 1)/k \leq x$.

Soit $q = m + j / k$. Il est clair que q est un nombre rationnel, et puisque $j \in S$, $q = m + j / k > x$. De plus, en combinant les observations selon lesquelles $m + (j - 1)/k \leq x$ et $1/k < y - x$, on obtient

$$q = m + \frac{j}{k} = m + \frac{j-1}{k} + \frac{1}{k} < x + (y - x) = y.$$

Ainsi, nous avons $x < q < y$, comme requis. \square

Preuve du théorème 8.3.3. Comme indiqué précédemment, nous savons déjà que $\mathcal{P}(\mathbb{Z}^+) \lesssim \mathbb{R}$. Considérons maintenant la fonction $f: \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$ définie comme suit :

$$f(x) = \{q \in \mathbb{Q} \mid q < x\}.$$

On prétend que f est injectif. Pour comprendre pourquoi, supposons $x \in \mathbb{R}$, $y \in \mathbb{R}$ et $x \neq y$. Alors soit $x < y$ soit $y < x$. Supposons d'abord que $x < y$. D'après [le lemme 8.3.4](#), on peut choisir un nombre rationnel q tel que $x < q < y$. Mais alors $q \in f(y)$ et $q \notin f(x)$, donc $f(x) \neq f(y)$. Un argument similaire montre que si $y < x$ alors $f(x) \neq f(y)$, donc f est injectif.

Comme f est bijectif, nous avons montré que $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Q})$. Mais nous savons aussi que $\mathbb{Q} \sim \mathbb{Z}^+$, donc par [l'exercice 5](#) de [la section 8.1](#) il s'ensuit que $\mathcal{P}(\mathbb{Q}) \sim \mathcal{P}(\mathbb{Z}^+)$. Ainsi, $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Q}) \lesssim \mathcal{P}(\mathbb{Z}^+)$, donc par transitivité de \lesssim (voir [exercice 1](#)) on a $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Z}^+)$. En combinant ceci avec le fait que $\mathcal{P}(\mathbb{Z}^+) \lesssim \mathbb{R}$ et en appliquant le théorème de Cantor-Schröder-Bernstein, on conclut que $\mathbb{R} \sim \mathcal{P}(\mathbb{Z}^+)$. \square

Nous avons annoncé au début de ce chapitre que nous montrions que l'infini existe en différentes tailles. Nous constatons maintenant que, jusqu'à présent, nous n'avons trouvé que deux tailles d'infini. L'une est représentée par les ensembles dénombrables, tous équinombreux entre eux. Les seuls exemples d'ensembles infinis non dénombrables que nous avons donnés jusqu'à présent sont $\mathcal{P}(\mathbb{Z}^+)$ et \mathbb{R} , dont nous savons maintenant qu'ils sont équinombreux. En fait, il existe bien d'autres tailles d'infini. Par exemple, $\mathcal{P}(\mathbb{R})$ est un ensemble infini qui n'est ni dénombrable ni équinombre avec \mathbb{R} . Il représente donc une troisième taille d'infini. Pour plus d'informations, voir [l'exercice 8](#).

Puisque $\mathbb{Z}^+ \lessdot \mathbb{R}$, il est naturel de considérer l'ensemble des nombres réels comme *plus grand* que l'ensemble des entiers positifs. En 1878, Cantor s'est demandé s'il existait une taille infinie entre ces deux

tailles. Plus précisément, existe-t-il un ensemble X tel que $\mathbb{Z}^+ < X < \mathbb{R}$? Cantor a conjecturé que la réponse était non, mais il n'a pas pu la prouver. Sa conjecture est connue sous le nom *d'hypothèse du continu*. Lors du deuxième Congrès international des mathématiciens en 1900, David Hilbert (1862-1943) a donné une conférence célèbre dans laquelle il a énuméré ce qu'il croyait être les problèmes mathématiques non résolus les plus importants de l'époque, et la preuve ou la réfutation de l'hypothèse du continu était en tête de sa liste.

Le statut de l'hypothèse du continu a été remarquablement « résolu » par les travaux de Kurt Gödel (1906-1978) en 1939 et de Paul Cohen (1934-2007) en 1963. Cette résolution requiert des analyses encore plus approfondies que celles présentées dans cet ouvrage, tant de la notion de preuve que des hypothèses fondamentales de la théorie des ensembles. Une fois ces analyses effectuées, il est possible de démontrer des théorèmes sur ce qui est démontrable et ce qui ne l'est pas. Gödel et Cohen ont démontré qu'en utilisant les méthodes de preuve mathématique et les hypothèses de la théorie des ensembles acceptées par la plupart des mathématiciens actuels, il est impossible de démontrer l'hypothèse du continu, et il est également impossible de la réfuter !

Exercices

*1. Démontrer que \precsim est réflexif et transitif. Autrement dit :

- (a) Pour tout ensemble A , $A \precsim A$.
- (b) Pour tous les ensembles A , B et C , si $A \precsim B$ et $B \precsim C$ alors $A \precsim C$.

2. Démontrer que $<$ est irréflexif et transitif. Autrement dit :

- (a) Pour tout ensemble A , $A < A$.
- (b) Pour tous les ensembles A , B et C , si $A < B$ et $B < C$ alors $A < C$.

3. Supposons que $A \subseteq B \subseteq C$ et $A \sim C$. Démontrer que $B \sim C$.

4. Supposons que $A \precsim B$ et $C \precsim D$.

- (a) Démontrer que $A \times C \precsim B \times D$.
- (b) Démontrer que si A et C sont disjoints et B et D sont disjoints, alors $A \cup C \precsim B \cup D$.
- (c) Démontrer que $\mathcal{P}(A) \precsim \mathcal{P}(B)$.

*5. Pour la signification de la notation utilisée dans cet exercice, voir l'[exercice 23 de la section 8.1](#). Supposons que $A \precsim B$ et $C \precsim D$.

- (a) Démontrer que si $A \neq \emptyset$ alors ${}^A C \precsim {}^B D$.
- (b) L'hypothèse selon laquelle $A \neq \emptyset$ est-elle nécessaire dans la partie (a) ?

6. (a) Démontrer que si $A \precsim B$ et B est fini, alors A est fini et $|A| \leq |B|$.

(b) Démontrer que si $A \prec B$ et B est fini, alors A est fini et $|A| < |B|$.

7. Démontrer que pour tout ensemble A , $A \prec \mathcal{P}(A)$. (Indice : voir [l'exercice 5 de la section 8.2](#). Notons en particulier que si A est fini et $|A| = n$ alors, comme vous l'avez montré dans [l'exercice 11 de la section 6.2](#), et de nouveau dans [l'exercice 6\(c\) de la section 8.2](#), $|\mathcal{P}(A)| = 2^n$. Il en résulte, par [l'exercice 6\(b\)](#), que $2^n > n$. Bien sûr, vous l'avez déjà démontré, par une méthode différente, dans [l'exercice 12\(a\) de la section 6.3](#).)

*8. Soit $A_1 = \mathbb{Z}^+$, et pour tout $n \in \mathbb{Z}^+$ soit $A_{n+1} = \mathcal{P}(A_n)$.

(a) Démontrer que pour tout $n \in \mathbb{Z}^+$ et $m \in \mathbb{Z}^+$, si $n < m$ alors $A_n \prec A_m$.

(b) Les ensembles A_n , pour $n \in \mathbb{Z}^+$, représentent une infinité de tailles de l'infini. Existe-t-il d'autres tailles de l'infini ? Autrement dit, peut-on imaginer un ensemble infini qui ne soit pas équinombreux avec A_n pour tout $n \in \mathbb{Z}^+$?

9. La démonstration du théorème de Cantor-Schröder-Bernstein fournit une méthode pour construire une fonction bijective $h : A \rightarrow B$ à partir des fonctions bijectives $f : A \rightarrow B$ et $g : B \rightarrow A$. Cette méthode permet de trouver une fonction bijective $h : [0, 1] \rightarrow (0, 1)$. Commençons par les fonctions $f : (0, 1] \rightarrow (0, 1)$ et $g : (0, 1) \rightarrow (0, 1]$ données par les formules :

$$f(x) = \frac{x}{2}, \quad g(x) = x.$$

10. Soit $\mathcal{E} = \{R \mid R \text{ est une relation d'équivalence sur } \mathbb{Z}^+\}$.

(a) Démontrer que $\mathcal{E} \subseteq \mathcal{P}(\mathbb{Z}^+)$.

(b) Soit $A = \mathbb{Z}^+ \setminus \{1, 2\}$ et soit \mathcal{P} l'ensemble de toutes les partitions de \mathbb{Z}^+ . Définissez $f : \mathcal{P}(A) \rightarrow \mathcal{P}$ par la formule $f(X) = \{X \cup \{1\}, (A \setminus X) \cup \{2\}\}$. Démontrez que f est bijectif.

(c) Démontrer que $\mathcal{E} \sim \mathcal{P}(\mathbb{Z}^+)$.

11. Soit $\mathcal{T} = \{R \mid R \text{ est un ordre total sur } \mathbb{Z}^+\}$. Démontrer que $\mathcal{T} \sim \mathcal{P}(\mathbb{Z}^+)$. (Indice : Imiter la solution de [l'exercice 10](#).)

12. (a) Démontrer que si A a au moins deux éléments et $A \times A \sim A$ alors $\mathcal{P}(A) \times \mathcal{P}(A) \sim \mathcal{P}(A)$.

(b) Démontrer que $\mathbb{R} \times \mathbb{R} \sim \mathbb{R}$.

13. Un *intervalle* est un ensemble $I \subseteq \mathbb{R}$ possédant la propriété que, pour tous les nombres réels x, y et z , si $x \in I, z \in I$ et $x < y < z$, alors $y \in I$. Un intervalle est *non dégénéré* s'il contient au moins deux

nombres réels différents. Supposons que \mathcal{F} soit un ensemble d'intervalles non dégénérés et que \mathcal{F} soit deux à deux disjoint. Démontrer que \mathcal{F} est dénombrable. (Indice : D'après [le lemme 8.3.4](#), tout intervalle non dégénéré contient un nombre rationnel.)

14. Pour la signification de la notation utilisée dans cet exercice, voir [l'exercice 23 de la section 8.1](#).
- (a) Démontrer que ${}^{\mathbb{R}}\mathbb{R} \sim \mathcal{P}(\mathbb{R})$.
 - (b) Démontrer que ${}^{\mathbb{Q}}\mathbb{R} \sim \mathbb{R}$.
 - (c) (Pour les lecteurs connaissant le calcul différentiel et intégral.) Soit $\mathcal{C} = \{f \in {}^{\mathbb{R}}\mathbb{R} \mid f \text{ est continue}\}$. Démontrer que $\mathcal{C} \sim \mathbb{R}$. (Indice : Montrer que si f et g sont des fonctions continues et $\forall x \in \mathbb{Q} (f(x) = g(x))$, alors $f = g$.)

[1](#) Il faut être un peu plus prudent ici. Il est possible que deux développements décimaux différents représentent le même nombre. Par exemple, en cours de calcul, vous avez peut-être appris le fait surprenant que $0,999\dots = 1,000\dots$. Cependant, cela ne se produit qu'avec des développements décimaux se terminant soit par une suite infinie de 9, soit par une suite infinie de 0. Pour les développements décimaux composés de 3 et de 7, des développements décimaux différents représentent toujours des nombres différents.

Appendice

Solutions aux exercices sélectionnés

Introduction

1. (a) Une réponse possible est $32\ 767 = 31 \cdot 1057$.
(b) Une réponse possible est $x = 2^{31} - 1 = 2\ 147\ 483\ 647$.
3. (a) La méthode donne le nombre premier 211.
(b) La méthode donne deux nombres premiers, 3 et 37.

Chapitre 1

Section 1.1

1. (a) $(R \vee H) \wedge \neg(H \wedge T)$, où R représente l'énoncé « Nous aurons un devoir de lecture », H représente « Nous aurons des problèmes de devoirs » et T représente « Nous aurons un test ».

(b) $\neg G \vee (G \wedge \neg S)$, où G signifie « Vous irez skier » et S signifie « Il y aura de la neige ».

(c) $\neg[(\sqrt{7} < 2) \vee (\sqrt{7} = 2)]$.

6. (a) Je n'achèterai pas le pantalon sans la chemise .

(b) Je n'achèterai pas le pantalon et je n'achèterai pas la chemise.

(c) Soit je n'achèterai pas le pantalon, soit je n'achèterai pas la chemise.

Section 1.2

$$\begin{array}{ccc} P & Q & \neg P \vee Q \\ \hline F & F & T \\ F & T & T \\ T & F & F \\ \hline S & G & (S \vee G) \wedge (\neg S \vee \neg G) \\ \hline F & F & F \\ F & T & T \\ T & F & T \\ \hline T & T & F \end{array}$$

$$\begin{array}{ccc} P & Q & P \downarrow Q \\ \hline F & F & T \\ F & T & F \\ T & F & F \\ \hline T & T & F \end{array}$$

$$\begin{array}{ccc} 5. (a) & & \\ (b) \neg(P \vee Q). & & \end{array}$$

(c) $\neg P$ est équivalent à $P \downarrow P$, $P \vee Q$ est équivalent à $(P \downarrow Q) \downarrow (P \downarrow Q)$, et $P \wedge Q$ est équivalent à $(P \downarrow P) \downarrow (Q \downarrow Q)$.

7. (a) et (c) sont valides; (b) et (d) sont invalides.

9. (a) n'est ni une contradiction ni une tautologie ; (b) est une contradiction ; (c) et (d) sont des tautologies .

11. (a) $P \vee Q$.

(b) P .

(c) $\neg P \vee Q$.

14. Nous utilisons la loi associative pour \wedge deux fois :

$[P \wedge (Q \wedge R)] \wedge S$ is equivalent to $[(P \wedge Q) \wedge R] \wedge S$
which is equivalent to $(P \wedge Q) \wedge (R \wedge S)$.

16. $P \vee \neg Q$.

Section 1.3

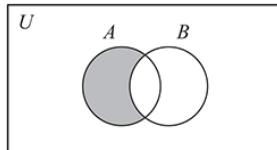
1. (a) $D(6) \wedge D(9) \wedge D(15)$, où $D(x)$ signifie « x est divisible par 3 ».
(b) $D(x, 2) \wedge D(x, 3) \wedge \neg D(x, 4)$, où $D(x, y)$ signifie « x est divisible par y ».
(c) $N(x) \wedge N(y) \wedge [(P(x) \wedge \neg P(y)) \vee (P(y) \wedge \neg P(x))]$, où $N(x)$ signifie « x est un nombre naturel » et $P(x)$ signifie « x est premier ».
3. (a) $\{x \mid x \text{ est une planète}\}$.
(b) $\{x \mid x \text{ est une école de l'Ivy League}\}$.
(c) $\{x \mid x \text{ est un État des États-Unis}\}$.
(d) $\{x \mid x \text{ est une province ou un territoire du Canada}\}$.
5. (a) $(-3 \in \mathbb{R}) \supset \wedge \neg (-3 > 1)$. Variables liées : x ; aucune variable libre. Cette affirmation est vraie.
(b) $(4 \in \mathbb{R}) \wedge (4 < 0) \wedge (13 - 2(4) > 1)$. Variables liées : x ; aucune variable libre. Cette affirmation est fausse.
(c) $\neg[(5 \in \mathbb{R}) \wedge (13 - 2(5) > c)]$. Variables liées : x ; variables libres : c .
8. (a) $\{x \mid \text{Elizabeth Taylor a été mariée à } x\} = \{\text{Conrad Hilton Jr., Michael Wilding, Michael Todd, Eddie Fisher, Richard Burton, John Warner, Larry Fortensky}\}$.
(b) $\{x \mid x \text{ est un connecteur logique étudié dans la section 1.1}\} = \{\wedge, \vee, \neg\}$.
(c) $\{x \mid x \text{ est l'auteur de ce livre}\} = \{\text{Daniel J. Velleman}\}$.

Section 1.4

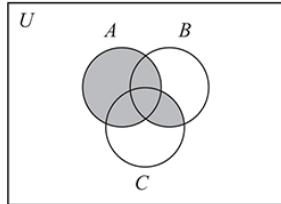
1. (a) $\{3, 12\}$.
(b) $\{1, 12, 20, 35\}$.
(c) $\{1, 3, 12, 20, 35\}$.

Les ensembles des parties (a) et (b) sont tous deux des sous-ensembles de l'ensemble de la partie (c).

4. (a) Les deux diagrammes de Venn ressemblent à ceci :



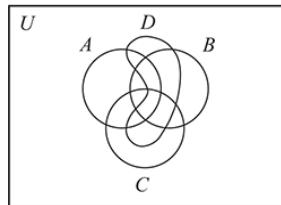
- (b) Les deux diagrammes de Venn ressemblent à ceci :



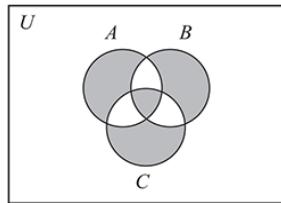
9. Les ensembles (a), (d) et (e) sont égaux, et les ensembles (b) et (c) sont égaux .

12. (a) Il n'existe pas de région correspondant à l'ensemble $(A \cap D) \setminus (B \cup C)$, mais cet ensemble pourrait avoir des éléments.

(b) Voici une possibilité :



14. Les diagrammes de Venn pour les deux ensembles ressemblent à ceci :



Section 1.5

1. (a) $(S \vee \neg E) \rightarrow \neg H$, où S signifie « Ce gaz a une odeur désagréable », E signifie « Ce gaz est explosif » et H signifie « Ce gaz est de l'hydrogène ».

(b) $(F \wedge H) \rightarrow D$, où F signifie « Georges a de la fièvre », H signifie « Georges a un mal de tête » et D signifie « Georges ira chez le médecin ».

(c) $(F \rightarrow D) \wedge (H \rightarrow D)$, où les lettres ont la même signification que dans la partie (b).

(d) $(x \neq 2) \rightarrow (P(x) \rightarrow O(x))$, où $P(x)$ signifie « x est premier » et $O(x)$ signifie « x est impair ».

4. (a) et (b) sont valides, mais (c) est invalide.

7. (a) Soit établir une table de vérité, soit raisonner comme suit :

$(P \rightarrow R) \wedge (Q \rightarrow R)$ is equivalent to $(\neg P \vee R) \wedge (\neg Q \vee R)$
which is equivalent to $(\neg P \wedge \neg Q) \vee R$
which is equivalent to $\neg(P \vee Q) \vee R$
which is equivalent to $(P \vee Q) \rightarrow R$

(b) $(P \rightarrow R) \vee (Q \rightarrow R)$ est équivalent à $(P \wedge Q) \rightarrow R$.

9. $\neg(P \rightarrow \neg Q)$.

Chapitre 2

Section 2.1

1. (a) $\forall x [\exists y F(x, y) \rightarrow S(x)]$, où $F(x, y)$ signifie « x a pardonné y » et $S(x)$ signifie « x est un saint ».
(b) $\neg\exists x [C(x) \wedge \forall y (D(y) \rightarrow S(x, y))]$, où $C(x)$ signifie « x est dans la classe de calcul », $D(y)$ signifie « y est dans la classe de mathématiques discrètes » et $S(x, y)$ signifie « x est plus intelligent que y ».
(c) $\forall x (\neg(x = m) \rightarrow L(x, m))$, où $L(x, y)$ signifie « x aime y » et m signifie Marie.
(d) $\exists x (P(x) \wedge S(j, x)) \wedge \exists y (P(y) \wedge S(r, y))$, où $P(x)$ signifie « x est un policier », $S(x, y)$ signifie « x a vu y », j signifie Jane et r signifie Roger.
(e) $\exists x (P(x) \wedge S(j, x) \wedge S(r, x))$, où les lettres ont les mêmes significations que dans la partie (d).
4. (a) Tous les hommes célibataires sont malheureux.
(b) y est la sœur de l'un des parents de x ; c'est-à-dire que y est la tante de sang de x .
8. (a), (d) et (e) sont vrais ; (b), (c) et (f) sont faux.

Section 2.2

1. (a) $\exists x [M(x) \wedge \forall y (F(x, y) \rightarrow \neg H(y))]$, où $M(x)$ signifie « x se spécialise en mathématiques », $F(x, y)$ signifie « x et y sont amis » et $H(y)$ signifie « y a besoin d'aide pour ses devoirs ». En français : Il y a un étudiant en mathématiques dont tous les amis n'ont pas besoin d'aide pour leurs devoirs.
(b) $\exists x \forall y (R(x, y) \rightarrow \exists z L(y, z))$, où $R(x, y)$ signifie « x et y sont colocataires » et $L(y, z)$ signifie « y aime z ». En français : Il y a quelqu'un dont tous les colocataires aiment au moins une personne.
(c) $\exists x [(x \in A \vee x \in B) \wedge (x \notin C \vee x \in D)]$.
(d) $\forall x \exists y [y > x \wedge \forall z (z^2 + 5z \neq y)]$.

4. Astuce : Commencez par remplacer $P(x)$ par $\neg P(x)$ dans la première loi de négation du quantificateur, pour obtenir le fait que $\neg\exists x P(x)$ est équivalent à $\forall x \neg\neg P(x)$.
6. Indice : Commencez par montrer que $\exists x (P(x) \vee Q(x))$ est équivalent à $\neg\forall x \neg(P(x) \vee Q(x))$.

8. $(\forall x \in AP(x)) \wedge (\forall x \in BP(x))$

is equivalent to $\forall x(x \in A \rightarrow P(x)) \wedge \forall x(x \in B \rightarrow P(x))$
which is equivalent to $\forall x[(x \in A \rightarrow P(x)) \wedge (x \in B \rightarrow P(x))]$
which is equivalent to $\forall x[(x \notin A \vee P(x)) \wedge (x \notin B \vee P(x))]$
which is equivalent to $\forall x[(x \notin A \wedge x \notin B) \vee P(x)]$
which is equivalent to $\forall x[\neg(x \in A \vee x \in B) \vee P(x)]$
which is equivalent to $\forall x[x \notin (A \cup B) \vee P(x)]$
which is equivalent to $\forall x[x \in (A \cup B) \rightarrow P(x)]$
which is equivalent to $\forall x \in (A \cup B) P(x)$.

11. $A \setminus B = \emptyset$ est équivalent à $\neg \exists x (x \in A \wedge x \notin B)$

which is equivalent to $\forall x \neg(x \in A \wedge x \notin B)$
which is equivalent to $\forall x(x \notin A \vee x \in B)$
which is equivalent to $\forall x(x \in A \rightarrow x \in B)$
which is equivalent to $A \subseteq B$.

14. $A \cap B = \emptyset$ est équivalent à $\neg \exists x (x \in A \wedge x \in B)$

which is equivalent to $\forall x \neg(x \in A \wedge x \in B)$
which is equivalent to $\forall x(x \notin A \vee x \notin B)$
which is equivalent to $\forall x(x \in A \rightarrow x \notin B)$
which is equivalent to $\forall x((x \notin B \wedge x \in A) \leftrightarrow x \in A)$

(par [la section 1.5 exercice 11\(b\)](#))

which is equivalent to $\forall x(x \in A \setminus B \leftrightarrow x \in A)$
which is equivalent to $A \setminus B = A$.

Section 2.3

1. (a) $\forall x (x \in \mathcal{F} \rightarrow \forall y (y \in x \rightarrow y \in A))$.

(b) $\forall x (x \in A \rightarrow \exists n \in \mathbb{N} (x = 2n + 1))$.

(c) $\forall n \in \mathbb{N} \exists m \in \mathbb{N} (n^2 + n + 1 = 2m + 1)$.

(d) $\exists x (\forall y (y \in x \rightarrow \exists i \in I (y \in A_i)) \wedge \forall i \in I \exists y (y \in x \wedge y \notin A_i))$.

4. $\cap \mathcal{F} = \{\text{red, blue}\}$ et $\cup \mathcal{F} = \{\text{red, green, blue, orange, purple}\}$.

8. (a) $A_2 = \{2, 4\}, A_3 = \{3, 6\}, B_2 = \{2, 3\}, B_3 = \{3, 4\}$.

(b) $\bigcap_{i \in I} (A_i \cup B_i) = \{3, 4\}$ and $(\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i) = \{3\}$.

(c) Ils ne sont pas équivalents.

12. Un exemple est $A = \{1, 2\}$ et $B = \{2, 3\}$.

14. (a) $B_3 = \{1, 2, 3, 4, 5\}$ et $B_4 = \{1, 2, 4, 5, 6\}$.

(b) $\bigcap_{j \in J} B_j = \{1, 2, 4, 5\}$.

(c) $\bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j}) = \{1, 2, 4\}$. This is not equal to the set in part (b).

(d) $x \in \bigcap_{j \in J} (\bigcup_{i \in I} A_{i,j})$ signifie $\forall j \in J \exists i \in I (x \in A_{i,j})$ et $x \in \bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j})$ signifie $\exists i \in I \forall j \in J (x \in A_{i,j})$. Ils ne sont pas équivalents.

Chapitre 3

Section 3.1

1. (a) Hypothèses : n est un entier supérieur à 1 et n n'est pas premier.
Conclusion : $2^n - 1$ n'est pas premier. Les hypothèses sont vraies lorsque $n = 6$; le théorème nous dit donc que $2^6 - 1$ n'est pas premier. C'est correct, car $2^6 - 1 = 63 = 9 \cdot 7$.
- (b) On peut conclure que 32 767 n'est pas premier. C'est exact, puisque $32\,767 = 151 \cdot 217$.
- (c) Le théorème ne nous dit rien ; 11 est premier, donc les hypothèses ne sont pas satisfaites.
4. Supposons que $0 < a < b$. Alors $b - a > 0$. En multipliant les deux côtés par le nombre positif $b + a$, on obtient $(b + a) \cdot (b - a) > (b + a) \cdot 0$, ou en d'autres termes $b^2 - a^2 > 0$. Puisque $b^2 - a^2 > 0$, il s'ensuit que $a^2 < b^2$. Par conséquent, si $0 < a < b$ alors $a^2 < b^2$.
8. Démontrons la contraposée. Supposons $x \notin B$. Alors, puisque $x \in A$, il en résulte que $x \in A \setminus B$. Mais nous savons aussi que $A \setminus B \subseteq C \cap D$, nous pouvons donc conclure que $x \in C \cap D$, et donc $x \in D$. Ainsi, si $x \notin D$ alors $x \in B$.
10. Indice : ajoutez b aux deux côtés de l'inégalité $a < b$.
12. Démontrons la contraposée. Supposons que $c \leq d$. En multipliant les deux côtés de cette inégalité par le nombre positif a , on obtient $ac \leq ad$. De même, en multipliant les deux côtés de l'inégalité donnée $a < b$ par le nombre positif d , on obtient $ad < bd$. En combinant $ac \leq ad$ et $ad < bd$, on conclut que $ac < bd$. Ainsi, si $ac \geq bd$ alors $c > d$.
15. Puisque $x > 3 > 0$, d'après le théorème de [l'exemple 3.2.1](#), $x^2 > 9$. De plus, en multipliant les deux côtés de l'inégalité donnée $y < 2$ par -2 (et en inversant le sens de l'inégalité, puisque -2 est négatif), on obtient $-2y > -4$. Enfin, en additionnant les inégalités $x^2 > 9$ et $-2y > -4$, on obtient $x^2 - 2y > 5$.

