Fondements et fondamentaux pour les mathématiques
Matériel de cours pour MAT 2762

Pieter Hofstra
Département de mathématiques et de statistique
Université d'Ottawa

Table des matières

Introduction

Au cours de la période initiale de notre apprentissage en mathématiques, les sujets nous sont souvent présentés de manière intuitive et relativement informelle. Notre première rencontre avec le calcul infinitésimal consiste en un explication intuitive de ce qu'est une fonction, de ce qu'est la continuité et la différentiabilité, et ainsi de suite ; mais nous n'allons pas dans les détails techniques. Lors de cette phase, nous mettons surtout l'accent sur la maîtrise des algorithmes ou des techniques pour résoudre des types spécifiques de problèmes. Cette phase se poursuit au moins jusqu'à la première année universitaire en mathématiques.

Par la suite, néanmoins, nous devons acquérir une compréhension plus précise et formelle. Par exemple, au lieu de concevoir la continuité d'une fonction comme l'équivalent de dessiner son graphe sans lever le crayon, nous étudions la définition mathématique en termes d'epsilons et de deltas. Ainsi, l'emphase se déplace plutôt sur la compréhension des subtilités associées à ces définitions, sur la capacité à les manier et à les tester à travers des exemples, à les relier à d'autres définitions et à d'autres concepts, puis à les combiner pour prouver des théorèmes.

L'objet du cours MAT2362/MAT2762 est d'aider les étudiants à faire la transition vers cette deuxième phase de précision mathématique, et ceci s'accomplit de deux façons :

Premièrement, il introduit certains blocs de construction essentiels aux mathématiques modernes, notamment la théorie des ensembles et la théorie des ensembles ordonnés. La grande majorité des mathématiques plus avancées dépend, directement ou indirectement, de la théorie des ensembles (ou, au moins, est formulée en termes d'ensembles). Conséquemment, un des objectifs est de rendre les étudiants à l'aise avec le langage de la théorie des ensembles et d'illustrer comment des concepts mathématiques plus sophistiqués peuvent être définis avec des ensembles. Ceci constitue la partie « fondements » de ce cours.

Deuxièmement, ce cours cherche à instaurer, chez l'étudiant, une habileté à analyser les définitions abstraites, à travailler avec ces définitions, avec les exemples et les concepts reliés, puis à écrire des preuves en bonne et due forme. (Ceci constitue la partie « fondamentaux » du cours.) Des concepts comme les correspondances bijectives et les relations d'équivalence surviennent dans toutes les branches des mathématiques ; les maîtriser est essentiel à la réussite dans des cours de mathématiques plus avancés. Ceci peut s'accomplir en mettant l'emphase sur la structure logique sous-jacente à la matière, en portant une attention particulière à la clareté des formulations, aux cas extrêmes, aux exemples et aux contre-exemples, et aux stratégies de preuve.

Organisation

Les notes pour ce cours sont divisées en 21 leçons. Cette subdivision a été choisie de manière à ce que chaque leçon présente une seule idée ou famille cohérente d'idées. Les leçons correspondent à peu près à celles menées en classe, quoique nous devrions insister sur le fait que certaines leçons dans ces notes sont plus difficiles que d'autres.

Chaque leçon est organisée de la même façon. Le phénomène ou la question à être étudié est tout d'abord introduit, puis les idées connexes et pertinentes sont développées. La leçon se conclue ensuite avec un bref sommaire (pour faciliter les références) et une série d'exercices. Des solutions pour certains exercices (mais pas tous) sont donnés dans l'annexe. Nous avisons l'étudiant que les exercices varient en difficulté, en passant de l'élémentaire (au sens que votre compréhension des définitions est testée à travers un petit exemple concret) au plus avancé, voire même spéculatif.

Les trois premières leçons abordent les principes de base de la logique mathématique, quoique de manière informelle. L'objet de ces leçons est de permettre aux étudiants de développer quelques outils analytiques qui serviront pour le reste du cours. Par la suite, nous ferons constamment appel à ces notions de logique lorsque nous soulignerons la structure logique d'une idée mathématique dans nos discussions. Bien comprendre cette structure constitue la clé de ce qui nous permettra de travailler avec elle.

Nous avons également inclu une annexe contenant des lignes directrices pour vous guider dans l'écriture de preuves. Je vous recommande d'y jeter un coup d'oeil une fois que vous aurez étudié les trois premières leçons, puis de la lire plus en détails à nouveau lorsque vous serez amené à écrire vous-même des preuves.

Remerciements

La majeure partie du matériel pour ces notes a été écrite lors des sessions d'automne 2011 et 2012, lorsque j'ai donné le cours en question. Beaucoup d'étudiants ont fourni une rétroinformation utile, allant de la déclaration d'une simple erreur typographique à la mise en évidence de certaines lacunes pédagogiques. L'enseignement de ce cours en parallèle avec P. Scott donna lieu à de nombreuses discussions utiles quant au contenu du cours et à la présentation du matériel. Finalement, certains des conseils à l'égard de l'écriture de preuves trouvent leur origine dans un document écrit (pour des raisons similaires) par E. Cheng.

LEÇON I

Raisonnement mathématique

Nous commençons par étudier quelques-uns des principes de base de la logique. La logique est souvent définie comme l'*étude du raisonnement* ; le raisonnement mathématique est donc considéré comme l'objet d'étude de la logique mathématique. En particulier, un de ces objectifs est de donner un sens précis à ce que nous entendons par « argument valide » ou « preuve ».

Pour les discussions à venir, notre intention n'est pas d'effectuer un traitement complet de la logique mathématique. Nous cherchons plutôt à introduire un minimum d'outils en logique pour vous permettre de comprendre et analyser la structure des définitions, des preuves et contre-preuves, et de vous familiariser avec les méthodes usuelles liées au raisonnement mathématique.

I.1 Logique propositionnelle

Il existe plusieurs formes de logique. Dans cette section, nous abordons une forme relativement simple, quoique très utile, appelée *logique propositionnelle*.

Proposition :
Une *proposition* est une phrase déclarative ayant une valeur de vérité bien définie.

En d'autres termes, une proposition est une phrase qui déclare un état de fait (c'est ce que nous entendons par « phrase déclarative »), et cette dernière est soit vraie, soit fausse. (Nous stipulons qu'il y a exactement deux valeurs de vérité ; simplement dit : une proposition est soit vraie, soit fausse, mais

ne peut être rien entre les deux.[1]) Les exemples qui suivent nous donneront une image plus claire de ce qui constitue une proposition, et de ce qui n'en constitue pas.

Exemples I.1.1.

1. « Il y a une infinité de nombres premiers. » est une proposition (laquelle est vraie).
2. « 17 est pair. » est une proposition (laquelle est fausse).
3. « Tout mammifère est un animal. » est une proposition (laquelle est vraie).
4. « Le chat est sur le toit. » est une proposition.
5. « Le chat est-il sur le toit ? » n'est pas une proposition, mais une question.
6. « Ouvrez la fenêtre s'il vous plaît ! » n'est pas une proposition, mais une phrase impérative (un ordre).
7. « Soit p un nombre premier. » n'est pas une proposition ; c'est une phrase impérative (équivalente à « Supposons que p est un nombre premier. »)

En cas de doute, demandez-vous s'il est logique de dire que la phrase en question est soit vraie, soit fausse. Si vous ne pouvez attribuer une valeur de vérité à cette phrase, alors ce n'est pas une proposition.

Il est à noter que certaines propositions sont vraies (ou fausses) par définition des mots ou notions mathématiques employés. Par exemple, « 17 est pair » est fausse par définition du terme « pair », et « Tout mammifère est un animal. » est vraie, en vertue du sens du mot « mammifère ». Par contre, une proposition telle que « Le chat est sur le toit. » peut être vraie ou fausse ; cela dépend de la situation. Il est à noter également qu'il est possible de reconnaître un énoncé comme étant une proposition, même si l'on ne peut pas établir sa valeur de vérité. Un exemple bien connu est la phrase « Il existe une infinité de nombres naturels x tels que x et $x + 2$ sont tous les deux premiers. » (ceci s'appelle la *conjecture des nombres premiers jumeaux*).

I.2 Le calcul des propositions

L'idée de base qui sous-tend la logique propositionnelle est que des propositions simples peuvent être combinées en de plus complexes en utilisant des *connectifs* tels que « et », « ou », « si ... alors », et ainsi de suite. On introduit des symboles spéciaux pour dénoter ces derniers.

Conjonction

Le premier connectif est la *conjonction*, notée $\wedge$. Le sens attribué à $p \wedge q$ est « p *et* q ».

[1] Toutefois, si vous décidez de suivre un cours en logique mathématique, vous apprendrez qu'il y a des formes de logiques *multivalentes*, au sens qu'il y a plus de valeurs de vérité que seulement vrai ou faux. Par exemple, la logique intuitionniste rejette la loi du tiers exclu, et insiste qu'il y a au moins une valeur de vérité de plus. En logique probabiliste, vrai et faux sont considérés comme les extrêmes d'un continuum de valeurs de vérité, lesquelles sont en correspondance avec l'intervalle unité réel fermé $[0, 1]$. Ceci correspond à l'idée que nous assignons des probabilités à des propositions, afin de représenter la mesure dans laquelle nous croyons qu'elles sont vraies ou non.

Disjonction

Le deuxième connectif est la *disjonction*, notée $\vee$. Le sens attribué à $p \vee q$ est $\ll p$ *ou* $q \gg$. Dans la langue française, il arrive que le $\ll$ ou $\gg$ soit intentionnellement *inclusif* (c'est-à-dire : p ou q, ou possiblement les deux), et parfois il est *exclusif* (c'est-à-dire : p ou q, mais pas les deux). En logique propositionnelle, nous adoptons la convention que $\vee$ est interprété au sens inclusif.

Implication

Le troisième connectif est l'*implication*, notée $\rightarrow$. Le sens intentionnellement attribué à $p \rightarrow q$ est $\ll$ *si* p , *alors* $q \gg$, ou $\ll p$ *implique* $q \gg$. Dans la langue française, il y a plusieurs autres formulations que nous pouvons traduire en correspondance avec le symbole $\rightarrow$; veuillez-vous référer au tableau I.1 pour plus d'informations.

Biconditionnel

Le quatrième connectif est le *biconditionnel*, noté $\leftrightarrow$. Le sens attribué à $p \leftrightarrow q$ est $\ll p$ *si et seulement si* $q \gg$. On peut concevoir cette proposition comme étant la conjonction de $p \rightarrow q$ et $q \rightarrow p$.

Négation

Le dernier connectif est la *négation*, notée $\neg$. Le sens attribué à $\neg p$ est $\ll$ *non* $p \gg$, ou $\ll p$ est faux $\gg$.

Nous allons maintenant décrire de manière précise comment des propositions sont construites à partir des connectifs. Puisque nous ne nous intéressons pas véritablement au contenu des propositions, mais seulement à leur forme logique, nous allons employer les lettres $p, q, r, \ldots$ pour dénoter des propositions simples. Ces dernières sont généralement appelées *variables propositionnelles* ou *lettres propositionnelles*.

Définition I.2.1 (Calcul propositionnel)**.** La collection $PROP$ des propositions (formelles) est définie selon les clauses suivantes :

- Chaque variable propositionnelle est un élément de $PROP$.
- $\bot$ est un élément de $PROP$ et $\top$ est un élément de $PROP$.
- Si α, β sont dans $PROP$, alors $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$, $(\alpha \leftrightarrow \beta)$, $\neg\alpha$ le sont aussi.

Certaines remarques sont de mise. Premièrement, cette définition est un exemple de *définition inductive* : elle nous dit quelles sont les propositions de base, et puis comment bâtir de nouvelles propositions à partir d'anciennes. Il est important de noter que tout ce qui ne peut pas être obtenu en utilisant cette recette n'est pas, par définition, une proposition. (Dans une leçon subséquente, nous allons étudier les définitions inductives plus en détail ; pour l'instant, il suffit de comprendre que la définition fournit une méthode pour générer systématiquement toutes les propositions possibles.)

Ensuite, le symbole $\bot$ dénote *falsum* (ou *absurdité*), et représente une proposition qui est toujours fausse. Similairement, $\top$ dénote *verum* (ou *vrai*), et représente une proposition qui est toujours vraie. (La présence de $\top$ dans la définition est en fait redondante puisque nous pouvons concevoir ce dernier comme une abréviation de $\neg\bot$, mais ce n'est pas incommodant de l'incorporer.)

Finalement, nous employons des parenthèses pour désambiguïser les expressions, de la même manière qu'elles sont employées en arithmétique pour une expression comme $2 - 3 + 4$. Par contre, il y a des cas pour lesquels nous n'omettons pas les parenthèses, lorsque ces dernières ne créent pas d'ambiguïté — voir les exemples ci-bas.

Exemples I.2.2.

1. $(p \to \bot)$ est une proposition.

2. $p \to \bot$ n'est pas une proposition, techniquement, car il manque des parenthèses. Par contre, nous allons adhérer à la convention que les parenthèses externes peuvent être omises.

3. $(p \vee q) \to (p \wedge r)$ est une proposition (nous avons suivi la convention d'omettre les parenthèses externes ici).

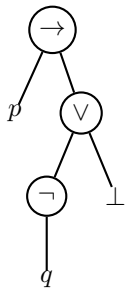
4. $p \vee q \wedge r$ n'est pas une proposition (l'expression est ambiguë car il y a deux façons de placer des parenthèses).

5. $\neg\neg\neg\neg\neg\top$ est une proposition.

6. $\neg \vee p$ n'est pas une proposition.

7. $p \wedge q \wedge r$ n'est pas une proposition, techniquement parlant, car les parenthèses internes sont absentes (on devrait écrire soit $p \wedge (q \wedge r)$, soit $(p \wedge q) \wedge r$). Tout de même, étant donné que nous verrons sous peu que les deux expressions avec des parenthèses sont logiquement équivalentes, nous allons omettre ces parenthèses. Le même principe s'applique pour des disjonctions itérées (mais *pas* pour des implications itérées !).

Une perspective un peu différente, quoique plus visuelle, est souvent utile. Étant donné une proposition, nous pouvons représenter cette dernière sous la forme d'un *arbre de construction*. Par exemple, la proposition $p \to (\neg q \vee \bot)$ peut être représentée par l'arbre



Ainsi, les *feuilles* de l'arbre sont des propositions de base (variables et $\top, \bot$) qui figurent dans la proposition $p \to (\neg q \vee \bot)$, tandis que les points de branchement sont étiquetés par des connectifs. Chaque proposition peut être représentée de cette façon, et nous pouvons toujours récupérer une proposition à partir de l'arbre qui la représente. Plus d'exemples liés à ces représentations sont donnés dans les exercices.

I.3 Traduction

Nous pouvons maintenant passer à l'art de traduire des énoncés (ou arguments) du français au calcul propositionnel. Nous présentons tout d'abord un exemple simple pour clarifier le type de procédure que nous avons à l'esprit.

Exemple I.3.1. Considérez la phrase suivante :

> S'il pleut et que vous n'avez pas de parapluie, vous allez vous mouiller.

Pour traduire cette phrase en logique propositionnelle, il est à noter qu'il s'agit d'une phrase composée, construite à partir de trois phrases plus petites. Nous assignons une lettre propositionnelle à chacune de ces phrases :

p – Il pleut.

q – Vous avez un parapluie.

r – Vous allez vous mouiller.

Une traduction possible est alors $(p \wedge \neg q) \rightarrow r$.

En général, lorsque vous traduisez un énoncé du français à la logique propositionnelle, identifiez toujours les propositions de base de l'énoncé pour commencer (i.e. les propositions qui ne peuvent pas être décomposées en phrases plus petites à l'intérieur de l'énoncé). Assignez des lettres propositionnelles à chacune de ces propositions de base et, ensuite, effectuez la traduction en considérant attentivement, dans l'énoncé, les mots français qui correspondent aux connectifs.

Pour de nombreux cas de traduction, il y a plusieurs solutions possibles. La traduction n'est pas nécessairement facile car il n'est pas toujours évident de savoir quels connectifs employer et comment les employer, et aussi, parce que le langage naturel comporte des connotations subtiles qu'on ne peut pas toujours facilement traduire dans le langage rigoureux du calcul propositionnel. De plus, le français (comme tout autre langage naturel) n'a pas été conçu avec la précision des mathématiques à l'esprit et, ainsi, certains énoncés en français peuvent être ambiguës ou imprécis du point de vue de la logique mathématique. Pour ces cas où il y a ambiguïtés, nous devons faire appel à notre meilleur jugement pour trouver la traduction dont le sens est le plus fidèle à l'original.

Une partie de l'objectif derrière ces exercices de traduction en logique formelle est d'éliminer ces ambiguïtés et de donner des formulations mathématiques précises. Le tableau I.1 donne une liste de certaines constructions standards et de leurs traductions. Il convient de porter une attention particulière à la différence entre « Si p , alors q », « p si q » et « p seulement si q ».

Français	Traduction
p et q (les deux)	$p \wedge q$
p ou q p et (ou) q	$p \vee q$
Soit p , soit q (mais pas les deux)	$(p \vee q) \wedge \neg(p \wedge q)$
p implique q Si p , alors q p seulement si q q si p p est une condition suffisante pour q q est une condition nécessaire pour p	$p \to q$
p à moins que q	$\neg q \to p$
p si et seulement si q p ssi q p est nécessaire et suffisant pour q	$p \leftrightarrow q$
p est faux non p Ce n'est pas le cas que p	$\neg p$

Tableau I.1 – Traductions courantes

Nous donnons quelques exemples de traductions. Pour chacun d'entre eux, nous utilisons les associations suivantes :

p – Les frites sont bonnes pour la santé.

q – Vous mettez de la mayonnaise sur vos frites.

r – Les frites sont délicieuses.

Exemples I.3.2. Traduisez les énoncés suivants du français à la logique propositionnelle :

(a) Si vous ne mettez pas de mayonnaise sur vos frites, alors elles ne sont pas délicieuses.

(b) Les frites sont délicieuses, mais elles ne sont pas bonnes pour la santé.

(c) Les frites sont mauvaises pour la santé seulement si vous mettez de la mayonnaise dessus.

(d) Les frites sont délicieuses, même sans mayonnaise.

(e) À moins que vous mettiez de la mayonnaise sur vos frites, celles-ci sont bonnes pour la santé.

(f) Il n'est pas vrai que les frites sont mauvaises pour la santé.

(g) Le fait que les frites sont délicieuses n'implique pas qu'elles sont bonnes pour la santé.

(h) Les frites ne sont pas délicieuses sans mayonnaise, mais elles ne sont pas bonnes pour la santé avec de la mayonnaise.

(i) Pour que des frites soient bonnes pour la santé, il est nécessaire mais pas suffisant que vous ne mettiez pas de mayonnaise sur elles.

Solutions. Comme stratégie générale, commencez par identifier le *connectif principal* de la phrase (à l'intérieur de l'arbre de construction, il correspond au connectif qui étiquette la racine de l'arbre). Ensuite, décomposez le problème en plus petites parties.

(a) $\neg q \to \neg r$. (Notez que le connectif principal est « si ..., alors ... ».)

(b) $r \wedge \neg p$.

(c) $\neg p \to q$.

(d) $r \wedge \neg(\neg q \to \neg r)$. (Littéralement : les frites sont délicieuses et ce n'est pas le cas qu'elles ne sont pas délicieuses si vous ne mettez pas de mayonnaise dessus.) Si vous aviez plutôt lu : « Les frites sont délicieuses avec de la mayonnaise, mais sans mayonnaise aussi. » alors vous pourriez employer $(q \to r) \wedge (\neg q \to r)$.

(e) $\neg p \to q$. Comme alternative, vous pourriez utiliser $\neg q \to p$.

(f) $\neg\neg p$.

(g) $\neg(r \to p)$.

(h) $(\neg q \to \neg r) \wedge (q \to \neg p)$.

(i) $(\neg q \to p) \wedge \neg(p \to \neg q)$.

I.4 Sommaire

La logique propositionnelle est utilisée pour mener un raisonnement sur des *propositions*, c'est-à-dire, sur des énoncés qui ont une valeur de vérité bien définie. L'idée de base qui sous-tend la logique propositionnelle est que les propositions sont construites à partir de propositions de base (des variables propositionnelles et les deux propositions spéciales $\bot$ et $\top$), en utilisant les *connectifs propositionnels* $\wedge$, $\vee$, $\to$, $\leftrightarrow$, $\neg$.