Section 3.2

1. (a) Supposons P . Puisque $P \rightarrow Q$, il s'ensuit que Q . Mais alors, puisque $Q \rightarrow R$, nous pouvons conclure R . Ainsi, $P \rightarrow R$.
- (b) Supposons P . Pour prouver que $Q \rightarrow R$, nous prouverons la contraposée, donc supposons $\neg R$. Puisque $\neg R \rightarrow (P \rightarrow \neg Q)$, il

s'ensuit que $P \rightarrow \neg Q$, et puisque nous connaissons P , nous pouvons conclure $\neg Q$. Ainsi, $\neg Q \rightarrow R$, donc $P \rightarrow (\neg Q \rightarrow R)$.

5. Supposons que $x \in A \setminus B$ et $x \in B \setminus C$. Puisque $x \in A \setminus B$, $x \in A$ et $x \notin B$, et puisque $x \in B \setminus C$, $x \in B$ et $x \notin C$. Mais maintenant nous avons $x \in B$ et $x \notin B$, ce qui est une contradiction. Il ne peut donc pas être vrai que $x \in A \setminus B$ et $x \in B \setminus C$.
6. Supposons que $a \in A \setminus B$. Cela signifie que $a \in A$ et $a \notin B$. Puisque $a \in A$ et $a \in C$, $a \in A \cap C$. Mais alors puisque $A \cap C \subseteq B$, il s'ensuit que $a \in B$, ce qui contredit le fait que $a \notin B$. Ainsi, $a \notin A \setminus B$.
9. Indice : Supposons que $a < 1 / a < b < 1 / b$. Démontrez maintenant que $a < 1$, puis utilisez ce fait pour prouver que $a < 0$, puis utilisez ce fait pour prouver que $a < -1$.

12. (a) La phrase « Alors $x = 3$ et $y = 8$ » est incorrecte. (Pourquoi ?)
 (b) Un contre-exemple est $x = 3, y = 7$.

P	Q	R	$P \rightarrow (Q \rightarrow R)$	$\neg R \rightarrow (P \rightarrow \neg Q)$
F	F	F	T	T
F	F	T	T	T
F	T	F	T	T
F	T	T	T	T
T	F	F	T	T
T	F	T	T	T
T	T	F	F	F
T	T	T	T	T

15.

Section 3.3

1. Supposons $\exists x (P(x) \rightarrow Q(x))$. Alors nous pouvons choisir un x_0 tel que $P(x_0) \rightarrow Q(x_0)$. Supposons maintenant que $\forall x P(x)$. Alors en particulier, $P(x_0)$, et puisque $P(x_0) \rightarrow Q(x_0)$, il s'ensuit que $Q(x_0)$. Puisque nous avons trouvé une valeur particulière de x pour laquelle $Q(x)$ est vraie, nous pouvons conclure que $\exists x Q(x)$. Ainsi $\forall x P(x) \rightarrow \exists x Q(x)$.
3. Supposons que $A \subseteq B \setminus C$, mais que A et C ne soient pas disjoints. On peut alors choisir un x tel que $x \in A$ et $x \in C$. Puisque $x \in A$ et $A \subseteq B \setminus C$, il s'ensuit que $x \in B \setminus C$, ce qui signifie que $x \in B$ et $x \notin C$. Or, on a maintenant $x \in C$ et $x \notin C$, ce qui est contradictoire. Ainsi, si $A \subseteq B \setminus C$ alors A et C sont disjoints.
7. Supposons que $x > 2$. Soit $y = (x + \sqrt{x^2 - 4})/2$ qui est défini puisque $x^2 - 4 > 0$. Alors

$$y + \frac{1}{y} = \frac{x + \sqrt{x^2 - 4}}{2} + \frac{2}{x + \sqrt{x^2 - 4}} = \frac{2x^2 + 2x\sqrt{x^2 - 4}}{2(x + \sqrt{x^2 - 4})} = x.$$

9. Supposons que \mathcal{F} soit une famille d'ensembles et que $A \in \mathcal{F}$.

Supposons $x \in \bigcap \mathcal{F}$ alors par définition de $\bigcap \mathcal{F}$, puisque $x \in \bigcap \mathcal{F}$ et $A \in \mathcal{F}$, $x \in A$. Mais x était un élément arbitraire de $\bigcap \mathcal{F}$, il s'ensuit que $\bigcap \mathcal{F} \subseteq A$.

12. Indice : Supposons que $\mathcal{F} \subseteq \mathcal{G}$ et que x soit un élément arbitraire de $\bigcup \mathcal{F}$.

Vous devez prouver ce $x \in \bigcup \mathcal{G}$, qui signifie $\exists A \in \mathcal{G} (x \in A)$, vous devriez donc essayer Trouver un énoncé $A \in \mathcal{G}$ tel que $x \in A$. Pour cela, écrivez les données en notation logique. Vous constaterez que l'une d'elles est universelle et l'autre existentielle. Appliquez l'instanciation existentielle à l'énoncé existentiel.

14. Supposons $x \in \bigcup_{i \in I} \mathcal{P}(A_i)$ que nous puissions choisir un $i \in I$ tel que $x \in \mathcal{P}(A_i)$, autrement dit $x \subseteq A_i$. Soit maintenant a un élément arbitraire de x . Alors $a \in A_i$, et donc $a \in \bigcup_{i \in I} A_i$. Puisque a était un élément arbitraire de x , il s'ensuit que $x \subseteq \bigcup_{i \in I} A_i$, ce qui signifie que $x \in \mathcal{P}(\bigcup_{i \in I} A_i)$. Ainsi $\bigcup_{i \in I} \mathcal{P}(A_i) \subseteq \mathcal{P}(\bigcup_{i \in I} A_i)$.

17. Indice : La dernière hypothèse signifie $\forall A \in \mathcal{F} \forall B \in \mathcal{G} (A \subseteq B)$, donc si au cours de la preuve vous rencontrez des ensembles $A \in \mathcal{F}$ et $B \in \mathcal{G}$, vous pouvez conclure que $A \subseteq B$. Commencez la preuve en laissant x arbitraire et en supposant $x \in \bigcup \mathcal{F}$, et prouvant que $x \in \bigcap \mathcal{G}$. Pour voir où aller à partir de là, écrivez ces affirmations sous forme de symboles logiques.

20. La phrase « Alors pour tout nombre réel x , $x^2 < 0$ » est incorrecte. (Pourquoi ?)

22. En fonction de la forme logique de l'énoncé à prouver, la preuve devrait avoir ce plan :

Let $x = \dots$
Let y be an arbitrary real number.
[Proof of $xy^2 = y - x$ goes here.]
Since y was arbitrary, $\forall y \in \mathbb{R} (xy^2 = y - x)$.
Thus, $\exists x \in \mathbb{R} \forall y \in \mathbb{R} (xy^2 = y - x)$.

Ce schéma indique clairement que y doit être introduit dans la preuve *après* x . Par conséquent, x ne peut être défini en fonction de y , car y n'aura pas encore été introduit dans la preuve au moment de la définition de x . Or, dans la preuve donnée, x est défini en fonction de y dès la première phrase. (L'erreur a été masquée par l'omission de la phrase « Soit y un nombre réel arbitraire ». Si vous essayez d'ajouter cette phrase à la preuve, vous constaterez qu'elle ne permet pas de prouver correctement le théorème erroné.)

25. Voici le début de la preuve : Soit x un nombre réel arbitraire. Soit $y = 2x$. Soit maintenant z un nombre réel arbitraire. Alors...

Section 3.4

1. (\rightarrow) Supposons $\forall x (P(x) \wedge Q(x))$. Soit y arbitraire. Alors puisque $\forall x (P(x) \wedge Q(x))$, $P(y) \wedge Q(y)$, et donc en particulier $P(y)$. Puisque y est arbitraire, cela montre que $\forall x P(x)$. Un argument similaire prouve $\forall x Q(x)$: pour y arbitraire, $P(y) \wedge Q(y)$, et donc $Q(y)$. Ainsi, $\forall x P(x) \wedge \forall x Q(x)$.

(\leftarrow) Supposons $\forall x P(x) \wedge \forall x Q(x)$. Soit y arbitraire. Alors puisque $\forall x P(x)$, $P(y)$, et de même puisque $\forall x Q(x)$, $Q(y)$. Ainsi, $P(y) \wedge Q(y)$, et puisque y était arbitraire, il s'ensuit que $\forall x (P(x) \wedge Q(x))$.

4. Supposons que $A \subseteq B$ et $A \not\subseteq C$. Puisque $A \not\subseteq C$, on peut choisir un $a \in A$ tel que $a \notin C$. Puisque $a \in A$ et $A \subseteq B$, $a \in B$. Puisque $a \in B$ et $a \notin C$, $B \not\subseteq C$.

7. Soient A et B des ensembles arbitraires. Soit x arbitraire, et supposons que $x \in \mathcal{P}(A \cap B)$. Alors $x \subseteq A \cap B$. Soit maintenant y un élément arbitraire de x . Alors, puisque $x \subseteq A \cap B$, $y \in A \cap B$, et donc $y \in A$. Puisque y est arbitraire, ceci montre que $x \subseteq A$, donc $x \in \mathcal{P}(A)$. Un argument similaire montre que $x \subseteq B$, et donc $x \in \mathcal{P}(B)$. Ainsi, $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

Supposons maintenant que $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Alors $x \in \mathcal{P}(A)$ et $x \in \mathcal{P}(B)$, donc $x \subseteq A$ et $x \subseteq B$. Supposons que $y \in x$. Alors puisque $x \subseteq A$ et $x \subseteq B$, $y \in A$ et $y \in B$, donc $y \in A \cap B$. Ainsi, $x \subseteq A \cap B$, donc $x \in \mathcal{P}(A \cap B)$.

9. Supposons que x et y soient impairs. On peut alors choisir des entiers j et k tels que $x = 2j + 1$ et $y = 2k + 1$. Par conséquent, $xy = (2j + 1)(2k + 1) = 4jk + 2j + 2k + 1 = 2(2jk + j + k) + 1$. Puisque $2jk + j + k$ est un entier, xy est impair.

13. Indice : Soit $x \in \mathbb{R}$ arbitraire, et démontrons les deux directions de la biconditionnelle séparément. Pour la direction « \rightarrow », utilisons l'instanciation existentielle et la preuve par contradiction. Pour la direction « \leftarrow », supposons que $x \neq 1$, puis résolvons l'équation $x + y = xy$ pour y afin de déterminer la valeur de y .

16. Supposons que $\cup \mathcal{F}$ and $\cap \mathcal{G}$ ne soient pas disjoints. Alors on peut choisir un x tel que $x \in \cup \mathcal{F}$ and $x \in \cap \mathcal{G}$. Puisqu'on peut choisir un $A \in \mathcal{F}$ tel que $x \in A$. Puisqu'on sait que tout élément de \mathcal{F} est disjoint d'un élément de \mathcal{G} , il doit exister un $B \in \mathcal{G}$ tel que $A \cap B = \emptyset$. Puisque $x \in A$

, il s'ensuit que $x \notin B$. Mais on a aussi $x \in \bigcap \mathcal{G}$ et $B \in \mathcal{G}$, d'où il s'ensuit que $x \in B$, ce qui est une contradiction. Ainsi, $\bigcup \mathcal{F}$ and $\bigcap \mathcal{G}$ doivent être disjoints.

18. (a) Supposons que nous puissions choisir un $A \in \mathcal{F} \cap \mathcal{G}$ tel que $x \in A$. Puisque $A \in \mathcal{F} \cap \mathcal{G}$, $A \in \mathcal{F}$ et $A \in \mathcal{G}$. Puisque $x \in A$ et $A \in \mathcal{F}$, $x \in \bigcup \mathcal{F}$, et de même puisque $x \in A$ et $A \in \mathcal{G}$, $x \in \bigcup \mathcal{G}$. Par conséquent, $x \in (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$. Puisque x était arbitraire, cela montre que $\bigcup (\mathcal{F} \cap \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$.

(b) La phrase « Ainsi, nous pouvons choisir un ensemble A tel que $A \in \mathcal{F}$, $A \in \mathcal{G}$ et $x \in A$ » est incorrecte. (Pourquoi ?)

(c) Un exemple est $\mathcal{F} = \{\{1\}, \{2\}\}$, $\mathcal{G} = \{\{1\}, \{1, 2\}\}$.

22. Supposons que $\bigcup \mathcal{F} \not\subseteq \bigcup \mathcal{G}$. Alors il existe un $x \in \bigcup \mathcal{F}$ tel que $x \notin \bigcup \mathcal{G}$. Puisque $x \in \bigcup \mathcal{F}$, nous pouvons choisir un $A \in \mathcal{F}$ tel que $x \in A$. Maintenant soit $B \in \mathcal{G}$ arbitraire. Si $A \subseteq B$, alors puisque $x \in A$, $x \in B$. Mais alors puisque $x \in B$ et $B \in \mathcal{G}$, $x \in \bigcup \mathcal{G}$, que nous savons déjà est faux. Donc $A \not\subseteq B$. Puisque B était arbitraire, cela montre que pour tout $B \in \mathcal{G}$, $A \not\subseteq B$. Ainsi, nous avons montré qu'il existe un $A \in \mathcal{F}$ tel que pour tout $B \in \mathcal{G}$, $A \not\subseteq B$.

24. (a) Supposons que nous puissions choisir un $i \in I$ tel que $x \in A_i \setminus B_i$, ce qui signifie que $x \in A_i$ et $x \notin B_i$. Puisque $x \in A_i$, $x \in \bigcup_{i \in I} A_i$ et puisque $x \notin B_i$, $x \notin \bigcap_{i \in I} B_i$. Ainsi, $x \in (\bigcup_{i \in I} A_i) \setminus (\bigcap_{i \in I} B_i)$.

(b) Un exemple est $I = \{1, 2\}$, $A_1 = B_1 = \{1\}$, $A_2 = B_2 = \{2\}$.

Section 3.5

1. Supposons que $x \in A \cap (B \cup C)$. Alors $x \in A$, et soit $x \in B$ soit $x \in C$.
Cas 1. $x \in B$. Alors puisque $x \in A$, $x \in A \cap B$, donc $x \in (A \cap B) \cup C$

Cas 2. $x \in C$. Alors clairement $x \in (A \cap B) \cup C$.

Puisque x est arbitraire, nous pouvons conclure que $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.

5. Supposons que $x \in A$. Nous considérons maintenant deux cas :

Cas 1. $x \in C$. Alors $x \in A \cap C$, donc puisque $A \cap C \subseteq B \cap C$, $x \in B \cap C$, et donc $x \in B$.

Cas 2. $x \notin C$. Puisque $x \in A$, $x \in A \cup C$, donc puisque $A \cup C \subseteq B \cup C$, $x \in B \cup C$. Mais $x \notin C$, donc nous devons avoir $x \in B$.

Ainsi, $x \in B$, et puisque x était arbitraire, $A \subseteq B$.

8. Indice : Supposons que $x \in \mathcal{P}(A) \cup \mathcal{P}(B)$, ce qui signifie que $x \in \mathcal{P}(A)$ ou $x \in \mathcal{P}(B)$. Considérez ces deux cas comme deux cas distincts. Dans le cas 1, supposons que $x \in \mathcal{P}(A)$, ce qui signifie $x \subseteq A$, et démontrons que $x \in \mathcal{P}(A \cup B)$, ce qui signifie $x \subseteq A \cup B$. Le cas 2 est similaire.

12. Soit x un nombre réel arbitraire.

(\leftarrow) Supposons que $|x - 4| > 2$.

Cas 1. $x - 4 \geq 0$. Alors $|x - 4| = x - 4$, donc $x - 4 > 2$, et donc $x > 6$. En ajoutant x des deux côtés, on obtient $2x > 6 + x$, donc $2x - 6 > x$. Puisque $x > 6$, cela implique que $2x - 6$ est positif, donc $|2x - 6| = 2x - 6 > x$.

Cas 2. $x - 4 < 0$. Alors $|x - 4| = 4 - x$, donc on a $4 - x > 2$, et donc $x < 2$. Par conséquent $3x < 6$, et en soustrayant $2x$ des deux côtés on obtient $x < 6 - 2x$. De plus, à partir de $x < 2$ on obtient $2x < 4$, donc $2x - 6 < -2$. Par conséquent $2x - 6$ est négatif, donc $|2x - 6| = 6 - 2x > x$.

(\rightarrow) Astuce : Imitez la direction « \leftarrow » en utilisant les cas $2x - 6 \geq 0$ et $2x - 6 < 0$.

16. (a) Supposons que nous puissions choisir un $A \in \mathcal{F} \cup \mathcal{G}$ tel que $x \in A$. Puisque $A \in \mathcal{F} \cup \mathcal{G}$, soit $A \in \mathcal{F}$ soit $A \in \mathcal{G}$.

Cas 1. $A \in \mathcal{F}$. Puisque $x \in A$ et $A \in \mathcal{F}$, $x \in \bigcup \mathcal{F}$, so $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.

Cas 2. $A \in \mathcal{G}$. Puisque $x \in A$ et $A \in \mathcal{G}$, $x \in \bigcup \mathcal{G}$, so $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.

Ainsi, $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.

Supposons maintenant que $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$. Alors soit $x \in \bigcup \mathcal{F}$ ou $x \in \bigcup \mathcal{G}$.

Cas 1. $x \in \bigcup \mathcal{F}$. Alors on peut choisir un $A \in \mathcal{F}$ tel que $x \in A$. Puisque $A \in \mathcal{F}$, $A \in \mathcal{F} \cup \mathcal{G}$, donc puisque $x \in A$, il s'ensuit que $x \in (\bigcup \mathcal{F} \cup \mathcal{G})$.

Cas 2. $x \in \bigcup \mathcal{G}$. Un argument similaire montre que $x \in (\bigcup \mathcal{F} \cup \mathcal{G})$.

Ainsi, $x \in (\bigcup \mathcal{F} \cup \mathcal{G})$.

(b) Le théorème est : $\bigcap(\mathcal{F} \cup \mathcal{G}) = (\bigcap \mathcal{F}) \cap (\bigcap \mathcal{G})$.

20. (\rightarrow) Supposons que $A \Delta B$ et C soient disjoints. Soit x un élément arbitraire de $A \cap C$. Alors $x \in A$ et $x \in C$. Si $x \notin B$, alors puisque $x \in A$, $x \in A \setminus B$, et donc $x \in A \Delta B$. Mais aussi $x \in C$, donc cela contredit notre hypothèse que $A \Delta B$ et C sont disjoints. Donc $x \in B$. Puisque nous connaissons aussi $x \in C$, nous avons $x \in B \cap C$. Puisque x était un élément arbitraire de $A \cap C$, cela montre que $A \cap C \subseteq B \cap C$. Un argument similaire montre que $B \cap C \subseteq A \cap C$.

(\leftarrow) Supposons que $A \cap C = B \cap C$. Supposons que $A \Delta B$ et C ne soient pas disjoints. Alors on peut choisir un x tel que $x \in A \Delta B$ et $x \in C$. Puisque $x \in A \Delta B$, soit $x \in A \setminus B$ soit $x \in B \setminus A$.

Cas 1. $x \in A \setminus B$. Alors $x \in A$ et $x \notin B$. Puisque nous connaissons aussi $x \in C$, nous pouvons conclure que $x \in A \cap C$ mais $x \notin B \cap C$. Ceci contredit le fait que $A \cap C = B \cap C$.

Cas 2. $x \in B \setminus A$. De même, cela conduit à une contradiction.

Nous pouvons donc conclure que $A \Delta B$ et C sont disjoints.

23. (a) Indice : Supposons que $x \in A \setminus C$, puis décomposez la preuve en cas, selon que $x \in B$. (b) Indice : Appliquez la partie (a).

24. (a) Supposons que $x \in (A \cup B) \Delta C$. Alors soit $x \in (A \cup B) \setminus C$ soit $x \in C \setminus (A \cup B)$.

Cas 1. $x \in (A \cup B) \setminus C$. Alors, soit $x \in A$, soit $x \in B$, et $x \notin C$. On divise maintenant le cas 1 en deux sous-cas, selon que $x \in A$ ou $x \in B$:

Cas 1a. $x \in A$. Alors $x \in A \setminus C$, donc $x \in A \Delta C$, donc $x \in (A \Delta C) \cup (B \Delta C)$.

Cas 1b. $x \in B$. De même, $x \in B \Delta C$, donc $x \in (A \Delta C) \cup (B \Delta C)$.

Cas 2. $x \in C \setminus (A \cup B)$. Alors $x \in C$, $x \notin A$ et $x \notin B$. Il s'ensuit que $x \in A \Delta C$ et $x \in B \Delta C$, donc certainement $x \in (A \Delta C) \cup (B \Delta C)$.

(b) Voici un exemple : $A = \{1\}$, $B = \{2\}$, $C = \{1, 2\}$.

27. La preuve est incorrecte, car elle établit seulement que $0 < x$ ou $x < 6$, mais ce qui doit être prouvé, c'est que $0 < x$ et $x < 6$. Cependant, cela peut être corrigé.

29. La preuve est correcte.

31. Indice : Voici un contre-exemple au théorème : $A = \{1, 2\}$, $B = \{1\}$, $C = \{2\}$.

Section 3.6

1. Soit x un nombre réel arbitraire. Soit $y = x / (x^2 + 1)$. Alors

$$x - y = x - \frac{x}{x^2 + 1} = \frac{x^3 + x}{x^2 + 1} - \frac{x}{x^2 + 1} = \frac{x^3}{x^2 + 1} = x^2 \cdot \frac{x}{x^2 + 1} = x^2 y.$$

Pour voir que y est unique, supposons que $x^2 z = x - z$. Alors $z(x^2 + 1) = x$, et puisque $x^2 + 1 \neq 0$, nous pouvons diviser les deux côtés par $x^2 + 1$ pour conclure que $z = x / (x^2 + 1) = y$.

4. Supposons que $x \neq 0$. Soit $y = 1/x$. Soit maintenant z un nombre réel arbitraire. Alors $zy = z(1/x) = z/x$, comme requis.

Pour voir que y est unique, supposons que y' soit un nombre possédant la propriété que $\forall z \in \mathbb{R} (zy' = z/x)$. Alors, en particulier, en prenant $z = 1$, nous avons $y' = 1/x$, donc $y' = y$.

6. (a) Soit $A = \emptyset \in \mathcal{P}(U)$. Alors clairement pour tout $B \in \mathcal{P}(U)$, $A \cup B = \emptyset \cup B = B$.

Pour voir que A est unique, supposons que $A' \in \mathcal{P}(U)$ et pour tout $B \in \mathcal{P}(U)$, $A' \cup B = B$. Alors en particulier, en prenant $B = \emptyset$, nous pouvons conclure que $A' \cup \emptyset = \emptyset$. Mais clairement $A' \cup \emptyset = A'$, donc nous avons $A' = \emptyset = A$.

(b) Indice : Soit $A = U$.

11. Existence : On nous donne que pour tout $\mathcal{G} \subseteq \mathcal{F}, \bigcup \mathcal{G} \in \mathcal{F}$, donc en particulier, puisque $\mathcal{F} \subseteq \mathcal{F}, \bigcup \mathcal{F} \in \mathcal{F}$. Let $A = \bigcup \mathcal{F}$. Supposons maintenant $B \in \mathcal{F}$. Puis par l'exercice 8 de la section 3.3, $B \subseteq \bigcup \mathcal{F} = A$, comme requis.

Unicité : Supposons que $A_1 \in \mathcal{F}, A_2 \in \mathcal{F}, \forall B \in \mathcal{F} (B \subseteq A_1)$ et $\forall B \in \mathcal{F} (B \subseteq A_2)$. En appliquant ce dernier fait avec $B = A_1$ nous pouvons conclure que $A_1 \subseteq A_2$, et de même le fait précédent implique que $A_2 \subseteq A_1$. Ainsi $A_1 = A_2$.

Section 3.7

1. Astuce : comparer (b) à l'exercice 16 de la section 3.3 peut vous donner une idée de ce qu'il faut utiliser pour A .

5. Supposons $\mathcal{P}(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} \mathcal{P}(A_i)$, qu'il soit clair que $\bigcup_{i \in I} A_i \subseteq \bigcup_{i \in I} A_i$ ainsi $\bigcup_{i \in I} A_i \in \mathcal{P}(\bigcup_{i \in I} A_i)$ et donc $\bigcup_{i \in I} A_i \in \bigcup_{i \in I} \mathcal{P}(A_i)$. Par définition de l'union d'une famille, cela signifie qu'il existe un $i \in I$ tel que Soit $\bigcup_{i \in I} A_i \subseteq A_i$. maintenant $j \in I$ arbitraire. Alors par l'exercice 8 de la section 3.3, $A_j \subseteq \bigcup_{i \in I} A_i$, donc $A_j \subseteq A_i$.

8. Supposons que $\lim_{x \rightarrow c} f(x) = L > 0$. Soit $\epsilon = L$. Alors, par définition de limite, nous pouvons choisir un $\delta > 0$ tel que pour tout x , si $0 < |x - c| < \delta$ alors $|f(x) - L| < \epsilon = L$. Maintenant, soit x un nombre réel arbitraire et supposons $0 < |x - c| < \delta$. Alors $|f(x) - L| < L$, donc $-L < f(x) - L < L$ et donc $0 < f(x) < 2L$. Par conséquent, pour tout nombre réel x , si $0 < |x - c| < \delta$ alors $f(x) > 0$.

10. La preuve est correcte.

Chapitre 4

Section 4.1

1. (a) $\{(x, y) \in P \times P \mid x \text{ est un parent de } y\} = \{(Bill Clinton, Chelsea Clinton), (Goldie Hawn, Kate Hudson), \dots\}$.
(b) $\{(x, y) \in C \times U \mid \text{il y a quelqu'un qui vit en } x \text{ et fréquente } y\}$. Si vous êtes étudiant à l'université, alors soit x la ville dans laquelle vous vivez, et soit y l'université que vous fréquentez ; (x, y) sera alors un élément de cet ensemble de vérité.