- Chaque proposition peut être représentée sous la forme d'un *arbre de construction*.
- Les connectifs propositionnels ont un sens précis dans le calcul propositionnel, alors qu'en français, il peut y avoir plusieurs mots ou phrases pour lesquels la traduction emploie le même connectif (par exemple, « Si p , alors q » et « p seulement si q » se traduisent tous les deux par $p \to q$).

I.5 Exercices

Exercice 1. Parmi les énoncés suivants, lesquels sont des propositions ? Expliquez pourquoi (ou pourquoi pas).

(a) Il n'existe pas de telle chose qu'un dîner gratuit.

(b) Si un dîner est gratuit, alors il y a une attrape.

(c) Quelle est l'attrape avec ce dîner gratuit ?

(d) J'ai faim, mangeons !

(e) $2 + 2 = 5$.

(f) Supposons que f est une fonction différentiable ; alors f est continue.

(g) Si f est une fonction différentiable, alors elle est aussi continue.

(h) Trouvez une dérivée de f et servez-vous de cette dernière pour démontrer que f est continue.

(i) La logique propositionnelle est inutile.

(j) Ceci n'est pas une proposition.

Exercice 2. Parmi les expressions suivantes, lesquelles sont des formules propositionnelles bien formées (des éléments de $PROP$) ? Pour les expressions qui sont des propositions bien formées, indiquez le connectif principal.

(a) $p \wedge (q \vee r)$

(b) $p \wedge q \wedge r$

(c) $p \neg q$

(d) $p \leftrightarrow q \leftrightarrow r$

(e) $\neg(p \rightarrow r) \wedge \neg s$

(f) $p \wedge (p \wedge (p \wedge (p \wedge p)))$

(g) $((((p \vee p) \vee p) \vee p$

(h) $\bot \leftrightarrow \top$

(i) $\neg\bot \vee \neg$

(j) $\neg\neg\neg\top\top$

Exercice 3. Pour chacune des formules propositionnelles suivantes, dessinez l'arbre de construction.

(a) $p \wedge q$

(b) $\bot$

(c) $\neg\neg\neg\top$

(d) $(p \vee q) \wedge (q \rightarrow \neg p)$

(e) $\neg\bot \vee \neg\top$

Exercice 4. Dans le calcul propositionnel, les parenthèses sont nécessaires pour désambiguïser des expressions. Lorsqu'on utilise un arbre de construction par contre, nous n'avons pas besoin de parenthèses. Expliquez pourquoi cela ne constitute pas un problème dans ce cas. Plus précisément, expliquez pourquoi différents agencements de parenthèses pour une même expression donneront des arbres de construction différents.

Exercice 5. Considérez les propositions suivantes :

p – Les politiciens sont corrompus.

q – Les politiciens gardent leurs promesses.

r – Voter a du sens.

Traduisez les phrases suivantes en logique propositionnelle :

(a) Voter n'a pas de sens si les politiciens ne gardent pas leurs promesses.

(b) Voter a du sens seulement si les politiciens gardent leurs promesses.

(c) Quoique les politiciens soient corrompus, ils gardent quand même leurs promesses.

(d) Les politiciens ne gardent pas leurs promesses, même s'ils ne sont pas corrompus.

(e) Voter a du sens seulement lorsque les politiciens ne sont pas corrompus et qu'ils ne brisent pas leurs promesses.

(f) Si les politiciens ne gardent pas leurs promesses ou s'ils sont corrompus, voter n'a pas de sens.

Exercice 6. Traduisez les énoncés suivants en logique propositionnelle.

(a) Je porte des gants s'il fait très froid.

(b) Lorsque je porte des gants, je ne peux pas cuisiner.

(c) Soit je ne porte pas de gants et je suis en mesure de cuisiner, soit je porte des gants mais je ne peux pas cuisiner.

(d) Est-ce que le fait que je porte des gants est une condition nécessaire pour qu'il fasse froid, ou est-ce seulement une condition suffisante ?

(e) Je peux cuisiner de la nourriture, à moins qu'il fasse froid ou que je porte des gants.

(f) Non seulement je ne suis pas en mesure de cuisiner, mais il fait également très froid.

Exercice 7. Analysez la structure propositionnelle de l'énoncé

> La conjecture des nombres premiers jumeaux implique qu'il existe une infinité de nombres premiers, mais ces deux propositions ne sont pas équivalentes.

(Vous pouvez traduire « p est équivalent à q » par $p \leftrightarrow q$, et considérer la conjecture des nombres premiers jumeaux comme une proposition de base.)

LEÇON II

Vérité et validité

Maintenant que la logique propositionnelle a été introduite, nous nous tournons vers la question de ce qui constitue une valeur de vérité pour une proposition, et de ce qui constitue un raisonnement valide. Nous explorons deux techniques pour étudier ces aspects : les lois de l'algèbre booléenne et les tables de vérité. (Il y a d'autres méthodes utiles (notamment les arbres de vérité), mais à cet effet, nous allons référer le lecteur intéressé à d'autres textes.)

II.1 Tables de vérité

Rappelons-nous que la collection des propositions est définie par induction, au sens que nous avons tout d'abord spécifié des propositions de base, et ensuite des méthodes pour construire de nouvelles propositions à partir d'anciennes. Ceci guarantit que chaque proposition est construite à partir de propositions de base en employant des connectifs, et ainsi, nous pouvons systématiquement décomposer une proposition en ses composantes. Ceci est particulièrement utile lorsque nous sommes intéressés à la *valeur de vérité* d'une proposition ; c'est-à-dire, lorsque nous voulons savoir si une proposition est vraie ou fausse. La définition qui suit présente une des multiples façons de spécifier comment la valeur de vérité d'une proposition complexe dépend de celle de chacune de ses composantes. Pour ce qui suit, nous écrivons V et F pour désigner les deux valeurs de vérité possibles (vrai et faux, respectivement) ; comme alternative, nous employons aussi 1 et 0. (Certains textes utilisent $\top$ et $\bot$, mais nous avons déjà réservé ces symboles pour désigner autre chose ; i.e., ils représentent verum et falsum, deux propositions spéciales de base.)

Définition II.1.1 (Valuation)**.** Une *valuation* est une fonction[1] $v : \text{PROP} \to \{\mathsf{V}, \mathsf{F}\}$ avec les propriétés suivantes :

- $v(\top) = \mathsf{V}$
- $v(\bot) = \mathsf{F}$
- $v(\alpha \wedge \beta) = \begin{cases} \mathsf{V} & \text{si } v(\alpha) = \mathsf{V} = v(\beta) \\ \mathsf{F} & \text{autrement.} \end{cases}$
- $v(\alpha \vee \beta) = \begin{cases} \mathsf{V} & \text{si } v(\alpha) = \mathsf{V} \text{ ou } v(\beta) = \mathsf{V} \text{ (ou les deux)} \\ \mathsf{F} & \text{autrement.} \end{cases}$
- $v(\alpha \to \beta) = \begin{cases} \mathsf{F} & \text{si } v(\alpha) = \mathsf{V} \text{ et } v(\beta) = \mathsf{F} \\ \mathsf{V} & \text{autrement.} \end{cases}$
- $v(\alpha \leftrightarrow \beta) = \begin{cases} \mathsf{V} & \text{si } v(\alpha) = v(\beta) \\ \mathsf{F} & \text{autrement.} \end{cases}$
- $v(\neg\alpha) = \begin{cases} \mathsf{F} & \text{si } v(\alpha) = \mathsf{V} \\ \mathsf{V} & \text{si } v(\alpha) = \mathsf{F}. \end{cases}$

Remarquez qu'il n'y a pas de conditions sur les valeurs de vérité assignées aux variables propositionnelles. Or, l'idée derrière cette définition est que, dans la mesure où nous avons spécifié les valeurs de vérité pour les variables propositionnelles, les clauses ci-haut nous disent précisément ce que sont les valeurs de vérité des propositions complexes.

À remarquer également en ce qui a trait à la règle de l'implication : une implication est fausse lorsque son *antécédent* est vrai et son *conséquent* faux. Autrement, *une implication est automatiquement vraie lorsque son antécédent est faux*, et elle est aussi automatiquement vraie lorsque son conséquent est vrai. (On se réfère parfois à ces cas comme étant des cas de *vérité vide* (c'est-à-dire vide de sens.)) Par exemple, l'implication

> Si la lune est faite de fromage bleu, alors 3+3=5.

est vraie, parce que son hypothèse « La lune est faite de fromage bleu » est fausse. Similairement,

> Si les frites sont bonnes pour la santé, alors 2+2=4.

est vraie, parce que sa conclusion « $2 + 2 = 4$ » est vraie. (Cela n'importe pas que les frites soient bonnes ou non pour la santé.)

Voici quelques exemples illustrant la méthode de calcul pour déterminer des valeurs de vérité.

Exemple II.1.2. Supposons que v est une valuation telle que $v(p) = v(q) = \mathsf{V}$ et $v(r) = \mathsf{F}$. Alors,

1. $v(p \wedge (q \vee r)) = \mathsf{V}$ car $v(q \vee r) = \mathsf{V} = v(p)$.
2. $v(p \to \neg q) = \mathsf{F}$ car $v(p) = \mathsf{V}$ et $v(\neg q) = \mathsf{F}$.

[1] Je suppose que vous savez déjà ce qu'est une fonction, à un niveau informel au moins. Les précisions viendront plus tard.

3. $v(p \to \neg r) = \mathsf{V}$ car $v(\neg r) = \mathsf{V}$.
4. $v(\bot \to (p \wedge r)) = \mathsf{V}$ car $v(\bot) = \mathsf{F}$.

Il existe une autre méthode pour déterminer la valeur de vérité d'une proposition complexe en fonction de ses composantes. Il s'agit de la méthode des *tables de vérité*. L'idée est de faire la liste de toutes les combinaisons possibles de valeurs de vérité pour les propositions de base qui figurent dans la proposition complexe, puis d'utiliser les règles pour les connectifs afin d'établir la valeur de vérité de la proposition complexe pour chaque combinaison.

Pour la proposition $p \wedge q$, par exemple, nous avons la table de vérité suivante :

p	q	$p \wedge q$
F	F	F
F	V	F
V	F	F
V	V	V

Notons qu'il y a quatre rangées : chacun de p et q a deux valeurs de vérité possibles, V ou F ; donc, il y a $2 \cdot 2 = 4$ combinaisons possibles.

Voici les tables de vérité pour les autres connectifs :

p	q	$p \vee q$
F	F	F
F	V	V
V	F	V
V	V	V

p	q	$p \to q$
F	F	V
F	V	V
V	F	F
V	V	V

p	q	$p \leftrightarrow q$
F	F	V
F	V	F
V	F	F
V	V	V

p	$\neg p$
F	V
V	F

Nous pouvons maintenant nous servir de ces dernières pour déterminer les tables de vérité de propositions plus compliquées. Par exemple, la table de vérité de $\neg p \leftrightarrow (q \vee \neg p)$ est

p	q	$\neg p$	$q \vee \neg p)$	$\neg p \leftrightarrow (q \vee \neg p)$
F	F	V	V	V
F	V	V	V	V
V	F	F	F	V
V	V	F	V	F

La table de vérité de $(p \wedge q) \to (p \vee (\neg r \wedge \neg q))$ est

p	q	r	$\neg q$	$\neg r$	$\neg r \wedge \neg q$	$p \vee (\neg r \wedge \neg q)$	$p \wedge q$	$(p \wedge q) \to (p \vee (\neg r \wedge \neg q))$
F	F	F	V	V	V	V	F	V
F	F	V	V	F	F	F	F	V
F	V	F	F	V	F	F	F	V
F	V	V	F	F	F	F	F	V
V	F	F	V	V	V	V	F	V
V	F	V	V	F	F	V	F	V
V	V	F	F	V	F	V	V	V
V	V	V	F	F	F	V	V	V

Cette table de vérité a un trait particulier : dans chaque rangée, la valeur de vérité de la proposition $(p \wedge q) \to (p \vee (\neg r \wedge \neg q))$ est V. On attribue un nom particulier à ce genre de proposition :

Définition II.1.3 (Tautologie)**.** Une proposition est appelée une *tautologie* lorsque sa valeur de vérité est V dans chaque rangée de sa table de vérité.

Ceci veut dire qu'une tautologie est vraie, peu importe les valeurs de vérité assignées aux lettres propositionnelles. À l'extrême opposé, nous avons :

Définition II.1.4 (Contradiction)**.** Une proposition est une *contradiction* lorsque sa valeur de vérité est F dans chaque rangée de sa table de vérité.

Il est clair qu'une proposition ne peut être une tautologie et une contradiction en même temps.

Définition II.1.5 (Contingence)**.** Une proposition est dite *contingente* (aussi : *satisfaisable*) lorsque sa valeur de vérité est V dans au moins une rangée de sa table de vérité.

Exemple II.1.6. La formule $(p \vee q) \leftrightarrow (\neg q \wedge \neg p)$ est une contradiction. Sa table de vérité est

p	q	$\neg p$	$\neg q$	$\neg q \wedge \neg p$	$p \vee q$	$(p \vee q) \leftrightarrow (\neg q \wedge \neg p)$
F	F	V	V	V	F	F
F	V	V	F	F	V	F
V	F	F	V	F	V	F
V	V	F	F	F	V	F

et nous pouvons observer que la formule en question est fausse dans chaque rangée ci-haut.

Exemple II.1.7. Considérez la proposition $(p \vee q) \to (\neg q \wedge \neg p)$. Sa table de vérité est

p	q	$\neg p$	$\neg q$	$\neg q \wedge \neg p$	$p \vee q$	$(p \vee q) \to (\neg q \wedge \neg p)$
F	F	V	V	V	F	V
F	V	V	F	F	V	F
V	F	F	V	F	V	F
V	V	F	F	F	V	F

Puisque la formule en question est vraie pour au moins une des rangées, il s'agit d'une formule contingente. D'ailleurs, à travers cet exemple, nous pouvons constater que certaines propositions sont ni une contradiction, ni une tautologie.

Le dernier concept que nous introduisons pour cette section est celui d'une équivalence logique.

Définition II.1.8 (Équivalence logique)**.** Deux propositions p et q sont *logiquement équivalentes* lorsque p et q ont les mêmes valeurs de vérité pour chaque rangée de leur table de vérité.

Notation : $p \equiv q$.

De manière équivalente, $p \equiv q$ lorsque la proposition $p \leftrightarrow q$ est une tautologie.

Exemple II.1.9. Les propositions $p \to \neg q$ et $\neg(p \wedge q)$ sont équivalentes. En effet, considérez la table de vérité suivante :

p	q	$p \to \neg q$	$\neg(p \wedge q)$
F	F	V	V
F	V	V	V
V	F	V	V
V	V	F	F

Dans chaque rangée, les deux propositions ont les mêmes valeurs de vérité.

Par contraste, les propositions $p \to \neg q$ et $\neg p \vee q$ ne sont pas équivalentes, et on peut le constater avec la table suivante :

p	q	$p \to \neg q$	$\neg p \vee q$
F	F	V	V
F	V	V	V
V	F	V	F
V	V	F	V

Dans les rangées 3 et 4, les propositions ont des valeurs de vérité qui diffèrent.

II.2 Validité des arguments

Il y a davantage au raisonnement que de simplement déterminer la valeur de vérité d'une seule proposition. La plupart du temps, nous voulons savoir si une chaîne d'inférence est correcte, étape par étape. Pour commencer, nous définissons la forme générale que prend un argument.

Définition II.2.1. Un *argument* consiste en deux choses :

- Une collection de propositions appelées *hypothèses* (ou *suppositions*)
- Une proposition appelée *conclusion*.

En général, on peut aisément déterminer quelle partie de l'argument est une conclusion, car celle-ci est souvent précédée du mot « Donc ». (Par contre, dans certains cas, l'ordre est inversé : la conclusion est énoncée en premier, puis les hypothèses sont listées, typiquement précédées par « Parce que ».) Schématiquement, un argument prend la forme suivante :

$$\begin{array}{c} \text{Hypothèse 1} \\ \text{Hypothèse 2} \\ \vdots \\ \text{Hypothèse } n \\ \hline \text{Conclusion} \end{array}$$

Voici un exemple d'argument :

> S'il pleut et si vous n'avez pas de parapluie, alors vous allez vous mouiller. Il pleut, et vous avez un parapluie. Donc, vous n'allez pas vous mouiller.

En séparant les suppositions de la conclusion, nous obtenons

$$\frac{\begin{array}{c}\text{S'il pleut et si vous n'avez pas de parapluie, alors vous allez vous mouiller.}\\ \text{Il pleut, et vous avez un parapluie.}\end{array}}{\text{Vous n'allez pas vous mouiller.}}$$

Est-ce un argument valide ? Nous devons d'abord préciser ce que nous entendons par « argument valide ». Un argument tend à affirmer que la conclusion suit logiquement des hypothèses. Il importe peu que les hypothèses soient vraies ou non ; l'important est que la conclusion soit vraie lorsque les hypothèses sont vraies. Ceci nous mène à :

Définition II.2.2 (Validité d'un argument)**.** Considérez un argument dont les hypothèses sont $p_1, \ldots, p_n$ et dont la conclusion est q. On dit que cet argument est *valide* si pour chaque valuation v pour laquelle $v(p_1) = \mathsf{V}, \ldots, v(p_n) = \mathsf{V}$, on a $v(q) = \mathsf{V}$ aussi.

Cette condition peut être vérifiée en utilisant des tables de vérité : pour qu'un argument soit valide, il faut s'assurer que dans chaque rangée où tous les p_i sont vraies, on a que q est vraie également. Dans le cas contraire où nous voulons vérifier si un argument est invalide, nous devons trouver une rangée dans la table de vérité où tous les p_i sont vraies, mais où q est faux.

Retournons à l'argument donné en exemple. Afin d'effectuer une analyse de ce dernier, nous le traduisons en logique propositionnelle en premier. Assignons les lettres propositionnelles suivantes :

- p – Il pleut.
- q – Vous avez un parapluie.
- r – Vous allez vous mouiller.

La traduction de l'argument est ensuite donnée par

$$\frac{\begin{array}{c}(p \wedge \neg q) \to r\\ p \wedge q\end{array}}{\neg r}$$

La table de vérité pour cet argument est

p	q	r	$(p \wedge \neg q) \to r$	$p \wedge q$	$\neg r$
F	F	F	V	F	V
F	F	V	V	F	F
F	V	F	V	F	V
F	V	V	V	F	F
V	F	F	F	F	V
V	F	V	V	F	F
V	V	F	V	V	V
V	V	V	V	V	F

Il y a exactement deux rangées de la table dans lesquelles toutes les hypothèses sont vraies ; il s'agit des 7^e et 8^e rangées. Nous devons vérifier si la conclusion $\neg r$ est également vraie dans ces rangées. En fait, nous observons que $\neg r$ est fausse dans la 8^e. Ceci veut dire que l'argument est invalide. (Si vous avez imaginé que l'argument était valide à priori, vous avez omis de considérer la possibilité que vous pouvez vous mouiller, même en ayant un parapluie — en raison de l'éclaboussure causée par une voiture passante, par exemple.)

Proposition II.2.3. *Un argument avec hypothèses $p_1, \ldots, p_n$ et conclusion q est valide si et seulement si la proposition $p_1 \wedge p_2 \wedge \cdots \wedge p_n \to q$ est une tautologie.*

Démonstration. C'est une conséquence de la définition des tables de vérité et des connectifs $\wedge$ et $\to$. □

J'aimerais terminer cette section en soulignant qu'il y a un aspect peu compris par rapport à la validation d'un argument, c'est-à-dire : *Si une des hypothèses de l'argument est une contradiction, alors l'argument est automatiquement valide !* (Aussi, si la conclusion est une tautologie, alors l'argument est valide, peu importe en quoi consistent les hypothèses.) Ceci est une conséquence de la définition de la table de vérité pour l'implication.

II.3 Lois de l'algèbre booléenne

Les tables de vérité sont fiables et fournissent une méthode directe pour déterminer si une proposition est une tautologie, une contradiction ou une contingence. Elles peuvent également être utilisées pour déterminer la validité d'un argument et pour tester une équivalence logique entre des propositions. Toutefois, il faut beaucoup de temps pour construire les tables de vérité, et dans plusieurs cas, une approche plus algébrique est utile.

L'approche algébrique se base sur le fait qu'un petit nombre d'équivalences logiques omniprésentes suffit pour obtenir toutes les autres. Nous faisons la liste de ces équivalences importantes dans le tableau II.1.