4. $A \times (B \cap C) = (A \times B) \cap (A \times C) = \{(1, 4), (2, 4), (3, 4)\}$,

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C) = \{(1, 1), (2, 1), (3, 1), (1, 3), (2, 3), \\ &\quad (3, 3), (1, 4), (2, 4), (3, 4)\}, \\ (A \times B) \cap (C \times D) &= (A \cap C) \times (B \cap D) = \emptyset, \\ (A \times B) \cup (C \times D) &= \{(1, 1), (2, 1), (3, 1), (1, 4), (2, 4), (3, 4), (3, 5), (4, 5)\}, \\ (A \cup C) \times (B \cup D) &= \{(1, 1), (2, 1), (3, 1), (4, 1), (1, 4), (2, 4), (3, 4), (4, 4), \\ &\quad (1, 5), (2, 5), (3, 5), (4, 5)\}. \end{aligned}$$

6. Les cas ne sont pas exhaustifs.

8. Oui, c'est vrai.

10. Supposons que $(x, y) \in (A \setminus C) \times (B \setminus D)$. Alors $x \in A \setminus C$ et $y \in B \setminus D$, ce qui signifie $x \in A$, $x \notin C$, $y \in B$ et $y \notin D$. Puisque $x \in A$ et $y \in B$, $(x, y) \in A \times B$. Et puisque $x \notin C$, $(x, y) \notin C \times D$. Par conséquent $(x, y) \in (A \times B) \setminus (C \times D)$.

15. Le théorème est incorrect. Contre-exemple : $A = \{1\}$, $B = C = D = \emptyset$. Remarquez que $A \not\subseteq C$. Où est l'erreur dans la preuve que $A \subseteq C$?

Section 4.2

1. (a) Domaine = $\{p \in P \mid p \text{ a un enfant vivant}\}$; Plage = $\{p \in P \mid p \text{ a un parent vivant}\}$.

(b) Domaine = \mathbb{R} ; Portée = \mathbb{R}^+ .

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

(b) $\{(4, 4), (5, 5), (5, 6), (6, 5), (6, 6)\}$.

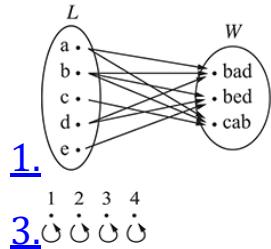
8. $E \circ E \subseteq F$.

11. Nous démontrons les contraposées des deux directions.

(\rightarrow) Supposons que $\text{Ran}(R)$ et $\text{Dom}(S)$ ne soient pas disjoints. Alors on peut choisir un $b \in \text{Ran}(R) \cap \text{Dom}(S)$. Puisque $b \in \text{Ran}(R)$, on peut choisir un $a \in A$ tel que $(a, b) \in R$. De même, puisque $b \in \text{Dom}(S)$, on peut choisir un $c \in C$ tel que $(b, c) \in S$. Mais alors $(a, c) \in S \circ R$, donc $S \circ R \neq \emptyset$.

(\leftarrow) Supposons que $S \circ R \neq \emptyset$. Alors on peut choisir des $(a, c) \in S \circ R$. Par définition de $S \circ R$, cela signifie qu'on peut choisir des $b \in B$ tels que $(a, b) \in R$ et $(b, c) \in S$. Mais alors $b \in \text{Ran}(R)$ et $b \in \text{Dom}(S)$, donc $\text{Ran}(R)$ et $\text{Dom}(S)$ ne sont pas disjoints.

Section 4.3



5. $S \circ R = \{(a, y), (a, z), (b, x), (c, y), (c, z)\}$.

7. (\rightarrow) Supposons que R soit réflexif. Soit (x, y) un élément arbitraire de i_A . Alors, par définition de i_A , $x = y \in A$. Puisque R est réflexif, $(x, y) = (x, x) \in R$. Puisque (x, y) est arbitraire, cela montre que $i_A \subseteq R$.

(\leftarrow) Supposons que $i_A \subseteq R$. Soit $x \in A$ arbitraire. Alors $(x, x) \in i_A$, donc puisque $i_A \subseteq R$, $(x, x) \in R$. Puisque x est arbitraire, cela montre que R est réflexif.

10. Supposons que $(x, y) \in i_D$. Alors $x = y \in D = \text{Dom}(S)$, donc il existe un $z \in A$ tel que $(x, z) \in S$. Par conséquent $(z, x) \in S^{-1}$, donc $(x, y) = (x, x) \in S^{-1} \circ S$. Ainsi, $i_D \subseteq S^{-1} \circ S$. La preuve de l'autre affirmation est similaire.

13. (a) Oui. Pour le prouver, supposons que R_1 et R_2 soient réflexifs, et supposons que $a \in A$. Puisque R_1 est réflexif, $(a, a) \in R_1$, donc $(a, a) \in R_1 \cup R_2$.

(b) Oui. Pour le prouver, supposons que R_1 et R_2 sont symétriques, et supposons $(x, y) \in R_1 \cup R_2$. Alors soit $(x, y) \in R_1$ soit $(x, y) \in R_2$. Si $(x, y) \in R_1$ alors puisque R_1 est symétrique, $(y, x) \in R_1$, donc $(y, x) \in R_1 \cup R_2$. Un raisonnement similaire montre que si $(x, y) \in R_2$ alors $(y, x) \in R_1 \cup R_2$.

(c) Non. Contre-exemple : $A = \{1, 2, 3\}$, $R_1 = \{(1, 2)\}$, $R_2 = \{(2, 3)\}$.

17. Notons d'abord que, selon la partie 2 du [théorème 4.3.4](#), puisque R et S sont symétriques, $R = R^{-1}$ et $S = S^{-1}$. Par conséquent

$$\begin{aligned} R \circ S \text{ is symmetric iff } & R \circ S = (R \circ S)^{-1} \\ \text{iff } & R \circ S = S^{-1} \circ R^{-1} \\ \text{iff } & R \circ S = S \circ R. \end{aligned}$$

([Théorème 4.3.4](#), partie 2)

([Théorème 4.2.5](#), partie 5)

20. Supposons que R soit transitif, et supposons que $(X, Y) \in S$ et $(Y, Z) \in S$. Pour prouver que $(X, Z) \in S$, il faut montrer que $\forall x \in X \forall z \in Z (xRz)$, donc soient $x \in X$ et $z \in Z$ arbitraires. Puisque $Y \in B$, $Y \neq \emptyset$, on peut donc choisir $y \in Y$. Puisque $(X, Y) \in S$ et $(Y, Z) \in S$, par définition de S , on a xRy et yRz . Mais puisque R est transitif, xRz , comme requis. L'ensemble vide a dû être exclu de B pour que nous puissions obtenir $y \in Y$ dans cette preuve. (Pouvez-vous trouver un contre-exemple où l'ensemble vide n'est pas exclu ?)
23. Indice : Supposons aRb et bRc . Pour prouver aRc , supposons que $X \subseteq A \setminus \{a, c\}$ et $X \cup \{a\} \in \mathcal{F}$; vous devez prouver que $X \cup \{c\} \in \mathcal{F}$. Pour ce faire, vous pouvez considérer deux cas : $b \notin X$ ou $b \in X$. Dans le second cas, essayez de travailler avec les ensembles $X' = (X \cup \{a\}) \setminus \{b\}$ et $X'' = (X \cup \{c\}) \setminus \{b\}$.

Section 4.4

1. (a) Ordre partiel, mais pas ordre total. (b) Pas un ordre partiel. (c) Ordre partiel, mais pas ordre total.

4. (\rightarrow) Supposons que R soit à la fois antisymétrique et symétrique. Supposons que $(x, y) \in R$. Alors puisque R est symétrique, $(y, x) \in R$, et puisque R est antisymétrique, il s'ensuit que $x = y$. Par conséquent $(x, y) \in i_A$. Puisque (x, y) était arbitraire, cela montre que $R \subseteq i_A$.

(\leftarrow) Supposons que $R \subseteq i_A$. Supposons que $(x, y) \in R$. Alors $(x, y) \in i_A$, donc $x = y$, et donc $(y, x) = (x, y) \in R$. Ceci montre que R est symétrique. Pour voir que R est antisymétrique, supposons que $(x, y) \in R$ et $(y, x) \in R$. Alors $(x, y) \in i_A$, donc $x = y$.

8. Pour voir que T est réflexif, considérons un arbitraire $(a, b) \in A \times B$. Puisque R et S sont tous deux réflexifs, nous avons aRa et bSb . Par définition de T , il s'ensuit que $(a, b) T (a, b)$. Pour voir que T est antisymétrique, supposons que $(a, b) T (a', b')$ et $(a', b') T (a, b)$. Alors aRa' et $a'Ra$, donc puisque R est antisymétrique, $a = a'$. De même, bSb' et $b'Sb$, donc puisque S est antisymétrique, nous avons aussi $b = b'$. Ainsi $(a, b) = (a', b')$, comme requis. Enfin, pour voir que T est transitif, supposons que $(a, b) T (a', b')$ et $(a', b') T (a'', b'')$. Alors aRa' et $a'Ra''$, donc puisque R est transitif,

aRa ". De même, bSb' et $b'Sb''$, donc bSb'' , et donc $(a, b) T (a'', b'')$.

Même si R et S sont tous deux des ordres totaux, T n'a pas besoin d'être un ordre total.

11. Les éléments minimaux de B sont les nombres premiers. B n'a pas de plus petit élément.

14. (a) b est le R -plus grand élément de B

$$\begin{aligned} &\text{iff } b \in B \text{ and } \forall x \in B (x R b) \\ &\text{iff } b \in B \text{ and } \forall x \in B (b R^{-1} x) \\ &\text{iff } b \text{ is the } R^{-1}\text{-smallest element of } B. \end{aligned}$$

(b) b est un élément R -maximal de B

$$\begin{aligned} &\text{iff } b \in B \text{ and } \neg \exists x \in B (b R x \wedge b \neq x) \\ &\text{iff } b \in B \text{ and } \neg \exists x \in B (x R^{-1} b \wedge x \neq b) \\ &\text{iff } b \text{ is an } R^{-1}\text{-minimal element of } B. \end{aligned}$$

17. Non. Soit $A = \mathbb{R} \times \mathbb{R}$, et soit $R = \{((x, y), (x', y')) \in A \times A \mid x \leq x' \text{ et } y \leq y'\}$. (Vous pourriez vouloir comparer cela à [l'exercice 8.](#)) Soit $B = \{(0, 0)\} \cup (\{1\} \times \mathbb{R})$. Nous vous laisserons le soin de vérifier que R est un ordre partiel sur A , et que $(0, 0)$ est le seul élément minimal de B , mais qu'il n'est pas un plus petit élément.

21. (a) Supposons que $x \in U$ et xRy . Pour prouver que $y \in U$, il faut montrer que y est un majorant pour B ; supposons donc que $b \in B$. Puisque $x \in U$, x est un majorant pour B ; d'où bRx . Mais on a aussi xRy ; par la transitivité de R , on peut donc conclure que bRy . Puisque b est arbitraire, cela montre que y est un majorant pour B .

(b) Supposons que $b \in B$. Pour prouver que b est une borne inférieure pour U , soit x un élément quelconque de U . Alors, par définition de U , x est une borne supérieure pour B , donc bRx . Puisque x est arbitraire, cela montre que b est une borne inférieure pour U .

(c) Indice : Supposons que x soit la plus grande borne inférieure de U . Utilisez d'abord la partie (b) pour montrer que x est une borne supérieure de B , et donc $x \in U$. Utilisez ensuite le fait que x soit une borne inférieure de U pour montrer que x est le plus petit élément de U ; autrement dit, c'est la plus petite borne supérieure de B .

24. (a) Supposons que $(x, y) \in S$. Alors soit $(x, y) \in R$, soit $(x, y) \in R^{-1}$. Si $(x, y) \in R$, alors $(y, x) \in R^{-1}$, donc $(y, x) \in S$. Si $(x, y) \in R^{-1}$, alors $(y, x) \in R$, donc $(y, x) \in S$. Par conséquent, S est symétrique. Puisque $S = R \cup R^{-1}$, il est clair que $R \subseteq S$.

(b) Supposons que T soit une relation symétrique sur A et $R \subseteq T$. Pour montrer que $S \subseteq T$, soit (x, y) un élément arbitraire de S . Alors soit $(x, y) \in R$ soit $(x, y) \in R^{-1}$. Si $(x, y) \in R$, alors puisque $R \subseteq T$,

$(x, y) \in T$. Si $(x, y) \in R^{-1}$, alors $(y, x) \in R$, donc puisque $R \subseteq T$, $(y, x) \in T$. Mais T est symétrique, il s'ensuit que $(x, y) \in T$.

27. (a) Tout d'abord, notons que $R_1 \subseteq R$ et $R_2 \subseteq R$. Il s'ensuit, par [l'exercice 26](#), que $S_1 \subseteq S$ et $S_2 \subseteq S$, donc $S_1 \cup S_2 \subseteq S$. Pour l'autre direction, notons que $R = R_1 \cup R_2 \subseteq S_1 \cup S_2$, et par [l'exercice 13\(b\) de la section 4.3](#), $S_1 \cup S_2$ est symétrique. Par conséquent, par [l'exercice 24\(b\)](#), $S \subseteq S_1 \cup S_2$.
- (b) En imitant la première moitié de la preuve de la partie (a), nous pouvons utiliser [l'exercice 26](#) pour montrer que $T_1 \cup T_2 \subseteq T$. Cependant, la réponse à [l'exercice 13\(c\) de la section 4.3](#) étant négative, nous ne pouvons pas imiter la seconde moitié de la preuve. En fait, l'exemple donné dans la solution de [l'exercice 13\(c\)](#) fonctionne comme un exemple pour lequel $T_1 \cup T_2 \neq T$.

Section 4.5

1. Voici une liste de toutes les partitions :

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

3. (a) R est une relation d'équivalence. Il existe 26 classes d'équivalence, une pour chaque lettre de l'alphabet. Ces classes d'équivalence sont : l'ensemble des mots commençant par a ; l'ensemble des mots commençant par b ; . . . , l'ensemble des mots commençant par z ;
- (b) S n'est pas une relation d'équivalence, car elle n'est pas transitive.
- (c) T est une relation d'équivalence. Les classes d'équivalence sont : l'ensemble des mots d'une lettre, l'ensemble des mots de deux lettres, etc. Pour tout entier positif n , s'il existe au moins un mot anglais de longueur n , alors l'ensemble des mots de longueur n constitue une classe d'équivalence.
6. L'hypothèse nécessaire est que pour chaque date d , une personne est née à la date d . Que se passerait-il si, par hasard, personne n'était né le 23 avril ? Où cette hypothèse est-elle utilisée dans la démonstration ?
10. Puisque S est la relation d'équivalence déterminée par \mathcal{F} , la preuve du [théorème 4.5.6](#) montre que $A / S = \mathcal{F} = A / R$. La conclusion souhaitée découle maintenant de [l'exercice 9](#).

13. Voir le lemme 7.3.4.

16. Par l'exercice 16(a) de la section 3.5, $\bigcup(\mathcal{F} \cup \mathcal{G}) = (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G}) = A \cup B$. voir que $\mathcal{F} \cup \mathcal{G}$ est deux à deux disjoint, supposons que $X \in \mathcal{F} \cup \mathcal{G}$, $Y \in \mathcal{F} \cup \mathcal{G}$ et $X \cap Y \neq \emptyset$. Si $X \in \mathcal{F}$ et $Y \in \mathcal{G}$ alors $X \subseteq A$ et $Y \subseteq B$, et puisque A et B sont disjoints il s'ensuit que X et Y sont disjoints, ce qui est une contradiction. Ainsi, il ne peut pas être le cas que $X \in \mathcal{F}$ et $Y \in \mathcal{G}$, et un argument similaire peut être utilisé pour exclure la possibilité que $X \in \mathcal{G}$ et $Y \in \mathcal{F}$. Ainsi, X et Y sont soit tous deux des éléments de \mathcal{F} soit tous deux des éléments de \mathcal{G} . S'ils sont tous deux dans \mathcal{F} , alors puisque \mathcal{F} est deux à deux disjoint, $X = Y$. Un argument similaire s'applique s'ils sont tous deux dans \mathcal{G} . Finalement, nous avons $\forall X \in \mathcal{F} (X \neq \emptyset)$ et $\forall X \in \mathcal{G} (X \neq \emptyset)$, et il résulte de l'exercice 8 de la section 2.2 que $\forall X \in \mathcal{F} \cup \mathcal{G} (X \neq \emptyset)$.

20. (a) Voici la preuve de transitivité : Supposons que $(x, y) \in T$ et $(y, z) \in T$. Alors puisque $T = R \cap S$, $(x, y) \in R$ et $(y, z) \in R$, donc puisque R est transitif, $(x, z) \in R$. De même, $(x, z) \in S$, donc $(x, z) \in R \cap S = T$.

(b) Supposons que $x \in A$. Alors pour tout $y \in A$,

$$\begin{aligned} y \in [x]_T &\text{ iff } (y, x) \in T \text{ iff } (y, x) \in R \wedge (y, x) \in S \\ &\text{ iff } y \in [x]_R \wedge y \in [x]_S \text{ iff } y \in [x]_R \cap [x]_S. \end{aligned}$$

(c) Supposons $X \in A / T$. Alors, puisque A / T est une partition, $X \neq \emptyset$. De plus, pour un certain $x \in A$, $X = [x]_T = [x]_R \cap [x]_S$, donc puisque $[x]_R \in A / R$ et $[x]_S \in A / S$, $X \in (A / R) \cdot (A / S)$.

Supposons maintenant $X \in (A / R) \cdot (A / S)$. Alors, pour certains y et z dans A , $X = [y]_R \cap [z]_S$. De plus, $X \neq \emptyset$, nous pouvons donc choisir un certain $x \in X$. Par conséquent $x \in [y]_R$ et $x \in [z]_S$, et par la partie 2 du lemme 4.5.5 il s'ensuit que $[x]_R = [y]_R$ et $[x]_S = [z]_S$. Par conséquent $X = [x]_R \cap [x]_S = [x]_T \in A / T$.

22. $\mathcal{F} \otimes \mathcal{F} = \{\mathbb{R}^+ \times \mathbb{R}^+, \mathbb{R}^- \times \mathbb{R}^+, \mathbb{R}^- \times \mathbb{R}^-, \mathbb{R}^+ \times \mathbb{R}^-, \mathbb{R}^+ \times \{0\}, \mathbb{R}^- \times \{0\}, \{0\} \times \mathbb{R}^+, \{0\} \times \mathbb{R}^-, \{(0, 0)\}\}$. En termes géométriques, ce sont les quatre quadrants du plan, les axes des x positifs et négatifs, les axes des y positifs et négatifs, et l'origine.

24. (a) Indice : Soit $T = \{(X, Y) \in A / S \times A / S \mid \exists x \in X \exists y \in Y (xRy)\}$.
(b) Supposons que $x, y, x', y' \in A$, xSx' et ySy' . Alors $[x]_S = [x']_S$ et $[y]_S = [y']_S$, donc xRy ssi $[x]_S T [y]_S$ ssi $[x']_S T [y']_S$ ssi $x'Ry'$.

Chapitre 5

Section 5.1

1. (a) Oui.

(b) Non.

(c) Oui.

3. (a) $f(a) = b, f(b) = b, f(c) = a$.

(b) $f(2) = 0$.

(c) $f(\pi) = 3$ et $f(-\pi) = -4$.

5. $L \circ H : N \rightarrow N$, et pour tout $n \in N$, $(L \circ H)(n) = n$. Ainsi, $L \circ H = i_N$.

$H \circ L : C \rightarrow C$, et pour tout $c \in C$, $(H \circ L)(c)$ = la capitale du pays dans lequel c est situé.

7. (a) Supposons que $c \in C$. Nous devons prouver qu'il existe un unique $b \in B$ tel que $(c, b) \in f \upharpoonright C$.

Existence : Soit $b = f(c) \in B$. Alors $(c, b) \in f$ et $(c, b) \in C \times B$, et donc $(c, b) \in f \cap (C \times B) = f \upharpoonright C$.

Unicité : Supposons que $(c, b_1) \in f \upharpoonright C$ et $(c, b_2) \in f \upharpoonright C$. Alors $(c, b_1) \in f$ et $(c, b_2) \in f$, donc puisque f est une fonction, $b_1 = b_2$.

Ceci prouve que $f \upharpoonright C$ est une fonction de C vers B . Finalement, pour déduire la formule de $(f \upharpoonright C)(c)$, supposons que $c \in C$ et soit $b = f(c)$. Nous avons montré dans la moitié de la preuve que $(c, b) \in f \upharpoonright C$. Il s'ensuit que

$$f(c) = b = (f \upharpoonright C)(c).$$

(b) (\rightarrow) Supposons $g = f \upharpoonright C$. Alors $g = f \cap (C \times B)$, donc clairement $g \subseteq f$. (\leftarrow) Supposons $g \subseteq f$. Supposons $c \in C$, et soit $b = g(c)$. Alors $(c, b) \in g$, donc $(c, b) \in f$, et donc $f(c) = b$. Mais alors par la partie (a), $(f \upharpoonright C)(c) = f(c) = b = g(c)$. Puisque c était arbitraire, il s'ensuit, d'après le théorème 5.1.4, que $g = f \upharpoonright C$.

(c) $h \upharpoonright \mathbb{Z} = h \cap (\mathbb{Z} \times \mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x + 3\} \cap (\mathbb{Z} \times \mathbb{R}) = \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = 2x + 3\} = g$.

10. Puisque $f \neq g$, d'après le théorème 5.1.4, nous pouvons choisir un $a \in A$ tel que $f(a) \neq g(a)$. Par conséquent, $(a, f(a)) \in f$ et $(a, f(a)) \notin g$, donc par définition de différence symétrique, $(a, f(a)) \in f \Delta g$, et de même $(a, g(a)) \in f \Delta g$. Puisque $f(a) \neq g(a)$, il s'ensuit que $f \Delta g$ n'est pas une fonction.

13. (a) Supposons que $b \in B$. Puisque $\text{Dom}(S) = B$, on sait qu'il existe un $c \in C$ tel que $(b, c) \in S$. Pour voir qu'il est unique, supposons

que $c' \in C$ et $(b, c') \in S$. Puisque $\text{Ran}(R) = B$, on peut choisir un $a \in A$ tel que $(a, b) \in R$. Mais alors $(a, c) \in S \circ R$ et $(a, c') \in S \circ R$, et puisque $S \circ R$ est une fonction, il s'ensuit que $c = c'$.

(b) $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$, $R = \{(1, 2), (1, 3)\}$, $S = \{(2, 4), (3, 4)\}$.

15. (a) Non. Exemple : $A = \{1\}$, $B = \{2, 3\}$, $f = \{(1, 2)\}$, $R = \{(1, 1)\}$.

(b) Oui. Supposons que R soit symétrique. Supposons que $(x, y) \in S$.

Alors nous pouvons choisir des u et v dans A tels que $f(u) = x$, $f(v) = y$, et $(u, v) \in R$. Puisque R est symétrique, $(v, u) \in R$, et donc $(y, x) \in S$.

(c) Non. Exemple : $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7\}$, $f = \{(1, 5), (2, 6), (3, 6), (4, 7)\}$, $R = \{(1, 2), (3, 4)\}$.

19. (a) Soit $a = 3$ et $c = 8$. Alors pour tout $x > a = 3$,

$$|f(x)| = |7x + 3| = 7x + 3 < 7x + x = 8x < 8x^2 = c|g(x)|.$$

Ceci montre que $f \in O(g)$.

Supposons maintenant que $g \in O(f)$. Alors nous pouvons choisir $a \in \mathbb{Z}^+$ et $c \in \mathbb{R}^+$ tels que $\forall x > a (|g(x)| \leq c|f(x)|)$, ou en d'autres termes, $\forall x > a (x^2 \leq c(7x + 3))$. Soit x un entier positif plus grand que a et $10c$. En multipliant les deux côtés de l'inégalité $x > 10c$ par x , nous pouvons conclure que $x^2 > 10cx$. Mais comme $x > a$, nous avons aussi $x^2 \leq c(7x + 3) \leq c(7x + 3x) = 10cx$, nous avons donc atteint une contradiction. Par conséquent $g \notin O(f)$.

(b) Clairement, pour toute fonction $f \in \mathcal{F} \Leftrightarrow$ nous avons $\forall x \in \mathbb{Z}^+ (|f(x)| \leq 1 \cdot |f(x)|)$, donc $f \in O(f)$, et donc $(f, f) \in S$. Ainsi, S est réflexive. Pour voir qu'elle est aussi transitive, supposons $(f, g) \in S$ et $(g, h) \in S$. Alors, il existe des entiers positifs a_1 et a_2 et des réels positifs c_1 et c_2 tels que $\forall x > a_1 (|f(x)| \leq c_1|g(x)|)$ et $\forall x > a_2 (|g(x)| \leq c_2|h(x)|)$. Soit a le maximum de a_1 et a_2 , et soit $c = c_1c_2$. Alors pour tout $x > a$,

$$|f(x)| \leq c_1|g(x)| \leq c_1c_2|h(x)| = c|h(x)|.$$

Français Ainsi, $(f, h) \in S$, donc S est transitif. Finalement, pour voir que S n'est pas un ordre partiel, on montre qu'il n'est pas antisymétrique. Soient f et g les fonctions de \mathbb{Z}^+ dans \mathbb{R} définies par les formules $f(x) = x$ et $g(x) = 2x$. Alors pour tout $x \in \mathbb{Z}^+$, $|f(x)| \leq |g(x)|$ et $|g(x)| \leq 2|f(x)|$, donc $f \in O(g)$ et aussi $g \in O(f)$. Donc $(f, g) \in S$ et $(g, f) \in S$, mais $f \neq g$.

(c) Puisque $f_1 \in O(g)$, on peut choisir $a_1 \in \mathbb{Z}^+$ et $c_1 \in \mathbb{R}^+$ tels que $\forall x > a_1 (|f_1(x)| \leq c_1|g(x)|)$. De même, puisque $f_2 \in O(g)$ on peut

choisir $a_2 \in \mathbb{Z}^+$ et $c_2 \in \mathbb{R}^+$ tels que $\forall x > a_2 (|f_2(x)| \leq c_2 |g(x)|)$. Soit a le maximum de a_1 et a_2 , et soit $c = |s|c_1 + |t|c_2 + 1$. (Nous j'ai ajouté 1 ici juste pour m'assurer que c est positif, comme requis dans la définition de O .) Alors pour tout $x > a$,

$$\begin{aligned}|f(x)| &= |sf_1(x) + tf_2(x)| \leq |s||f_1(x)| + |t||f_2(x)| \\ &\leq |s|c_1|g(x)| + |t|c_2|g(x)| = (|s|c_1 + |t|c_2)|g(x)| \leq c|g(x)|.\end{aligned}$$

Par conséquent $f \in O(g)$.

21. (a) Indice : Soit $h = \{(X, y) \in A / R \times B \mid \exists x \in X (f(x) = y)\}$.
 (b) Astuce : utilisez le fait que pour tous les x et y dans A , si xRy alors $[x]_R = [y]_R$.

Section 5.2

2. (a) f n'est pas une fonction.

(b) f n'est pas une fonction. g est une fonction qui est sur, mais pas bijective.

(c) R est bijectif et sur.

5. (a) Supposons que $x_1 \in A$, $x_2 \in A$ et $f(x_1) = f(x_2)$. On peut alors effectuer les opérations algébriques suivantes :

$$\begin{aligned}\frac{x_1+1}{x_1-1} &= \frac{x_2+1}{x_2-1}, \\ (x_1+1)(x_2-1) &= (x_2+1)(x_1-1), \\ x_1x_2 - x_1 + x_2 - 1 &= x_1x_2 - x_2 + x_1 - 1, \\ 2x_2 &= 2x_1, \\ x_2 &= x_1.\end{aligned}$$

Cela montre que f est bijectif.

Pour montrer que f est sur, supposons que $y \in A$. Soit

$$x = \frac{y+1}{y-1}.$$

Notez que ceci est défini, puisque $y \neq 1$, et aussi clairement $x \neq 1$, donc $x \in A$. Alors

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

(b) Pour tout $x \in A$,

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

9. (a) $\{1, 2, 3, 4\}$.

(b) f est sur, mais pas bijectif.

13. (a) Supposons que f soit bijectif. Supposons que $c_1 \in C, c_2 \in C$ et $(f \upharpoonright C)(c_1) = (f \upharpoonright C)(c_2)$. D'après [l'exercice 7\(a\)](#) de [la section 5.1](#), il s'ensuit que $f(c_1) = f(c_2)$, donc puisque f est bijectif, $c_1 = c_2$.

(b) Supposons que $f \upharpoonright C$ soit sur. Supposons que $b \in B$. Alors puisque $f \upharpoonright C$ est sur, on peut choisir un $c \in C$ tel que $(f \upharpoonright C)(c) = b$. Mais alors $c \in A$, et par [l'exercice 7\(a\)](#) de [la section 5.1](#), $f(c) = b$.

(c) Soit $A = B = \mathbb{R}$ et $C = \mathbb{R}^+$. Pour (a), utilisez $f(x) = |x|$, et pour (b), utilisez $f(x) = x$.

17. (a) Supposons que R soit réflexif et f sur. Soit $x \in B$ arbitraire. Puisque f est sur, on peut choisir un $u \in A$ tel que $f(u) = x$. Puisque R est réflexif, $(u, u) \in R$. Par conséquent $(x, x) \in S$.

(b) Supposons que R soit transitif et f soit bijectif. Supposons que $(x, y) \in S$ et $(y, z) \in S$. Puisque $(x, y) \in S$, on peut choisir des u et v dans A tels que $f(u) = x, f(v) = y$, et $(u, v) \in R$. De même, puisque $(y, z) \in S$, on peut choisir p et q dans A tels que $f(p) = y, f(q) = z$, et $(p, q) \in R$. Puisque $f(v) = y = f(p)$ et f est bijectif, $v = p$. Par conséquent $(v, q) = (p, q) \in R$. Puisque nous avons aussi $(u, v) \in R$, par la transitivité de R il s'ensuit que $(u, q) \in R$, donc $(x, z) \in S$.

20. (a) Soit $b \in B$ arbitraire. Puisque f est sur, on peut choisir un $a \in A$ tel que $f(a) = b$. Par conséquent $g(b) = (g \circ f)(a) = (h \circ f)(a) = h(b)$. Puisque b est arbitraire, cela montre que $\forall b \in B (g(b) = h(b))$, donc $g = h$.

(b) Soient c_1 et c_2 deux éléments distincts de C . Supposons $b \in B$. Soient g et h des fonctions de B dans C telles que $\forall x \in B (g(x) = c_1), \forall x \in B \setminus \{b\} (h(x) = c_1)$, et $h(b) = c_2$. (Formellement, $g = B \times \{c_1\}$ et $h = [(B \setminus \{b\}) \times \{c_1\}] \cup \{(b, c_2)\}$.) Alors $g \neq h$, donc par hypothèse $g \circ f \neq h \circ f$, et donc on peut choisir un $a \in A$ tel que $g(f(a)) \neq h(f(a))$. Mais par la façon dont g et h ont été définis, le seul $x \in B$ pour lequel $g(x) \neq h(x)$ est $x = b$, il s'ensuit donc que $f(a) = b$. Puisque b était arbitraire, cela montre que f est sur.

Section 5.3

1. $R^{-1}(p)$ = la personne assise immédiatement à droite de p .

3. Soit $g(x) = (3x - 5)/2$. Alors, pour tout $x \in R$

$$f(g(x)) = \frac{2(3x - 5)/2 + 5}{3} = \frac{3x - 5 + 5}{3} = \frac{3x}{3} = x$$

et

$$g(f(x)) = \frac{3(2x+5)/3 - 5}{2} = \frac{2x+5 - 5}{2} = \frac{2x}{2} = x.$$

Par conséquent, $f \circ g = i_{\mathbb{R}}$ et $g \circ f = i_{\mathbb{R}}$, et d'après [les théorèmes 5.3.4](#) et [5.3.5](#), il s'ensuit que f est bijectif et sur et $f^{-1} = g$.

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

9. Supposons que $f : A \rightarrow B$, $g : B \rightarrow A$ et $f \circ g = i_B$. Soit b un élément arbitraire de B . Soit $a = g(b) \in A$. Alors $f(a) = f(g(b)) = (f \circ g)(b) = i_B(b) = b$. Puisque b est arbitraire, cela montre que f est sur.

11. (a) Supposons que f soit bijectif et que $f \circ g = i_B$. D'après la deuxième partie du [théorème 5.3.3](#), f est également sur, donc $f^{-1} : B \rightarrow A$ et $f^{-1} \circ f = i_A$. Cela nous donne suffisamment d'informations pour reproduire le raisonnement de la preuve du [théorème 5.3.5](#):

$$g = i_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ i_B = f^{-1}.$$

(b) Indice : imitez la solution de la partie (a).

(c) Astuce : utilisez les parties (a) et (b), ainsi que le théorème 5.3.3.

14. (a) Supposons que $x \in A' = \text{Ran}(g)$. Alors nous pouvons choisir un $b \in B$ tel que $g(b) = x$. Par conséquent $(g \circ f)(x) = g(f(g(b))) = g((f \circ g)(b)) = g(i_B(b)) = g(b) = x$.

(b) Par les informations données, $(f \upharpoonright A') \circ g = i_B$, et par la partie (a), $g \circ (f \upharpoonright A') = i_{A'}$. Par conséquent, par [le théorème 5.3.4](#), $f \upharpoonright A'$ est une fonction bijective, sur de A' vers B , et par [le théorème 5.3.5](#), $g = (f \upharpoonright A')^{-1}$.

16. Indice : Supposons que $x \in \mathbb{R}$, $\mathbb{P} \times \approx$ dé \approx e \backslash > $\exists \times e \backslash \sim \exists x \in \text{Ran}(f)$ ou non , vous devez chercher un nombre réel y tel que $f(y) = x$. Autrement dit, vous devez essayer de résoudre l'équation $4y - y^2 = x$ pour y en fonction de x . Notez que cette méthode est similaire à celle utilisée dans la partie 1 de [l'exemple 5.3.6](#) . Cependant, dans ce cas, vous constaterez que pour certaines valeurs de x , il n'existe pas de solution pour y , et que pour certaines valeurs de x , il existe plusieurs solutions pour y .

18. Puisque g est bijectif et sur, $g^{-1} : C \rightarrow B$. Soit $h = g^{-1} \circ f$. Alors $h : A \rightarrow B$ et

$$\begin{aligned}
 g \circ h &= g \circ (g^{-1} \circ f) \\
 &= (g \circ g^{-1}) \circ f \\
 &= i_C \circ f \\
 &= f
 \end{aligned}$$

(Théorème 4.2.5)

([Théorème 5.3.2](#))
([exercice 9 de la section 4.3](#)).

Section 5.4

1. (a) Non.

(b) Oui.

(c) Oui.

(d) Non.

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

7. Supposons que $C \subseteq A$ et que C soit fermé par f . Supposons que $x \in A \setminus C$, donc $x \in A$ et $x \notin C$. Alors $f^{-1}(x) \in A$. Supposons que $f^{-1}(x) \in C$. Alors puisque C est fermé par f , $x = f(f^{-1}(x)) \in C$, ce qui est une contradiction. Par conséquent $f^{-1}(x) \notin C$, donc $f^{-1}(x) \in A \setminus C$. Puisque x est un élément arbitraire de $A \setminus C$, cela montre que $A \setminus C$ est fermé par f^{-1} .

9. (a) Supposons que $x \in C_1 \cup C_2$. Alors soit $x \in C_1$ soit $x \in C_2$.

Cas 1. $x \in C_1$. Alors puisque C_1 est fermé par f , $f(x) \in C_1$, donc $f(x) \in C_1 \cup C_2$.

Cas 2. $x \in C_2$. Alors puisque C_2 est fermé sous f , $f(x) \in C_2$, donc $f(x) \in C_1 \cup C_2$.

Par conséquent $f(x) \in C_1 \cup C_2$. Puisque x est arbitraire, nous pouvons conclure que $C_1 \cup C_2$ est fermé sous f .

(b) Oui. Preuve : Supposons que $x \in C_1 \cap C_2$. Alors $x \in C_1$ et $x \in C_2$.

Puisque $x \in C_1$ et C_1 est fermé par f , $f(x) \in C_1$. De même, $f(x) \in C_2$. Par conséquent $f(x) \in C_1 \cap C_2$, donc puisque x est arbitraire, $C_1 \cap C_2$ est fermé par f .

(c) Non. Voici un contre-exemple : $A = \{1, 2\}$, $f = \{(1, 2), (2, 2)\}$, $C_1 = \{1, 2\}$, $C_2 = \{2\}$.

12. (a) \mathbb{Z} .

(b) $\{X \subseteq \mathbb{N} \mid X \text{ est fini}\}$.

14. \mathbb{Z} .

17. (a) Oui.

(b) Oui.

(c) Oui.

(d) Non. (La composition de deux fonctions strictement décroissantes est strictement croissante.)

20. (b) et (e) sont fermés sous f .

Chapitre 6

Section 6.1

1. Cas de base : lorsque $n = 0$, les deux côtés de l'équation sont 0.

Étape d'induction : Supposons que $n \in \mathbb{N}$ et $0+1+2+\cdots+n = n(n+1)/2$. Alors

$$\begin{aligned}0 + 1 + 2 + \cdots + (n+1) &= (0 + 1 + 2 + \cdots + n) + (n+1) \\&= \frac{n(n+1)}{2} + (n+1) \\&= (n+1)\left(\frac{n}{2} + 1\right) = \frac{(n+1)(n+2)}{2},\end{aligned}$$

selon les besoins.

3. Cas de base : lorsque $n = 0$, les deux côtés de l'équation sont 0.

Étape d'induction : Supposons que $n \in \mathbb{N}$ et $0^3 + 1^3 + 2^3 + \cdots + n^3 = [n(n+1)/2]^2$. Alors

$$\begin{aligned}0^3 + 1^3 + 2^3 + \cdots + (n+1)^3 &= (0^3 + 1^3 + 2^3 + \cdots + n^3) + (n+1)^3 \\&= \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 \\&= (n+1)^2 \left[\frac{n^2}{4} + n + 1\right] \\&= (n+1)^2 \cdot \frac{n^2 + 4n + 4}{4} \\&= \left[\frac{(n+1)(n+2)}{2}\right]^2.\end{aligned}$$

7. Indice : la formule est $(3^{n+1} - 1)/2$.

10. Cas de base : Lorsque $n = 0$, $9^n - 8n - 1 = 0 = 64 \cdot 0$, donc $64 \mid (9^n - 8n - 1)$.

Étape d'induction : Supposons que $n \in \mathbb{N}$ et $64 \mid (9^n - 8n - 1)$. Il existe alors un entier k tel que $9^n - 8n - 1 = 64k$. Par conséquent

$$\begin{aligned}9^{n+1} - 8(n+1) - 1 &= 9^{n+1} - 8n - 9 \\&= 9^{n+1} - 72n - 9 + 64n \\&= 9(9^n - 8n - 1) + 64n \\&= 9(64k) + 64n \\&= 64(9k + n),\end{aligned}$$

donc $64 \mid (9^{n+1} - 8(n+1) - 1)$.

12. (a) Cas de base : lorsque $n = 0$, $7^n - 5^n = 0 = 2 \cdot 0$, donc $7^n - 5^n$ est pair.

Étape d'induction : Supposons que $n \in \mathbb{N}$ et que $7^n - 5^n$ soit pair. Il existe alors un entier k tel que $7^n - 5^n = 2k$. Par conséquent

$$\begin{aligned} 7^{n+1} - 5^{n+1} &= 7 \cdot 7^n - 5 \cdot 5^n = 2 \cdot 7^n + 5 \cdot (7^n - 5^n) \\ &= 2 \cdot 7^n + 5 \cdot 2k = 2(7^n + 5k), \end{aligned}$$

donc $7^{n+1} - 5^{n+1}$ est pair.

- (b) Pour l'étape d'induction, vous pourriez trouver utile de compléter l'équation suivante : $2 \cdot 7^{n+1} - 3 \cdot 5^{n+1} + 1 = 2 \cdot 7^n - 3 \cdot 5^n + 1 + \underline{\quad}$.

15. Cas de base : lorsque $n = 10$, $2^n = 1024 > 1000 = n^3$.

Étape d'induction : Supposons que $n \geq 10$ et $2^n > n^3$. Alors

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2n^3 && \text{(inductive hypothesis)} \\ &= n^3 + n^3 \\ &\geq n^3 + 10n^2 && \text{(since } n \geq 10\text{)} \\ &= n^3 + 3n^2 + 7n^2 \\ &\geq n^3 + 3n^2 + 70n && \text{(since } n \geq 10\text{)} \\ &= n^3 + 3n^2 + 3n + 67n \\ &> n^3 + 3n^2 + 3n + 1 = (n+1)^3. \end{aligned}$$

20. (a) Cas de base : Lorsque $n = 1$, l'énoncé à prouver est $0 < a < b$, ce qui a été donné.

Étape d'induction : Supposons que $n \geq 1$ et $0 < a^n < b^n$. En multipliant cette inégalité par le nombre positif a , on obtient $0 < a^{n+1} < ab^n$, et en multipliant l'inégalité $a < b$ par le nombre positif b^n , on obtient $ab^n < b^{n+1}$. En combinant ces inégalités, on peut conclure que $0 < a^{n+1} < b^{n+1}$.

- (b) Indice : Notez d'abord que $\sqrt[n]{a}$ et $\sqrt[n]{b}$ sont tous deux positifs. (Pour n impair, cela découle de [l'exercice 19](#). Pour n pair, chacun de a et b a deux racines n -ièmes, une positive et une négative, mais $\sqrt[n]{a}$ et $\sqrt[n]{b}$ sont par définition les racines positives.) Utilisez maintenant la preuve par contradiction et appliquez la partie (a).
- (c) Indice : L'inégalité à prouver peut être réorganisée pour se lire $a^{n+1} - ab^n - ba^n + b^{n+1} > 0$. Factorisez maintenant le côté gauche de cette inégalité.
- (d) Indice : Utiliser l'induction mathématique. Pour le cas de base, utiliser le cas $n = 1$ de la partie (c). Pour l'étape d'induction, multiplier les deux côtés de l'hypothèse inductive par $(a+b)/2$, puis appliquer la partie (c).

Section 6.2

1. (a) Il faut prouver que R' est réflexif (sur A'), transitif et antisymétrique. Pour le premier, supposons $x \in A'$. Puisque R est réflexif (sur A') et $x \in A'$, $(x, x) \in R$, alors $(x, x) \in R \cap (A' \times A') = R'$. Ceci montre que R' est réflexif.

Ensuite, supposons que $(x, y) \in R'$ et $(y, z) \in R'$. Alors $(x, y) \in R$, $(y, z) \in R$ et $x, y, z \in A'$. Puisque R est transitif, $(x, z) \in R$, donc $(x, z) \in R \cap (A' \times A') = R'$. Par conséquent, R' est transitif.

Enfin, supposons que $(x, y) \in R'$ et $(y, x) \in R'$. Alors $(x, y) \in R$ et $(y, x) \in R$, donc puisque R est antisymétrique, $x = y$. Ainsi R' est antisymétrique.

(b) Pour voir que T est réflexif, supposons $x \in A$. Si $x = a$, alors $(x, x) = (a, a) \in \{a\} \times A \subseteq T$. Si $x \neq a$, alors $x \in A'$, donc puisque R' est réflexif, $(x, x) \in R' \subseteq T' \subseteq T$.

Pour la transitivité, supposons que $(x, y) \in T$ et $(y, z) \in T$. Si $x = a$ alors $(x, z) = (a, z) \in \{a\} \times A \subseteq T$. Supposons maintenant que $x \neq a$. Alors $(x, y) \notin \{a\} \times A$, donc puisque $(x, y) \in T = T' \cup (\{a\} \times A)$ nous devons avoir $(x, y) \in T'$. Mais $T' \subseteq A' \times A'$, donc $y \in A'$ et donc $y \neq a$. Un raisonnement similaire montre maintenant que $(y, z) \in T'$. Puisque T' est transitif, il s'ensuit que $(x, z) \in T' \subseteq T$.

Pour montrer que T est antisymétrique, supposons $(x, y) \in T$ et $(y, x) \in T$. Si $x = a$ alors $(y, x) \notin T'$, donc $(y, x) \in \{a\} \times A$ et donc $y = a = x$. De même, si $y = a$ alors $x = y$. Supposons maintenant que $x \neq a$ et $y \neq a$. Alors, comme dans la preuve de transitivité, il s'ensuit que $(x, y) \in T'$ et $(y, x) \in T'$, donc par antisymétrie de T' , $x = y$.

Français Nous savons maintenant que T est un ordre partiel. Pour voir qu'il est total, supposons $x \in A$ et $y \in A$. Si $x = a$ alors $(x, y) \in \{a\} \times A \subseteq T$. De même, si $y = a$ alors $(y, x) \in T$. Supposons maintenant $x \neq a$ et $y \neq a$. Alors $x \in A'$ et $y \in A'$, donc puisque T' est un ordre total, soit $(x, y) \in T' \subseteq T$ soit $(y, x) \in T' \subseteq T$.

Finalement, pour voir que $R \subseteq T$, supposons que $(x, y) \in R$. Si $x = a$ alors $(x, y) \in \{a\} \times A \subseteq T$. Supposons maintenant que $x \neq a$. Si $y = a$ alors le fait que $(x, y) \in R$ contredirait la R -minimalité de a . Par conséquent $y \neq a$. Mais alors $(x, y) \in R \cap (A' \times A') = R' \subseteq T' \subseteq T$.

4. (a) Nous allons démontrer l'affirmation : $\forall n \geq 1 \forall B \subseteq A [B \text{ a } n \text{ éléments} \rightarrow \exists x \in B \forall y \in B ((x, y) \in R \circ R)]$. Nous procérons par récurrence sur n .

Cas de base : Supposons que $n = 1$. Si $B \subseteq A$ et B a un élément, alors pour un certain $x \in B$, $B = \{x\}$. Puisque R est réflexif, $(x, x) \in R$, et donc $(x, x) \in R \circ R$. Mais x est le seul élément de B , donc $\forall y \in B ((x, y) \in R \circ R)$, comme requis.

Étape d'induction : Supposons que $n \geq 1$ et pour tout $B \subseteq A$, si B a n éléments alors $\exists x \in B \forall y \in B ((x, y) \in R \circ R)$. Supposons maintenant que $B \subseteq A$ et B a $n + 1$ éléments. Choisissons un certain $b \in B$, et soit $B' = B \setminus \{b\}$. Alors $B' \subseteq A$ et B' a n éléments, donc par hypothèse inductive il existe un certain $x \in B'$ tel que $\forall y \in B' ((x, y) \in R \circ R)$. Nous considérons maintenant deux cas.

Cas 1 : $(x, b) \in R \circ R$. Alors $\forall y \in B ((x, y) \in R \circ R)$, nous avons donc terminé.

Cas 2 : $(x, b) \notin R \circ R$. Dans ce cas, nous allons prouver que $\forall y \in B ((b, y) \in R \circ R)$. Pour ce faire, soit $y \in B$ arbitraire. Si $y = b$, alors comme R est réflexif, $(b, b) \in R$, et donc $(b, y) = (b, b) \in R \circ R$. Supposons maintenant que $y \neq b$. Alors $y \in B'$, donc par le choix de x nous savons que $(x, y) \in R \circ R$. Cela signifie que pour un certain $z \in A$, $(x, z) \in R$ et $(z, y) \in R$. Nous avons $(x, z) \in R$, donc si $(z, b) \in R$ alors $(x, b) \in R \circ R$, contrairement à l'hypothèse pour ce cas. Par conséquent $(z, b) \notin R$, donc par hypothèse sur R , $(b, z) \in R$. Mais alors puisque $(b, z) \in R$ et $(z, y) \in R$, nous avons $(b, y) \in R \circ R$, comme requis.

(b) Indice : Soit $A = B =$ l'ensemble des concurrents et soit $R = \{(x, y) \in A \times A \mid x \text{ bat } y\} \cup i_A$. Appliquez maintenant la partie (a).

8. (a) Soit $m = (a + b)/2$, la moyenne arithmétique de a et b , et soit $d = (a - b)/2$. Il est alors facile de vérifier que $m + d = a$ et $m - d = b$, donc

$$\sqrt{ab} = \sqrt{(m+d)(m-d)} = \sqrt{m^2 - d^2} \leq \sqrt{m^2} = m = \frac{a+b}{2}.$$

(b) Nous utilisons l'induction sur n .

Cas de base : $n = 1$. Ce cas est traité par la partie (a).

Étape d'induction : Supposons que $n \geq 1$ et que l'inégalité moyenne arithmétique-moyenne géométrique soit vraie pour des listes de longueur 2^n . Soit maintenant $a_1, a_2, \dots, a_{2^{n+1}}$ une liste de 2^{n+1} nombres réels positifs. Soit

$$m_1 = \frac{a_1 + a_2 + \dots + a_{2^n}}{2^n}, \quad m_2 = \frac{a_{2^n+1} + a_{2^n+2} + \dots + a_{2^{n+1}}}{2^n}.$$

On remarque que $a_1 + a_2 + \dots + a_{2^n} = m_1 2^n$, et de même $a_{2^n+1} + a_{2^n+2} + \dots + a_{2^{n+1}} = m_2 2^n$. De plus, par l'hypothèse inductive, nous savons que $m_1 \geq \sqrt[n]{a_1 a_2 \cdots a_{2^n}}$ et $m_2 \geq \sqrt[n]{a_{2^n+1} a_{2^n+2} \cdots a_{2^{n+1}}}$. Par conséquent

$$\begin{aligned} \frac{a_1 + a_2 + \dots + a_{2^{n+1}}}{2^{n+1}} &= \frac{m_1 2^n + m_2 2^n}{2^{n+1}} = \frac{m_1 + m_2}{2} \geq \sqrt{m_1 m_2} \\ &\geq \sqrt{\sqrt[2^n]{a_1 a_2 \cdots a_{2^n}} \sqrt[2^n]{a_{2^n+1} a_{2^n+2} \cdots a_{2^{n+1}}}} \\ &= \sqrt[2^{n+1}]{a_1 a_2 \cdots a_{2^{n+1}}}. \end{aligned}$$

(c) Nous utilisons l'induction sur n .

Cas de base : si $n = n_0$, alors par hypothèse l'inégalité moyenne arithmétique-moyenne géométrique échoue pour une liste de longueur n .

Étape d'induction : Supposons que $n \geq n_0$, et qu'il existe des nombres réels positifs a_1, a_2, \dots, a_n tels que

$$\frac{a_1 + a_2 + \dots + a_n}{n} < \sqrt[n]{a_1 a_2 \dots a_n}.$$

Soit $m = (a_1 + a_2 + \dots + a_n)/n$, et soit $a_{n+1} = m$. Alors nous avons $m < \sqrt[n]{a_1 a_2 \dots a_n}$, donc $m^n < a_1 a_2 \dots a_n$. En multipliant les deux côtés de cette inégalité par m , on obtient $m^{n+1} < a_1 a_2 \dots a_n m = a_1 a_2 \dots a_{n+1}$, donc $m < \sqrt[n+1]{a_1 a_2 \dots a_{n+1}}$. Mais remarquez que nous avons aussi $mn = a_1 + a_2 + \dots + a_n$, donc

$$\frac{a_1 + \dots + a_{n+1}}{n+1} = \frac{mn + m}{n+1} = \frac{m(n+1)}{n+1} = m < \sqrt[n+1]{a_1 a_2 \dots a_{n+1}}.$$

Nous avons donc une liste de longueur $n+1$ pour laquelle l'inégalité moyenne arithmétique – moyenne géométrique échoue.

(d) Supposons que l'inégalité moyenne arithmétique-moyenne géométrique soit invalide pour une liste de nombres réels positifs. Soit n_0 la longueur de cette liste, et choisissons un entier $n \geq 1$ tel que $n_0 \leq 2^n$. (En fait, nous pourrions simplement poser $n = n_0$, comme vous le montrerez dans [l'exercice 12\(a\) de la section 6.3](#).) Alors, d'après la partie (b), l'inégalité moyenne arithmétique-moyenne géométrique est vraie pour toutes les listes de longueur 2^n , mais d'après la partie (c), elle doit être invalide pour une liste de longueur 2^n . Ceci est une contradiction, donc l'inégalité doit toujours être vraie.

10. (a) Indice : Montrez que $(a_1 b_1 + a_2 b_2) - (a_1 b_2 + a_2 b_1) \geq 0$.

(b) Utiliser l'induction sur n . Pour l'étape d'induction, supposer que le résultat est vrai pour les suites de longueur n , et supposer que $a_1 \leq a_2 \leq \dots \leq a_n \leq a_{n+1}$, $b_1 \leq b_2 \leq \dots \leq b_n \leq b_{n+1}$, et f est une fonction onde bijective de $\{1, 2, \dots, n+1\}$ sur elle-même. Considérons maintenant deux cas. Pour le cas 1, supposer que $f(n+1) = n+1$, et utiliser l'hypothèse inductive pour compléter la preuve. Pour le cas 2, supposer que $f(n+1) < n+1$. Trouver une fonction onde bijective g de $\{1, 2, \dots, n+1\}$ à lui-même tel que g soit presque identique à f mais $g(n+1) = n+1$, et montrer que

$$\begin{aligned} a_1 b_{f(1)} + \cdots + a_{n+1} b_{f(n+1)} &\leq a_1 b_{g(1)} + \cdots + a_{n+1} b_{g(n+1)} \\ &\leq a_1 b_1 + \cdots + a_{n+1} b_{n+1}. \end{aligned}$$

11. On procède par récurrence sur n .

Cas de base : $n = 0$. Si A a 0 éléments, alors $A = \emptyset$, donc $\mathcal{P}(A) = \{\emptyset\}$, qui a $1 = 2^0$ éléments.