Ces équivalences sont appelées les lois de la logique propositionnelle, ou les lois de l'algèbre booléenne. Lorsqu'on parle d'une preuve algébrique de l'équivalence entre deux propositions, on veut dire une preuve qui consiste en une séquence d'applications de règles provenant du tableau II.1. (Ceci veut dire que vous ne pouvez pas utiliser d'autres équivalences que celles fournies dans ce tableau.)

1.	$p \wedge q$	$\equiv$	$q \wedge p$	commutativité de $\wedge$
2.	$p \wedge (q \wedge r)$	$\equiv$	$(p \wedge q) \wedge r$	associativité de $\wedge$
3.	$p \wedge p$	$\equiv$	p	idempotence de $\wedge$
4.	$p \wedge \top$	$\equiv$	p	$\top$ est un élément neutre pour $\wedge$
5.	$p \wedge \bot$	$\equiv$	$\bot$	$\bot$ est un élément absorbant pour $\wedge$
6.	$p \vee q$	$\equiv$	$q \vee p$	commutativité de $\vee$
7.	$p \vee (q \vee r)$	$\equiv$	$(p \vee q) \vee r$	associativité de $\vee$
8.	$p \vee p$	$\equiv$	p	idempotence de $\vee$
9.	$p \vee \top$	$\equiv$	$\top$	$\top$ est un élément absorbant pour $\vee$
10.	$p \vee \bot$	$\equiv$	p	$\bot$ est un élément neutre pour $\vee$
11.	$p \wedge (q \vee r)$	$\equiv$	$(p \wedge q) \vee (p \wedge r)$	distributivité de $\wedge$ sur $\vee$
12.	$p \vee (q \wedge r)$	$\equiv$	$(p \vee q) \wedge (p \vee r)$	distributivité de $\vee$ sur $\wedge$
13.	$\neg\neg p$	$\equiv$	p	double négation
14.	$\neg(p \wedge q)$	$\equiv$	$\neg p \vee \neg q$	Loi de De Morgan
15.	$\neg(p \vee q)$	$\equiv$	$\neg p \wedge \neg q$	Loi de De Morgan
16.	$p \vee \neg p$	$\equiv$	$\top$	Loi du tiers exclu
17.	$\neg\top$	$\equiv$	$\bot$	
18.	$p \to q$	$\equiv$	$\neg p \vee q$	
19.	$p \leftrightarrow q$	$\equiv$	$(p \to q) \wedge (q \to p)$	
20.	$p \leftrightarrow q$	$\equiv$	$(p \wedge q) \vee (\neg p \wedge \neg q)$	

Tableau II.1 – Lois de la logique propositionnelle

Voici quelques exemples d'équivalences :

Exemples II.3.1.

1. Prouvez que $p \wedge \neg p \equiv \bot$ en utilisant les lois de l'algèbre booléenne.

   Solution. En employant les équivalences du tableau II.1, nous avons

   $$\begin{array}{rcll} p \wedge \neg p & \equiv & \neg\neg p \wedge \neg p & \text{par 13.} \\ & \equiv & \neg(\neg p \vee p) & \text{par 15.} \\ & \equiv & \neg\top & \text{par 16.} \\ & \equiv & \bot & \text{par 17.} \end{array}$$

2. Prouvez que $\neg(p \vee q) \to r$ et $(p \vee r) \vee q$ sont équivalents.

   Solution. Il suffit d'utiliser les équivalences suivantes :

   $$\begin{array}{rcll} \neg(p \vee q) \to r & \equiv & \neg\neg(p \vee q) \vee r & \text{par 18.} \\ & \equiv & (p \vee q) \vee r & \text{par 13.} \\ & \equiv & p \vee (q \vee r) & \text{par 7.} \\ & \equiv & p \vee (r \vee q) & \text{par 6.} \\ & \equiv & (p \vee r) \vee q & \text{par 7.} \end{array}$$

3. Prouvez que $(p \wedge q) \wedge (p \wedge r) \equiv (p \wedge q) \wedge r$.

   Solution. Avec l'approche algébrique, nous avons

$$\begin{array}{rcll} (p \wedge q) \wedge (p \wedge r) & \equiv & ((p \wedge q) \wedge p) \wedge r & \text{par 2.} \\ & \equiv & ((q \wedge p) \wedge p) \wedge r & \text{par 1.} \\ & \equiv & (q \wedge (p \wedge p)) \wedge r & \text{par 2.} \\ & \equiv & (q \wedge p) \wedge r & \text{par 3.} \\ & \equiv & (p \wedge q) \wedge r & \text{par 1.} \end{array}$$

Plusieurs autres exemples de l'approche algébrique figurent dans les exercices pour cette leçon. Nous terminons cette section avec deux observations élémentaires, quoique importantes, en ce qui concerne les implications. Des erreurs sont souvent commises à ce niveau, donc assurez-vous de bien comprendre ces observations.

Définition II.3.2 (Réciproque, contraposée)**.** Soit $p \to q$, une implication propositionnelle. Alors,

- La *contraposée* de $p \to q$ est la proposition $\neg q \to \neg p$
- La *réciproque* de $p \to q$ est la proposition $q \to p$.

En utilisant les lois de l'algèbre booléenne, on peut démontrer que $p \to q$ est équivalent à sa contraposée $\neg q \to \neg p$:

$$\begin{array}{rcl} \neg q \to \neg p & \equiv & \neg\neg q \vee \neg p \\ & \equiv & q \vee \neg p \\ & \equiv & \neg p \vee q \\ & \equiv & p \to q \end{array}$$

(nous vous laissons comme exercice de trouver quelles règles du tableau II.1 ont été employées ci-haut). La contraposée est souvent utile en pratique : pour démontrer que p implique q, nous pouvons démontrer, comme alternative, que $\neg q$ implique $\neg p$. Par exemple, les énoncés

(i) Si une matrice est inversible, alors elle n'a pas de rangée de zéros.

(ii) Si une matrice a une rangée de zéros, alors elle n'est pas inversible.

sont des contraposées l'un par rapport à l'autre, et ainsi, ils sont logiquement équivalents.

Or, $p \to q$ n'est pas équivalent à sa réciproque $q \to p$ en général. En effet, l'énoncé

(iii) Si la matrice n'a pas de rangée de zéros, alors elle est inversible.

est la réciproque de (i), mais il est faux. (Tandis que (i) est vrai.)

Similairement, la *négation* $\neg(p \to q)$ n'est généralement pas équivalente à la contraposée de $p \to q$, ni même à sa réciproque. (Construisez les tables de vérité pour vous convaincre de ce fait.)

II.4 Chevaliers et coquins

L'île des chevaliers et des coquins est habitée par exactement deux types d'habitants : les chevaliers, qui disent toujours la vérité, et les coquins, qui disent toujours des mensonges. (Il n'existe pas d'autres types d'habitants sur l'île, et il n'y a pas de façon de dire si un habitant est un chevalier ou un coquin simplement en le regardant.) Ceci donne lieu à des situations énigmatiques telles que la suivante :

> Un jour, vous arrivez sur l'île, et deux habitants vous approchent. L'un d'eux vous dit : « Au moins l'un de nous est un coquin ».

Pouvez-vous déterminer le(s) type(s) de ces habitants ? Nous pouvons raisonner comme suit. Premièrement, nous remarquons qu'il n'est pas possible que ces deux habitants soient des chevaliers. Si c'était le cas, l'énoncé ci-haut serait faux, et ceci impliquerait que la personne qui l'a énoncé ment (contrairement à la supposition que nous sommes en présence de chevaliers). Donc, au moins un de ces habitants est un coquin, et ceci veut dire que l'énoncé ci-haut est vrai. Mais dans ce cas, la personne qui a formulé cet énoncé est un chevalier. Ceci veut dire que l'autre habitant est un coquin.

Des problèmes de ce genre, même s'ils semblent distants de la pratique des mathématiques au quotidien, sont inclus ici pour les raisons suivantes :

- Ils constituent de bons exercices pour le raisonnement systématique.
- Ils vous force à raisonner dans le cadre de la logique propositionnelle, en particulier, avec les négations.
- Même si cela est peu apparent, il y a des situations en mathématiques où l'on retrouve des problèmes présentant de nombreuses similarités avec ceux de l'île des chevaliers et coquins.

II.5 Sommaire

Un trait important de la logique propositionnelle est que la valeur de vérité d'une proposition complexe est complètement déterminée par la valeur de vérité des lettres propositionnelles qui figurent dans cette dernière. Pour déterminer la valeur de vérité d'une proposition complexe, il y a deux méthodes (essentiellement similaires) :

- La méthode des *valuations*
- La méthode des *tables de vérité*

Nous pouvons aussi identifier trois classes de propositions : les tautologies, les contradictions et les contingences. Les tables de vérité peuvent être employées pour déterminer à quelle catégorie une proposition appartient.

La notion d'*équivalence logique* est aussi définie en fonction des tables de vérité : deux formules sont équivalentes lorsque leurs tables de vérité sont identiques.

Un *argument* consiste en une collection d'hypothèses $p_1, \ldots, p_n$ et une conclusion q. Un tel argument est dit valide lorsque l'implication $p_1 \wedge \cdots \wedge p_n \to q$ est une tautologie.

Finalement, les lois de l'algèbre booléenne peuvent être employées pour générer des preuves efficaces pour des équivalences logiques. Lorsqu'on demande de prouver une équivalence à partir de ces lois, vous devez utiliser ces lois et aucune autre. Vous devez également spécifier, à chaque étape, laquelle de ces lois vous avez utilisée.

II.6 Exercices

Exercice 8. Construisez les tables de vérité pour chacune des formules propositionnelles suivantes. Utilisez ces tables de vérité pour répondrte aux questions suivantes : la formule est-elle une tautologie ? une contradiction ? une contingence ?

(a) $p \to \neg p$

(b) $\neg p \to p$

(c) $p \leftrightarrow \neg p$

(d) $p \to (q \to p)$

(e) $\neg(q \vee p) \to \neg p$

(f) $(p \to (q \to r)) \to ((p \wedge q) \to r)$

(g) $((p \to q) \to r) \to ((p \wedge q) \to r)$

(h) $(p \to \neg q) \leftrightarrow (q \to \neg p)$

(i) $(p \to \neg q) \leftrightarrow (\neg p \to q)$

(j) $\neg(p \to \neg q) \leftrightarrow (\neg p \to q)$

Exercice 9. Supposons que v est une valuation telle que $v(p) = \mathsf{V}$, $v(q) = \mathsf{F}$ et $v(r) = \mathsf{F}$. Déterminez les valeurs de vérité suivantes :

(a) $v(p \wedge (q \vee r))$

(b) $v(p \to (\neg q \to \neg r))$

(c) $v(\neg p \to \bot)$

(d) $v(p \vee (q \wedge (\neg r \to q)))$

Exercice 10. Supposons que v est une valuation telle que $v(p \wedge (\neg q \to r)) = \mathsf{F}$, $v(\neg q \wedge r) = \mathsf{F}$ et $v((q \vee r) \to p) = \mathsf{V}$. Que pouvez-vous conclure de $v(p)$, $v(q)$ et $v(r)$?

Exercice 11. Une formule propositionnelle X est construite à partir de deux variables propositionnelles, p et q. Supposons que la table de vérité de X est la suivante :

p	q	X
F	F	F
F	V	V
V	F	V
V	V	F

(a) Trouvez une telle formule propositionnelle X, en employant seulement p, q et les connectifs propositionnels.

(b) Trouvez une telle formule propositionnelle X, mais en employant seulement les connectifs $\vee$ et $\neg$ cette fois.

(c) Trouvez une telle formule propositionnelle X, mais en employant seulement les connectifs $\rightarrow$ et $\neg$ cette fois.

Exercice 12. Trouvez une formule propositionnelle Y qui emploie les trois lettres propositionnelles p, q, r, et telle que $v(Y) = \mathsf{F}$ précisément lorsque $v(p) = v(q) = \mathsf{V}$ ou lorsque $v(q) = v(r) = \mathsf{V}$. Ensuite, donnez une telle formule Y qui emploie seulement les connectifs $\rightarrow$ et $\neg$.

Exercice 13. Considérez l'énoncé « Si la conjecture des nombres premiers jumeaux n'est pas vraie, alors la théorie des nombres est moins intéressante que la combinatoire ». Quelle est la contraposée de cet énoncé ? Quelle est la réciproque ? Et la négation ?

Exercice 14. Considérez l'argument suivant :

> Si on supporte la candidate, elle sera élue. Si la candidate est élue, elle supportera notre cause. Donc, il faut supporter la candidate, si on veut qu'elle supporte notre cause.

Traduisez cet argument en logique propositionnelle et déterminez s'il est valide ou non.

Exercice 15. Considérez l'argument suivant :

> Si on supporte la candidate, elle sera élue. Si la candidate est élue, elle augmentera les taxes. Si les taxes sont augmentées, alors je ne pourrai pas me permettre une nouvelle voiture. Donc, si on ne supporte pas la candidate, je pourrai me permettre une nouvelle voiture.

Traduisez cet argument en logique propositionnelle et déterminez s'il est valide ou non.

Exercice 16. Considérez l'argument suivant :

> La candidate ne sera pas élue seulement si on ne la supporte pas. Si la candidate n'est pas élue ou si l'économie s'en va en empirant, alors les taxes augmenteront. Donc, les taxes vont augmenter, à moins que l'on supporte la candidate.

Traduisez cet argument en logique propositionnelle et déterminez s'il est valide ou non.

Exercice 17. Considérez les formules propositionnelles $p \rightarrow (q \vee r)$ et $(p \rightarrow q) \vee (p \rightarrow r)$. Sont-elles logiquement équivalentes ?

Exercice 18. Prouvez que $\neg p \equiv p \to \bot$.

Exercice 19. En utilisant les lois de l'algèbre booléenne, démontrez que $(\neg p \to q) \to r$ est équivalent à $(p \to r) \wedge (q \to r)$.

Exercice 20. En utilisant les lois de l'algèbre booléenne, trouvez une proposition qui est équivalente à $p \to (\neg p \vee q)$, mais qui est plus simple (en termes du nombre de connectifs employés).

Les exercices suivants se rapportent aux énigmes de l'île des chevaliers et coquins.

Exercice 21. Sur l'île des chevaliers et coquins, est-il possible qu'un habitant dise « Je suis un coquin. » ?

Exercice 22. Supposez maintenant que vous rencontrez deux habitants et que l'un d'entre eux dit : « Nous sommes tous les deux des coquins. » Que pouvez-vous conclure quant à la nature de ces deux habitants ?

Exercice 23. Supposez que vous rencontrez deux habitants, et que l'un dit qu'il y a exactement l'un d'entre eux qui est un coquin. Que pouvez-vous conclure ?

Exercice 24. Encore une fois, vous rencontrez deux habitants, mais cette fois-ci, l'un d'entre eux dit : « Soit nous sommes tous les deux des chevaliers, soit nous sommes tous les deux des coquins. » L'autre dit : « Ce n'est pas vrai. » Pouvez-vous déterminer le(s) type(s) de ces habitants ?

Exercice 25. Considérez deux habitants de l'île, A et B. Supposons que A dit : « Je suis un coquin, mais pas B ». Quel est le type de A et de B ?

Exercice 26. Si un coquin vous dit que la proposition p est vraie et qu'il dit également que la proposition q est vraie, alors la proposition $p \wedge q$ est-elle vraie ? La réciproque est-elle vraie ?

Exercice 27. Vous rencontrez quatre habitants (appelés A, B, C et D). Que pouvez-vous déduire de leurs énoncés ?

A : « Si je suis un chevalier, alors 2+2=4. »

B : « Si je suis un chevalier, alors 2+2=5. »

C : « Si je suis un coquin, alors 2+2=4. »

D : « Si je suis un coquin, alors 2+2=5. »

Exercice 28. Nous avons trois habitants, A, B et C, et chacun est soit un chevalier, soit un coquin. On dit que deux habitants sont du même type s'ils sont tous les deux des chevaliers ou tous les deux des coquins. A et B font les déclarations suivantes :

A : B est un coquin.

B : A et C sont du même type.

Quel est le type de C ?

Exercice 29. Encore une fois, nous avons trois habitants A, B et C. A dit « B et C sont du même type. » Quelqu'un demande ensuite à C : « Est-ce que A et B sont du même type ? ». Quelle est la réponse de C ?

Exercice 30. Quelqu'un demande à un habitant A : « Êtes-vous un chevalier ? ». Il répond « Si je suis un chevalier, alors je vais manger mon chapeau ». Prouvez que A doit manger son chapeau.

Exercice 31. Deux habitants, X et Y, sont jugés pour avoir participé à un vol. A et B sont deux témoins, et chacun d'eux peut être un chevalier ou un coquin. A et B donnent les témoignages suivants :

A : Si X est coupable, alors Y aussi.

B : Soit X est innocent, soit Y est coupable.

A et B sont-ils nécessairement du même type ? (i.e. tous les deux chevaliers ou tous les deux coquins.)

LEÇON III

Logique des prédicats

La logique des prédicats permet une analyse beaucoup plus fine des énoncés mathématiques que la logique propositionnelle. Considérons, par exemple, l'argument suivant :

Tous les avocats sont avares. Sarah est une avocate. Donc, Sarah est avare.

La plupart des gens s'entendent à dire que cet argument est valide (même s'ils avancaient que les valeurs de vérité des hypothèses sont discutables). Si nous analysions cet argument en utilisant la logique propositionnelle, nous ne serions pas en mesure de reconnaître cette validité. En effet, nous assignerions des lettres propositionnelles à chacune des trois propositions de base qui figurent dans l'argument, c'est-à-dire :

p - Tous les avocats sont avares

q - Sarah est une avocate

r - Sarah est avare

Mais alors, l'argument est de la forme « p et q, donc r ». Or, la formule $p \wedge q \rightarrow r$ n'est pas une tautologie, et ainsi, nous ne pouvons pas conclure que l'argument est valide.

Le problème, bien entendu, est que nous ne regardons pas d'assez près les phrases dans l'argument. Celui-ci suppose que *tous* les avocats ont une certaine propriété, et enchaîne avec la conclusion qu'*un* avocat en particulier a cette propriété. Établir la validité de cet argument à quelque chose à voir avec la formalisation du mot « tous ». À cet effet, la logique propositionnelle est inadéquate pour juger des mérites de ce dernier, et il importe de nous questionner sur la façon dont nous devrions raisonner avec des propriétés, des individus et des mots comme « tous ». Des raisonnements de ce genre sont précisément l'objet d'analyse de la logique des prédicats.

III.1 Syntaxe de la logique des prédicats

En logique propositionnelle, nous bâtissons des formules à partir de propositions de base p, q, r, ... en employant des connectifs propositionnels $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\leftrightarrow$. En logique des prédicats, nous avons toujours des connectifs, mais nous avons beaucoup plus que ça. Spécifiquement, les formules de la logique des prédicats sont construites à partir des ingrédients suivants :

- *Constantes*, ou *individus*, dénotés par les lettres minuscules a, b, c, ... Ceux-ci sont employés pour faire référence à des objets spécifiques, des éléments ou des individus.
- *Variables*, dénotées par x, y, z, u, v, w, ... Ces variables sont employées pour faire référence à des éléments non spécifiques, arbitraires, un peu comme nous le faisons dans le calcul infinitésimal lorsqu'on utilise des expressions tel que $f(x) = x^2$, où x réfère à un élément arbitraire dans le domaine de f.
- *Prédicats*, lesquels sont utilisés pour parler de propriétés pour des individus, et de relations entre individus. Les prédicats sont dénotés $P(x)$, $Q(x, y, z)$, $R(x, y)$, et cetera. Le nombre d'arguments du prédicat est appelé l'*arité* du prédicat. Ainsi, par exemple, $P(x)$ a une arité de 1, tandis que $Q(x, y, z)$ a une arité de 3.
- *Connectifs propositionnels*, lesquels sont précisément ceux de la logique propositionnelle.
- *Quantificateurs*, au nombre de deux : le *quantificateur existentiel*, dénoté $\exists$, et le *quantificateur universel*, dénoté $\forall$. Ces quantificateurs sont utilisés, respectivement, pour exprimer que *certains* individus ont une certaine propriété, ou que *tout* individu a une certaine propriété.

La définition inductive suivante explique comment les ingrédients ci-haut sont employés pour construire des formules :

- Si $P(x_1, \ldots, x_n)$ est un prédicat n-aire, et si chaque $t_1, \ldots, t_n$ est soit une variable, soit une constante, alors $P(t_1, \ldots, t_n)$ est une formule.
- Si ϕ, ψ sont des formules, alors $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$, $\phi \leftrightarrow \psi$ et $\neg\phi$ le sont aussi.
- Si ϕ est une formule et x est une variable, alors $\forall x.\phi$ et $\exists x.\phi$ sont des formules.