Étape d'induction : Supposons que pour tout ensemble A à n éléments, $\mathcal{P}(A)$ possède 2^n éléments. Supposons maintenant que A possède $n+1$ éléments. Soit a un élément quelconque de A , et soit $A' = A \setminus \{a\}$. Alors, A' possède n éléments, donc, par hypothèse inductive, $\mathcal{P}(A')$ possède 2^n éléments. Il existe deux types de sous-ensembles de A : ceux qui contiennent a comme élément, et ceux qui n'en contiennent pas. Les sous-ensembles qui ne contiennent pas a sont simplement les sous-ensembles de A' , et ils sont au nombre de 2^n . Ceux qui contiennent a sont les ensembles de la forme $X \cup \{a\}$, où $X \in \mathcal{P}(A')$, et il y en a aussi 2^n , puisqu'il y a 2^n choix possibles pour X . Ainsi, le nombre total d'éléments de $\mathcal{P}(A)$ est $2^n + 2^n = 2^{n+1}$.

14. Cas de base : $n = 1$. Une corde coupe le cercle en deux régions, et $(n^2 + n + 2)/2 = 2$.

Étape d'induction : Supposons que lorsque n cordes sont tracées, le cercle est découpé en $(n^2 + n + 2)/2$ régions. Lorsqu'une autre corde est tracée, elle coupe chacune des n premières cordes exactement une fois. Elle traverse donc $n+1$ régions, coupant chacune de ces régions en deux. (Chaque fois qu'elle traverse l'une des n premières cordes, elle passe d'une région à l'autre.) Le nombre de régions après le tracé de la corde suivante est donc

$$\frac{n^2 + n + 2}{2} + (n+1) = \frac{n^2 + 3n + 4}{2} = \frac{(n+1)^2 + (n+1) + 2}{2},$$

selon les besoins.

Section 6.3

1. Indice : La formule est

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

6. Cas de base : $n = 1$. Alors

$$\sum_{i=1}^n \frac{1}{i^2} = 1 \leq 1 = 2 - \frac{1}{n}.$$

Étape d'induction : Supposons que

$$\sum_{i=1}^n \frac{1}{i^2} \leq 2 - \frac{1}{n}.$$

Alors

$$\begin{aligned}\sum_{i=1}^{n+1} \frac{1}{i^2} &= \sum_{i=1}^n \frac{1}{i^2} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \\ &= 2 - \frac{n^2+n+1}{n(n+1)^2} < 2 - \frac{n^2+n}{n(n+1)^2} = 2 - \frac{1}{n+1}.\end{aligned}$$

8. (a) Soit m arbitraire et démontrons ensuite par récurrence que pour tout $n \geq m$, $H_n - H_m \geq (n - m)/n$.

Cas de base : $n = m$. Alors $H_n - H_m = 0 \geq 0 = (n - m)/n$.

Étape d'induction : Supposons que $n \geq m$ et $H_n - H_m \geq (n - m)/n$. Alors

$$\begin{aligned}H_{n+1} - H_m &= H_n + \frac{1}{n+1} - H_m \geq \frac{n-m}{n} + \frac{1}{n+1} \\ &\geq \frac{n-m}{n+1} + \frac{1}{n+1} = \frac{n+1-m}{n+1}.\end{aligned}$$

(b) Cas de base : Si $n = 0$ alors $H_2^n = H_1 = 1 \geq 1 = 1 + n/2$.

Étape d'induction : Supposons que $n \geq 0$ et $H_2^n \geq 1 + n/2$. Par la partie (a),

$$H_{2^{n+1}} - H_{2^n} \geq \frac{2^{n+1} - 2^n}{2^{n+1}} = \frac{1}{2}.$$

Donc

$$H_{2^{n+1}} \geq H_{2^n} + \frac{1}{2} \geq 1 + \frac{n}{2} + \frac{1}{2} = 1 + \frac{n+1}{2}.$$

(c) Puisque $\lim_{n \rightarrow \infty} (1 + n/2) = \infty$, par partie (b) $\lim_{n \rightarrow \infty} H_2^n = \infty$. De toute évidence, les H_n forment une suite croissante, donc $\lim_{n \rightarrow \infty} H_n = \infty$.

12. (a) Indice : essayez de prouver que $2^n \geq n + 1$, d'où découle la conclusion souhaitée.

(b) Cas de base : $n = 9$. Alors $n! = 362880 \geq 262144 = (2^n)^2$.

Étape d'induction : Supposons que $n \geq 9$ et $n! \geq (2^n)^2$. Alors

$$\begin{aligned}(n+1)! &= (n+1) \cdot n! \geq (n+1) \cdot (2^n)^2 \geq 10 \cdot 2^{2n} \geq 2^2 \cdot 2^{2n} \\ &= 2^{2n+2} = (2^{n+1})^2.\end{aligned}$$

(c) Cas de base : $n = 0$. Alors $n! = 1 \leq 1 = 2^{(n/2)}$.

Étape d'induction : Supposons que $n! \leq 2^{(n/2)}$. Alors

$$\begin{aligned}
2^{((n+1)^2)} &= 2^{n^2+2n+1} = 2^{(n^2)} \cdot 2^{2n+1} \geq 2^{(n^2)} \cdot 2^{n+1} \\
&> n! \cdot (n+1) \quad (\text{by inductive hypothesis and part (a)}) \\
&= (n+1)!.
\end{aligned}$$

15. Cas de base : $n = 0$. Alors $a_n = a_0 = 0 = 2^0 - 0 - 1 = 2^n - n - 1$.

Étape d'induction : Supposons que $n \in \mathbb{N}$ et $a_n = 2^n - n - 1$. Alors

$$\begin{aligned}
a_{n+1} &= 2a_n + n = 2(2^n - n - 1) + n \\
&= 2^{n+1} - 2n - 2 + n = 2^{n+1} - n - 2 = 2^{n+1} - (n+1) - 1.
\end{aligned}$$

18. (a) $\binom{n}{0} = n! / (0! n!) = 1$ and $\binom{n}{n} = n! / (n! 0!) = 1$.

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

(b)

(c) Nous suivons l'indice.

Cas de base : $n = 0$. Supposons que A soit un ensemble de 0 élément. Alors, $A = \emptyset$, la seule valeur de k à prendre en compte est $k = 0$, $\mathcal{P}_0(A) = \{\emptyset\}$, qui possède 1 élément, et $\binom{0}{0} = 1$.

Étape d'induction : Supposons que la conclusion souhaitée soit vraie pour les ensembles à n éléments, et que A soit un ensemble à $n+1$ éléments. Soit a un élément de A , et soit $A' = A \setminus \{a\}$, qui est un ensemble à n éléments. Supposons maintenant que $0 \leq k \leq n+1$. Considérons trois cas.

Cas 1 : $k = 0$. Alors $\mathcal{P}_k(A) = \{\emptyset\}$, qui a 1 élément, et $\binom{n+1}{k} = 1$.

Cas 2 : $k = n+1$. Alors $\mathcal{P}_k(A) = \{A\}$, qui a 1 élément, et $\binom{n+1}{k} = 1$.

Cas 3. $0 < k \leq n$. Il existe deux types de sous-ensembles k -éléments de A : ceux qui contiennent a comme élément, et ceux qui n'en contiennent pas. Les sous-ensembles k -éléments qui ne contiennent pas a sont simplement les sous-ensembles k -éléments de A' , et par hypothèse inductive, il existe. Ceux qui contiennent a sont les ensembles de la forme $X \cup \{a\}$, où $X \in \mathcal{P}_{k-1}(A')$, et par hypothèse inductive, il existe, car c'est le nombre de possibilités pour X . Par conséquent, d'après la partie (b), le nombre total de sous-ensembles k -éléments de A est

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

(d) Soit x et y arbitraires, puis nous prouvons l'équation par récurrence sur n .

Cas de base : $n = 0$. Les deux côtés de l'équation sont alors égaux à 1.

Étape d'induction : Nous utiliserons les parties (a) et (b). Supposons que

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

Alors

$$\begin{aligned} (x + y)^{n+1} &= (x + y)(x + y)^n \\ &= (x + y) \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \quad (\text{inductive hypothesis}) \\ &= (x + y) \left[\binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 \right. \\ &\quad \left. + \cdots + \binom{n}{n} y^n \right] \\ &= \binom{n}{0} x^{n+1} + \binom{n}{0} x^n y + \binom{n}{1} x^n y + \binom{n}{1} x^{n-1} y^2 \\ &\quad + \cdots + \binom{n}{n} x y^n + \binom{n}{n} y^{n+1} \\ &= x^{n+1} + \left[\binom{n}{0} + \binom{n}{1} \right] x^n y + \left[\binom{n}{1} + \binom{n}{2} \right] x^{n-1} y^2 \\ &\quad + \cdots + \left[\binom{n}{n-1} + \binom{n}{n} \right] x y^n + y^{n+1} \\ &= \binom{n+1}{0} x^{n+1} + \binom{n+1}{1} x^n y + \binom{n+1}{2} x^{n-1} y^2 \\ &\quad + \cdots + \binom{n+1}{n} x y^n + \binom{n+1}{n+1} y^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k. \end{aligned}$$

20. Indice : Étonnamment, il est plus facile de prouver que pour tout $n \geq 1$, $0 < a_n < 1/2$.

Section 6.4

1. (a) (\rightarrow) Supposons que $\forall n Q(n)$. Soit n arbitraire. Alors $Q(n+1)$ est vrai, ce qui signifie $\forall k < n+1 P(k)$. En particulier, puisque $n < n+1$, $P(n)$ est vrai. Puisque n est arbitraire, cela montre que $\forall n P(n)$.

(\leftarrow) Supposons que $\forall n P(n)$. Alors pour tout n , il est clairement vrai que $\forall k < n P(k)$, ce qui signifie que $Q(n)$ est vrai.

(b) Cas de base : $n = 0$. Alors $Q(n)$ est l'énoncé $\forall k < 0 P(k)$, ce qui est vide de sens.

Étape d'induction : Supposons que $Q(n)$ est vrai. Cela signifie que $\forall k < n P(k)$ est vrai, donc par hypothèse, il s'ensuit que $P(n)$ est vrai. Par conséquent $\forall k < n+1 P(k)$ est vrai, ce qui signifie que $Q(n+1)$ est vrai.

4. (a) Supposons que $\sqrt{6}$ soit rationnel. Soit $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+ (p/q = \sqrt{6})\}$. Alors $S \neq \emptyset$, donc nous pouvons laisser q être le plus petit élément de S , et nous pouvons choisir un entier positif p

tel que $p/q = \sqrt{6}$. Donc $p^2 = 6q^2$, donc p^2 est pair, et donc p est pair. Cela signifie que $p = 2\bar{p}$ pour un entier \bar{p} . Ainsi $4\bar{p}^2 = 6q^2$, donc $2\bar{p}^2 = 3q^2$ et donc $3q^2$ est pair. Il est facile de vérifier que si q est impair alors $3q^2$ est impair, donc q doit être pair, ce qui signifie que $q = 2\bar{q}$ pour un entier \bar{q} . Mais alors $\sqrt{6} = \bar{p}/\bar{q}$ et $\bar{q} < q$, contredisant le fait que q est le plus petit élément de S .

(b) Supposons que $\sqrt{2} + \sqrt{3} = p/q$. la mise au carré des deux côtés nous donne $5 + 2\sqrt{6} = p^2/q^2$, so $\sqrt{6} = (p^2 - 5q^2)/(2q^2)$. ce qui contredit la partie (a).

7. (a) Nous utilisons l'induction ordinaire sur n .

Cas de base : $n = 0$. Les deux côtés de l'équation sont égaux à 0.

Étape d'induction : Supposons que $\sum_{i=0}^n F_i = F_{n+2} - 1$. Alors

$$\sum_{i=0}^{n+1} F_i = \sum_{i=0}^n F_i + F_{n+1} = (F_{n+2} - 1) + F_{n+1} = F_{n+3} - 1.$$

(b) Nous utilisons l'induction ordinaire sur n .

Cas de base : $n = 0$. Les deux côtés de l'équation sont égaux à 0.

Étape d'induction. Supposons que $\sum_{i=0}^n (F_i)^2 = F_n F_{n+1}$. Alors

$$\begin{aligned} \sum_{i=0}^{n+1} (F_i)^2 &= \sum_{i=0}^n (F_i)^2 + (F_{n+1})^2 = F_n F_{n+1} + (F_{n+1})^2 \\ &= F_{n+1}(F_n + F_{n+1}) = F_{n+1} F_{n+2}. \end{aligned}$$

(c) Nous utilisons l'induction ordinaire sur n .

Cas de base : $n = 0$. Les deux côtés de l'équation sont égaux à 1.

Étape d'induction : Supposons que $\sum_{i=0}^n F_{2i+1} = F_{2n+2}$. Alors

$$\begin{aligned} \sum_{i=0}^{n+1} F_{2i+1} &= \sum_{i=0}^n F_{2i+1} + F_{2n+3} = F_{2n+2} + F_{2n+3} \\ &= F_{2n+4} = F_{2(n+1)+2}. \end{aligned}$$

(d) La formule est $\sum_{i=0}^n F_{2i} = F_{2n+1} - 1$.

9. (a) (\rightarrow) Supposons que a_0, a_1, a_2, \dots soit une suite de Fibonacci.

Alors, en particulier, $a_2 = a_0 + a_1$, ce qui signifie $c^2 = 1 + c$. La résolution de cette équation quadratique par la formule quadratique conduit à la conclusion suivante : $c = (1 \pm \sqrt{5})/2$.

(\leftarrow) Supposons que soit $c = (1 + \sqrt{5})/2$ or $c = (1 - \sqrt{5})/2$. Alors $c^2 = 1 + c$, et donc pour tout $n \geq 2$, $a_n = c^n = c^{n-2} c^2 = c^{n-2} (1 + c) = c^{n-2} + c^{n-1} = a_{n-2} + a_{n-1}$.

(b) Il sera commode d'introduire la notation $c_1 = (1 + \sqrt{5})/2$ et $c_2 = (1 - \sqrt{5})/2$. Alors pour tout $n \geq 2$, $a_n = sc_1^n + tc_2^n = sc_1^{n-2}c_1^2 + tc_2^{n-2}c_2^2 = sc_1^{n-2}(1 + c_1) + tc_2^{n-2}(1 + c_2) = (sc_1^{n-2} + tc_2^{n-2}) + (sc_1^{n-1} + tc_2^{n-1}) = a_{n-2} + a_{n-1}$.

(c) Indice : Soit $s = (5a_0 + (2a_1 - a_0)\sqrt{5})/10$ and $t = (5a_0 - (2a_1 - a_0)\sqrt{5})/10$.

11. Indice : La formule est $a_n = 2 \cdot 3^n - 3 \cdot 2^n$.

15. Soit a le plus grand de $5k$ et $k(k+1)$. Supposons maintenant que $n > a$, et, par l'algorithme de division, choisissons q et r tels que $n = qk + r$ et $0 \leq r < k$. Notons que si $q \leq 4$, alors $n = qk + r \leq 4k + r < 5k \leq a$, ce qui est contradictoire. Par conséquent, $q > 4$, donc $q \geq 5$, et l'[exemple 6.1.3](#) montre que $2^q \geq q^2$. Un raisonnement similaire montre que $q \geq k+1$, donc $q^2 \geq q(k+1) = qk + q > qk + k > qk + r = n$. Par conséquent, $2^n \geq 2^{qk} = (2^q)^k \geq (q^2)^k \geq n^k$.

18. Indice : La formule est $a_n = F_{n+2}/F_{n+1}$.

21. (a) Pour tous les nombres a, b, c et d ,

$$\begin{aligned} (ab)(cd) &= (cd)(ab) && \text{(commutative law)} \\ &= c(d(ab)) && \text{(associative law)} \\ &= c((da)b) && \text{(associative law)} \\ &= c((ad)b) && \text{(commutative law).} \end{aligned}$$

(b) Pour simplifier la notation, nous supposerons que tout produit est le produit groupé à gauche, sauf si des parenthèses sont utilisées pour indiquer le contraire. Nous utilisons l'induction forte sur n . Supposons que l'énoncé soit vrai pour les produits de moins de n termes, et considérons tout produit de a_1, a_2, \dots, a_n . Si $n = 1$, alors le seul produit est le produit groupé à gauche, il n'y a donc rien à prouver. Supposons maintenant $n > 1$. Alors notre produit a la forme pq , où p est un produit de a_1, \dots, a_{k-1} et q est un produit de a_k, \dots, a_n pour un certain k avec $2 \leq k \leq n$. Par l'hypothèse inductive, $p = a_1 \cdots a_{k-1}$ et $q = a_k \cdots a_n$ (où, par notre convention, ces deux produits sont groupés à gauche). Ainsi, il suffira de prouver que $(a_1 \cdots a_{k-1})(a_k \cdots a_n) = a_1 \cdots a_n$. Si $k = n$, alors le membre de gauche de cette équation est déjà groupé à gauche, il n'y a donc rien à prouver. Si $k < n$, alors

$$\begin{aligned} (a_1 \cdots a_{k-1})(a_k \cdots a_n) &= (a_1 \cdots a_{k-1})((a_k \cdots a_{n-1})a_n) && \text{(definition of left-grouped)} \\ &= ((a_1 \cdots a_{k-1})(a_k \cdots a_{n-1}))a_n && \text{(associative law)} \\ &= (a_1 \cdots a_{n-1})a_n && \text{(inductive hypothesis)} \\ &= a_1 \cdots a_n && \text{(definition of left-grouped).} \end{aligned}$$

(c) Par la partie (b), nous pouvons supposer que les deux produits sont groupés à gauche. Ainsi, nous devons prouver que si b_1, b_2, \dots, b_n est un réordre de a_1, a_2, \dots, a_n , alors $a_1 \cdots a_n = b_1 \cdots b_n$, où, comme dans la partie (b), nous supposons que les produits sont groupés à gauche sauf indication contraire entre parenthèses. Nous utilisons l'induction sur n . Si $n = 1$ alors les produits sont clairement égaux car $b_1 = a_1$. Supposons maintenant que l'énoncé

soit vrai pour des produits de longueur n , et supposons que b_1, \dots, b_{n+1} soit un réordre de a_1, \dots, a_{n+1} . Alors b_{n+1} est l'un des a_1, \dots, a_{n+1} . Si $b_{n+1} = a_{n+1}$ alors

$$\begin{aligned} b_1 \cdots b_{n+1} &= (b_1 \cdots b_n)a_{n+1} && (\text{definition of left-grouped}) \\ &= (a_1 \cdots a_n)a_{n+1} && (\text{inductive hypothesis}) \\ &= a_1 \cdots a_{n+1} && (\text{definition of left-grouped}). \end{aligned}$$

Supposons maintenant que $b_{n+1} = a_k$ pour un certain $k \leq n$. Nous écrirons $\widehat{a_1 \cdots a_k \cdots a_n}$ pour le produit (groupé à gauche) des nombres a_1, \dots, a_n en omettant le facteur a_k . Alors

$$\begin{aligned} b_1 \cdots b_{n+1} &= (b_1 \cdots b_n)a_k && (\text{definition of left-grouped}) \\ &= (a_1 \cdots \widehat{a_k} \cdots a_n)a_k && (\text{inductive hypothesis}) \\ &= ((a_1 \cdots \widehat{a_k} \cdots a_n)a_{n+1})a_k && (\text{definition of left-grouped}) \\ &= (a_1 \cdots \widehat{a_k} \cdots a_n)(a_{n+1}a_k) && (\text{associative law}) \\ &= (a_1 \cdots \widehat{a_k} \cdots a_n)(a_k a_{n+1}) && (\text{commutative law}) \\ &= ((a_1 \cdots \widehat{a_k} \cdots a_n)a_k)a_{n+1} && (\text{associative law}) \\ &= (a_1 \cdots a_n)a_{n+1} && (\text{inductive hypothesis}) \\ &= a_1 \cdots a_{n+1} && (\text{definition of left-grouped}). \end{aligned}$$

Section 6.5

1. $B_n = \{n\}$.

4. $B_0 = \{\emptyset\}$, $B_1 = \{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ a exactement un élément}\}$, $B_2 = \{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ a un ou deux éléments}\}$, ... En général, pour tout entier positif n , $B_n = \{X \in \mathcal{P}(\mathbb{N}) \mid X \neq \emptyset \text{ et } X \text{ a au plus } n \text{ éléments}\}$.

5. $\{n \in \mathbb{Z} \mid n \geq 2\}$.

7. (a) $B_0 = \{x \in \mathbb{R} \mid -2 \leq x \leq 0\}$, $B_1 = \{x \in \mathbb{R} \mid 0 \leq x \leq 4\}$, $B_2 = \{x \in \mathbb{R} \mid 0 \leq x \leq 16\}$, ... En général, pour tout entier positif n , $B_n = \{x \in \mathbb{R} \mid 0 \leq x \leq 2^{(2^n)}\}$.

(b) $\bigcup_{n \in \mathbb{N}} B_n = \{x \in \mathbb{R} \mid x \geq -2\}$. Par conséquent $-1, 3 \in \bigcup_{n \in \mathbb{N}} B_n$, mais $f(-1, 3) = -3 \notin \bigcup_{n \in \mathbb{N}} B_n$, so $\bigcup_{n \in \mathbb{N}} B_n$ n'est pas fermé par f . Autrement dit, la propriété 2 de [la définition 5.4.8](#) n'est pas vérifiée.

(c) \mathbb{R} .

10. On utilise l'induction sur n .

Cas de base : $n = 1$. Alors $x = 2! + 2 = 4$. La seule valeur de i dont nous devons nous soucier est $i = 0$, et pour cette valeur de i nous avons $i + 2 = 2$ et $x + i = 4$. Puisque $2 \mid 4$, nous avons $(i + 2) \mid (x + i)$, comme requis.

Étape d'induction : Supposons que n est un entier positif, et pour tout entier i , si $0 \leq i \leq n - 1$ alors $(i + 2) \mid ((n + 1)! + 2 + i)$.

Maintenant, soit $x = (n+2)! + 2$, et supposons que $0 \leq i \leq n$. Si $i = n$ alors nous avons

$$x + i = (n+2)! + 2 + i = (i+2)! + (i+2) = (i+2)((i+1)! + 1),$$

donc $(i+2) \mid (x+i)$. Supposons maintenant que $0 \leq i \leq n-1$. Par l'hypothèse inductive, nous savons que $(i+2) \mid ((n+1)! + 2 + i)$, nous pouvons donc choisir un entier k tel que $(n+1)! + 2 + i = k(i+2)$, et donc $(n+1)! = (k-1)(i+2)$. Par conséquent

$$\begin{aligned} x + i &= (n+2)! + 2 + i = (n+2)(n+1)! + (i+2) \\ &= (n+2)(k-1)(i+2) + (i+2) = (i+2)((n+2)(k-1) + 1), \end{aligned}$$

donc $(i+2) \mid (x+i)$.

14. Il est clair que T est une relation sur A et que $R = R^1 \subseteq T$. Pour voir que T est transitive, supposons $(x, y) \in T$ et $(y, z) \in T$. Alors, par définition de T , on peut choisir des entiers positifs n et m tels que $(x, y) \in R^n$ et $(y, z) \in R^m$. Ainsi, d'après [l'exercice 11](#), $(x, z) \in R^m \circ R^n = R^{m+n}$, donc $(x, z) \in \bigcup_{n \in \mathbb{Z}^+} R^n = T$. T est donc transitif.

Français Finalement, supposons $R \subseteq S \subseteq A \times A$ et S est transitif. Nous devons montrer que $T \subseteq S$, et clairement par la définition de T il suffit de montrer que $\forall n \in \mathbb{Z}^+ (R^n \subseteq S)$. Nous le prouvons par récurrence sur n . Nous avons supposé $R \subseteq S$, donc lorsque $n = 1$ nous avons $R^1 = R \subseteq S$. Pour l'étape de récurrence, supposons que n est un entier positif et $R^n \subseteq S$. Supposons maintenant $(x, y) \in R^{n+1}$. Alors par la définition de R^{n+1} nous pouvons choisir un $z \in A$ tel que $(x, z) \in R$ et $(z, y) \in R^n$. Par l'hypothèse $R \subseteq S$, et par l'hypothèse inductive $R^n \subseteq S$. Par conséquent $(x, z) \in S$ et $(z, y) \in S$, donc puisque S est transitif, $(x, y) \in S$. Puisque (x, y) était un élément arbitraire de R^{n+1} , cela montre que $R^{n+1} \subseteq S$.

16. (a) $R \cap S \subseteq R$ et $R \cap S \subseteq S$. Par conséquent, par [l'exercice 15](#), pour tout entier positif n , $(R \cap S)^n \subseteq R^n$ et $(R \cap S)^n \subseteq S^n$, donc $(R \cap S)^n \subseteq R^n \cap S^n$. Cependant, les deux ne sont pas nécessairement égaux. Par exemple, si $A = \{1, 2, 3, 4\}$, $R = \{(1, 2), (2, 4)\}$, et $S = \{(1, 3), (3, 4)\}$, alors $(R \cap S)^2 = \emptyset$ mais $R^2 \cap S^2 = \{(1, 4)\}$.

(b) $R^n \cup S^n \subseteq (R \cup S)^n$, mais ils ne sont pas nécessairement égaux. (Vous devriez pouvoir prouver la première affirmation et trouver un contre-exemple pour justifier la seconde.)

18. (a) Nous utilisons l'induction.

Cas de base : $n = 1$. Supposons que $(a, b) \in R^1 = R$. Soit $f = \{(0, a), (1, b)\}$. Alors f est un R -chemin de a à b de longueur 1. Pour l'autre direction, supposons que f est un R -chemin de a à b de

longueur 1. Par définition de R -chemin, cela signifie que $f(0) = a$, $f(1) = b$, et $(f(0), f(1)) \in R$. Par conséquent $(a, b) \in R = R^1$.

Étape d'induction : Supposons que n soit un entier positif et que $R^n = \{(a, b) \in A \times A \mid \text{il existe un } R\text{-chemin de } a \text{ à } b \text{ de longueur } n\}$. Supposons maintenant que $(a, b) \in R^{n+1} = R^1 \circ R^n$ par [l'exercice 11](#). Alors il existe un c tel que $(a, c) \in R^n$ et $(c, b) \in R$. Par hypothèse inductive, il existe un R -chemin f de a à c de longueur n . Alors $f \cup \{(n+1, b)\}$ est un R -chemin de a à b de longueur $n+1$. Dans l'autre sens, supposons que f est un R -chemin de a à b de longueur $n+1$. Soit $c = f(n)$. Alors $f \setminus \{(n+1, b)\}$ est un R -chemin de a vers c de longueur n , donc par l'hypothèse inductive $(a, c) \in R^n$. Mais aussi $(c, b) = (f(n), f(n+1)) \in R$, donc $(a, b) \in R^1 \circ R^n = R^{n+1}$.

(b) Ceci découle de la partie (a) et [de l'exercice 14](#).

Chapitre 7

Section 7.1

2. (a) $\text{pgcd}(775, 682) = 31 = -7 \cdot 775 + 8 \cdot 682$.
(b) $\text{pgcd}(562, 243) = 1 = 16 \cdot 562 - 37 \cdot 243$.