Voici quelques exemples :

Exemple III.1.1.

1. $P(a)$ est une formule (ici, P est un prédicat unaire et a est une constante).
2. $\forall x.P(x)$ est une formule.
3. $\exists y.R(y, a)$ est une formule.
4. $\forall x\, \exists y.R(x, y)$ est une formule.
5. $\forall x.(P(x) \rightarrow \exists y.R(y, x))$ est une formule.

Nous évitons d'écrire des formules dans lesquelles une variable est quantifiée plus qu'une fois. Par exemple, la formule $\forall x\, \exists x.P(x)$ est insensée. D'autre part, des formules telles que $\forall x.P(a)$ et $\forall x\, \forall y.P(x)$ sont acceptables. De plus, nous utilisons des parenthèses pour désambiguïser des expressions, tout comme en logique propositionnelle.

Nous concluons cette section avec un peu de terminologie. Dans une formule telle que $\exists x.\phi(x)$ ou $\forall x.\phi(x)$, on dit que les occurrences de la variable x dans ϕ sont *liées* par le quantificateur $\exists x$ ($\forall x$, respectivement). On dit également que la variable x dans ϕ est dans la *portée* du quantificateur. Des variables qui ne sont pas liées sont dites *libres*. On a une situation similaire en calcul infinitésimal lorsque, dans une expression telle que $\int f(x)\, dx$, la variable x est liée par dx. Le rôle des variables liées est seulement d'identifier un espace réservé, en vue d'une substitution, et celles-ci peuvent être commodément renommées. Par exemple, si on a une formule $\exists x.P(x)$ et une variable y qui ne figure pas dans P, alors $\exists y.P(y)$ est équivalent à $\exists x.P(x)$. Afin de comprendre pourquoi on exige que y ne figure pas dans P pour obtenir l'équivalence, considérez la formule $\exists x.x \neq y$. Si on change la lettre x pour y, on obtient la formule $\exists y.y \neq y$, laquelle est clairement fausse.

Quelques exemples rendront les concepts de variables libres et de variables liées plus clairs.

Exemple III.1.2.

1. Dans $\forall x.(P(x) \to \exists y.R(x, y, z))$, les variables x et y sont liées, tandis que z est libre.

2. Dans $\forall x.(P(y) \to \forall y.R(x, y, z))$, la variable x est liée et la variable z est libre ; la première occurrence de y est libre, tandis que la deuxième est liée.

3. Dans $\exists x.(P(x) \wedge P(y)) \to \exists z.P(x)$, la première occurrence de x est libre, sa seconde occurrence est liée, tandis que y est libre.

III.2 Traduction à la logique des prédicats

Nous commençons par étudier trois exemples qui illustrent comment la logique des prédicats peut être employée pour exprimer des idées mathématiques courantes.

Exemple III.2.1.

1. L'énoncé suivant :

   > Pour tous nombres réels x, y, il y a un entier positif n qui satisfait $\frac{1}{n} < x$.

   se traduit par : $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ \exists n \in \mathbb{N}.\, (n > 0 \wedge \frac{1}{n} < x)$.

2. L'énoncé suivant :

   > Il existe des nombres rationnels qui sont plus grands que leurs carrés.

   se traduit par : $\exists x \in \mathbb{Q}.\ x > x^2$.

3. L'énoncé suivant :

   > Si x est un nombre réel satisfaisant $x + y > xy$ pour tout nombre réel positif y, alors x est négatif.

   se traduit par : $\forall x \in \mathbb{R}.\,(\,\forall y \in \mathbb{R}.(x + y > xy) \;\rightarrow\; x < 0\,)$.

Dans le dernier exemple, il semble à première vue que le connectif principal est une implication (parce que l'énoncé a la forme « Si ..., alors ... »), mais ceci est déroutant : l'énoncé porte sur des nombres réels x, et peut être paraphrasé par « Pour tout nombre réel x : si x satisfait $x + y > xy$ pour tout entier positif y, alors x est négatif ». Il est souvent révélateur de reformuler un énoncé complexe de manière à clarifier la structure logique.

Nous nous tournons maintenant vers la traduction d'énoncés du français à la logique prédicative. Lorsque nous voulons traduire un énoncé français en logique prédicative, nous devons

- spécifier les constantes que nous employons,
- spécifier les prédicats que nous employons,
- effectuer la traduction en question.

Par exemple, si nous voulions traduire la phrase « Jean a faim », nous introduirions la constante qui se réfère à Jean et le prédicat unaire pour la propriété « a faim » comme suit :

a – Jean

$P(x)$ – x a faim

La traduction de « Jean a faim » est : $P(a)$.

Nous pouvons aussi traduire l'argument présenté au début de cette leçon. Notre lexique pour cet argument est :

s – Sarah

$A(x)$ – x est une avocate

$G(x)$ – x est avare

La traduction de l'argument est alors :

$$\frac{\begin{array}{c}\forall x.(A(x) \rightarrow G(x)) \\ A(s)\end{array}}{G(s)}$$

Remarquez que nous utilisons une implication (et non pas une conjonction) pour la première hypothèse ; nous voulons dire que *si* x est un avocat, *alors* x est avare. Nous ne voulons pas dire que toute personne x est un avocat et est avare !

Le tableau III.1 liste un certain nombre de constructions standards que nous allons rencontrer fréquemment. Pour certains de ces énoncés, nous employons l'*égalité*. Celle-ci est souvent considérée comme faisant implicitement partie du langage et elle permet une expressivité accrue. Aussi, nous allons employer la notation $x \neq y$ pour désigner l'énoncé $\not(x = y)$.

Français	Traduction
Tous les P sont des Q	$\forall x.(P(x) \to Q(x))$
Certains P sont des Q	$\exists x.(P(x) \wedge Q(x))$
Ce ne sont pas tous les P qui sont des Q	$\neg\, \forall x.(P(x) \to Q(x))$
Il n'y a pas de P qui est un Q	$\neg\, \exists x.(P(x) \wedge Q(x))$
Il y a au moins un P	$\exists x.P(x)$
Il y a au moins deux P	$\exists x\, \exists y.(P(x) \wedge P(y) \wedge x \neq y)$
Il y a au plus un P	$\forall x\, \forall y.(P(x) \wedge P(y) \to x = y)$
Il y a au plus deux P	$\forall x\, \forall y\, \forall z.(P(x) \wedge P(y) \wedge P(z) \to x = y \vee x = z \vee y = z)$
Il y a exactement un P	$\exists x.(P(x) \wedge \forall y.(P(y) \to x = y))$

Tableau III.1 – Traductions courantes en logique des prédicats

Nous procédons à des exemples de traduction. Dans chaque cas, nous faisons appel au lexique suivant :

a – Jean

b – Marie

$A(x, y)$ – x aime y

Exemple III.2.2.

1. Jean aime Marie — $A(a, b)$
2. Jean aime Marie, mais Marie n'aime pas Jean — $A(a, b) \wedge \neg A(b, a)$
3. Tout le monde aime Marie — $\forall x.A(x, b)$
4. Ce n'est pas tout le monde qui aime Jean — $\neg\, \forall x.A(x, a)$
5. Tout le monde aime au moins une personne — $\forall x\, \exists y.A(x, y)$
6. Ce n'est pas tout le monde qui est aimé par quelqu'un — $\neg\, \forall x\, \exists y.A(y, x)$
7. Certaines personnes ne s'aiment pas elles-mêmes — $\exists x.\neg A(x, x)$
8. Tout le monde, sauf Marie, aime Jean — $\forall x.(\neg\, x = b \to A(x, a))$
9. Jean aime au plus une personne — $\forall x\, \forall y.(A(a, x) \wedge A(a, y) \to x = y)$
10. Jean aime au moins deux personnes — $\exists x\, \exists y.(A(a, x) \wedge A(a, y) \wedge x \neq y)$
11. Jean aime exactement une personne — $\exists x.(A(a, x) \wedge \forall y.(A(a, y) \to x = y))$
12. Si tu ne t'aimes pas toi-même, tu ne peux aimer personne — $\forall x(\neg A(x, x) \to \neg\, \exists y.A(x, y))$
13. Certaines personnes n'aiment personne d'autre qu'elles-mêmes — $\exists x.(\neg\, \exists y.(A(x, y) \wedge x \neq y) \wedge A(x, x))$

III.3 Domaines et interprétations

Un grande part des énoncés mathématiques que l'on rencontre au quotidien peuvent acquérir un sens précis dans la mesure où nous les traduisons en logique prédicative. À titre d'exemple, nous pouvons considérer des énoncés en rapport avec la relation d'ordre $\leq$ sur les nombres naturels.

Exemple III.3.1. Dénotons l'ordre usuel sur $\mathbb{N}$ par $\leq$.

1. $\forall x.0 \leq x$ exprime que chaque x est plus grand ou égal à 0.
2. $\exists x \forall y.x \leq y$ évoque l'existence d'un élément x avec la propriété que tous les éléments sont plus grands ou égaux à x.
3. $\forall x \exists y.y \leq x$ exprime que pour chaque élément x, il existe un élément qui est plus petit ou égal à x.
4. $\forall x \exists y.(x \leq y \wedge x \neq y)$ exprime que pour chaque élément x, il existe un élément qui est strictement plus grand que x.
5. $\forall x \forall y.(x \leq y \vee y \leq x)$ exprime que deux éléments sont toujours comparables.

Notez que chaque énoncé ci-haut est en fait vrai en ce qui concerne l'ordre $\leq$ sur $\mathbb{N}$. Une façon un peu différente de dire la même chose est : lorsque nous interprétons le *symbole* $\leq$ comme étant la relation d'ordre sur $\mathbb{N}$, et le symbole 0 comme étant le nombre 0, alors les énoncés ci-haut sont vrais.

Néanmoins, considérez l'énoncé suivant : $\forall x \exists y.(y < x)$. (Ici, on peut utiliser $y < x$ comme une abréviation de $y \leq x \wedge y \neq x$.) Ceci exprime que, pour chaque élément x, il existe un élément strictement plus petit que x. Cet énoncé n'est pas vrai pour l'ordre sur $\mathbb{N}$. Similairement, l'énoncé $\forall x \forall y.(x < y \rightarrow \exists z.(x < z \wedge z < y))$ dit que pour n'importe quelle paire d'éléments distincts, il existe un élément qui est strictement entre les deux. Cet énoncé est également faux sur $\mathbb{N}$.

Par contraste, considérez maintenant l'ordre usuel sur les nombres rationnels $\mathbb{Q}$. Alors, l'énoncé $\forall x.0 \leq x$ est faux, car 0 n'est pas le plus petit nombre rationnel. Or, l'énoncé
$\forall x \forall y.(x < y \rightarrow \exists z.(x < z \wedge z < y))$ est vrai dans $\mathbb{Q}$, parce que si $x < y$, alors le nombre $\frac{x+y}{2}$ est strictement entre x et y.

Ce qu'il faut essentiellement retenir ici est que des énoncés de la logique des prédicats peuvent être vrais dans une situation, mais faux dans une autre. En d'autres termes, la vérité d'un énoncé dépend de la situation dans laquelle on l'interprète. Il est considéré de bonne pratique, en mathématiques, d'être explicite à ce niveau. Une méthode courante est d'énoncé dans quel ensemble les variables prennent leur valeurs. Par exemple, nous pourrions écrire

$$\forall x \in \mathbb{N} \exists y \in \mathbb{N}.x < y$$

ou

$$\forall x \in \mathbb{Q} \forall y \in \mathbb{Q}.(x < y \rightarrow \exists z \in \mathbb{Q}.(x < z \wedge z < y)).$$

Il est même possible de combiner et comparer divers ensembles, comme dans la formule

$$\forall x \in \mathbb{R} \exists y \in \mathbb{Z}.(x \leq y \wedge \forall z \in \mathbb{N}.(x \leq z \rightarrow y \leq z)).$$

L'ensemble dans lequel une variable prend ses valeurs est habituellement appelé *domaine de discours*. On peut omettre de préciser dans quel domaine une variable prend ses valeurs seulement lorsque ce domaine est clair dans le contexte donné, ou lorsqu'il importe peu en quoi consiste ce domaine.

Quoique cette façon de procéder soit assez commune, il vaut la peine d'indiquer qu'il y a une alternative : au lieu d'écrire $\forall x \in A.P(x)$ (où A est un ensemble), on peut écrire $\forall x.(x \in A \to P(x))$. Et au lieu de $\exists x \in A.P(x)$, on peut utiliser $\exists x.(x \in A \wedge P(x))$. Notons que dans le cas du quantificateur universel, une implication est utilisée (« Si x est dans A, alors il satisfait P »), tandis que pour le quantificateur existentiel, une conjonction est utilisée (« Il existe un x dans A qui satisfait aussi P »).

III.4 Raisonnement avec des prédicats

Maintenant que nous sommes familiers avec la syntaxe de la logique des prédicats, nous allons discuter des principes de raisonnement qui régissent cette logique. Pour la logique propositionnelle, nous avons donné une sémantique complète en termes de tables de vérité (complète au sens que n'importe quelle question se rapportant aux équivalences logiques et à la validité peut être résolue de manière décidable avec des tables de vérité). Nous n'essayerons pas d'accomplir quelque chose de similaire pour la logique des prédicats ; ceci requiert une technologie que nous n'avons pas encore développée. Notre but ici est plutôt de familiariser le lecteur avec les manipulations les plus courantes et les stratégies de preuve à un niveau informel, de telle sorte que nous pourrons les employer lors de leçons subséquentes.

Bien entendu, étant donné que la logique des prédicats est une extension de la logique propositionnelle, toutes les lois de la logique propositionnelle sont toujours valides. Ainsi, nous devons décrire comment le raisonnement fonctionne avec des quantificateurs. Le premier principe est le suivant :

> À partir de $\forall x.P(x)$, on peut inférer que $P(a)$ est vrai pour n'importe quel a.

Ce principe est appelé l'*instanciation* ; si P est vrai pour tout x, alors il est vrai pour n'importe quelle instance particulière a.

Exemple III.4.1. Supposons que nous sachions déjà que l'énoncé

$$\forall x \in \mathbb{N}\, \exists y \in \mathbb{N}.(x < y \wedge \text{Premier}(y))$$

est vrai. (Notez que cet énoncé dit qu'il existe des nombres premiers arbitrairement larges.) Nous pouvons alors déduire que

$$\exists y \in \mathbb{N}.(2012 < y \wedge \text{Premier}(y))$$

est vrai également.

Ensuite, supposons que nous voulons prouver une formule de la forme $\forall x.P(x)$.

> Pour prouver $\forall x.P(x)$, prenez un élément arbitraire x, et prouvez $P(x)$.

Il importe que, dans la preuve de $P(x)$, vous ne fassiez aucune supposition sur x ; sinon, ce dernier ne serait plus *arbitraire*.

Exemple III.4.2. Supposons que nous voulions prouver que $\forall x \in \mathbb{N}.(x > 1 \to x^2 > x)$. Nous pouvons procéder comme suit : Considérons un nombre naturel arbitraire x. Supposons que $x > 1$. Alors, $x < x^2$ (les détails de ce raisonnement sont omis car ils ne sont pas l'objet de notre attention). Ainsi, $x > 1 \to x^2 < x$ est vrai pour un x arbitraire. Nous pouvons conclure que $\forall x.(x > 1 \to x^2 > x)$.

Pour le quantificateur existentiel, nous avons également deux principes de base. Le premier est le suivant :

> Pour prouver $\exists x.P(x)$, il faut démontrer $P(a)$ pour un élément a.

Par exemple, puisque 12 est un nombre qui satisfait $12 > 10 \wedge 12^2 < 150$, nous pouvons inférer $\exists x \in \mathbb{N}.(x > 10 \wedge x^2 < 150)$.

Le second principle nous explique comment faire des déductions à partir de $\exists x.P(x)$, comme suit :

> Supposons que $\exists x.P(x)$ est vrai, et que Q est un énoncé dans lequel x ne figure pas. Si $P(x)$ implique Q pour un x arbitraire, alors Q est vrai.

Ce principe correspond à la ligne de raisonnement suivante : si nous pouvons prouver Q à partir de la supposition $P(x)$, et si nous ne faisons aucune autre supposition sur x (à l'exception du fait qu'il satisfait P), alors Q découle de la supposition qu'il existe un x tel que $P(x)$.

Les quatre principes ci-haut dictent comment nous pouvons prouver des énoncés de la forme $\forall x.P(x)$ et $\exists x.P(x)$, et comment nous pouvons inférer des résultats à partir de ces derniers. En utilisant ces principes (et les règles de la logique propositionnelle), nous pouvons prouver plusieurs autres principes valides de la logique des prédicats. Comme pour la logique propositionnelle, nous écrivons $\alpha \equiv \beta$ pour indiquer que α et β sont logiquement équivalents. Aussi, nous disons que α est une tautologie (ou contradiction) lorsque $\alpha \equiv \top$ (ou $\alpha \equiv \bot$).

Exemple III.4.3. La formule $\forall x.P(x) \to \exists x.P(x)$ est une tautologie.

Pour prouver ceci, supposons que $\forall x.P(x)$ est vrai. Ceci implique $P(a)$ pour un a arbitraire. Ainsi, nous obtenons $\exists x.P(x)$. Finalement, $\forall x.P(x) \to \exists x.P(x)$ est vrai.[1]

Un exemple un peu plus compliqué est le suivant :

Exemple III.4.4. La formule $(\forall x.(P(x) \to Q(x)) \wedge \forall x.P(x)) \to \forall x.Q(x)$ est une tautologie.

Pour constater ce fait, supposons que $\forall x.(P(x) \to Q(x)) \wedge \forall x.P(x)$ est vrai. Pour démontrer que $\forall x.Q(x)$ est également vrai, considérons un x arbitraire. À partir de $\forall x.(P(x) \to Q(x))$, nous obtenons

[1] Ceci fonctionne seulement parce que nous faisons habituellement la supposition que notre raisonnement s'effectue sur un domaine où au moins un objet existe.

que $P(x) \to Q(x)$. De $\forall x.P(x)$, nous obtenons $P(x)$. En appliquant Modus Ponens, on déduit $Q(x)$. Puisque x était arbitraire, nous pouvons conclure que $\forall x.Q(x)$.

Dans le tableau III.2, nous listons un certain nombre d'équivalences fréquemment utilisées dans la logique des prédicats.

$\forall x\,\forall y.P(x,y)$	$\equiv$	$\forall y\,\forall x.P(x,y)$
$\exists x\,\exists y.P(x,y)$	$\equiv$	$\exists y \exists x.P(x,y)$
$\neg\,\forall x.P(x)$	$\equiv$	$\exists x.\neg P(x)$
$\neg\,\exists x.P(x)$	$\equiv$	$\forall x.\neg P(x)$
$\forall x.(P(x) \wedge Q(x))$	$\equiv$	$\forall x.P(x) \wedge \forall x.Q(x)$
$\exists x.(P(x) \vee Q(x))$	$\equiv$	$\exists x.P(x) \vee \exists x.Q(x)$
$\exists x\,\forall y.P(x,y) \to \forall y\,\exists x.P(x,y)$	$\equiv$	$\top$

Tableau III.2 – Équivalences pour la logique des prédicats

Exemple III.4.5. La formule $\forall y\,\exists x.P(x,y) \to \exists x\,\forall y.P(x,y)$ *n'est pas* une tautologie. Par exemple, lorsque $P(x,y)$ est le prédicat $x > y$ et que le domaine de discours est l'ensemble des entiers, on a que $\forall y \in \mathbb{Z}\,\exists x \in \mathbb{Z}.x > y$ est certainement vrai. Par contre, $\exists x \in \mathbb{Z}\,\forall y \in \mathbb{Z}.x > y$ est de toute évidence faux.

Plusieurs autres exemples de tautologies et équivalences figurent dans les exercices à la fin de cette leçon.

Les règles qui agencent une interaction entre les quantificateurs et la négation méritent une attention particulière, car elle nous disent comment manipuler la négation d'énoncés quantifiés. En particulier, dans le cas de formules avec plusieurs quantificateurs, des erreurs sont souvent commises ; il faut donc être vigilant dans ces cas. Par exemple, considérez l'énoncé :

Pour chaque nombre réel x, il existe des nombres réels y, z tels que $x^2 > y$ et $z + y = x + z^2$.

Quelle est la négation de cet énoncé ? Dans le langage de la logique des prédicats, l'énoncé se lit

$$\forall x \in \mathbb{R}\,\exists y, z \in \mathbb{R}.(x^2 > y \wedge z + y = x + z^2).$$

La négation est alors

$$\neg\,\forall x \in \mathbb{R}\,\exists y, z \in \mathbb{R}.(x^2 > y \wedge z + y = x + z^2),$$

et en utilisant les règles du tableau III.2, nous déduisons que ceci est équivalent à

$$\exists x \in \mathbb{R}\,\forall y, z \in \mathbb{R}.\neg(x^2 > y \wedge z + y = x + z^2).$$

Or, ce dernier est équivalent (par les lois de la logique propositionnelle et certains faits se rapportant à l'ordre sur $\mathbb{R}$) à

$$\exists x \in \mathbb{R}\,\forall y, z \in \mathbb{R}.(x^2 \leq y \vee z + y \neq x + z^2).$$

III.5 Sommaire

La logique des prédicats est plus expressive que la logique propositionnelle : elle analyse la structure fine des propositions en employant des prédicats et des quantificateurs.

- $\forall x.P(x)$ veut dire « pour tout x, $P(x)$ est vrai » ; le symbole $\forall$ est le *quantificateur universel*.
- $\exists x.P(x)$ veut dire « il existe x pour lequel $P(x)$ est vrai » ; le symbole $\exists$ est le *quantificateur existentiel*.

La plupart du temps, lorsque nous employons la logique des prédicats, nous avons un certain *domaine de discours* à l'esprit ; il s'agit d'un ensemble dans lequel les variables prennent leurs valeurs. La vérité d'un énoncé de la logique des prédicats dépend essentiellement de ce domaine ; ce dernier est souvent explicitement mentionné dans la notation, comme l'ensemble A dans $\forall x \in A.P(x)$ ou $\exists x \in A.P(x)$.

Plusieurs concepts de la logique propositionnelle peuvent être généralisés à la logique des prédicats : l'équivalence logique, la tautologie, la contradiction.

La négation de $\forall x.P(x)$ est $\neg\,\forall x.P(x)$, laquelle est équivalente à $\exists x.\neg P(x)$.

La négation de $\exists x.P(x)$ est $\neg\,\exists x.P(x)$, laquelle est équivalente à $\forall x.\neg P(x)$.

III.6 Exercices

Exercice 32. Écrivez les énoncés mathématiques suivants en logique des prédicats :

(a) Certains nombres naturels sont pairs, et certains sont premiers.

(b) Ce ne sont pas tous les nombres impairs qui sont premiers.

(c) Il existe un nombre premier qui est pair.

(d) Ce ne sont pas tous les nombres premiers qui sont impairs.

(e) Si un nombre est premier et qu'il n'est pas égal à 2, alors il est impair.

(f) Certains nombres sont ni premiers, ni pairs.

(g) Si un nombre n'est pas premier, alors, soit il n'est pas impair, soit il n'est pas égal à 2.

Exercice 33. Pour chacun des énoncés suivants, déterminez s'il est vrai ou faux.

(a) $\forall x \in \mathbb{N}\,\forall y \in \mathbb{N}.x + y \leq xy$

(b) $\forall x \in \mathbb{N}\,\forall y \in \mathbb{N}.((x > 0 \wedge y > 0) \rightarrow x + y \leq xy)$

(c) $\forall x \in \mathbb{R}\,\exists y \in \mathbb{N}.x < y$

(d) $\forall x \in \mathbb{N}.(x > 0 \rightarrow \exists y \in \mathbb{R}.xy = 1)$

(e) $\forall x \in \mathbb{R}.(x > 0 \to \exists y \in \mathbb{N}.xy = 1)$

(f) $\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}.(y \leq 0 \vee xy < y)$

(g) $\exists x \in \mathbb{Z}.[\forall y \in \mathbb{R}.(xy = y) \wedge \forall z \in \mathbb{R}.((\forall y \in \mathbb{R}.zy = y) \to x = z)]$

(h) $\exists x \in \mathbb{N}\, \forall y \in \mathbb{N}\, \forall z \in \mathbb{N}.(xy > z \vee zx > y)$

Exercice 34. Nous considérons des matrices 3×3 avec la notation usuelle

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Parmi les matrices suivantes, déterminez pour lesquelles l'énoncé suivant est vrai :

$$\forall i \in \{1,2,3\} \exists j \in \{1,2,3\} \left[a_{ij} \leq -5 \vee \exists n \in \mathbb{N}.(a_{ij} = (n+1)^2)\right].$$

$$A = \begin{bmatrix} 1 & 4 & -7 \\ -1 & 2 & 0 \\ 2 & 0 & 3 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 1 & -1 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} \quad C = \begin{bmatrix} 1 & 1 & -10 \\ 0 & 16 & 0 \\ 49 & -12 & 36 \end{bmatrix}$$
$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad E = \begin{bmatrix} 1 & 0 & -6 \\ -7 & 4 & 25 \\ 0 & 0 & 9 \end{bmatrix} \quad F = \begin{bmatrix} -1 & 0 & -6 \\ 0 & 4 & 2 \\ -1 & 0 & 0 \end{bmatrix}$$

Exercice 35. Guillaume et Daniel sont en désaccord par rapport à l'énoncé suivant :

$$\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}.(0 < y \wedge y \leq x \to y^2 < y).$$

Guillaume : « Cet énoncé est vrai ; prenons, par exemple, $x = -1$. Il s'ensuit que pour tout y, $0 < y \wedge y \leq x$ est faux, et ainsi, l'énoncé est vrai intégralement. »

Daniel : « Cet énoncé est faux ; prenons, par exemple, $x = 1$. Ensuite, considérons $y = 1$. Nous avons $0 < y \leq 1$, mais $1^2 = 1$, donc la conclusion ne tient pas. »

Qui a tort ?

Exercice 36. Une fois de plus, considérons l'énoncé

$$\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}.((0 < y \wedge y \leq x) \to y^2 < y).$$

Quelle est la négation de cet énoncé ?

(a) $\forall y \in \mathbb{R}\, \exists x \in \mathbb{R}.((0 \geq y \vee x < y) \to y \leq y^2)$

(b) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}.((0 < y \wedge y \leq x) \wedge y \leq y^2)$

(c) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}.((0 \geq y \vee x < y) \wedge y \leq y^2)$

(d) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}.(y^2 < y \to (0 < y \wedge y \leq x))$

Exercice 37. Traduisez en logique des prédicats :

(a) Ce n'est pas tout le monde qui aime Jean.

(b) Certaines personnes n'aiment qu'elles-mêmes.

(c) Ce n'est pas tout le monde qui est aimé par tout le monde.

(d) Au moins deux personnes aiment Marie.

(e) Au moins une personne s'aime elle-même.

(f) Il y a exactement une personne qui aime Jean, et ce n'est pas Jean lui-même.

Exercice 38. Traduisez les énoncés suivants en logique des prédicats :

(a) Tous les chiens chassent les chats.

(b) Il y a des chiens qui ne chassent pas de chats.

(c) Certains chiens chassent seulement certains chats.

(d) Les gros chiens ne chassent pas les petits chats.

(e) Les gros chats sont chassés seulement par les gros chiens.

(f) Il y a des gros chats qui ne sont chassés par aucun chien.

(g) Ce ne sont pas tous les petits chiens qui chassent les gros chats.

(h) Un chat chasse seulement un chien s'il est un gros chat et que le chien est petit.

Exercice 39. Considérez les formules $\alpha = \exists x(P(x) \wedge Q(x))$ et $\beta = \exists x.P(x) \wedge \exists x.Q(x)$.

(a) Montrez que $\alpha \to \beta$ est une tautologie.

(b) Donnez un exemple pour démontrer que $\beta \to \alpha$ n'est pas une tautologie.

Exercice 40. Considérez la formule $\forall x.(\exists y.L(x,y) \vee \forall z.L(z,x))$. Est-ce une tautologie ? Si oui, prouvez-le. Sinon, donnez un exemple pour démontrer pourquoi elle n'en est pas une.

Exercice 41. Lesquelles des formules suivantes sont des tautologies ? S'il s'agit d'une tautologie, expliquez pourquoi. Sinon, donnez un exemple pour démontrer pourquoi pas.

(a) $\forall x\, \forall y.R(x,y) \to \forall x.R(x,x)$

(b) $\forall x.P(x) \vee \forall x.\neg P(x)$

(c) $\exists x.P(x) \vee \exists x.\neg P(x)$

(d) $\forall x.(\bot \to P(x))$

Exercice 42. Trouvez les négations des formules suivantes. Écrivez-les sous une forme dans laquelle le symbole de négation apparaît seulement directement en avant des symboles de prédicats.

(a) $\exists x\, \exists y.P(x,y)$

(b) $\exists x\, \exists y.(P(x,y) \vee Q(x,y))$

(c) $\exists x\, \exists y.(P(x,y) \wedge Q(x,y))$

(d) $\forall x\, \forall y.P(x,y)$

(e) $\forall x\, \forall y.(P(x,y) \rightarrow Q(x,y))$

(f) $\exists x\, \forall y.P(x,y)$

(g) $\exists x\, \forall y.(P(x,y) \rightarrow Q(x,y))$

(h) $\forall x\, \exists y.P(x,y)$

(i) $\forall x.(\exists y.P(x,y) \vee \exists z.Q(x,z))$

(j) $\exists x.(P(x) \rightarrow \forall y.P(y))$

(k) $\forall x.(\exists y.P(x,y) \rightarrow \forall z.Q(x,y))$

Exercice 43. Déterminez si l'argument suivant est valide ou non :

> Tous les hommes sont mortels. Tous les mortels ont peur. Donc, tous les hommes ont peur.

Exercice 44. Déterminez si l'argument suivant est valide ou non :

> Toute personne capable de grimper le mont Everest est très forte. Si vous êtes fort, alors vous n'avez aucune peur. Les seuls personnes qui ont peur sont celles qui sont mortelles. Donc, tous ceux qui sont mortels ne peuvent pas grimper le mont Everest.

Exercice 45. Déterminez si l'argument suivant est valide ou non :

> Jean aime tout le monde, sauf lui-même. Marie aime tout le monde qui aime Jean. Donc, Marie et Jean s'aiment l'un l'autre.

Exercice 46. Traduisez attentivement la version suivante de la conjecture des nombres premiers jumeaux en logique des prédicats : « Pour tout nombre naturel x, il existe un nombre strictement plus grand y pour lequel y et $y+2$ sont tous les deux premiers. »

Exercice 47. Sur l'île des chevaliers et des coquins, vous rencontrez deux habitants. Le premier habitant dit : « Tous les habitants de cette île sont des coquins. » Le deuxième répond : « Ce n'est pas vrai ! ».

Que pouvez-vous conclure par rapport au(x) type(s) des deux habitants ?

Exercice 48. Ensuite, vous rencontrez deux habitants, A et B, qui semblent agir étrangement. Vous leur demandez si l'un d'entre eux est soûl. Ils vous donnent les réponses suivantes :

A : Tous les coquins sur cette île sont soûls. Je suis parfaitement sobre par contre.

B : (Avec acquiescement.) Je suis un coquin et je suis soûl !

Pouvez-vous déterminer lequel est soûl ?

LEÇON IV

Ensembles et fondements

IV.1 Questionnement

Les mathématiques étudient une grande variété de choses, entre autres : le calcul infinitésimal aborde la différentiation et l'intégration de fonctions, l'algèbre linéaire est centré sur l'étude des espaces vectoriels et des transformations linéraires, la géométrie étudie les formes dans l'espace, la logique mathématique s'intéresse aux preuves et aux calculs, et ainsi de suite.

Quoique certains des concepts plus avancés d'une branche des mathématiques puissent sembler plus abstraits et distants par rapport aux notions élémentaires avec lesquelles nous sommes plus familiers, il est toujours possible de décomposer des définitions complexes en termes plus simples, itérativement, jusqu'à ce que nous rejoignons les notions de base. Essayons d'appliquer cette idée à un exemple familier de structure mathématique, soit un espace vectoriel (réel).

Vous : *Qu'est-ce qu'un espace vectoriel ?*

Algébriste : C'est un ensemble X équipé d'une opération d'addition, d'un zéro et d'une multiplication scalaire satisfaisant certains axiomes.

Vous : *Que voulez-vous dire par « opération d'addition » ?*

Algébriste : Une opération d'addition sur un ensemble X est une fonction de $X \times X$ dans X. Les axiomes disent que l'addition devrait être associative et commutative.

Vous : *Une fonction de $X \times X$ dans X ? Qu'est-ce que $X \times X$ exactement ?*

Algébriste : C'est un produit cartésien de l'ensemble X avec lui-même. Vous pouvez le concevoir comme l'ensemble de toutes les paires d'éléments de X.

Vous : *Ah. Que voulez-vous dire par une paire ?*

Algébriste : Vous ne savez pas ce qu'est une paire ? ?

Vous : *J'ai une idée intuitive de quoi il s'agit, mais je veux m'assurer que j'ai la bonne définition.*

Algébriste : Ok donc. Pour définir une paire (x, y), on peut employer un truc inventé par le mathématicien Kuratowski, soit définir une paire (x, y) comme étant l'ensemble $\{x, \{x, y\}\}$.

Vous : *C'est une approche intéressante, quoique je ne suis pas certain de comprendre pourquoi un ensemble de toutes ces paires existe en toutes circonstances.*

Algébriste : Ce n'est qu'un fait élémentaire à propos des ensembles : étant donné deux ensembles, on peut toujours former leur produit. On peut même former le produit d'une infinité d'ensembles si on veut. Si on ne peut pas former de produit, on est tout aussi bien de laisser tomber les mathématiques.

Vous : *Je ne veux pas laisser tomber les mathématiques ; mais, tout de même, je ne comprends toujours pas pourquoi il est permissible d'évoquer l'existence d'un produit de deux ensembles, peu importe ces ensembles. Pouvez-vous me le prouver ?*

Algébriste : Bon d'accord, mais on dirait que nous nous n'aurons pas la chance de faire de l'algèbre linéaire aujourd'hui ! Si on utilise la définition de paire de Kuratowski, alors un élément de $X \times Y$ est simplement un sous-ensemble particulier de l'union $X \cup \mathcal{P}(X \cup Y)$, où $\mathcal{P}$ est l'opération pour l'ensemble des parties.

Vous : *Je vois, mais ça n'adresse pas réellement mes préoccupations à propos de l'existence d'un tel ensemble de paires. Il semblerait que nous devrions nous fier à l'existence de quelque chose d'encore plus complexe, notamment les ensembles de parties.*

Algébriste : Vous ne croyez pas, qu'étant donné un ensemble, vous pouvez former l'ensemble de tous les sous-ensembles de ce dernier ?

Vous : *Ça semble définitivement plausible qu'on puisse le faire, et cela apporterait certainement une solution à mon problème. Mais êtes-vous en train de dire que l'existence d'ensembles de parties n'est pas quelque chose que l'on peut prouver, et que l'on doit simplement croire en leur existence ?*

Algébriste : Ultimement, nous devons être réceptif à la vérité de certains énoncés lorsqu'elle va de soi ; sinon, on ne peut rien accomplir.

Comme vous pouvez le constater, en cherchant continuellement à décomposer les définitions, et en questionnant l'existence des entités mathématiques de base, nous arrivons ultimement à révéler l'acceptation de certains principes fondamentaux de la théorie des ensembles (dans le dialogue ci-haut, nous étions confronter à l'existence des ensembles de parties). La plupart des mathématiciens croient effectivement[1], qu'en bout de ligne, les mathématiques reposent sur cette théorie. De plus, ils considèrent certains axiomes se rapportant aux ensembles comme étant vrais et allant de soi.

En supposant que les ensembles sont en effet d'importance première dans le fondement des mathématiques, plusieurs questions nous interpellent :

1. Qu'est-ce qu'un ensemble, réellement ?
2. Quels sont les principes qui gouvernent les ensembles ?

[1] Plusieurs mathématiciens ne veulent simplement pas se préoccuper des questions se rapportant au fondement des mathématiques. C'est un peu comme si vous ne vouliez pas réfléchir à quel parti politique voter, simplement parce que vous n'êtes confortable avec aucun d'entre eux.

3. Comment pouvons-nous raisonner correctement avec des ensembles, et avec des structures plus complexes que nous construisons avec ceux-ci ?

4. Est-ce que la vérité ou la fausseté de n'importe quel énoncé mathématique peut être déterminée à partir de faits sur les ensembles ?

Fait intéressant, les mathématiciens ne s'entendent pas tous sur les réponses à ces questions. Il y a des axiomes de la théorie des ensembles, par exemple, ceux qui postulent l'existence de certains ensembles très larges, qui ne sont pas universellement acceptés. Certains mathématiciens rejettent l'existence systématique des ensembles de parties, ou même l'idée d'un ensemble infini ! Et qui plus est, il y a désaccord sur la validité de certains principes de raisonnement ou de la logique. En fin de compte, ces questions sont d'ordre philosophique.

Tout de même, il n'y a pas de doute que les ensembles jouent un rôle très important en mathématiques et que l'apprentissage des notions de base liées à la théorie des ensembles est nécessaire pour comprendre des mathématiques plus avancées. Quoique nous puissions être en désaccord sur l'importance des ensembles comme *fondement* des mathématiques, ceux-ci sont certainement *fondamentaux* !

Alternatives pour le fondement

Quoique la majorité des mathématiciens conçoivent que la théorie des ensembles, sous une forme ou une autre, donne une fondation convenable pour les mathématiques, il existe des alternatives qui peuvent servir de système pour le fondement des mathématiques. La *théorie des catégories* est une telle alternative ; c'est une approche conceptuelle aux mathématiques qui met l'emphase sur les patrons et structures qui surviennent couramment en mathématiques. La *théorie des types* en est une autre, dont l'approche est plus orientée vers la logique.

IV.2 Qu'est ce qu'un ensemble ?

Jusqu'ici, nous avons argumenté que les ensembles sont importants, autant dans une perspective de fondement des mathématiques, que dans la pratique des mathématiques. Toutefois, nous n'avons pas réellement tenté de définir attentivement la notion d'ensemble. C'est, bien entendu, une omission sérieuse lorsque nous avançons qu'une grande partie des mathématiques se construit sur des ensembles. Nous avons intérêt à rendre cette notion précise.

La plupart des gens, lorsque pressés de définir ce qu'est un ensemble, arrivent avec la définition suivante :

Définition IV.2.1 (Définition naïve d'un ensemble)**.** Un *ensemble* est une collection de choses.

Mieux vaut affiner cette notion un peu plus, et remplacer le terme « choses » par « objets mathématiques ». Mais ceci demeure suspect : dans la mesure où nous cherchons à établir un fondement pour les mathématiques, nous ne devrions certainement pas supposer que nous savons déjà ce que sont des objets mathématiques. D'autant plus douteux, le mot « collection » semble dire pratiquement la même chose que le mot « ensemble ». Donc, n'avons nous pas remplacer un mot problématique pour un autre ?

Oui, c'est ce que nous avons fait. Toutefois, même si nous avions trouvé un meilleur mot ou une meilleure phrase pour décrire les ensembles, nous pourrions de nouveau objecter que nous n'avons que remplacé des mots par des mots, et nous pourrions toujours demander des clarifications.

Régression à l'infini

Une *régression à l'infini* est une situation où une solution à un problème n'est jamais atteinte car le problème ne fait que se répéter encore et encore, indéfiniment.
Cette situation se produit avec des définitions, lorsque l'on cherche continuellement à définir un concept en fonction de d'autres : On définit un concept A en termes de d'autres concepts B et C, et on doit maintenant définir B et C. Lorsque l'on entreprend ceci (en termes de d'autres concepts, disons D, E, F), on doit maintenant définir D, E, F aussi. Ce processus n'a pas de fin, à moins que l'on accepte certains *axiomes*.

En somme, si nous voulons continuer, nous devons nous résoudre à quelque chose, et la définition (IV.2.1) semble suffisamment bonne à des fins pratiques. Bien entendu, si nous sommes intéressés aux *fondements*, nous devons clarifier ce que nous acceptons comme objets mathématiques et comment nous nous permettons de les regrouper en un ensemble. Pour le moment, nous mettons cette question de côté et nous essayons plutôt de donner l'élan qu'il faut pour démarrer la théorie.

En adoptant cette définition et en acceptant le fait qu'elle demeure intrinsèquement vague, quoique suffisamment utile pour des raisons pratiques, nous adhérons à ce que nous appelons la *théorie naïve des ensembles*. Dans cette théorie, on ne fait que développer la théorie des ensembles sans trop se préoccuper d'une définition formelle pour les ensembles. Dans la leçon qui suit, par contre, nous expliquons comment cette théorie naïve peut occasionner certains problèmes, nous incitant à adopter une approche plus prudente.