5. Soit n un entier arbitraire.

(→) Supposons que n soit une combinaison linéaire de a et b . Alors il existe des entiers s et t tels que $n = sa + tb$. Puisque $d = \text{pgcd}(a, b)$, $d | a$ et $d | b$, il existe donc des entiers j et k tels que $a = jd$ et $b = kd$. Par conséquent $n = sa + tb = sjd + tkd = (sj + tk)d$, donc $d | n$.

(←) Supposons $d | n$. Alors il existe un entier k tel que $n = kd$. D'après [le théorème 7.1.4](#), il existe des entiers s et t tels que $d = sa + tb$. Par conséquent $n = kd = k(sa + tb) = ksa + ktb$, donc n est une combinaison linéaire de a et b .

7. (a) Non. Contre-exemple : $a = b = 2$, $a' = 3$, $b' = 4$.
(b) Oui. Supposons $a | a'$ et $b | b'$. Soit $d = \text{pgcd}(a, b)$. Alors $d | a$ et $d | b$. Puisque $d | a$ et $a | a'$, d'après [le théorème 3.3.7](#), $d | a'$. De même, $d | b'$. Par conséquent, d'après [le théorème 7.1.6](#), $d | \text{pgcd}(a', b')$.

9. Nous utilisons l'induction forte sur le maximum de a et b . Autrement dit, nous démontrons l'affirmation suivante par induction forte :

$$\begin{aligned} \forall k \in \mathbb{Z}^+ [\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ (\max(a, b) = k \\ \rightarrow \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1)], \end{aligned}$$

où $\max(a, b)$ désigne le maximum de a et b .

Soit $k \in \mathbb{Z}^+$ arbitraire et supposons que pour tout entier positif $k' < k$,

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ (\max(a, b) = k' \rightarrow \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1).$$

maintenant a et b des entiers positifs arbitraires et supposons que $\max(a, b) = k$. On peut supposer que $a \geq b$, sinon on peut échanger les valeurs de a et b . Considérons deux cas.

Cas 1. $a = b$. Alors

$$\begin{aligned} \gcd(2^a - 1, 2^b - 1) &= \gcd(2^a - 1, 2^a - 1) = 2^a - 1 = 2^{\gcd(a, a)} - 1 \\ &= 2^{\gcd(a, b)} - 1. \end{aligned}$$

Cas 2. $a > b$. Soit $c = a - b > 0$, de sorte que $a = c + b$. Soit $k' = \max(c, b)$. Puisque $b < a$ et $c < a$, $k' < a = \max(a, b) = k$. Par conséquent

$$\begin{aligned}
\gcd(2^a - 1, 2^b - 1) &= \gcd(2^c - 1 + 2^a - 2^c, 2^b - 1) \\
&= \gcd(2^c - 1 + 2^c(2^b - 1), 2^b - 1) \\
&= \gcd(2^c - 1, 2^b - 1) \quad (\text{exercice 6}) \\
&= 2^{\gcd(c,b)} - 1 \quad (\text{inductive hypothesis}) \\
&= 2^{\gcd(c+b,b)} - 1 \quad (\text{exercice 6}) \\
&= 2^{\gcd(a,b)} - 1.
\end{aligned}$$

12. (a) $\operatorname{pgcd}(55, 34) = 1$. Les nombres r_i sont les nombres de Fibonacci. Il y a 8 divisions.

(b) $\operatorname{pgcd}(F_{n+1}, F_n) = 1$. Il y a $n - 1$ étapes de division.

Section 7.2

2. 14950.

5. Supposons qu'un nombre premier p apparaisse dans les factorisations premières de a et b . Alors $p \mid a$ et $p \mid b$, donc $\operatorname{pgcd}(a, b) \geq p > 1$, et donc a et b ne sont pas premiers entre eux.

Supposons maintenant que a et b ne soient pas premiers entre eux. Soit $d = \operatorname{pgcd}(a, b) > 1$. Soit p un nombre premier quelconque dans la factorisation première de d . Alors, puisque $d \mid a$ et $d \mid b$, p doit apparaître dans les factorisations premières de a et de b .

8. Soit $d = \operatorname{pgcd}(a, b)$ et $x = ab / \operatorname{pgcd}(a, b) = ab / d$.

(a) Puisque $d = \operatorname{pgcd}(a, b)$, $d \mid b$, il existe donc un entier k tel que $b = kd$. Par conséquent $x = akd / d = ak$, donc x est un entier et $a \mid x$. Un argument similaire montre que $b \mid x$, donc x est un multiple commun de a et b . Puisque m est le plus petit commun multiple, $m \leq x$.

(b) Supposons que $r > 0$. Puisque $a \mid m$, il existe un entier t tel que $m = ta$. Par conséquent, $r = ab - qm = ab - qta = (b - qt)a$, donc $a \mid r$. De même, $b \mid r$. Mais $r < m$, ce qui contredit la définition de m comme le plus petit entier positif divisible par a et b . Par conséquent, $r = 0$.

(c) Avec t défini comme dans la partie (b), $ab = qm = qta$. En divisant les deux côtés par a , on obtient $b = qt$, donc $q \mid b$. La preuve que $q \mid a$ est semblable.

(d) Puisque $q \mid a$ et $q \mid b$, $q \leq \operatorname{pgcd}(a, b)$. Par conséquent $ab = qm \leq \operatorname{pgcd}(a, b)m$, donc $m \geq ab / \operatorname{pgcd}(a, b)$.

11. Astuce : Une approche consiste à laisser q et r être le quotient et le reste lorsque m est divisé par $\operatorname{lcm}(a, b)$, et à prouver que $r = 0$.

13. Soit $b = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ la factorisation première de b . Alors la factorisation de b^2 est $b^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$. Puisque $a^2 \mid b^2$, tout facteur premier de a doit être l'un des p_1, p_2, \dots, p_k , donc $a = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ pour un certain entiers

naturels f_1, f_2, \dots, f_k . Par conséquent $a^2 = p_1^{2f_1} p_2^{2f_2} \cdots p_k^{2f_k}$. Puisque $a^2 \mid b^2$, pour tout i nous devons avoir $2f_i \leq 2e_i$, et donc $f_i \leq e_i$. Ainsi $a \mid b$.

16. Soit p_1, p_2, \dots, p_k une liste de tous les nombres premiers qui apparaissent dans la factorisation première de a ou de b , de sorte que

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

pour certains nombres naturels e_1, e_2, \dots, e_k et f_1, f_2, \dots, f_k . Pour $i = 1, 2, \dots, k$, soit

$$g_i = \begin{cases} e_i, & \text{if } e_i \geq f_i, \\ 0, & \text{if } e_i < f_i, \end{cases} \quad h_i = \begin{cases} 0, & \text{if } e_i \geq f_i, \\ f_i, & \text{if } e_i < f_i. \end{cases}$$

Laisser

$$c = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}, \quad d = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}.$$

Alors, pour tout i , $g_i \leq e_i$ et $h_i \leq f_i$, et donc $c \mid a$ et $d \mid b$. De plus, c et d n'ont aucun facteur premier en commun ; par conséquent, d'après l'[exercice 5](#), c et d sont premiers entre eux. Finalement,

$$cd = p_1^{g_1+h_1} \cdots p_k^{g_k+h_k} = p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)} = \text{lcm}(a, b).$$

19. (a) Puisque x est un nombre rationnel positif, il existe des entiers positifs m et n tels que $x = m / n$. Soit $d = \text{pgcd}(m, n)$. Par l'[exercice 9](#), on peut poser a et b des entiers positifs tels que $m = da$, $n = db$, et $\text{pgcd}(a, b) = 1$. Alors

$$x = \frac{m}{n} = \frac{da}{db} = \frac{a}{b}.$$

(b) Puisque $a / b = c / d$, $ad = bc$. Par conséquent $a \mid bc$. Puisque $\text{pgcd}(a, b) = 1$, d'après le théorème 7.2.2, $a \mid c$. Un argument similaire montre $c \mid a$, donc $a = c$. Par conséquent $ad = bc = ba$, et en divisant les deux côtés par a nous concluons que $b = d$.

(c) D'après la partie (a), nous avons $x = a / b$, où a et b sont des entiers positifs premiers entre eux. Soit les factorisations premières de a et b

$$a = r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}, \quad b = s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}.$$

Notez que d'après l'[exercice 5](#), ces factorisations n'ont aucun nombre premier en commun. Alors

$$x = \frac{r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}}{s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}} = r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j} s_1^{-h_1} s_2^{-h_2} \cdots s_l^{-h_l}.$$

En réorganisant les nombres premiers $r_1, \dots, r_j, s_1, \dots, s_l$ dans l'ordre croissant, on obtient le produit requis $p_1^{e_1} \cdots p_k^{e_k}$.

- (d) Commençons par inverser les étapes de la partie (c). Soient r_1, r_2, \dots, r_j les premiers du produit $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ dont les exposants sont positifs, classés par ordre croissant, et s_1, s_2, \dots, s_l ceux dont les exposants sont négatifs. En réécrivant chaque nombre premier élevé à une puissance négative comme le nombre premier élevé à une puissance positive au dénominateur, on obtient

$$x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \frac{r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}}{s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}},$$

où tous les exposants g_i et h_i sont des entiers positifs. Le numérateur et le dénominateur n'ont aucun facteur premier en commun ; ils sont donc premiers entre eux. De même, le produit $q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$ peut être réécrit sous forme de fraction dont tous les exposants sont positifs :

$$x = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m} = \frac{v_1^{y_1} v_2^{y_2} \cdots v_t^{y_t}}{w_1^{z_1} w_2^{z_2} \cdots w_u^{z_u}}.$$

Par la partie (b), $r_1^{g_1} \cdots r_j^{g_j} = v_1^{y_1} \cdots v_t^{y_t}$ et $s_1^{h_1} \cdots s_l^{h_l} = w_1^{z_1} \cdots w_u^{z_u}$ par l'unicité des factorisations premières, $j = t$ et pour tout $i \in \{1, \dots, j\}$, $r_i = v_i$ et $g_i = y_i$, et aussi $l = u$ et pour tout $i \in \{1, \dots, l\}$, $s_i = w_i$ et $h_i = z_i$. En réécrivant les nombres premiers au dénominateur comme des nombres premiers élevés à des puissances négatives, nous constatons que les deux produits originaux $p_1^{e_1} \cdots p_k^{e_k}$ and $q_1^{f_1} \cdots q_m^{f_m}$ sont les mêmes.

Section 7.3

4. (a) Puisque $Z1$ est un élément identité additif, $Z1 + Z2 = Z2$. Et puisque $Z2$ est un élément identité additif, $Z1 + Z2 = Z1$. Par conséquent, $Z1 = Z1 + Z2 = Z2$.

- (b) Puisque X' est un inverse additif pour X , $X'_1 + X + X'_2 = [0]_m + X'_2 = X'_2$. De même, puisque X'_2 est un inverse additif pour X , $X'_1 + X + X'_2 = X'_1 + [0]_m = X'_1$. Donc $X'_1 = X'_2$.

- (c) Supposons que O_1 et O_2 soient des éléments neutres multiplicatifs. Alors $O_1 = O_1 \cdot O_2 = O_2$.

- (d) Supposons que X'_1 et X'_2 soient des inverses multiplicatifs de X . Alors $X'_1 = X'_1 \cdot [1]_m = X'_1 \cdot X \cdot X'_2 = [1]_m \cdot X'_2 = X'_2$.

8. Soient a et b des entiers arbitraires. Alors

$$\begin{aligned} na \equiv nb \pmod{nm} &\quad \text{iff} \quad \exists k \in \mathbb{Z} (nb - na = knm) \\ &\quad \text{iff} \quad \exists k \in \mathbb{Z} (b - a = km) \quad \text{iff} \quad a \equiv b \pmod{m}. \end{aligned}$$

10. (a) $x \in [95]_{237}$.

(b) $x \in [12]_{59}$.

13. Soient a et b des entiers arbitraires. Supposons d'abord que $a \equiv b \pmod{m}$. Alors $[a]_m = [b]_m$, donc $[na]_m = [n]_m \cdot [a]_m = [n]_m \cdot [b]_m = [nb]_m$, et donc $na \equiv nb \pmod{m}$.

Supposons maintenant que $na \equiv nb \pmod{m}$, donc $[n]_m \cdot [a]_m = [na]_m = [nb]_m = [n]_m \cdot [b]_m$. Puisque m et n sont premiers entre eux, $[n]_m$ possède une inverse multiplicative. En multipliant les deux côtés de l'équation $[n]_m \cdot [a]_m = [n]_m \cdot [b]_m$ par $[n]_m^{-1}$, on obtient $[a]_m = [b]_m$, donc $a \equiv b \pmod{m}$.

15. Indice : Démontrer que si $a \equiv b \pmod{m}$ alors $D(m) \cap D(a) = D(m) \cap D(b)$.

17. (a) Notons d'abord que $10 \equiv 1 \pmod{3}$, donc $[10]_3 = [1]_3$. Par conséquent, $[10^2]_3 = [10]_3 \cdot [10]_3 = [1]_3 \cdot [1]_3 = [1]_3$, $[10^3]_3 = [10^2]_3 \cdot [10]_3 = [1]_3 \cdot [1]_3 = [1]_3$, et, en général, pour tout $i \in \mathbb{N}$, $[10^i]_3 = [1]_3$. (Une preuve plus précise pourrait être faite par récurrence.) Ainsi

$$\begin{aligned} [n]_3 &= [d_0 + 10d_1 + \cdots + 10^k d_k]_3 \\ &= [d_0]_3 + [10]_3 \cdot [d_1]_3 + \cdots + [10^k]_3 \cdot [d_k]_3 \\ &= [d_0]_3 + [1]_3 \cdot [d_1]_3 + \cdots + [1]_3 \cdot [d_k]_3 \\ &= [d_0 + d_1 + \cdots + d_k]_3. \end{aligned}$$

En d'autres termes, $n \equiv (d_0 + d_1 + \cdots + d_k) \pmod{3}$.

(b) $3 \mid n$ ssi $[n]_3 = [0]_3$ ssi $[d_0 + \cdots + d_k]_3 = [0]_3$ ssi $3 \mid (d_0 + \cdots + d_k)$.

19. (a) Supposons que $n \geq 10$. Notons d'abord que

$$10f(n) = (d_k \cdots d_1 d_0)_{10} + 50d_0 = (d_k \cdots d_1 d_0)_{10} + 49d_0 + d_0 = n + 49d_0.$$

Par conséquent, $3f(n) - n = 49d_0 - 7f(n) = 7(7d_0 - f(n))$, donc $n \equiv 3f(n) \pmod{7}$, ou de manière équivalente $[n]_7 = [3]_7 \cdot [f(n)]_7$. Puisque $[3]_7^{-1} = [5]_7$, il s'ensuit que $[f(n)]_7 = [5]_7 \cdot [n]_7$, donc $f(n) \equiv 5n \pmod{7}$.

(b) Supposons que $n \geq 10$. Si $7 \mid n$ alors $[n]_7 = [0]_7$, donc $[f(n)]_7 = [5n]_7 = [5]_7 \cdot [0]_7 = [0]_7$, et donc $7 \mid f(n)$. De même, si $7 \mid f(n)$ alors $[f(n)]_7 = [0]_7$, donc $[n]_7 = [3f(n)]_7 = [3]_7 \cdot [0]_7 = [0]_7$ et $7 \mid n$.

(c) $f(627334) = 62733 + 5 \cdot 4 = 62753$; $f(62753) = 6275 + 5 \cdot 3 = 6290$; $f(6290) = 629 + 5 \cdot 0 = 629$; $f(629) = 62 + 5 \cdot 9 = 107$; $f(107) = 10 + 5 \cdot 7 = 45$; $f(45) = 4 + 5 \cdot 5 = 29$. Puisque $7 \nmid 29$, $7 \nmid 627334$.

Section 7.4

2. (a) $\varphi(539) = 420$.

(b) $\varphi(540) = 144$.

(c) $\varphi(541) = 540$.

6. Supposons que $a \equiv b \pmod{mn}$. Alors $mn \mid (b - a)$, donc pour un entier k , $b - a = kmn$. Par conséquent $m \mid (b - a)$ et $n \mid (b - a)$, donc $a \equiv b \pmod{m}$ et $a \equiv b \pmod{n}$.

Supposons maintenant que $a \equiv b \pmod{m}$ et $a \equiv b \pmod{n}$. Puisque $a \equiv b \pmod{n}$, $n \mid (b - a)$, il existe donc un entier j tel que $b - a = jn$. Puisque $a \equiv b \pmod{m}$, $m \mid (b - a)$, donc $m \mid jn$. Mais $\text{pgcd}(m, n) = 1$, donc d'après [le théorème 7.2.2](#) il s'ensuit que $m \mid j$. Soit k un entier tel que $j = km$. Alors $b - a = jn = kmn$. Donc $mn \mid (b - a)$, donc $a \equiv b \pmod{mn}$.

8. La première moitié de la solution de [l'exercice 6](#) n'utilise pas l'hypothèse que m et n sont premiers entre eux ; le sens de gauche à droite de l'énoncé « ssi » est donc correct même si cette hypothèse est abandonnée. Voici un contre-exemple pour l'autre sens : $a = 0$, $b = 12$, $m = 4$, $n = 6$.

10. Supposons que p soit premier et a un entier positif. Considérons deux cas.

Cas 1. $p \nmid a$. Alors p et a sont premiers entre eux, donc d'après [le théorème 7.4.2](#), $[a]_p^{p-1} = [1]_p$. donc $[a^p]_p = [a]_p^{p-1} \cdot [a]_p = [1]_p \cdot [a]_p = [a]_p$. $a \equiv a \pmod{p}$.

Cas 2. $p \mid a$. Alors $[a]_p = [0]_p$, donc $[a^p]_p = [0]_p^p = [0]_p = [a]_p$ et donc $a^p \equiv a \pmod{p}$.

13. Indice : utilisez [le lemme 7.4.6](#) et l'induction sur k .

15. (a) On procède par induction sur k .

Cas de base : Lorsque $k = 1$, l'énoncé à prouver est que pour tout entier positif m_1 et tout entier a_1 , il existe un entier r tel que $1 \leq r \leq m_1$ et $r \equiv a_1 \pmod{m_1}$. Ceci est vrai car $\{1, 2, \dots, m_1\}$ est un système résiduel complet modulo m_1 .

Étape d'induction : Supposons que l'énoncé soit valable pour des listes de k entiers positifs deux à deux premiers, et soit m_1, m_2, \dots, m_{k+1} une liste de $k + 1$ entiers positifs deux à deux premiers. Soit $M' = m_1 m_2 \cdots m_k$ et $M = m_1 m_2 \cdots m_{k+1} = M' m_{k+1}$. Soient a_1, a_2, \dots, a_{k+1} des entiers arbitraires. Par l'hypothèse inductive, il existe un entier r' tel que pour tout $i \in \{1, 2, \dots, k\}$, $r' \equiv a_i \pmod{m_i}$. Par [l'exercice 13](#), $\text{pgcd}(M', m_{k+1}) = 1$, donc par [le lemme 7.4.7](#) il existe un entier r tel que $1 \leq r \leq M$, $r \equiv r' \pmod{M'}$, et $r \equiv a_{k+1} \pmod{m_{k+1}}$.

). Par l'exercice 14, pour tout $i \in \{1, 2, \dots, k\}$, $r \equiv r' \pmod{m_i}$, et donc $r \equiv a_i \pmod{m_i}$.

(b) Supposons que $1 \leq r_1, r_2 \leq M$ et pour tout $i \in \{1, 2, \dots, k\}$, $r_1 \equiv a_i \pmod{m_i}$ et $r_2 \equiv a_i \pmod{m_i}$. Alors pour tout $i \in \{1, 2, \dots, k\}$, $r_1 \equiv r_2 \pmod{m_i}$, donc par l'exercice 14, $r_1 \equiv r_2 \pmod{M}$. Par conséquent $r_1 = r_2$.

17. Supposons que m et n soient premiers entre eux. Soient les éléments de $D(m)$ a_1, a_2, \dots, a_s , et les éléments de $D(n)$ b_1, b_2, \dots, b_t . Alors $\sigma(m) = a_1 + a_2 + \dots + a_s$ et $\sigma(n) = b_1 + b_2 + \dots + b_t$. En utilisant la fonction f de la partie (b) de l'exercice 16, nous voyons que les éléments de $D(mn)$ sont tous des produits de la forme $a_i b_j$, où $1 \leq i \leq s$ et $1 \leq j \leq t$. Ainsi, nous pouvons organiser les éléments de $D(mn)$ dans un tableau avec s lignes et t colonnes, où l'entrée dans la ligne i , colonne j du tableau est $a_i b_j$; chaque élément de $D(mn)$ apparaît exactement une fois dans ce tableau. Pour calculer $\sigma(mn)$, nous devons additionner toutes les entrées de ce tableau. Nous le ferons en additionnant d'abord chaque ligne du tableau, puis en additionnant ces sommes de lignes.

Pour $1 \leq i \leq s$, soit r_i la somme de la ligne i du tableau. Alors

$$r_i = a_i b_1 + a_i b_2 + \dots + a_i b_t = a_i(b_1 + b_2 + \dots + b_t) = a_i \sigma(n).$$

Donc

$$\begin{aligned} \sigma(mn) &= r_1 + r_2 + \dots + r_s = a_1 \sigma(n) + a_2 \sigma(n) + \dots + a_s \sigma(n) \\ &= (a_1 + a_2 + \dots + a_s) \sigma(n) = \sigma(m) \sigma(n). \end{aligned}$$

Section 7.5

2. (a) $n = 5893$, $\varphi(n) = 5740$, $d = 2109$.

(b) $c = 3421$.

5. (a) $n = 17 \cdot 29$.

(b) $d = 257$.

(c) $m = 183$.

7. (a) $c = 72$.

(b) $d = 63$.

(c) 288.

(d) $\varphi(n) = 144$, $d = 47, 18$.

9. On utilise l'induction forte. Supposons que a soit un entier positif, et que pour tout entier positif $k < a$, le calcul de X^k utilise au plus $2 \log_2 k$ multiplications.

Cas 1. $a = 1$. Alors $X^a = X^1 = X$, donc aucune multiplication n'est nécessaire, et $2 \log_2 a = 2 \log_2 1 = 0$.

Cas 2. a est pair. Alors $a = 2k$ pour un entier positif $k < a$, et pour calculer X^a on utilise la formule $X^a = X^k \cdot X^k$. Soit m le nombre de multiplications utilisé pour calculer X^k . Par l'hypothèse inductive, $m \leq 2 \log_2 k$. Pour calculer X^a nous utilisons une multiplication supplémentaire (pour multiplier X^k par lui-même), donc le nombre de multiplications est

$$m + 1 \leq 2 \log_2 k + 1 < 2(\log_2 k + 1) = 2 \log_2(2k) = 2 \log_2 a.$$

Cas 3. $a > 1$ et a est impair. Alors $a = 2k + 1$ pour un entier positif $k < a$, et pour calculer X^a on utilise la formule $X^a = X^k \cdot X^k \cdot X$. Comme dans le cas 2, si l'on laisse m le nombre de multiplications utilisées pour calculer X^k alors on a $m \leq 2 \log_2 k$. Pour calculer X^a nous utilisons deux multiplications supplémentaires, donc le nombre de multiplications est

$$m + 2 \leq 2 \log_2 k + 2 = 2(\log_2 k + 1) = 2 \log_2(2k) < 2 \log_2(2k+1) = 2 \log_2 a.$$

12. Puisque $a \in R_2$, $[a]_n^{n-1} \neq [1]_n$ et puisque $\text{pgcd}(n, a) = 1$, $[a]_n$ a un inverse multiplicatif.

- (a) Supposons que $x \in R_1$. Alors $2 \leq x \leq n - 1$ et $[x]_n^{n-1} = [1]_n$ puisque $\{0, 1, \dots, n - 1\}$ est un système résiduel complet modulo n , il existe un unique y tel que $0 \leq y \leq n - 1$ et $ax \equiv y \pmod{n}$, donc $[a]_n \cdot [x]_n = [y]_n$. Il faut prouver que $y \in R_2$. Si $y = 0$ alors $[x]_n = [a]_n^{-1} \cdot [y]_n = [a]_n^{-1} \cdot [0]_n = [0]_n$, ce qui contredit le fait que $2 \leq x \leq n - 1$. Par conséquent $1 \leq y \leq n - 1$. Et $[y]_n^{n-1} = [a]_n^{n-1} \cdot [x]_n^{n-1} = [a]_n^{n-1} \cdot [1]_n = [a]_n^{n-1} \neq [1]_n$. Par conséquent, $y^{n-1} \not\equiv 1 \pmod{n}$. Il s'ensuit que $y \neq 1$, donc $2 \leq y \leq n - 1$.
- (b) Supposons que $f(x_1) = f(x_2) = y$. Alors $[a]_n \cdot [x_1]_n = [y]_n = [a]_n \cdot [x_2]_n$, $[x_1]_n = [a]_n^{-1} \cdot [y]_n = [x_2]_n$ donc $x_1 = x_2$.
- (c) D'après la partie (b), R_1 possède le même nombre d'éléments que $\text{Ran}(f)$. Puisque $\text{Ran}(f) \subseteq R_2$, R_2 possède au moins autant d'éléments que R_1 . Ainsi, au moins la moitié des éléments de R sont dans R_2 .

Chapitre 8

Section 8.1

1. (a) Définissez $f: \mathbb{Z}^+ \rightarrow \mathbb{N}$ par la formule $f(n) = n - 1$. Il est facile de vérifier que f est bijectif et sur.

(b) Soit $E = \{n \in \mathbb{Z} \mid n \text{ est pair}\}$, et définissons $f: \mathbb{Z} \rightarrow E$ par la formule $f(n) = 2n$. Il est facile de vérifier que f est bijectif et sur, donc $\mathbb{Z} \sim E$. Mais nous savons déjà que $\mathbb{Z}^+ \sim \mathbb{Z}$, donc d'après [le théorème 8.1.3](#), $\mathbb{Z}^+ \sim E$, et donc E est dénombrable.

4. (a) Non. Contre-exemple : Soit $A = B = C = \mathbb{Z}^+$ et $D = \{1\}$.

(b) Non. Contre-exemple : Soit $A = B = \mathbb{N}$, $C = \mathbb{Z}^-$ et $D = \emptyset$.

6. (a) Nous prouvons que $\forall n \in \mathbb{N} \ \forall m \in \mathbb{N} \ (\ I_n \sim I_m \rightarrow n = m)$ par récurrence sur n .

Cas de base : $n = 0$. Supposons que $m \in \mathbb{N}$ et que f est bijective et surjective : $I_n \rightarrow I_m$. Puisque $n = 0$, $I_n = \emptyset$. Mais puisque f est surjective, nous devons aussi avoir $I_m = \emptyset$, donc $m = 0 = n$.

Étape d'induction : Supposons que $n \in \mathbb{N}$, et pour tout $m \in \mathbb{N}$, si $I_n \sim I_m$ alors $n = m$. Supposons maintenant que $m \in \mathbb{N}$ et $I_{n+1} \sim I_m$. Soit $f : I_{n+1} \rightarrow I_m$ une fonction surjective et bijective. Soit $k = f(n+1)$, et remarquons que $1 \leq k \leq m$, donc m est positif. En utilisant le fait que f est surjective, choisissez un $j \leq n+1$ tel que $f(j) = m$.