IV.3 La relation d'appartenance

Une des choses de base que nous pouvons exprimer avec des ensembles est l'appartenance, c'est-à-dire si un objet est dans un ensemble ou non. Lorsque X est un ensemble (on emploie des lettres majuscules romaines pour désigner des ensembles) et a est un objet quelconque, nous écrivons $a \in X$ pour énoncer que a est un élément de l'ensemble X. Si nous voulons exprimer que a n'est pas un élément de X, nous écrivons $a \notin X$.

Relation d'appartenance :
$a \in X$ veut dire : a est un élément de l'ensemble X.
$a \notin X$ veut dire : a n'est pas un élément de l'ensemble X.

Lorsque a est un élément de X, nous disons aussi que a est un *membre* de X, ou que a *appartient à* X. Le symbole $\in$ est la lettre grecque epsilon, et est appelé le symbole d'*appartenance*.[2]

[2]Dans une leçon subséquente, nous expliquerons en quel sens technique la relation d'appartenance est une relation.

Souvent, nous voudrons décrire un ensemble en faisant explicitement la liste de tous ses éléments. Dans ce cas, on utilise la notation avec des accolades ensemblistes $\{\ldots\}$. Par exemple, si nous voulons introduire l'ensemble X dont les éléments sont les nombres 1, 4 et 22, nous pouvons écrire

$$X = \{1, 4, 22\}.$$

En combinant ceci avec la notation pour l'appartenance, nous pouvons formuler plusieurs énoncés à propos de cet ensemble, comme :

$$1 \in X, \qquad 3 \notin X, \qquad 4 \notin X, \qquad 6 \in X.$$

Les deux premiers énoncés sont vrais, tandis que les deux derniers sont faux.

Une chose importante à retenir est que l'ordre dans lequel nous faisons la liste des éléments n'est pas important. De ce fait, nous aurions pu écrire X comme $X = \{22, 1, 4\}$ ou $X = \{4, 22, 1\}$. De plus, les ensembles ne tiennent pas compte de la multiplicité des éléments (c'est-à-dire, le nombre de fois qu'un élément est listé). Ainsi, il est également vrai que $X = \{1, 4, 4, 4, 22, 22\}$; de dire à trois reprises que le nombre 4 est un élément de X ne change rien. Dans la prochaine leçon, nous donnerons un sens précis à la notion d'égalité entre des ensembles, i.e. pour que deux ensembles soient le même.

Considérons maintenant quelques collections d'objets mathématiques que nous utiliserons constamment :

Exemples IV.3.1.

1. $\mathbb{N} = \{0, 1, 2, \ldots\}$ est l'ensemble des *nombres naturels*
2. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ est l'ensemble des *entiers*
3. $\mathbb{Q}$ est l'ensemble des *nombres rationnels*
4. $\mathbb{R}$ est l'ensemble des *nombres réels*
5. $\mathbb{C}$ est l'ensemble des *nombres complexes*
6. L'ensemble $\{\mathsf{V}, \mathsf{F}\}$ (aussi appelé 2) est l'ensemble des *valeurs de vérité*.

Notez que pour les deux premiers ensembles, nous avons employé la notation de points de suspension $(\ldots)$ pour indiquer que la liste continue indéfiniment. Cette notation devrait être employée seulement dans la mesure où nous pouvons clairement concevoir de quelle manière la liste se prolonge !

Une façon très utile de décrire un ensemble fait appel à la *notation d'un ensemble en compréhension*. Voici un exemple :

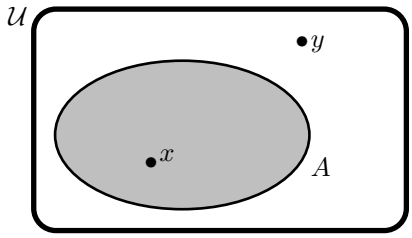
$$P = \{x | x \text{ est premier}\}.$$

Ici, nous définissons un ensemble, appelé P, dont les éléments sont tous les nombres qui sont premiers. La barre verticale | peut être prononcée « tels que ». Malheureusement, la définition ci-haut est ambiguë, puisqu'elle ne spécifie pas si nous voulons intégrer les nombres négatifs aussi. Vaut mieux utiliser $\{x \in \mathbb{N} | x \text{ est premier }\}$ ou $\{x \in \mathbb{Z} | x \text{ est premier }\}$. Morale : il faut être explicite lorsque nous voulons éviter des ambiguïtés potentielles !

IV.4 Diagrammes de Venn

Il y a un outil qui est fort utile pour visualiser des ensembles et des constructions sur ces derniers. Un *diagramme de Venn* est une représentation imagée d'un ou plusieurs ensembles, ainsi que de la relation entre ces ensembles. Typiquement, les ensembles sont dessinés comme des ellipses, tandis que les éléments sont représentés par des points. Par exemple, si un point nommé x est dessiné à l'intérieur d'une ellipse nommée A, alors notre intention est d'indiquer que $x \in A$. Si un élément y est dessiné à l'extérieur de A, notre intention est d'indiquer que $y \notin A$.

Souvent, nous travaillons dans un contexte mathématique spécifique où il y a un ensemble ambiant dans lequel tout objet d'intérêt est inclu. Par exemple, si nous « faisons de la théorie des nombres », nous pouvons nous confiner à l'ensemble des entiers. Dans une telle situation, où l'on considère les éléments et les sous-ensembles d'un ensemble particulier donné, nous faisons souvent référence à cet ensemble comme étant l'*univers de discours*, ou simplement l'*univers*. Il est coutumier de dénoter un tel univers par le symbole $\mathcal{U}$. Dans un diagramme de Venn, le rectangle qui établit le périmètre externe (à l'intérieur duquel toutes choses d'intérêt sont considérées) est un univers. La figure IV.1 illustre une telle situation.



Un *diagramme de Venn* avec

- Univers $\mathcal{U}$
- Un ensemble A
- Un élément $x \in A$
- Un élément $y \notin A$

Figure IV.1 – Diagramme de Venn

Quoique les diagrammes de Venn soient fort utiles comme outil de visualisation pour des ensembles, il est important de garder à l'esprit qu'ils ne forment pas de substituts pour la précision du raisonnement mathématique.

IV.5 Sommaire

La théorie naïve des ensembles est une théorie informelle des ensembles qui ignore certains problèmes philosophiques ; elle constitue l'approche théorique courante que les mathématiciens adoptent au quotidien pour travailler avec des ensembles.

- La définition naïve d'un ensemble, quoique fonctionnelle, est « une collection d'objets mathématiques ».
- L'appartenance ensembliste est la notion la plus fondamentale dans la théorie des ensembles.

- Lorsqu'on fait la liste des éléments d'un ensemble, l'ordre et la multiplicité des éléments n'a pas d'importance.
- Il y a plusieurs façons de décrire des ensembles : en listant tous les éléments d'un ensemble, ou en employant la notation d'un ensemble en compréhension. À des fins d'aide visuelle informelle, les diagrammes de Venn peuvent être utiles.

LEÇON V

La théorie formelle des ensembles

La version naïve de la théorie des ensembles est suffisante à toutes fins pratiques. Toutefois, des problèmes surviennent lorsque nous la poussons à ses limites ! Cette leçon explique en quoi consiste ces problèmes, et les conditions sous lesquelles ils se manifestent. Aussi, nous allons survoler brièvement la théorie formelle des ensembles et comment celle-ci évite les problèmes en question.

V.1 Le paradoxe de Russell

Jusqu'ici, la théorie naïve des ensembles nous a donné un langage simple pour parler de l'appartenance d'éléments vis-à-vis d'ensembles et décrire des ensembles avec la notation d'un ensemble en compréhension.

Il est important de savoir reconnaître et apprécier la puissance et la flexibilité de ces concepts. Rappelons-nous qu'un ensemble se définit comme étant une collection d'objets mathématiques. Nous devrions certainement être en mesure de considérer les ensembles eux-mêmes comme des objets mathématiques. Donc, il est sensé de parler d'ensembles dont les éléments sont eux-mêmes des ensembles. Par exemple, nous avons l'ensemble $\{\mathbb{N}, \mathbb{Q}, \mathbb{R}\}$. Comme vous pouvez le constater, ceci nous donne une certaine mesure d'expressivité : la seule limite que nous avons en définissant de nouveaux ensembles est notre imagination.

Or, considérez l'ensemble suivant (défini en compréhension) :

$$X = \{\, U \mid U \notin U \,\}.$$

Pour comprendre en quoi cet ensemble constitue un problème,

> **Analyse logique**
>
> Pour rendre la forme schématique du paradoxe de Russell plus explicite, considérez l'hypothèse A. Supposons maintenant que, avec l'aide de A, nous puissions prouver les deux énoncés suivants :
>
> - $P \to \neg P$
> - $\neg P \to P$
>
> où P est un autre énoncé quelconque (cela importe peu en quoi P consiste, le nôtre était $X \in X$). Ces deux énoncés forment une contradiction (vérifiez la table de vérité !). Ainsi, nous avons démontré $A \to \bot$. Ceci équivaut à dire que A est faux.

nous devrions analyser ce X de plus près. Il y a deux types d'ensembles : ceux qui sont membres d'eux-mêmes, et ceux qui ne le sont pas. De quel type est l'ensemble X en question ? Supposons que X est membre de lui-même, i.e. que $X \in X$. Par définition de l'ensemble X, ceci veut dire X n'est pas un membre de lui-même (parce que X est l'ensemble qui regroupe *tous* les ensembles qui ne sont pas membres d'eux-mêmes). Donc, $X \notin X$. Ceci est une contradiction. Ensuite, supposons que X n'est pas un membre de lui-même, i.e. $X \notin X$. Alors, par définition, X appartient à X (encore une fois, c'est parce que X regroupe *tous* les ensembles qui ne sont pas membres d'eux-mêmes). Donc, $X \in X$. Nous avons une contradiction à nouveau.

V.2 Théorie formelle des ensembles

Le paradoxe de Russell survient parce qu'il n'y a pas de restriction sur la façon dont on définit de nouveaux ensembles. Ceci a amené les mathématiciens à développer diverses formes de la théorie des ensembles qui évitent ce genre d'inconsistances[1], telles que nous les retrouvons dans la théorie naïve des ensembles.

L'approche la plus commune est de travailler avec un *système formel* ; l'idée n'est pas de donner une définition directe de ce qu'est un ensemble, mais d'axiomatiser les propriétés essentielles d'un ensemble dans le cadre d'un système de logique bien contrôlé (et ensuite, de nous permettre d'appeler tout ce qui a les propriétés en question, un ensemble). La version la plus courante de la théorie formelle des ensembles est appelée la théorie des ensembles de *Zermelo-Fränkel* ou ZFC[2].

Grosso modo, ce système fonctionne de la manière suivante :

- En premier lieu, on spécifie un *langage*. Pour ZFC et ses variantes, le langage est généré à partir d'un seul symbole de base, soit $\in$. On peut ensuite écrire des *formules* en utilisant le symbole d'appartenance, les connectifs propositionnels et les quantificateurs. Par exemple, $\forall x \, \exists y.(y \in x \vee x \in y)$ est une formule de ce genre. (Techniquement, ZFC est une théorie élaborée dans la logique des prédicats de premier ordre.)

- Ensuite, on choisit des *axiomes*. Ces axiomes nous disent quels genres d'ensembles peuvent être construits et comment ils se comportent. Par exemple, un de ces axiomes nous dit que l'ensemble des parties d'un ensemble (bien défini à priori) existe toujours.

- Finalement, on peut utiliser les règles de la logique des prédicats pour prouver des théorèmes à propos des ensembles.

Le fait que que nous travaillons avec un système formel, accompagné d'une série d'axiomes appropriés, nous guarantit que des problèmes comme le paradoxe de Russell ne surviennent pas. Bien entendu, nous voudrions tout de même avoir suffisamment d'expressivité, et nous voudrions avoir une méthode similaire à la notation d'un ensemble en compréhension pour construire de nouveaux ensembles à partir d'anciens. Ceci nous mène à l'axiome suivant, souvent appelé *compréhension restreinte*.

[1] Une théorie est dite *inconsistante* lorsqu'on peut en dériver une contradiction. Pratiquement tout le monde — à l'exception notable de quelques australiens — s'entend à dire qu'il s'agit d'un défaut fatal.

[2] Le « C » signifie « choix », et se réfère à l'axiome du choix qui fait partie de ce système.

Axiome de compréhension restreinte :
Supposons que X est un ensemble et que $\phi(x)$ est une propriété que les éléments de X peuvent avoir. Alors, l'ensemble

$$A = \{\, x \in X \mid \phi(x) \,\}$$

existe et est caractérisé par $x \in A \Leftrightarrow \phi(x)$.

Le terme « restreinte » réfère au fait que nous pouvons appliquer cet axiome seulement dans les cas où nous faisons une sélection d'éléments à l'intérieur d'un ensemble bien défini à priori, en spécifiant quelles propriétés les éléments doivent satisfaire.

V.3 Sommaire

Les points clés de cette leçon sont

- Sans aucune restriction, la théorie naïve des ensembles mène au paradoxe de Russell.
- Afin d'éviter le paradoxe de Russell et des problèmes similaires, nous pouvons travailler avec une théorie formelle des ensembles comme ZFC.
- Dans un tel système, le paradoxe de Russell est évité en employant une formulation plus prudente de la construction en compréhension pour ensembles, c'est-à-dire l'axiome de compréhension restreinte.

V.4 Exercices

Exercice 49. Dans un certain village, il y a un homme barbier qui rase tout homme qui ne se rase pas lui-même. Expliquez en quoi ceci est un paradoxe, et comment il est relié au paradoxe de Russell.

Exercice 50. Existe-t-il un ensemble X tel que $X \in X$? Pourquoi (ou pourquoi pas) ?

Exercice 51. Supposons que nous définissons $X = \{\, U \mid U \text{ est un ensemble } \}$. C'est-à-dire, X est l'ensemble qui contient tous les ensembles. Est-ce que ceci mène à un paradoxe également ?

Exercice 52. Une régression infinie est-elle nécessairement une chose mauvaise ? Ou y a-t-il des situations où une régression infinie est inoffensive ?

Exercice 53. Supposons que nous mettons par écrit un certain nombres d'axiomes que les ensembles devraient satisfaire, à notre avis. Comment savons-nous si la théorie qui en résulte est consistante ou non ?

LEÇON VI

SOUS-ENSEMBLES ET ÉGALITÉ

Nous allons maintenant étudier certains concepts de base de la théorie des ensembles. Nous avons déjà présenté la relation d'appartenance et les différentes méthodes pour spécifier un ensemble. Cette leçon introduit un autre concept fondamental, celui de la *relation de sous-ensemble*. Nous allons également travailler avec un autre axiome de la théorie des ensembles, c'est-à-dire l'*axiome d'extensionnalité*, lequel gouverne l'égalité entre les ensembles.

VI.1 SOUS-ENSEMBLE

Nous avons souvent l'occasion d'exprimer qu'un ensemble est contenu dans un autre. Par exemple, les nombres naturels sont contenus dans les entiers. La définition suivante donne un sens plus précis par rapport à cette idée :

Définition VI.1.1 (Sous-ensemble)**.** Étant donné deux ensembles A, B, on dit que A *est un sous-ensemble de* B lorsque tous les éléments de A sont également des éléments de B. Dans ce cas, on écrit $A \subseteq B$. La notation logique est :

$$A \subseteq B \Leftrightarrow_{\text{déf}} \forall x(x \in A \to x \in B).$$

Si A n'est pas un sous-ensemble de B, on écrit $A \not\subseteq B$. Notez que ceci n'est *pas* la même chose que de dire $B \subseteq A$. (Voir les exemples ci-bas.)

PROCÉDURE DE PREUVE

Pour prouver $A \subseteq B$, vous devez

- prendre un élément arbitraire $x \in A$, et ensuite démontrer que $x \in B$.

Dans le cas contraire, pour réfuter $A \subseteq B$, vous devez

- démontrer qu'il existe un élément $x \in A$ tel que $x \notin B$.

Exemples VI.1.2.

1. Nous avons $\{2, 3, 4\} \subseteq \{2, 3, 4, 5\}$.

2. Par contre, $\{2,3,4\} \not\subseteq \{2,3\}$; le premier ensemble contient l'élément 4, mais ce dernier n'appartient pas au deuxième ensemble.

3. Nous avons $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, et ainsi de suite. (Ceci est une conséquence de la définition de ces ensembles de nombres.) Nous avons aussi $\mathbb{Z} \not\subseteq \mathbb{N}$, car le premier ensemble a un élément qui n'appartient pas au second, par exemple, -4.

4. Aussi, nous avons $\{2,3\} \not\subseteq \{2,4\}$ et $\{2,4\} \not\subseteq \{2,3\}$.

ASPECTS LOGIQUES

À partir de la définition de sous-ensemble, nous avons

$$A \subseteq B \quad \equiv_{\text{déf}} \quad \forall x(x \in A \to x \in B)$$

Nous remarquons que la *négation* de $A \subseteq B$ peut être formulée de manière équivalente comme suit :

$$\begin{aligned} A \not\subseteq B \quad &\equiv_{\text{déf}} \quad \neg\forall x(x \in A \to x \in B) \\ &\equiv \quad \exists x\neg(x \in A \to x \in B) \\ &\equiv \quad \exists x(x \in A \wedge x \notin B). \end{aligned}$$

VI.2 QUAND EST-CE QUE DEUX ENSEMBLES SONT ÉGAUX ?

Considérez les ensembles suivants : $A = \{4\}$, $B = \{12,4\}$, $C = \{4,12\}$, $D = \{4,12,4\}$. Il y a un trait notable (la cardinalité) qui nous permet de différencier les ensembles A et B : A contient un seul élément[1] veut dire $X \subseteq A$. », tandis que B en a deux. Est-ce que B et C sont différents ? La seule différence est que les éléments ne sont pas listés dans le même ordre. Et la seule différence entre C et D est que D fait deux fois mention de l'élément 4. Nous introduisons l'axiome suivant pour définir la notion d'*égalité* entre des ensembles, lequel dit grosso modo que deux ensembles sont complètement déterminés par leurs éléments.

Axiome d'extensionnalité :
Deux ensembles sont égaux précisément lorsqu'ils ont les mêmes éléments. La notation logique est

$$X = Y \Leftrightarrow \forall z(z \in X \leftrightarrow z \in Y).$$

[1] L'expression « A contient un élément X » veut dire $X \in A$, tandis que « A contient X

Aspects logiques

Nous avons les énoncés équivalents suivants :

$$\begin{aligned} X = Y &\equiv_{\text{déf}} \forall z(z \in X \leftrightarrow z \in Y) \\ &\equiv \forall z((z \in X \to z \in Y) \wedge (z \in Y \to z \in X)) \\ &\equiv \forall z(z \in X \to z \in Y) \wedge \forall z(z \in Y \to z \in X). \end{aligned}$$

Ainsi, la *négation* de $X = Y$ peut être formulée de manière équivalente comme suit :

$$\begin{aligned} X \neq Y &\equiv_{\text{déf}} \neg\forall z(z \in X \leftrightarrow z \in Y) \\ &\equiv \neg[\forall z(z \in X \to z \in Y) \wedge \forall z(z \in Y \to z \in X)] \\ &\equiv [\neg\forall z(z \in X \to z \in Y)] \vee [\neg\forall z(z \in Y \to z \in X)] \\ &\equiv [\exists z\neg(z \in X \to z \in Y)] \vee [\exists z\neg(z \in Y \to z \in X)] \\ &\equiv [\exists z(z \in X \wedge z \notin Y)] \vee [\exists z(z \in Y \wedge z \notin X)]. \end{aligned}$$

Donc, deux ensembles sont distincts lorsque l'un d'entre eux contient un élément qui n'est pas contenu dans l'autre. Étant donné que l'ensemble B ci-haut contient un élément 12 qui n'est pas dans A, ceci veut dire que $A \neq B$. Toutefois, nous avons $B = C$: chaque élément de B se trouve dans C et vice versa. Similairement, nous avons $C = D$.

Comme pour n'importe quelle définition, vous devriez toujours vous demander ce qu'il faut faire pour prouver qu'un certain exemple satisfait une définition ou non (voir l'encadré : procédure de preuve).

Exercice 54. Considérez les ensembles suivants : $X = \{1, 2, 3\}$, $Y = \{0, 1, 0, 2, 0, 3\}$, $Z = \{3, 1, 2, 3\}$. Lesquels sont égaux ?

Exercice 55. Considérez les ensembles $A = \{a\}$, $B = \{\{a\}\}$, et $C = \{a, \{a\}\}$. Y a-t-il de ces ensembles qui sont égaux ? Lesquels sont des sous-ensembles desquels ?

Procédure de preuve

Afin de prouver que $X = Y$, vous devez

- prendre un élément arbitraire $z \in X$, et prouver que $z \in Y$, **ET**
- prendre un élément arbitraire $z \in Y$, et prouver que $z \in X$.

Afin de prouver que $X \neq Y$, vous devez

- démontrer qu'il existe un élément z tel que $z \in X$ et $z \notin Y$, **OU**
- démontrer qu'il existe un élément z tel que $z \in Y$ et $z \notin X$.

VI.3 Sous-ensembles et égalité

La notion de sous-ensemble est étroitement liée à celle de l'égalité d'ensembles ; la proposition suivante peut en témoigner.

Proposition VI.3.1. *Pour n'importe quels ensembles A, B, nous avons $A = B$ précisément lorsque $A \subseteq B$ et $B \subseteq A$ en même temps.*

Démonstration. Soient A et B, deux ensembles arbitraires. Supposons en premier que $A = B$. Ensuite, considérons un élément $x \in A$. Puisque $A = B$, alors $x \in B$ (par définition de l'égalité d'ensembles). Ceci démontre que $A \subseteq B$. De plus, étant donné un élément $x \in B$, nous obtenons $x \in A$ (encore une fois, parce que $A = B$). Ceci nous donne $B \subseteq A$.

Pour l'autre direction, supposons que $A \subseteq B$ et $B \subseteq A$. Nous devons montrer que $A = B$. Considérons un élément $x \in A$. Puisque $A \subseteq B$, il s'ensuit que $x \in B$ aussi. Ensuite, considérons un élément $x \in B$. Puisque $B \subseteq A$, nous obtenons $x \in A$. Or, A et B ont les mêmes éléments, donc $A = B$. □

La preuve ci-haut donne un peu plus de détails que celles que nous voyons habituellement. Notre intention était de clarifier (a) en quoi consiste la structure de la preuve et (b) comment nous servir des différentes définitions en jeu dans le raisonnement logique. Au fur et à mesure que nous progressons, nous allons sauter certains détails avec lesquels nous sommes plus familiers lors de l'écriture de preuves (afin de rendre ces dernières plus lisibles). Néanmoins, vous devriez toujours être en mesure de remplir ces détails !

VI.4 Sommaire

Nous avons introduit un axiome définissant l'égalité entre des ensembles :

- *Axiome d'extensionnalité* : deux ensembles sont égaux lorsqu'ils ont les mêmes éléments.

De plus, nous avons défini la relation de sous-ensemble et nous avons établi le fait élémentaire (quoique important) suivant :

- $A = B$ si et seulement si $A \subseteq B$ et $B \subseteq A$.

Une chose importante que nous devons garder à l'esprit est qu'une définition donne implicitement (ou parfois explicitement) une recette pour prouver ou réfuter qu'un objet mathématique satisfait cette dernière.

VI.5 Exercices

Exercice 56. Trouvez tous les sous-ensembles de l'ensemble $X = \{a, b, c\}$.

Exercice 57. Trouvez tous les sous-ensembles de $X = \{a, b, c, d\}$.

Exercice 58. Supposons que X a n éléments. Combien y a-t-il de sous-ensembles de X ?

Exercice 59. Considérez les ensembles

$$A = \{a, b\}, \quad B = \{a, \{a\}, \{b\}\}, \quad C = \{\{a\}, \{b\}, a, b\}, \quad D = \{\{a\}, \{b\}, \{a, b\}\}.$$

Déterminez lesquels de ces ensembles sont des éléments de quels autres ensembles. Aussi, déterminez lesquels sont des sous-ensembles de quels autres.

Exercice 60. Vrai ou faux ? N'importe quels deux ensembles qui ont tous les deux exactement 6 éléments sont égaux. (Si c'est vrai, donnez une preuve. Sinon, donnez un contre-exemple.)

Exercice 61. Prouvez que pour n'importe quel ensemble A, nous avons $A \subseteq A$. Utilisez ce résultat pour prouver que $A = A$.

Exercice 62. Prouver que si $A \subseteq B$ et $B \subseteq C$, alors $A \subseteq C$ aussi. Utilisez ce résultat pour prouver : si $A = B$ et $B = C$, alors $A = C$.

Exercice 63. Prouvez que $A = B$ implique $B = A$.

Exercice 64. Nous introduisons la notation suivante :

$$A \subset B \Leftrightarrow_{\text{déf}} A \subseteq B \text{ et } A \neq B.$$

Démontrez que $A \subset B$ et $B \subset C$ implique $A \subset C$.

Exercice 65. (Cet exercice emploi la notation du précédent.) L'énoncé suivant est-il vrai ? $A \subset B$ et $B \subseteq C$ implique $A \subset C$. Donnez une preuve ou un contre-exemple.

Exercice 66. Même question, mais avec l'énoncé : $A \subset B$ et $B \subseteq C$ implique $A \subseteq C$.

Exercice 67. Est-il possible que pour deux ensembles A, B, nous ayons $A \subset B$ et $B \subset A$ en même temps ? Pourquoi (ou pourquoi pas) ?

Exercice 68. Est-il possible que pour deux ensembles A, B, nous ayons $A \subseteq B$ et $A \in B$ en même temps ? Pourquoi (ou pourquoi pas) ?

Exercice 69. Trouvez des ensembles A, B, C tels que $A \in B$, $B \in C$ et $A \in C$. Est-il vrai, en général, que $A \in B$ et $B \in C$ implique $A \in C$? Expliquez pourquoi (ou pourquoi pas).

LEÇON VII

EXISTENCE

Dans les leçons précédentes, nous avons été exposés à certains ensembles bien connus, dont l'ensemble des entiers. Par contre, nous avons sauté une étape : le but était de construire les mathématiques en utilisant des ensembles, et seulement des ensembles, mais lorsque nous avons introduit des ensembles comme $\mathbb{Z}$, nous avons présupposé leur existence sans justifications.

Donc, revenons en arrière un peu, et ne présupposons pas l'existence d'objets mathématiques de cette manière. La question à se poser : De quels genres d'ensembles pouvons-nous démontrer l'existence ? Malheureusement, il n'y a pas de raison pour laquelle un ensemble en particulier devrait exister plutôt qu'un autre ! Cette leçon introduit des axiomes qui guarantissent l'existence de plusieurs ensembles intéressants.

VII.1 L'ENSEMBLE VIDE

Pour démarrer la théorie, nous devons postuler l'existence d'au moins un ensemble.

Axiome d'existence :
Il existe un ensemble $\emptyset$ qui n'a aucun élément.

Ceci pourrait sembler étrange d'introduire un ensemble vide, plutôt qu'un ensemble un peu plus sophistiqué ; nous devrons nous assurer que cet axiome aura quelques utilités.[1] Nous allons voir que,

[1] Cet axiome peut être déduit à partir des autres axiomes de la théorie (dont plusieurs seront abordés plus tard), mais nous avons intérêt à faire cela seulement si nous cherchons à obtenir un ensemble d'axiomes qui est minimal.

en conjonction avec l'axiome de l'ensembles de parties défini dans la section suivante, nous pouvons effectivement construire bien d'autres ensembles.

Pour l'instant, étudions l'ensemble vide. Premièrement, notons que :

Lemme VII.1.1. *Pour n'importe quel ensemble A, nous avons $\emptyset \subseteq A$.*

Démonstration. Nous devons montrer que tout élément de $\emptyset$ est également un élément de A. Mais il n'y a pas d'éléments dans $\emptyset$, donc il n'y a rien à vérifier.[2] □

En d'autres mots, l'ensemble vide est un sous-ensemble de n'importe quel ensemble.

Proposition VII.1.2. *L'ensemble vide est unique. C'est-à-dire, il y a exactement un ensemble vide.*

Démonstration. Nous savons déjà qu'il existe au moins un ensemble vide ; nous avons imposé cela à travers l'axiome. Donc, tout ce que nous devons vérifier est qu'il ne peut y en avoir plus qu'un. Pour entreprendre cela, nous devons faire la supposition que nous avons deux ensembles vides, puis prouver que ces derniers doivent être égaux.

Ainsi, supposons que $\emptyset$ et $\emptyset'$ sont tous les deux des ensembles vides. Par le lemme VII.1.1, nous savons qu'un ensemble vide est contenu dans n'importe quel autre ensemble. En appliquant ceci deux fois, nous trouvons que $\emptyset \subseteq \emptyset'$ et $\emptyset' \subseteq \emptyset$. Mais par la proposition VI.3.1, il s'ensuit que $\emptyset = \emptyset'$. □

ASPECTS LOGIQUES

L'énoncé $\emptyset \subseteq A$ veut dire

$$\forall x(x \in \emptyset \to x \in A).$$

Mais, $x \in \emptyset$ est toujours faux, donc ceci devient

$$\forall x(\bot \to x \in A).$$

Une implication $\bot \to p$ est toujours vraie, et donc l'énoncé est vrai dans l'ensemble.

VII.2 L'AXIOME DE L'ENSEMBLE DES PARTIES

Nous avons introduit l'ensemble vide, mais il n'est pas déraisonnable d'en demander davantage. Le constructeur de l'*ensemble des parties* nous permet de former de nouveaux ensembles à partir d'anciens : lorsque X est un ensemble, nous pouvons définir un nouvel ensemble

$$\mathcal{P}(X) = \{\, U \mid U \subseteq X \,\}.$$

C'est-à-dire, $\mathcal{P}(X)$ est défini comme l'ensemble dont les éléments sont tous les sous-ensembles de X. $\mathcal{P}(X)$ est appelé l'*ensemble des parties de X*. Un des axiomes de la théorie des ensembles stipule que l'ensemble des parties de X existe pour n'importe quel ensemble X [3] :

[2] Les énoncés qui sont vrais parce qu'il n'y a pas de cas à vérifier sont parfois appelés des *vérités vides*.

[3] Ceci est un des axiomes controversés, et il y a plusieurs mathématiciens qui le rejette dans sa forme générale ; un affaiblissement approprié donne lieu à une formulation de la théorie des ensembles appelée *théorie prédicative des ensembles*.

Axiome de l'ensemble des parties :
Étant donné un ensemble X, il existe un ensemble $\mathcal{P}(X)$ avec la propriété : $U \in \mathcal{P}(X)$ si et seulement si $U \subseteq X$.

Des exemples vont illustrer le fonctionnement de cet axiome (veuillez consulter les trois premiers exercices de la leçon précédente si vous avez de la difficulté à comprendre les exemples qui suivent) :

Exemples VII.2.1.

1. Pour $X = \{a\}$, nous avons $\mathcal{P}(X) = \{\emptyset, \{a\}\}$.
2. Pour $X = \{a, b\}$, nous avons $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
3. Pour $X = \{a, b, c\}$, nous avons
$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$
4. $\mathcal{P}(\emptyset) = \{\emptyset\}$. En effet, l'ensemble vide a exactement un sous-ensemble, à savoir lui-même. C'est le seul élément de $\mathcal{P}(\emptyset)$.
5. $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. (Cet exemple est un cas particulier du premier exemple avec $X = \{a\}$.)

Le lemme suivant est une conséquence évidente de la définition (faites-en la vérification vous-même !) :

Lemme VII.2.2. *Pour n'importe quel ensemble X, nous avons*
$$\emptyset \in \mathcal{P}(X) \qquad \textit{et} \qquad X \in \mathcal{P}(X).$$

Exercice 70. Supposons que l'ensemble X a n éléments. Combien d'éléments l'ensemble $\mathcal{P}(X)$ a-t-il ?

Exercice 71. Déterminez $\mathcal{P}(\mathcal{P}(\{0, 1\}))$.

Comme nous pouvons le constater à travers les exemples, l'axiome de l'ensemble des parties nous donne des ensembles authentiquement nouveaux, par exemple $\{\emptyset\}$ (vérifiez par vous-même que cet ensemble est différent de $\emptyset$!).

Maintenant, qu'en est-il d'un ensemble tel que $A = \{\{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$? Ce dernier n'est pas un ensemble des parties de quelque ensemble que ce soit (vérifiez cela !) ; donc, son existence ne découle pas directement de l'axiome de l'ensembles de parties. Néanmoins, l'axiome de compréhension peut nous aider ici. Premièrement, nous avons effectivement l'ensemble
$$B = \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$
Par la compréhension, nous pouvons définir B comme un sous-ensemble de A :
$$A = \{\, U \in B \mid U \neq \emptyset \,\}.$$
Ceci prouve que A existe !

Exercice 72. Utilisez la compréhension pour démontrer que $C = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ existe.

VII.3 Propriétés des ensembles de parties

Nous allons maintenant prouver un résultat typique en ce qui concerne les ensembles de parties. Vous devriez mettre l'accent principalement sur les méthodes de preuve employées, car elles constituent de bons exemples de déballages systématiques de définitions et d'utilisation de la logique pour obtenir les conclusions désirées.

Proposition VII.3.1. *Pour n'importe quels ensembles A, B, nous avons $A \subseteq B$ si et seulement si $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.*

Démonstration. Considérons des ensembles arbitraires A et B. Premièrement, nous prouvons que $A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$. Supposons $A \subseteq B$. Ceci veut dire que : pour tout x, si $x \in A$, alors $x \in B$.

Nous devons montrer que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, c'est-à-dire que : pour chaque U, si $U \in \mathcal{P}(A)$, alors $U \in \mathcal{P}(B)$. Par définition d'un ensemble des parties, ceci équivaut à dire : pour chaque U, si $U \subseteq A$, alors $U \subseteq B$.

Donc, supposons que nous avons un U tel que $U \subseteq A$. Pour démontrer $U \subseteq B$, considérons un élément arbitraire $x \in U$. Puisque $U \subseteq A$, il s'ensuit que $x \in A$. Par hypothèse, nous avons $A \subseteq B$, et il s'ensuit que $x \in B$ également. Donc, $x \in U$ implique $x \in B$, et ceci veut dire que $U \subseteq B$, tel que voulu. Ceci démontre que $U \subseteq A$ implique $U \subseteq B$.

Pour l'autre direction de la preuve, supposons que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, ou de manière équivalente : pour tout U, $U \subseteq A$ implique $U \subseteq B$. En particulier, ceci est vrai pour $U = A$ (car $A \subseteq A$), et nous obtenons $A \subseteq B$, tel que voulu. □

Une façon courante de se référer à la première partie de ce résultat est de dire que $\mathcal{P}$ est une opération *monotone*. (Une notion générale de la monotonicité est présentée dans la leçon XX.)

Observez que la deuxième partie de la preuve emploie un petit truc : afin d'utiliser l'hypothèse $\forall U(U \subseteq A \to U \subseteq B)$, nous devons choisir un U qui convient. À travers cet exemple, nous pouvons concevoir que l'écriture de preuves n'est pas toujours une entreprise automatique ; des choix ingénieux sont parfois requis.

La première partie de cette preuve est plus directe, mais nous devons procéder de façon systématique. La figure VII.1 met en évidence, sous forme de tableau, la structure de la preuve et sa « dynamique », i.e. l'ordre dans lequel le raisonnement s'effectue.

Étant donné/suppositions	**À prouver**	**Auxiliaire**	**Justification**
$--$	$A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)$		
$A \subseteq B$	$\mathcal{P}(A) \subseteq \mathcal{P}(B)$		strat. de preuve pour $\to$
$\forall x(x \in A \to x \in B)$	$\forall U(U \in \mathcal{P}(A) \to U \in \mathcal{P}(B))$		déf. de $\subseteq$
$\forall x(x \in A \to x \in B)$	$\forall U(U \subseteq A \to U \subseteq B)$		déf. de $\mathcal{P}$
$\forall x(x \in A \to x \in B)$ $U -$ arbitraire	$U \subseteq A \to U \subseteq B$		strat. de preuve pour $\forall$
$\forall x(x \in A \to x \in B)$ $U -$ arbitraire $U \subseteq A$	$U \subseteq B$		strat. de preuve pour $\to$
$\forall x(x \in A \to x \in B)$ $U -$ arbitraire $\forall x(x \in U \to x \in A)$	$\forall x(x \in U \to x \in B)$		déf. de $\subseteq$
$\forall x(x \in A \to x \in B)$ $U -$ arbitraire $\forall x(x \in U \to x \in A)$ $x -$ arbitraire	$x \in U \to x \in B$		strat. de preuve pour $\forall$
$\forall x(x \in A \to x \in B)$ $U -$ arbitraire $\forall x(x \in U \to x \in A)$ $x -$ arbitraire $x \in U$	$x \in B$		strat. de preuve pour $\to$
$\boxed{\forall x(x \in A \to x \in B)}$ $U -$ arbitraire $\boxed{\forall x(x \in U \to x \in A)}$ $x -$ arbitraire $x \in U$	$x \in B$	$\boxed{\boxed{x \in A \to x \in B}}$ $\boxed{\boxed{x \in U \to x \in A}}$	instanciation
$\forall x(x \in A \to x \in B)$ $U -$ arbitraire $\forall x(x \in U \to x \in A)$ $x -$ arbitraire $\boxed{x \in U}$	$x \in B$	$x \in A \to x \in B$ $\boxed{x \in U \to x \in A}$ $\boxed{\boxed{x \in A}}$	Modus ponens
$\forall x(x \in A \to x \in B)$ $U -$ arbitraire $\forall x(x \in U \to x \in A)$ $x -$ arbitraire $x \in U$	$\boxed{\boxed{x \in B}}$	$\boxed{x \in A \to x \in B}$ $x \in U \to x \in A$ $\boxed{x \in A}$	Modus ponens

FIGURE VII.1 – Une preuve que $A \subseteq B$ implique $\mathcal{P}(A) \subseteq \mathcal{P}(B)$

VII.4 Sommaire

Cette leçon introduit deux nouveaux axiomes :

- *Axiome d'existence* : un ensemble vide existe
- *Axiome de l'ensemble des parties* : l'ensemble des parties existe pour n'importe quel ensemble

En utilisant ces axiomes, nous pouvons construire une panoplie d'ensembles. En les combinant avec l'axiome de compréhension (restreinte), nous pouvons également démontrer l'existence d'une variété d'autres ensembles (comme les sous-ensembles d'un ensemble de parties). Ceci requiert habituellement d'arriver avec une description qui caractérise les éléments du sous-ensemble que nous cherchons à définir.

Nous avons également établi l'unicité de l'ensemble vide, et nous avons prouvé que l'opération de l'ensemble des parties est *monotone*, c'est-à-dire que $A \subseteq B$ implique $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

VII.5 Exercices

Exercice 73. Pour chacun des ensembles suivants, décrivez tous les éléments dans cet ensemble.

(a) $\mathcal{P}(\mathcal{P}(\emptyset))$

(b) $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$

(c) $\{x \in \mathcal{P}(\mathcal{P}(\emptyset)) | x \subseteq \mathcal{P}(\emptyset)\}$

(d) $\{x \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) | \emptyset \in x\}$

(e) $\{x \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) | \{\emptyset\} \in x\}$

(f) $\{x \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) | \mathcal{P}(\emptyset) \subseteq x\}$

Exercice 74. Lesquels des énoncés suivants sont vrais ?

(a) $\emptyset \in \mathcal{P}(\emptyset)$

(b) $\emptyset \subseteq \mathcal{P}(\emptyset)$

(c) $\mathcal{P}(\emptyset) \in \mathcal{P}\mathcal{P}(\emptyset)$

(d) $\mathcal{P}(\emptyset) \in \mathcal{P}\mathcal{P}\mathcal{P}(\emptyset)$

(e) $\mathcal{P}(\emptyset) \subseteq \mathcal{P}\mathcal{P}\mathcal{P}(\emptyset)$

(f) $\{X\} \in \mathcal{P}(X)$

(g) $\{X\} \subseteq \mathcal{P}(X)$

(h) $\{X\} \in \mathcal{P}(\{X\})$

(i) $\{X\} \subseteq \mathcal{P}(\{X\})$

Exercice 75. Démontrez que $A = B$ implique $\mathcal{P}(A) = \mathcal{P}(B)$. La réciproque est-elle vraie ?

Exercice 76. L'ensemble $\{a, \{a\}, \{\{a\}\}, \{\{\{a\}\}\}\}$ est-il un ensemble de parties ?

Exercice 77. Peut-il exister un ensemble X tel que $\mathcal{P}(X) \subseteq X$? Si oui, donnez un exemple. Sinon, expliquez pourquoi pas.