Nous définissons maintenant $g : I_n \rightarrow I_{m-1}$ comme suit :

$$g(i) = \begin{cases} f(i), & \text{if } i \neq j, \\ k, & \text{if } i = j. \end{cases}$$

Nous laissons au lecteur le soin de vérifier que g est bijectif et sur. Par hypothèse inductive, il en résulte que $n = m - 1$, donc $n + 1 = m$.

- (b) Supposons que A soit fini. Alors, par définition de « fini », nous savons qu'il existe au moins un $n \in \mathbb{N}$ tel que $I_n \sim A$. Pour voir qu'il est unique, supposons que n et m soient des entiers naturels, $I_n \sim A$, et $I_m \sim A$. Alors, d'après [le théorème 8.1.3](#), $I_n \sim I_m$, donc d'après la partie (a), $n = m$.

8. (a) Nous utilisons l'induction sur n .

Cas de base : $n = 0$. Supposons que $A \subseteq I_n = \emptyset$. Alors $A = \emptyset$, donc $|A| = 0$.

Étape d'induction : Supposons que $n \in \mathbb{N}$, et pour tout $A \subseteq I_n$, A est fini, $|A| \leq n$, et si $A \neq I_n$ alors $|A| < n$. Supposons maintenant que $A \subseteq I_{n+1}$. Si $A = I_{n+1}$ alors clairement $A \sim I_{n+1}$, donc A est fini et $|A| = n + 1$. Supposons maintenant que $A \neq I_{n+1}$. Si $n + 1 \notin A$, alors $A \subseteq I_n$, donc par l'hypothèse inductive, A est fini et $|A| \leq n$. Si $n + 1 \in A$, alors il doit exister un $k \in I_n$ tel que $k \notin A$. Soit $A' = (A \cup \{k\}) \setminus \{n + 1\}$. Ensuite, en faisant correspondre k avec $n + 1$, il n'est pas difficile de montrer que $A' \sim A$. De plus, $A' \subseteq I_n$, donc par l'hypothèse inductive, A' est fini et $|A'| \leq n$. Par conséquent, par [l'exercice 7](#), A est fini et $|A| \leq n$.

(b) Supposons que A soit fini et que $B \subseteq A$. Soit $n = |A|$, et soit $f: A \rightarrow I_n$ injectif et sur. Alors $f(B) \subseteq I_n$, donc par la partie (a), $f(B)$ est fini, $|f(B)| \leq n$, et si $B \neq A$ alors $f(B) \neq I_n$, donc $|f(B)| < n$. Puisque $B \sim f(B)$, la conclusion souhaitée s'ensuit.

[10](#). Indice : Définissez $g: B \rightarrow I_n$ par la formule

$$g(x) = \text{the smallest } i \in I_n \text{ such that } f(i) = x,$$

et montrer que g est bijectif.

[12](#). Notons d'abord que $i + j - 2$ ou $i + j - 1$ est pair, donc $f(i, j)$ est un entier positif, et donc f est une fonction de $\mathbb{Z}^+ \times \mathbb{Z}^+$ dans \mathbb{Z}^+ , comme indiqué. Il est utile de vérifier deux faits concernant la fonction f . Les deux faits ci-dessous peuvent être vérifiés par des calculs algébriques simples :

(a) Pour tout $j \in \mathbb{Z}^+$, $f(1, j + 1) - f(1, j) = j$.

(b) Pour tout $i \in \mathbb{Z}^+$ et $j \in \mathbb{Z}^+$, $f(1, i + j - 1) \leq f(i, j) < f(1, i + j)$. Il s'ensuit que $i + j$ est le plus petit $k \in \mathbb{Z}^+$ tel que $f(i, j) < f(1, k)$.

Pour voir que f est bijectif, supposons que $f(i_1, j_1) = f(i_2, j_2)$. Alors, d'après le fait (b) ci-dessus,

$$\begin{aligned} i_1 + j_1 &= \text{the smallest } k \in \mathbb{Z}^+ \text{ such that } f(i_1, j_1) < f(1, k) \\ &= \text{the smallest } k \in \mathbb{Z}^+ \text{ such that } f(i_2, j_2) < f(1, k) \\ &= i_2 + j_2. \end{aligned}$$

En utilisant la définition de f , il s'ensuit que

$$\begin{aligned} i_1 &= f(i_1, j_1) - \frac{(i_1 + j_1 - 2)(i_1 + j_1 - 1)}{2} \\ &= f(i_2, j_2) - \frac{(i_2 + j_2 - 2)(i_2 + j_2 - 1)}{2} \\ &= i_2. \end{aligned}$$

Mais comme $i_1 = i_2$ et $i_1 + j_1 = i_2 + j_2$, nous devons aussi avoir $j_1 = j_2$, donc $(i_1, j_1) = (i_2, j_2)$. Cela montre que f est bijectif.

Pour voir que f est sur, supposons $n \in \mathbb{Z}^+$. Il est facile de vérifier que $f(1, n+1) > n$, donc on peut poser k comme le plus petit entier positif tel que $f(1, k) > n$. On remarque que $f(1, 1) = 1 \leq n$, donc $k \geq 2$. Puisque k est le plus petit, $f(1, k-1) \leq n$, et donc, par le fait (a),

$$0 \leq n - f(1, k-1) < f(1, k) - f(1, k-1) = k-1.$$

En ajoutant 1 à tous les termes, nous obtenons

$$1 \leq n - f(1, k-1) + 1 < k.$$

Ainsi, si nous posons $i = n - f(1, k-1) + 1$ alors $1 \leq i < k$. Soit $j = k - i$, et remarquons que $i \in \mathbb{Z}^+$ et $j \in \mathbb{Z}^+$. Avec ce choix pour i et j nous avons

$$\begin{aligned} f(i, j) &= \frac{(i+j-2)(i+j-1)}{2} + i \\ &= \frac{(k-2)(k-1)}{2} + n - f(1, k-1) + 1 \\ &= \frac{(k-2)(k-1)}{2} + n - \left[\frac{(k-2)(k-1)}{2} + 1 \right] + 1 = n. \end{aligned}$$

15. (a) Si $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\} = \emptyset$ alors $B \subseteq \{f(m) \mid m \in \mathbb{Z}^+, m < n\}$, donc d'après [les exercices 8 et 10](#), B est fini. Mais nous avons supposé que B était infini, donc c'est impossible.

(b) On utilise l'induction forte. Supposons que $\forall m < n, f(m) \geq m$. Supposons maintenant que $f(n) < n$. Soit $m = f(n)$. Alors par l'hypothèse inductive, $f(m) \geq m$. De plus, par définition de $f(n)$, $m = f(n) \in B \setminus \{f(k) \mid k \in \mathbb{Z}^+, k < n\} \subseteq B \setminus \{f(k) \mid k \in \mathbb{Z}^+, k < m\}$. Mais puisque $f(m)$ est le *plus petit* élément de ce dernier ensemble, il s'ensuit que $f(m) \leq m$. Puisque nous avons $f(m) \geq m$ et $f(m) \leq m$, nous pouvons conclure que $f(m) = m$. Mais alors $m \notin B \setminus \{f(k) \mid k \in \mathbb{Z}^+, k < n\}$, nous avons donc une contradiction.

(c) Supposons que $i \in \mathbb{Z}^+, j \in \mathbb{Z}^+$, et $i \neq j$. Alors soit $i < j$ soit $j < i$. Supposons d'abord que $i < j$. Alors selon la définition de $f(j)$, $f(j) \in B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < j\}$, et clairement $f(i) \in \{f(m) \mid m \in \mathbb{Z}^+, m < j\}$. Il s'ensuit que $f(i) \neq f(j)$. Un argument similaire montre que si $j < i$ alors $f(i) \neq f(j)$. Cela montre que f est bijectif.

Pour voir que f est sur, supposons que $n \in B$. Par la partie (b), $f(n+1) \geq n+1 > n$. Mais selon la définition de f , $f(n+1)$ est le plus petit élément de $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n+1\}$. Il s'ensuit que $n \notin B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n+1\}$. Mais $n \in B$, il doit donc être le cas

que $n \in \{f(m) \mid m \in \mathbb{Z}^+, m < n + 1\}$. En d'autres termes, pour un entier positif $m < n + 1$, $f(m) = n$.

17. Supposons que $B \subseteq A$ et que A soit dénombrable. Alors, d'après le [théorème 8.1.5](#), il existe une fonction bijective $f : A \rightarrow \mathbb{Z}^+$. D'après l'[exercice 13 de la section 5.2](#), $f \upharpoonright B$ est une fonction bijective de B vers \mathbb{Z}^+ , donc B est dénombrable. (Voir l'[exercice 7 de la section 5.1](#) pour la définition de la notation utilisée ici.)
19. En suivant l'indication, nous définissons récursivement les ordres partiels R_n , pour $n \in \mathbb{N}$, de sorte que $R = R_0 \subseteq R_1 \subseteq R_2 \subseteq \dots$ et

$$\forall i \in I_n \forall j \in \mathbb{Z}^+ ((a_i, a_j) \in R_n \vee (a_j, a_i) \in R_n). (*)$$

Soit $R_0 = R$. Étant donné R_n , pour définir R_{n+1} on applique l'[exercice 2 de la Section 6.2](#), avec $B = \{a_i \mid i \in I_{n+1}\}$. Finalement, soit $T = \bigcup_{n \in \mathbb{N}} R_n$. Clairement T est réflexif, car tout R_n l'est. Pour voir que T est transitif, supposons que $(a, b) \in T$ et $(b, c) \in T$. Alors pour des entiers naturels m et n , $(a, b) \in R_m$ et $(b, c) \in R_n$. Si $m \leq n$ alors $R_m \subseteq R_n$, et donc $(a, b) \in R_n$ et $(b, c) \in R_n$. Puisque R_n est transitif, il s'ensuit que $(a, c) \in R_n \subseteq T$. Un argument similaire montre que si $n < m$ alors $(a, c) \in T$, donc T est transitif. La preuve que T est antisymétrique est similaire. Finalement, pour voir que T est un ordre total, supposons $x \in A$ et $y \in A$. Puisque nous avons numéroté les éléments de A , nous savons que pour certains entiers positifs m et n , $x = a_m$ et $y = a_n$. Mais alors par $(*)$ nous savons que soit (a_m, a_n) soit (a_n, a_m) est un élément de R_n , et donc aussi un élément de T .

22. (a) Nous suivons l'indication.

Cas de base : $n = 0$. Supposons que A et B soient des ensembles finis et $|B| = 0$. Alors $B = \emptyset$, donc $A \times B = \emptyset$ et $|A \times B| = 0 = |A| \cdot 0$.

Étape d'induction : Soit n un entier naturel arbitraire, et supposons que pour tout ensemble fini A et B , si $|B| = n$ alors $A \times B$ est fini et $|A \times B| = |A| \cdot n$. Supposons maintenant que A et B sont des ensembles finis et $|B| = n + 1$. Choisissez un élément $b \in B$, et soit $B' = B \setminus \{b\}$, un ensemble à n éléments. Alors $A \times B = A \times (B' \cup \{b\}) = (A \times B') \cup (A \times \{b\})$, et puisque $b \notin B'$, $A \times B'$ et $A \times \{b\}$ sont disjoints. Par l'hypothèse inductive, $A \times B'$ est fini et $|A \times B'| = |A| \cdot n$. De plus, il n'est pas difficile de voir que $A \sim A \times \{b\}$ – il suffit de faire correspondre chaque $x \in A$ avec $(x, b) \in A \times \{b\}$ – donc $A \times \{b\}$ est fini et $|A \times \{b\}| = |A|$. D'après le [théorème 8.1.7](#), il s'ensuit que $A \times B$ est fini et $|A \times B| = |A \times B'| + |A \times \{b\}| = |A| \cdot n + |A| = |A| \cdot (n + 1)$.

(b) Pour commander un repas, on nomme un élément de $A \times B$, où $A = \{\text{steak, poulet, côtelettes de porc, crevettes, spaghetti}\}$ et $B = \{\text{glace, gâteau, tarte}\}$. Le nombre de repas est donc $|A \times B| = |A| \cdot |B| = 5 \cdot 3 = 15$.

24. (a) Cas de base : $n = 0$. Si $|A| = 0$ alors $A = \emptyset$, donc $F = \{\emptyset\}$, et $|F| = 1 = 0!$.

Étape d'induction : Supposons que n soit un entier naturel et que la conclusion souhaitée soit vraie pour n . Soit maintenant A un ensemble à $n + 1$ éléments, et soit $F = \{f \mid f \text{ est une fonction online bijective de } I_{n+1} \text{ à } A\}$. Soit $g : I_{n+1} \rightarrow A$ une fonction online bijective. Pour tout $i \in I_{n+1}$, soit $A_i = A \setminus \{g(i)\}$, un ensemble à n éléments, et soit $F_i = \{f \mid f \text{ est une fonction online bijective de } I_n \text{ à } A_i\}$. Par l'hypothèse inductive, F_i est fini et $|F_i| = n!$. Soit maintenant $F'_i = \{f \in F \mid f(n+1) = g(i)\}$. Définissons une fonction $h : F_i \rightarrow F'_i$ par la formule $h(f) = f \cup \{(n+1, g(i))\}$. Il n'est pas difficile de vérifier que h est inexact et sur, donc F'_i est fini et $|F'_i| = |F_i| = n!$. Enfin, notez que $F = \bigcup_{i \in I_{n+1}} F'_i$ et $\forall i \in I_{n+1} \forall j \in I_{n+1} (i \neq j \rightarrow F'_i \cap F'_j = \emptyset)$. Il s'ensuit, par [l'exercice 21](#), que F est fini et $|F| = \sum_{i=1}^{n+1} |F'_i| = (n+1) \cdot n! = (n+1)!$.

(b) Indice : Définissez $h : F \rightarrow L$ par la formule $h(f) = \{(a, b) \in A \times A \mid f^{-1}(a) \leq f^{-1}(b)\}$. (Vous devriez vérifier que cet ensemble est un ordre total sur A .) Pour voir que h est inexact, supposons que $f \in F$, $g \in F$ et $f \neq g$. Soit i le plus petit élément de I_n pour lequel $f(i) \neq g(i)$. Maintenant, montrons que $(f(i), g(i)) \in h(f)$ mais $(f(i), g(i)) \notin h(g)$, donc $h(f) \neq h(g)$. Pour voir que h est sur, supposons que R est un ordre total sur A . Définissez $g : A \rightarrow I_n$ par la formule $g(a) = |\{x \in A \mid xRa\}|$. Montrez que $\forall a \in A \forall b \in A (aRb \leftrightarrow g(a) \leq g(b))$, et utilisez ce fait pour montrer que $g^{-1} \in F$ et $h(g^{-1}) = R$.

(c) $5! = 120$.

27. Cas de base : $n = 1$. Alors $I_n = \{1\}$, $P = \{\{1\}\}$ et $A_{\{1\}} = A_1$. Par conséquent $|\bigcup_{i \in I_n} A_i| = |A_1|$ et $\sum_{S \in P} (-1)^{|S|+1} |A_S| = (-1)^2 |A_{\{1\}}| = |A_1|$.

Étape d'induction : Supposons que le principe d'inclusion-exclusion soit valable pour n ensembles, et supposons que A_1, A_2, \dots, A_{n+1} soient des ensembles finis. Soient $P_n = \mathcal{P}(I_n) \setminus \{\emptyset\}$ et $P_{n+1} = \mathcal{P}(I_{n+1}) \setminus \{\emptyset\}$. D'après [les exercices 26\(a\)](#) et [23\(a\)](#) de [la section 3.4](#), et l'hypothèse inductive,

$$\begin{aligned}
\left| \bigcup_{i \in I_{n+1}} A_i \right| &= \left| \left(\bigcup_{i \in I_n} A_i \right) \cup A_{n+1} \right| \\
&= \left| \bigcup_{i \in I_n} A_i \right| + |A_{n+1}| - \left| \left(\bigcup_{i \in I_n} A_i \right) \cap A_{n+1} \right| \\
&= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + |A_{n+1}| - \left| \bigcup_{i \in I_n} (A_i \cap A_{n+1}) \right|.
\end{aligned}$$

Notez maintenant que pour chaque $S \in P_n$,

$$\bigcap_{i \in S} (A_i \cap A_{n+1}) = \left(\bigcap_{i \in S} A_i \right) \cap A_{n+1} = A_{S \cup \{n+1\}}.$$

Par conséquent, par une autre application de l'hypothèse inductive,

$$\left| \bigcup_{i \in I_n} (A_i \cap A_{n+1}) \right| = \sum_{S \in P_n} (-1)^{|S|+1} |A_{S \cup \{n+1\}}|.$$

Ainsi

$$\begin{aligned}
\left| \bigcup_{i \in I_{n+1}} A_i \right| &= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + |A_{n+1}| - \sum_{S \in P_n} (-1)^{|S|+1} |A_{S \cup \{n+1\}}| \\
&= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + (-1)^2 |A_{\{n+1\}}| \\
&\quad + \sum_{S \in P_n} (-1)^{|S \cup \{n+1\}|+1} |A_{S \cup \{n+1\}}|.
\end{aligned}$$

Enfin, notez qu'il existe trois types d'éléments de P_{n+1} : ceux qui sont des éléments de P_n , l'ensemble $\{n+1\}$ et les ensembles de la forme $S \cup \{n+1\}$, où $S \in P_n$. Il s'ensuit que la dernière formule ci-dessus est tout $\sum_{S \in P_{n+1}} (-1)^{|S|+1} |A_S|$ aussi requise.

Section 8.2

1. (a) D'après [le théorème 8.1.6](#), \mathbb{Q} est dénombrable. Si $\mathbb{R} \setminus \mathbb{Q}$ était dénombrable alors, d'après le [théorème 8.2.1](#), $\mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q}) = \mathbb{R}$ serait dénombrable, ce qui contredit [le théorème 8.2.6](#). Ainsi, $\mathbb{R} \setminus \mathbb{Q}$ doit être indénombrable.
- (b) Soit $A = \{\sqrt{2} + n \mid n \in \mathbb{Z}^+\}$. Il n'est pas difficile de voir que A et \mathbb{Q} sont disjoints, puisque $\sqrt{2}$ est irrationnel, et A est dénombrable. Appliquez maintenant [les théorèmes 8.1.6 et 8.2.1](#) pour conclure que $A \cup \mathbb{Q}$ est dénombrable, et donc $A \cup \mathbb{Q} \sim A$. Enfin, observez que $\mathbb{R} = (\mathbb{R} \setminus (A \cup \mathbb{Q})) \cup (A \cup \mathbb{Q})$ et $\mathbb{R} \setminus \mathbb{Q} = (\mathbb{R} \setminus (A \cup \mathbb{Q})) \cup A$, et appliquez la partie 2 du [théorème 8.1.2](#).
5. Supposons que $A \sim \mathcal{P}(A)$. Alors il existe une fonction $f: A \rightarrow \mathcal{P}(A)$ qui est bijective et sur. Soit $X = \{a \in A \mid a \notin f(a)\} \in \mathcal{P}(A)$. Puisque f est sur, il doit exister un $a \in A$ tel que $f(a) = X$. Mais alors selon la

définition de X , $a \in X$ ssi $a \notin f(a)$, donc $X \neq f(a)$, ce qui est une contradiction.

8. Indice : définissez $f: \mathcal{P}(A) \times \mathcal{P}(B) \rightarrow \mathcal{P}(A \cup B)$ par la formule $f(X, Y) = X \cup Y$, et prouvez que f est bijectif et sur.

10. Pour tout entier positif n , soit $A_n = \{x \in A \mid x \geq 1/n\}$. Clairement $\bigcup_{n \in \mathbb{Z}^+} A_n \subseteq A$, supposons maintenant $x \in A$. Alors $x \in \mathbb{R}^+$, donc $x > 0$. Soit n un entier positif suffisamment grand pour que $n \geq 1/x$. Alors $x \geq 1/n$, donc $x \in A_n$. Nous concluons que $A \subseteq \bigcup_{n \in \mathbb{Z}^+} A_n$ et donc $\bigcup_{n \in \mathbb{Z}^+} A_n = A$.

Supposons que a_1, a_2, \dots, a_k soient des éléments distincts de A_n . Alors

$$b \geq a_1 + a_2 + \dots + a_k \geq \frac{1}{n} + \frac{1}{n} + \dots + \frac{1}{n} = \frac{k}{n},$$

donc $k \leq bn$. Par conséquent, A_n est fini, et en fait $|A_n| \leq bn$. D'après le théorème 8.2.2, il s'ensuit que $A = \bigcup_{n \in \mathbb{Z}^+} A_n$ est dénombrable.

13. Indice : Notez d'abord que si $\mathcal{F} = \emptyset$ alors g peut être n'importe quelle fonction. Si $\mathcal{F} \neq \emptyset$, alors puisque $\mathbb{N} \sqsupseteq \mathbb{Z}^+$ dénombrable, nous pouvons écrire ses éléments dans une liste : $\mathcal{F} = \{f_1, f_2, \dots\}$. Définissons maintenant $g: \mathbb{Z}^+ \rightarrow \mathbb{R}$ par la formule $g(n) = \max\{|f_1(n)|, |f_2(n)|, \dots, |f_n(n)|\}$.

15. (a) Si Q est dénombrable, alors d'après la partie 2 du théorème 8.2.1, $P \cup Q$ est dénombrable. Or, $P \cup Q = \mathcal{P}(\mathbb{Z}^+)$, qui est indénombrable d'après le théorème de Cantor. Par conséquent, Q est indénombrable.

(b) Supposons $A \in Q$. Pour tout $n \in \mathbb{Z}^+$, $A \cap I_n \subseteq I_n$, donc d'après l'exercice 8(a) de la section 8.1, $A \cap I_n$ est fini. Par conséquent $S_A \subseteq P$. Supposons maintenant que S_A est fini. Alors il existe un entier positif n tel que $S_A = \{A \cap I_1, A \cap I_2, \dots, A \cap I_n\}$. Nous affirmons maintenant que $A \subseteq I_n$; cela complètera la preuve, car cela implique que A est fini, ce qui contredit notre hypothèse que $A \in Q$. Pour prouver cette affirmation, supposons que $m \in A$. Alors $A \cap I_m \in S_A$, il existe donc un $k \leq n$ tel que $A \cap I_m = A \cap I_k \subseteq I_k \subseteq I_n$. Mais $m \in A \cap I_m$, on conclut donc que $m \in I_n$, comme requis.

(c) Supposons que $A \in Q, B \in Q$ et $A \neq B$. Alors il existe un entier positif n tel que soit $n \in A$ et $n \notin B$ soit $n \in B$ et $n \notin A$. Nous supposerons $n \in A$ et $n \notin B$; la preuve pour l'autre cas est similaire. Nous affirmons maintenant que $S_A \cap S_B \subseteq \{A \cap I_1, A \cap I_2, \dots, A \cap I_{n-1}\}$; ceci

complète la preuve, car cela implique que $S_A \cap S_B$ est fini. Pour prouver cette affirmation, supposons que $X \in S_A \cap S_B$. Alors, il existe des entiers positifs n_A et n_B tels que $X = A \cap I_{n_A}$ et $X = B \cap I_{n_B}$. Si $n_A \geq n_B$ alors

$$n \in A \cap I_{n_A} = X = B \cap I_{n_B} \subseteq B,$$

ce qui est une contradiction. Par conséquent, $n_A < n_B$, donc $X = A \cap I_{n_A} \in \{A \cap I_1, \dots, A \cap I_{n_B}\}$, comme requis.

(d) Si $A \in Q$ alors $S_A \subseteq P$, donc puisque $g : P \rightarrow \mathbb{Z}^+$, $g(S_A) \subseteq \mathbb{Z}^+$. De plus, puisque S_A est infini et g est injectif, $g(S_A)$ est aussi infini. Ceci prouve que $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$ et que tout élément de \mathcal{F} est infini. Pour voir que \mathcal{F} est presque disjoint deux à deux, supposons $X, Y \in \mathcal{F}$ et $X \neq Y$. Alors il existe des ensembles $A, B \in Q$ tels que $X = g(S_A)$ et $Y = g(S_B)$. Puisque $X \neq Y$, $A \neq B$, donc d'après la partie (c), $S_A \cap S_B$ est fini, et donc $g(S_A \cap S_B)$ est fini. D'après [le théorème 5.5.2](#), $g(S_A \cap S_B) = g(S_A) \cap g(S_B) = X \cap Y$, donc X et Y sont presque disjoints. Finalement, définissons $h : Q \rightarrow \mathcal{F}$ par la formule $h(A) = g(S_A)$. Il est facile de vérifier que h est bijectif et sur, donc $\mathcal{F} \sim Q$ et donc, d'après la partie (a), \mathcal{F} est indénombrable.

Section 8.3

1. (a) La fonction $i_A : A \rightarrow A$ est bijective.

(b) Supposons que $A \lesssim B$ et $B \lesssim C$. Il existe alors des fonctions bijectives $f : A \rightarrow B$ et $g : B \rightarrow C$. D'après la partie 1 du [théorème 5.2.5](#), $g \circ f : A \rightarrow C$ est bijective, donc $A \lesssim C$.

5. Soient $g : A \rightarrow B$ et $h : C \rightarrow D$ des fonctions bijectives .

(a) Puisque $A \neq \emptyset$, nous pouvons choisir un $a_0 \in A$. Remarquez que $g^{-1} : \text{Ran}(g) \rightarrow A$. Définissons $j : B \rightarrow A$ comme suit :

$$j(b) = \begin{cases} g^{-1}(b), & \text{if } b \in \text{Ran}(g), \\ a_0, & \text{otherwise.} \end{cases}$$

Nous vous laissons vérifier que j est sur.

Définissons maintenant $F : {}^A C \rightarrow {}^B D$ par la formule $F(f) = h \circ f \circ j$. Pour voir que F est injectif, supposons que $f_1, f_2 \in {}^A C$ et $F(f_1) = F(f_2)$, ce qui signifie $h \circ f_1 \circ j = h \circ f_2 \circ j$. Soit $a \in A$

arbitraire. Puisque j est sur, il existe un $b \in B$ tel que $j(b) = a$. Par conséquent $h(f_1(a)) = (h \circ f_1 \circ j)(b) = (h \circ f_2 \circ j)(b) = h(f_2(a))$, et puisque h est injectif, il s'ensuit que $f_1(a) = f_2(a)$. Comme a est arbitraire, cela montre que $f_1 = f_2$.

- (b) Oui. (Vous devriez pouvoir justifier cette réponse par un contre-exemple.)

8. (a) Soit n arbitraire, puis procédons par induction sur m . Le cas de base est $m = n + 1$, et il est traité par [l'exercice 7](#). Pour l'étape d'induction, appliquez [l'exercice 2\(b\)](#).

- (b) $\bigcup_{n \in \mathbb{Z}^+} A_n$ est un ensemble infini qui n'est pas équinumère avec A_n pour tout $n \in \mathbb{Z}^+$. En fait, pour tout entier positif n , $A_n \prec \bigcup_{n \in \mathbb{Z}^+} A_n$. Pouvez-vous trouver des ensembles infinis encore plus grands ?

10. (a) Notons que $\mathcal{E} \subseteq \mathcal{P}(\mathbb{Z}^+ \times \mathbb{Z}^+)$. Il s'ensuit, en utilisant [l'exercice 5 de la section 8.1](#), que $\mathcal{E} \leq \mathcal{P}(\mathbb{Z}^+ \times \mathbb{Z}^+) \sim \mathcal{P}(\mathbb{Z}^+)$.

(b) Supposons que $f(X) = f(Y)$. Alors $X \cup \{1\} \in f(X) = f(Y) = \{Y \cup \{1\}, (A \setminus Y) \cup \{2\}\}$, donc soit $X \cup \{1\} = Y \cup \{1\}$, soit $X \cup \{1\} = (A \setminus Y) \cup \{2\}$. Mais clairement $2 \notin X \cup \{1\}$, donc la deuxième possibilité peut être exclue. Par conséquent $X \cup \{1\} = Y \cup \{1\}$. Puisque ni X ni Y ne contiennent 1, il s'ensuit que $X = Y$.

(c) Il est clair que A est dénombrable, et nous avons montré à la fin de [la section 5.3](#) que $\mathcal{P} \sim \mathcal{E}$. Il s'ensuit que $\mathcal{P}(\mathbb{Z}^+) \sim \mathcal{P}(A) \leq \mathcal{P} \sim \mathcal{E}$. En combinant cela avec la partie (a) et en appliquant le théorème de Cantor-Schröder-Bernstein, on obtient la conclusion souhaitée.

14. (a) Selon la définition de la fonction, $\mathbb{R} \subseteq \mathcal{P}(\mathbb{R} \times \mathbb{R})$ et donc par [l'exercice 12\(b\)](#) et [l'exercice 5 de la section 8.1](#), $\mathbb{R} \leq \mathcal{P}(\mathbb{R} \times \mathbb{R}) \sim \mathcal{P}(\mathbb{R})$.

De toute évidence $\{\text{oui, non}\} \leq \mathbb{R}$, donc par [l'exercice 6\(c\)](#) de [la section 8.2](#) et [l'exercice 5](#), $\mathcal{P}(\mathbb{R}) \sim \mathbb{R}$ $\{\text{oui, non}\} \leq \mathbb{R} \leq \mathbb{R}$. Puisque nous avons à la fois $\mathbb{R} \leq \mathcal{P}(\mathbb{R})$ et $\mathcal{P}(\mathbb{R}) \leq \mathbb{R}$, par le théorème de Cantor-Schröder-Bernstein, $\mathbb{R} \sim \mathcal{P}(\mathbb{R})$.

(b) Par [les théorèmes 8.1.6 et 8.3.3](#), [l'exercice 23\(a\)](#) de [la section 8.1](#) et [l'exercice 6\(d\)](#) de [la section 8.2](#), $\mathbb{Q} \sim \mathbb{Z}^+ \mathcal{P}(\mathbb{Z}^+) \sim \mathcal{P}(\mathbb{Z}^+) \sim \mathbb{R}$.

(c) Définissons $F : \mathcal{C} \rightarrow \mathbb{Q}$ par la formule $F(f) = f \upharpoonright \mathbb{Q}$. (Voir [l'exercice 7 de la section 5.1](#) pour la signification de la notation utilisée ici.) Supposons que $f \in \mathcal{C}$, $g \in \mathcal{C}$ et $F(f) = F(g)$. Alors $f \upharpoonright \mathbb{Q} = g \upharpoonright \mathbb{Q}$, ce qui signifie que pour tout $x \in \mathbb{Q}$, $f(x) = g(x)$. Soit maintenant x un nombre réel arbitraire. Utiliser [le lemme 8.3.4](#) pour construire une suite x_1, x_2, \dots de nombres rationnels tels que $\lim_{n \rightarrow \infty} x_n = x$. Alors puisque f et g sont continues, $f(x) = \lim_{n \rightarrow \infty} f(x_n) = \lim_{n \rightarrow \infty} g(x_n) = g(x)$. Puisque x est arbitraire, cela montre que $f = g$. Par

conséquent, F est bijectif, donc $\mathcal{C} \leq^Q \mathbb{R}$. En combinant cela avec la partie (b), nous pouvons conclure que $\mathcal{C} \leq \mathbb{R}$.

Définissons maintenant $G : \mathbb{R} \rightarrow \mathcal{C}$ par la formule $G(x) = \mathbb{R} \times \{x\}$. En d'autres termes, $G(x)$ est la fonction constante dont la valeur pour tout nombre réel est x . Clairement, G est bijectif, donc $\mathbb{R} \leq \mathcal{C}$. D'après le théorème de Cantor-Schröder-Bernstein, il s'ensuit que $\mathcal{C} \sim \mathbb{R}$.

Suggestions de lectures complémentaires

- Barker-Plummer, D., Barwise, J., et Etchemendy, J., *Language, Proof and Logic*, 2e édition. Stanford : CSLI Publications, 2011.
- Burton, D., *Elementary Number Theory*, 7e édition. Boston : McGraw-Hill, 2011.
- Eccles, P., *Introduction au raisonnement mathématique : nombres, ensembles et fonctions*. Cambridge : Cambridge University Press, 1997.
- Enderton, H., *Introduction mathématique à la logique*, 2e édition. San Diego : Harcourt/Academic Press, 2001.
- Enderton, H., *Éléments de théorie des ensembles*. San Diego : Academic Press, 1977.
- Epp, S., *Mathématiques discrètes : Introduction au raisonnement mathématique*. Boston : Brooks/Cole Cengage Learning, 2011.
- Halmos, P., *Théorie naïve des ensembles*. Mineola, New York : Dover Publications, 2017.
- Hamilton, A., *Logique pour les mathématiciens*, édition révisée. Cambridge : Cambridge University Press, 1988.
- Hamilton, A., *Nombres, ensembles et axiomes : l'appareil des mathématiques*. Cambridge : Cambridge University Press, 1982.
- Leary, C. et Kristiansen, L., *Une introduction conviviale à la logique mathématique*, Geneseo, New York : Milne Library, 2015.
- Mendelson, E., *Introduction à la logique mathématique*, 6e édition. Boca Raton, Floride : CRC Press, 2015.
- Polya, G., *Comment résoudre ce problème : un nouvel aspect de la méthode mathématique*, 2e édition. Princeton : Princeton University Press, 2014.
- Rosen, K., *Mathématiques discrètes et ses applications*, 7e édition. New York : McGraw-Hill, 2012.
- Rosen, K., *Théorie élémentaire des nombres et ses applications*, 6e édition. Boston : Pearson, 2010.
- Silverman, J., *Une introduction conviviale à la théorie des nombres*, 4e édition. Boston : Pearson, 2012.
- van Dalen, D., Doets, H., et deSwart, H., *Ensembles : naïf, axiomatique et appliqué*, Oxford : Pergamon Press, 1978.

Résumé des techniques de preuve

Pour prouver un objectif de la forme :

1. $\neg P$:

- (a) Réexprimer sous forme d'affirmation positive.
- (b) Utilisez la preuve par contradiction ; c'est-à-dire supposez que P est vrai et essayez de parvenir à une contradiction.

2. $P \rightarrow Q$:

- (a) Supposons que P est vrai et prouvons Q .
- (b) Démontrer la contraposée ; c'est-à-dire supposer que Q est faux et prouver que P est faux.

3. $P \wedge Q$:

Démontrer P et Q séparément . Autrement dit, considérer ces deux objectifs comme distincts : P et Q .

4. $P \vee Q$:

- (a) Supposons que P est faux et prouvons Q , ou supposons que Q est faux et prouvons P .
- (b) Utilisez la preuve par cas. Dans chaque cas, prouvez P ou prouvez Q .

5. $P \leftrightarrow Q$:

Prouver $P \rightarrow Q$ et $Q \rightarrow P$ en utilisant les méthodes énumérées dans la partie 2.

6. $\forall xP(x)$:

Soit x pour un objet quelconque et démontrons $P(x)$. (Si la lettre x représente déjà quelque chose dans la démonstration, vous devrez utiliser une lettre différente pour l'objet quelconque.)

7. $\exists xP(x)$: Trouvez une valeur de x qui rend $P(x)$ vrai. Démontrez $P(x)$ pour cette valeur de x .

8. $\exists! xP(x)$:

- (a) Démontrer $\exists xP(x)$ (existence) et $\forall y \forall z ((P(y) \wedge P(z)) \rightarrow y = z)$ (unicité).
- (b) Démontrer l'énoncé équivalent $\exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x))$.

9. $\forall n \in \mathbb{N} P(n)$:

- (a) Induction mathématique : Prouver $P(0)$ (cas de base) et $\forall n \in \mathbb{N} (P(n) \rightarrow P(n+1))$ (étape d'induction).
- (b) Induction forte : Démontrer que $\forall n \in \mathbb{N} [(\forall k < n P(k)) \rightarrow P(n)]$.

Pour utiliser une donnée de la forme :

1. $\neg P$:

- (a) Réexprimer sous forme d'affirmation positive.
- (b) Dans une preuve par contradiction, vous pouvez parvenir à une contradiction en prouvant P .

2. $P \rightarrow Q$:

- (a) Si l'on vous donne également P , ou si vous pouvez prouver que P est vrai, alors vous pouvez conclure que Q est vrai.
- (b) Utilisez la contraposée : si l'on vous donne ou si vous pouvez prouver que Q est faux, alors vous pouvez conclure que P est faux.

3. $P \wedge Q$:

Considérez ceci comme deux données : P et Q .

4. $P \vee Q$:

- (a) Utiliser la preuve par cas. Dans le cas 1, supposer que P est vraie, et dans le cas 2, supposer que Q est vraie.
- (b) Si l'on sait également que P est faux, ou si l'on peut prouver que P est faux, alors on peut conclure que Q est vrai. De même, si l'on sait que Q est faux, alors on peut conclure que P est vrai.

5. $P \leftrightarrow Q$:

Considérez ceci comme deux données : $P \rightarrow Q$ et $Q \rightarrow P$.

6. $\forall x P(x)$:

Vous pouvez saisir n'importe quelle valeur, par exemple a , pour x , et conclure que $P(a)$ est vrai.

7. $\exists x P(x)$:

Introduisez une nouvelle variable, disons x_0 , dans la preuve, pour représenter un objet particulier pour lequel $P(x_0)$ est vrai.

8. $\exists! x P(x)$:

Introduisez une nouvelle variable, par exemple x_0 , dans la preuve, pour représenter un objet particulier pour lequel $P(x_0)$ est vraie. Vous pouvez également supposer que $\forall y (P(y) \rightarrow y = x_0)$.

Techniques pouvant être utilisées dans toute preuve :

1. Preuve par contradiction : supposez que l'objectif est faux et déduisez une contradiction.
2. Preuve par cas : Considérez plusieurs cas exhaustifs , c'est-à-dire incluant toutes les possibilités. Démontrez l'objectif dans chaque cas.

Indice

lois d'absorption, [21](#)
Adleman, Léonard, [360](#)
Alford, WR, [370](#)
nombre algébrique, [388](#)
presque disjoints, [389](#)
numéros amicaux, [7](#)
antécédent, [45](#)
antisymétrique, [200](#)
objet arbitraire, [113](#)
moyenne arithmétique, [290](#)
inégalité moyenne arithmétique-moyenne géométrique, [290](#)
lois associatives
 pour Δ , [45](#)
 pour \wedge et \vee , [21](#), [26](#)
 pour la composition des relations, [186](#)
 pour l'arithmétique modulaire, [344](#)
 pour la multiplication, [316](#)

cas de base, [273](#), [304](#)
Bernstein, Félix, [390](#)
biconditionnel, [54](#)
 table de vérité pour, [54](#)
grand-oh, [239](#), [301](#), [303](#), [314](#), [388](#)
bijection, [246](#)
opération binaire, [264](#)
relation binaire, [193](#)
coefficient binomial, [301](#), [312](#)
théorème du binôme, [302](#)
variable liée, [29](#), [59](#)
quantificateur borné, [72](#)

Cantor, Georg, [384](#), [390](#)
Théorème de Cantor, [384](#), [388](#)
Théorème de Cantor-Schröder-Bernstein, [390](#)

cardinalité, [372](#)
Carmichael, Robert Daniel, [370](#)
Numéro Carmichael, [370](#)
Produit cartésien, [174](#)
cas, preuve par, [142](#)
Théorème du reste chinois, [358](#)
fermé, [259](#), [263](#)
fermeture, [260](#), [264](#), [316](#)
Coqs, Clifford, [360](#)
Cohen, Paul, [394](#)
lois commutatives
 pour \wedge et \vee , [21](#)
 pour l'arithmétique modulaire, [344](#)
 pour la multiplication, [316](#)
compatible, [227](#), [239](#), [248](#)
système de résidus complet, [342](#)
nombre composé, [1](#)
composition, [183](#), [191](#), [192](#), [234](#)
conclusion, [8](#), [90](#)
conditionnel, [45](#)
 antécédent de, [45](#)
 conséquent de, [45](#)
 lois, [49](#)
 table de vérité pour, [46](#) – [47](#), [49](#), [148](#)
congruent, [215](#), [224](#), [341](#)
conjecture, [2](#)
conjonction, [10](#)
 table de vérité pour, [15](#)
symbole connectif, [10](#)
conséquent, [45](#)
fonction constante, [238](#), [247](#), [249](#)
hypothèse du continuum, [394](#)
contradiction, [22](#), [26](#), [42](#)
 lois, [23](#)
 preuve par, [102](#), [105](#)
contraposée, [51](#), [96](#)
 loi, [51](#)
converse, [51](#)
coordonnée, [173](#)
ensemble dénombrable, [375](#), [382](#) – [389](#)
contre-exemple, [2](#), [90](#)
cryptographie
 clé publique, [359](#) – [371](#)
 symétrique, [360](#)

De Morgan, Auguste, [21](#)
Lois de De Morgan, [21](#), [25](#)
en baisse, [267](#)
décrypter, [359](#)
ensemble dénombrable, [375](#), [394](#)
diagonalisation, [386](#)
différence d'ensembles, [35](#)
signature numérique, [368](#)
graphe orienté, [194](#)
disjoint, [41](#)
 par paires, [161](#), [216](#)
disjonction, [10](#)
 table de vérité pour, [15](#)
syllogisme disjonctif, [149](#)
lois distributives
 pour \cap et \cup , [39](#), [40](#)
 pour \exists et \vee , [77](#)
 pour \forall et \wedge , [74](#), [86](#)
 pour \wedge et \vee , [21](#), [25](#), [39](#), [40](#)
 pour l'arithmétique modulaire, [344](#)
divise, [126](#)
algorithme de division, [305](#), [313](#), [325](#), [342](#)
diviseur, [324](#)
domaine, [183](#), [191](#), [233](#)
domine, [390](#)
loi de double négation, [21](#), [25](#)
variable fictive, [29](#)

bord, [191](#)
élément, [28](#)
ensemble vide, [33](#)
crypter, [359](#)
équinombreux, [372](#)
classe d'équivalence, [216](#), [217](#)
relation d'équivalence, [215](#) - [228](#), [239](#), [381](#)
formules équivalentes, [20](#)
Euclide, [4](#), [5](#), [327](#), [358](#)
Algorithme d'Euclide, [327](#), [331](#)
 étendu, [329](#), [346](#), [364](#)
 plus petit reste absolu, [332](#)
Euler, Léonhard, [5](#), [289](#), [340](#), [351](#), [359](#), [369](#)
Fonction phi d'Euler, [351](#), [354](#)
Théorème d'Euler, [353](#), [360](#), [362](#), [369](#), [371](#)
Fonction indicatrice d'Euler, [351](#), [354](#)
entier pair, [132](#), [377](#)

cas exclusifs, [144](#)
exclusif ou, [15](#), [24](#)
cas exhaustifs, [142](#)
instanciation existentielle, [120](#)
quantificateur existentiel, [58](#)
exponentiation en arithmétique modulaire, [353](#), [357](#), [361](#), [368](#)
calcul efficace, [364](#), [369](#)

factorielle, [5](#), [165](#), [294](#), [296](#)
famille d'ensembles, [79](#)
Fermat, Pierre de, [289](#), [340](#), [369](#)
Numéro de Fermat, [289](#), [340](#), [369](#)
Test de primalité de Fermat, [369](#) – [371](#)
Pseudo-premier de Fermat, [369](#) – [371](#)
Témoin de Fermat, [369](#) – [371](#)
Petit théorème de Fermat, [357](#), [369](#)
Fibonacci, [307](#)
Nombres de Fibonacci, [306](#), [311](#), [312](#), [331](#)
suite finie, [383](#)
ensemble fini, [246](#), [280](#) – [283](#), [289](#), [292](#), [322](#), [372](#)
point fixe, [259](#)
formule, [12](#)
variable libre, [29](#), [59](#)
fonction, [229](#)
compatible avec une relation d'équivalence, [239](#), [248](#)
composition de, [234](#)
constante, [238](#), [247](#), [249](#)
domaine de, [233](#)
identité, [230](#), [251](#) – [256](#)
inverse de, [249](#) – [259](#)
de deux variables, [263](#)
un à un, [240](#)
sur, [240](#)
gamme de, [233](#), [242](#)
restriction de, [237](#), [247](#), [258](#)
strictement décroissant, [267](#)
strictement croissant, [267](#)
théorème fondamental de l'arithmétique, [335](#)

Gödel, Kurt, [394](#)
moyenne géométrique, [290](#)
Séquence de Gibonacci, [312](#)
donné, [93](#)
but, [93](#)
nombre d'or, [315](#)

Granville, André, [370](#)
graphique, [194](#)
plus grand diviseur commun, [324](#)
plus grande limite inférieure (glb), [167](#), [208](#), [209](#)

moyenne harmonique, [290](#)
nombres harmoniques, [300](#)
Hilbert, David, [340](#), [394](#)
nombre de Hilbert, [340](#)
Nombre premier de Hilbert, [340](#)
hypothèse, [90](#)

lois idempotentes, [21](#)

identité

éléments en arithmétique modulaire, [344](#), [349](#)

fonction, [230](#), [251](#) – [256](#)

relation, [193](#), [215](#), [230](#)

si et seulement, [54](#)

image, [230](#), [233](#), [268](#) – [272](#)

principe d'inclusion-exclusion, [381](#)

inclus ou, [15](#)

en augmentation, [267](#)

indice, [78](#)

ensemble d'index, [78](#)

famille indexée, [78](#), [79](#)

induction, [273](#)

fort, [304](#), [311](#)

étape d'induction, [273](#)

hypothèse inductive, [276](#), [304](#)

ensemble infini, [372](#)

injection, [240](#)

exemple d'un théorème, [90](#)

entier, [32](#)

intersection

de la famille d'ensembles, [81](#), [82](#)

de la famille indexée d'ensembles, [84](#)

de deux ensembles, [35](#), [82](#)

intervalle, [378](#), [396](#)

inverse

additif en arithmétique modulaire, [344](#), [349](#)

multiplicatif en arithmétique modulaire, [345](#), [349](#), [351](#)

d'une fonction, [249](#) – [259](#)

d'une relation, [183](#), [191](#)

image inversée, [268](#) – [272](#)

nombre irrationnel, [171](#), [310](#), [387](#)

irréfléchi, [214](#)

clé, [360](#)

public, [360](#)

le plus grand élément, [208](#)

plus petit commun multiple, [337](#)

plus petite limite supérieure (lub), [209](#)

lemme, [219](#)

Léonard de Pise, [307](#)

limite, [168](#)

combinaison linéaire, [328](#)

logarithme, [256](#)

boucle, [194](#)

limite inférieure, [167](#), [208](#)

Lucas, Édouard, [313](#)

Numéros de Lucas, [313](#)

connecteur principal, [17](#)

induction mathématique, voir [induction](#)

élément maximal, [208](#)

signifier

arithmétique, [290](#)

géométrique, [290](#)

harmonique, [290](#)

Mersenne, Marin, [5](#)

Miller, Gary L., [371](#)

Test de Miller-Rabin, [371](#)

Témoin Miller-Rabin, [371](#)

élément minimal, [203](#), [280](#)

arithmétique modulaire, [341](#) – [351](#)

modulo, [217](#)

mode ponens, [108](#)

modus tollens, [108](#), [113](#)

fonction multiplicative, [354](#), [358](#)

nand, [25](#)

nombre naturel, [32](#)

condition nécessaire, [52](#)

négation, [10](#)

table de vérité pour, [15](#)

ni, [24](#)

ensemble nul, [33](#)

entier impair, [132](#)

un à un, [240](#)
 correspondance biunivoque, [246](#)
 sur, [240](#)
 paire ordonnée, [173](#)
 ordonné triple ou quadruple, [179](#)

disjoints deux à deux, [161](#), [216](#)
 ordre partiel, [200](#), [280](#), [282](#), [380](#)
 strict, [214](#)
 partition, [216](#)
 Pascal, Blaise, [302](#)
 Triangle de Pascal, [302](#)
 nombre parfait, [5](#), [358](#), [359](#)
 point périodique, [322](#)
 principe du casier, [378](#)
 polynôme, [314](#)
 Pomerance, Carl, [370](#)
 ensemble de puissance, [80](#), [384](#)
 prémissse, [8](#)
 précommande, [228](#), [239](#), [249](#)
 test de primalité, [363](#)
 Fermat, [369 – 371](#)
 Miller-Rabin, [371](#)
 probabiliste, [363](#), [369 – 371](#)
 factorisation première, [4](#), [164](#), [306](#), [332](#), [335](#), [363](#)
 nombre premier, [1](#), [75](#), [78](#), [163 – 166](#), [306](#), [320](#)
 le plus grand connu, [5](#)
 Mersenne, [5](#)
 jumeaux, [6](#)
 preuve, [1](#), [89](#)
 par cas, [143 – 147](#)
 par contradiction, [102](#), [105](#)
 Concepteur d'épreuves, xi, [128](#)
 stratégie de preuve
 pour une donnée de la forme
 $P \rightarrow Q$, [108](#)
 $P \leftrightarrow Q$, [132](#)
 $P \vee Q$, [143](#), [149](#)
 $P \wedge Q$, [131](#)
 $\exists xP(x)$, [120](#)
 $\exists! xP(x)$, [159](#)
 $\forall xP(x)$, [121](#)
 $\neg P$, [105](#), [108](#)
 pour un but de la forme
 $P \rightarrow Q$, [92](#), [95](#), [96](#)

$P \leftrightarrow Q$, [132](#)
 $P \vee Q$, [145](#), [147](#)
 $P \wedge Q$, [130](#)
 $\exists xP(x)$, [118](#)
 $\exists! xP(x)$, [156](#), [158](#)
 $\forall n \in \mathbb{N} P(n)$, [273](#), [304](#)
 $\forall xP(x)$, [114](#)
 $\neg P$, [101](#), [102](#)
pseudopremier, [369](#) – [371](#)
clé publique, [360](#)
cryptographie à clé publique, [359](#) – [371](#)

quantificateur, [58](#) – [67](#)
délimité, [72](#)
existentiel, [58](#)
lois de négation, [68](#), [70](#), [73](#), [135](#) – [136](#)
existentiel unique, [71](#), [153](#) – [162](#)
universel, [58](#)
quotient, [305](#), [313](#), [325](#) – [330](#), [342](#)

Rabin, Michael O., [371](#)
gamme, [183](#), [191](#), [233](#), [242](#)
nombre rationnel, [32](#), [171](#), [377](#), [393](#), [396](#)
nombre réel, [32](#)
inégalité de réarrangement, [291](#)
récuratif
 définition, [294](#)
 procédure, [288](#)
affiner, [228](#)
réflexif, [194](#)
relation, [182](#)
 antisymétrique, [200](#)
 binaire, [193](#)
 compatible avec une relation d'équivalence, [227](#)
 composition de, [183](#), [191](#), [192](#)
 domaine de, [183](#), [191](#)
 identité, [193](#), [215](#), [230](#)
 inverse de, [183](#), [191](#)
 irréfléchi, [214](#)
 gamme de, [183](#), [191](#)
 réflexif, [194](#)
 symétrique, [194](#)
 transitif, [194](#)
relativement premier, [333](#)

reste, [146](#), [305](#), [313](#), [325](#) – [330](#), [342](#)
restriction, [237](#), [247](#), [258](#)
Rivest, Ron, [360](#)
RSA, [360](#)
règle d'inférence, [108](#), [120](#), [121](#), [149](#)
Russell, Bertrand, [88](#)
Le paradoxe de Russell, [88](#)

Schröder, Ernst, [390](#)
ensemble, [28](#), voir aussi [ensemble dénombrable](#); [ensemble dénombrable](#); [ensemble vide \(ou nul\)](#); [famille d'ensembles](#); [ensemble fini](#); [ensemble d'indices](#); [ensemble infini](#); [ensemble de puissances](#); [sous-ensemble](#); [ensemble de vérité](#)
Shamir, Adi, [360](#)
 σ , [358](#)
notation Σ , [295](#)
plus petit élément, [203](#)
ordre partiel strict, [214](#)
ordre total strict, [214](#)
domine strictement, [390](#)
induction forte, [304](#), [311](#)
sous-ensemble, [41](#)
condition suffisante, [52](#)
Soleil Zi, [358](#)
projection, [240](#)
symétrique, [194](#)
fermeture symétrique, [214](#)
cryptographie symétrique, [360](#)
différence symétrique, [38](#), [45](#), [150](#) – [152](#), [161](#)

τ , [358](#)
tautologie, [22](#), [26](#)
 lois, [23](#)
théorème, [90](#)
commande totale, [201](#), [282](#), [381](#)
 strict, [214](#)
transitif, [194](#)
fermeture transitive, [214](#), [322](#)
inégalité triangulaire, [151](#)
ensemble de vérité, [27](#), [31](#), [38](#), [173](#), [179](#)
table de vérité, [15](#) – [24](#)
valeur de vérité, [15](#)

ensemble indénombrable, [375](#), [382](#) – [389](#)
union

de la famille d'ensembles, [81](#), [82](#)
de la famille indexée d'ensembles, [84](#)
de deux ensembles, [35](#), [82](#)
instanciation universelle, [121](#)
quantificateur universel, [58](#)
univers du discours, [32](#)
limite supérieure, [208](#)

déclaration vide de sens, [74](#)
argument valide, [9](#), [18](#)
variable, [26](#)
 lié, [29](#), [59](#)
 mannequin, [29](#)
 gratuit, [29](#), [59](#)
Diagramme de Venn, [37](#), [41](#)
sommet, [191](#)

formule bien formée, [12](#)
principe de bon ordre, [309](#), [327](#)

Zhang, Yitang, [6 ans](#)