Exercice 78. Prouvez que l'existence d'un ensemble vide peut être démontré à partir de l'axiome de l'ensemble des parties et de l'axiome de compréhension restreinte.

Exercice 79. Peut-il exister des ensembles A, B, C tels que $A \subseteq B \subseteq C, A \in B \in C$ et $A \in C$? Donnez un exemple ou prouvez que c'est impossible.

Exercice 80. Peut-il exister des ensembles A, B tels que $\{A\} \subseteq \{B\}$ et $B \in A$? Donnez un exemple ou prouvez que c'est impossible.

LEÇON VIII

OPÉRATIONS

Cette leçon introduit les *opérations booléennes*[1] sur des ensembles. Non seulement ces opérations surviennent constamment en pratique et aident à définir de nouveaux ensembles, mais elles sont aussi étroitement liées au raisonnement logique, comme nous allons le constater.

VIII.1 QUATRE OPÉRATIONS

L'opération la plus simple que nous introduisons est *l'intersection (binaire)* : étant donné deux ensembles A et B, nous définissons

$$A \cap B =_{\text{déf}} \{\, x \mid x \in A \wedge x \in B \,\}.$$

Ensuite, l'*union (binaire)* de deux ensembles A et B se définit par

$$A \cup B =_{\text{déf}} \{\, x \mid x \in A \vee x \in B \,\}.$$

Ici, le mot « ou » réfère au « ou inclusif », i.e. une disjonction.

L'opération de *complémentation* a un sens seulement lorsque nous travaillons à l'intérieur d'un univers $\mathcal{U}$. Dans ce cas, nous pouvons définir le *complément* d'un ensemble A par

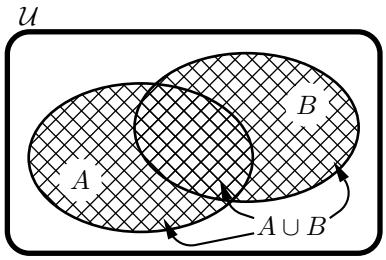
$$A^c =_{\text{déf}} \{\, x \in \mathcal{U} \mid x \notin A \,\}.$$

Finalement, nous définissons la *différence* de deux ensembles A et B comme étant

$$A - B =_{\text{déf}} \{\, x \mid x \in A \wedge x \notin B \,\}.$$

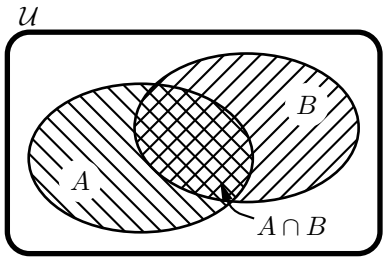
La figure VIII.1 illustre les quatre opérations avec des diagrammes de Venn. Dans chacun des quatre cas, la région doublement quadrillée est celle qui représente l'ensemble défini.

[1] Nommées d'après George Boole (1815–1864), auteur de *The Laws of Thought*, ouvrage repère qui développe les principes gouvernant autant la logique propositionnelle que les opérations sur des ensembles tels que discutés ici.



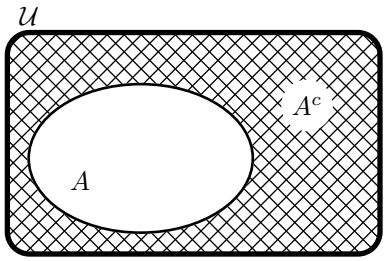
Union

Définition : $A \cup B = \{\, x \mid x \in A \vee x \in B \,\}$
Français : Les éléments qui sont dans A **ou** dans B (ou les deux)
Diagramme : La région recouverte par A et B intégralement



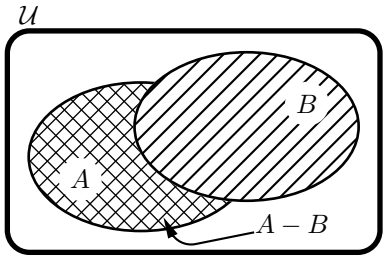
Intersection

Définition : $A \cap B = \{\, x \mid x \in A \wedge x \in B \,\}$
Français : Les éléments qui sont à la fois dans A **et** dans B
Diagramme : La région où A et B se chevauchent



Complément

Définition : $A^c = \{\, x \in \mathcal{U} \mid a \notin A \,\}$
Français : Les éléments qui ne sont **pas** dans A
Diagramme : Tout ce qui est à l'extérieur de A



Différence

Définition : $A - B = \{\, x \mid x \in A \wedge x \notin B \,\}$
Français : Les éléments qui sont dans A **mais pas** dans B
Diagramme : A moins la partie où A et B se chevauchent

FIGURE VIII.1 – Union, intersection, complément et différence.

Comme vous pouvez le constater, ces opérations sont définies en termes de connectifs logiques $\wedge, \vee, \neg$. Conséquemment, si vous voulez prouver quelque chose à propos d'intersections, d'unions, de différences ou de compléments, vous devez employer la logique propositionnelle.

Avant détudier des exemples, nous introduisons une autre définition importante :

Définition VIII.1.1 (Ensembles disjoints)**.** Deux ensembles A et B sont dits *disjoints* si $A \cap B = \emptyset$.

En termes français : A et B sont disjoints précisément lorsqu'ils n'ont pas d'éléments en commun.

VIII.2 Exemples

Nous allons maintenant illustrer les opérations booléennes à travers quelques exemples. La présentation de ces exemples demeure relativement informelle dans la présente section car nous voulons simplement avoir une idée générale du fonctionnement des opérations. Dans la section subséquente, nous étudierons des preuves plus détaillées.

Commençons avec un exemple concret. Supposons que nous avons les ensembles suivants :

$$A = \{a, b, c\}, \qquad B = \{b, c, d, e\}, \qquad C = \{c, e, f, g\}.$$

Nous avons alors :

- $A \cap B = \{b, c\}$
- $A \cap C = \{c\}$
- $B \cap C = \{c, e\}$
- $A \cup B = \{a, b, c, d, e\}$
- $A \cup C = \{a, b, c, e, f, g\}$
- $B \cup C = \{b, c, d, e, f, g\}$
- $A - B = \{a\}$
- $A - C = \{a, b\}$
- $B - C = \{b, d\}$
- $A \cap B \cap C = \{c\}$
- $A \cup B \cup C = \{a, b, c, d, e, f, g\}$.

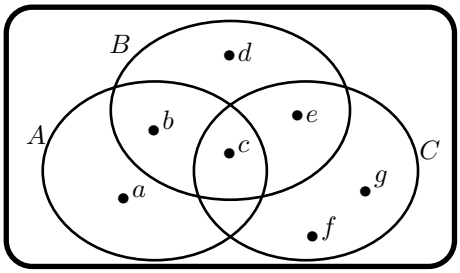


Figure VIII.2 – Trois ensembles

Abordons maintenant un problème un peu plus élaboré, basé sur l'exemple ci-haut : essayons de déterminer l'ensemble $((A \cap B) - C) \cup (C - (A \cup B))$. Nous pouvons accomplir cela en quelques étapes :

1. Premièrement, $A \cap B = \{b, c\}$, donc $(A \cap B) - C = \{b, c\} - \{c, e, f, g\} = \{b\}$.
2. Ensuite, $A \cup B = \{a, b, c, d, e\}$, donc $C - (A \cup B) = \{c, e, f, g\} - \{a, b, c, d, e\} = \{f, g\}$.

3. Finalement, l'ensemble que nous cherchons est

$$((A \cap B) - C) \cup (C - (A \cup B)) = \{b\} \cup \{f, g\} = \{b, f, g\}.$$

Vous pouvez aussi vérifier ce résultat en déterminant la région correspondante dans un diagramme de Venn.

Voici maintenant un exemple différent : supposons que nous travaillons dans l'univers $\mathcal{U} = \mathbb{N}$, l'ensemble des nombres naturels. Définissons

$$X = \{\, x \in \mathbb{N} \mid x \text{ est premier} \,\}, \qquad Y = \{\, x \in \mathbb{N} \mid x < 8 \,\}, \qquad Z = \{\, x \in \mathbb{N} \mid x \text{ est impair} \,\}.$$

Nous avons alors les calculs suivants :

1. $X \cap Y \cap Z = \{\, x \in \mathbb{N} \mid x \text{ est premier et } x \text{ est impair et } x < 8 \,\} = \{3, 5, 7\}$.
2. $(X^c - Z) \cap Y = \{\, x \in \mathbb{N} \mid x \text{ n'est pas premier et } x \text{ n'est pas impair et } x < 8 \,\} = \{0, 4, 6\}$.
3. $$\begin{aligned} ((Y - X^c) \cup (X \cup Z)^c) - Y &= (\{2, 3, 5, 7\} \cup \{1, 2, 3, 5, 7, 9, 11, 13, \ldots\}^c) - Y \\ &= \{0, 4, 6, 8, 10, 12, \ldots\} - Y \\ &= \{8, 10, 12, \ldots\}. \end{aligned}$$

VIII.3 Opérations booléennes et logique propositionnelle

Comme nous l'avons indiqué précédemment, les définitions des opérations booléennes font appel aux connectifs logiques. Supposons que, à partir d'ensembles quelconques $A_1, \ldots, A_n$, nous nous servions des opérations pour former un nouvel ensemble A. (Par exemple, A pourrait être quelque chose comme $A = A_2 \cup (A_5^c - A_3)$.) Nous pourrions ensuite nous demander qu'est-ce que ça veut dire lorsqu'un élément x satisfait $x \in A$. Lorsque nous déballons les définitions, nous obtenons une expression complexe, bâtie à partir d'énoncés de la forme $x \in A_i$, qui emploie les connectifs $\wedge$, $\vee$, $\neg$ (ou leurs correspondances en français). Pour l'exemple donné ci-haut (entre parenthèses), nous aurions

$$x \in A \Leftrightarrow x \in A_2 \vee (\neg x \in A_5 \wedge \neg x \in A_3).$$

Pour rendre ceci un peu plus lisible, nous pouvons introduire des lettres propositionnelles α_i (avec l'interprétation : $x \in A_i$). Ainsi, l'énoncé $x \in A$ prend la forme suivante :

$$\alpha_2 \vee (\neg\alpha_5 \wedge \neg\alpha_3).$$

Ensuite, supposons que nous ayons un autre ensemble, B, également construit à partir des ensembles $A_1, \ldots, A_n$. (Afin de garder l'exemple concret, supposons que $B = (A_3 - A_2)^c \cup (A_5^c \cap A_2)$.) Nous pourrions traduire l'énoncé $x \in B$ comme suit :

$$\neg(\alpha_3 \wedge \neg\alpha_2) \vee (\neg\alpha_5 \wedge \alpha_2).$$

Soient A, B des ensembles construits à partir des ensembles $A_1, \ldots, A_n$ en utilisant les opérations booléennes.
Étape 1. Introduire des lettres propositionnelles $\alpha_1, \ldots, \alpha_n$.
Étape 2. Définir une traduction τ comme suit :

$$\begin{aligned} \tau(A_i) &= \alpha_i \\ \tau(X \cap Y) &= \tau(X) \wedge \tau(Y) \\ \tau(X \cup Y) &= \tau(X) \vee \tau(Y) \\ \tau(X^c) &= \neg\tau(X) \\ \tau(X - Y) &= \tau(X) \wedge \neg\tau(Y) \end{aligned}$$

Étape 3. Pour déterminer si $A \subseteq B$, vérifier si $\tau(A)$ implique logiquement $\tau(B)$; de manière équivalente, vérifier si $\tau(A) \to \tau(B)$ est une tautologie. Pour déterminer si $A = B$, vérifier si $\tau(A)$ et $\tau(B)$ sont logiquement équivalents ; ou bien, vérifier si $\tau(A) \leftrightarrow \tau(B)$ est une tautologie.

FIGURE VIII.3 – Traduction des ensembles aux propositions

Finalement, supposons que nous voulons savoir si $A \subseteq B$. Dit d'une autre façon, nous voulons savoir si $x \in A$ implique $x \in B$. Ce problème se réduit à la vérification que l'implication

$$[\alpha_2 \vee (\neg\alpha_5 \wedge \neg\alpha_3)] \to [\neg(\alpha_3 \wedge \neg\alpha_2) \vee (\neg\alpha_5 \wedge \alpha_2)]$$

est une tautologie ou non ; c'est quelque chose que nous pouvons vérifier avec des manipulations logiques ou des tables de vérité.

La figure VIII.3 donne un résumé de la procédure.

À titre d'exemple, nous prouvons l'énoncé $A-(B\cup C) = (A-B)\cap(A-C)$ de deux manières, l'une informelle, et l'autre employant la notation logique.

Preuve 1. Considérons un élément arbitraire $x \in A - (B \cup C)$ pour commencer. Par définition de la différence, ceci veut dire que $x \in A$ et $x \notin B \cup C$. Si x n'est pas un élément de $B \cup C$, alors nous ne pouvons avoir $x \in B$ et nous ne pouvons avoir $x \in C$. Donc, $x \in A$, $x \notin B$ et $x \notin C$. Mais alors, $x \in A - B$ et $x \in A - C$, et nous obtenons $x \in (A - B) \cap (A - C)$.

Pour l'autre direction, considérons un $x \in (A - B) - (A - C)$. Il s'ensuit que $x \in (A - B)$ et $x \in (A - C)$. Le premier veut dire que $x \in A$ et $x \notin B$. Le second veut dire que $x \in A$ et $x \notin C$. À partir de $x \notin B$ et $x \notin C$, nous pouvons inférer $x \notin B \cup C$ (car si $x \in B \cup C$, nous aurions $x \in B$ ou $x \in C$, aucun desquels n'est possible). Donc, $x \in A$ et $x \notin B \cup C$, c'est-à-dire $x \in A - (B \cup C)$. □.

Preuve 2. En traduisant en logique propositionnelle, nous observons que nous devons prouver l'équivalence logique suivante :

$$\alpha \wedge \neg(\beta \vee \gamma) \equiv (\alpha \wedge \neg\beta) \wedge (\alpha \wedge \neg\gamma).$$

Mais nous avons

$$\begin{aligned} \alpha \wedge \neg(\beta \vee \gamma) &\equiv \alpha \wedge (\neg\beta \wedge \neg\gamma) && \text{par De Morgan} \\ &\equiv (\alpha \wedge \alpha) \wedge (\neg\beta \wedge \neg\gamma) && \text{par l'idempotence de } \wedge \\ &\equiv (\alpha \wedge \neg\beta) \wedge (\alpha \wedge \neg\gamma) && \text{par l'associativité et la commutativité de } \wedge \end{aligned}$$

□

Notez que dans la première preuve, nous ne faisons que déballer systématiquement les définitions de $\cap$, $\cup$ et $-$, afin d'obtenir des énoncés en français qui emploient les connectifs « et », « ou » et « non », respectivement. Par la suite, nous utilisons informellement la logique propositionnelle pour manipuler ces énoncés, puis nous les remballons pour obtenir à nouveau des opérations booléennes sur des ensembles. La deuxième preuve contourne toutes ces traductions et, ainsi, elle est beaucoup plus efficace. Tout de même, il importe de comprendre ces deux types de preuves !

VIII.4 Sommaire

Les *opérations booléennes* d'*intersection*, d'*union*, de *complément* et de *différence* nous permettent de former de nouvelles combinaisons d'ensembles.

Lorsque nous raisonnons avec de telles combinaisons, nous pouvons

- traduire les énoncés en français et employer la logique informellement, ou
- traduire formellement les énoncés en logique propositionnelle et employer des méthodes logiques formelles comme les tables de vérité pour établir des résultats.

VIII.5 Exercices

Exercice 81. Soient $A = \{0, 1, 2\}$, $B = \{2, 3, 4, 5\}$, $C = \{1, 3, 5\}$, et supposons que $\mathcal{U} = \mathbb{N}$. Déterminez les ensembles suivants :

(a) $A \cap B$

(b) $A \cup B$

(c) $A \cap B \cap C$

(d) $A - B$

(e) $A^c - B^c$

(f) $(A - B)^c$

(g) $(A^c \cap C^c)^c$

Exercice 82. Donnez une description simple de chacun des ensembles suivants (en employant l'ensemble universel $\mathbb{R}$) :

(a) $\mathbb{Q}^c - \{\, x \in \mathbb{R} \mid x > 0 \,\}$

(b) $(\mathbb{Q} \cap \{\, x \in \mathbb{R} \mid 0 < x < 1 \,\})^c - \{\, x \in \mathbb{R} \mid e^x \leq 1 \,\}$

(c) $[0,1] - \{\, x \in \mathbb{R} \mid x^3 < 1 \,\}$ (ici, $[0,1]$ dénote l'intervalle unité fermé)

Exercice 83. Démontrez que pour n'importe quel ensemble A, nous avons

(a) $A \cap \emptyset = \emptyset$

(b) $A \cup \emptyset = A$

(c) $A \cup A = A$

(d) $A \cap A = A$

(e) $A - A = \emptyset$

Exercice 84. Démontrez que $A \subseteq B$ si et seulement si $A \cap B = A$.

Exercice 85. Démontrez que $A \subseteq B$ si et seulement si $A \cup B = B$.

Exercice 86. Prouvez les identités suivantes pour n'importe quels ensembles A, B, C.

(a) $(A \cap B) \cap C = A \cap (B \cap C)$

(b) $A \cap B = B \cap A$

(c) $(A \cup B) \cup C = A \cup (B \cup C)$

(d) $A \cup B = B \cup A$

Exercice 87. Vrai ou faux ? $A - B = B - A$. Si c'est vrai, donnez une preuve. Sinon, donnez un contre-exemple.

Exercice 88. Vrai ou faux ? $A - (B - C) = (A - B) - C$. Si c'est vrai, donnez une preuve. Sinon, donnez un contre-exemple.

Exercice 89. Prouvez $(A - B) \cap (B - A) = \emptyset$.

Exercice 90. On définit la *différence symétrique* de A et B comme étant

$$A \Delta B =_{\text{déf}} (A - B) \cup (B - A).$$

(a) Démontrez que $x \in A \Delta B$ si et seulement si $x \in A \leftrightarrow x \notin B$ est vrai.

(b) Démontrez que $A \Delta A = \emptyset$.

(c) Démontrez que $(A \Delta B) = (A \cup B) - (A \cap B)$.

(d) Démontrez que $A \Delta B = B \Delta A$.

(e) Prouvez ou réfutez $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

Exercice 91. Prouvez ou réfutez $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Exercice 92. Prouvez ou réfutez $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

Exercice 93. Prouvez ou réfutez $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$.

LEÇON IX

PRODUITS ET SOMMES

Les opérations booléennes que nous avons introduites dans la dernière leçon ont aidé à construire une variété de nouveaux ensembles. Cette leçon introduit deux autres opérations pour construire de nouveaux ensembles. Ces opérations sont appelées *produit cartésien* et *somme disjointe* (ou *coproduit*).

IX.1 PRODUITS ET PAIRES

Soient A, B des ensembles. Informellement parlant, nous voulons définir un nouvel ensemble $A \times B$ dont les éléments sont des paires (a, b), telles que $a \in A$ et $b \in B$. Deux questions nous interpellent : Primo, qu'est ce qu'une paire (a, b) ? (C'est une question authentique car nous voulons tout construire en termes de ce que nous avons déjà établi.) Secundo, comment savons-nous que la collection de toutes ces paires forme un ensemble ?

Afin de répondre à la première question, prenons le temps de considérer les attentes que nous avons vis-à-vis des paires. Premièrement, nous nous attendons à ce que, pour tout choix d'éléments $a \in A$ et $b \in B$, nous pouvons combiner ces derniers pour former une paire (a, b). Deuxièmement, étant donné une paire (a, b), nous voulons être en mesure d'extraire les composantes a et b. Aussi, étant donné deux paires (a, b) et (a', b'), nous voulons que ces paires soient égales précisément lorsque $a = a'$ et $b = b'$. Ainsi, une paire devrait être complètement déterminée par ses deux coordonnées.

Pouvons-nous, étant donné a, b tels que ci-haut, créer un ensemble (a, b) avec les conditions désirées ? Notre premier essai pourrait être d'utiliser l'ensemble $\{a, b\}$. Mais il y a un problème : supposons que A et B sont en fait le même ensemble. Puisque $\{a, b\} = \{b, a\}$, nous ne serions pas en mesure de différencier les paires (a, b) et (b, a). Puisque ces paires doivent être distinctes, nous devons choisir des ensembles différents pour les représenter.

Pour ce faire, nous pouvons employer un truc, attribué à Kuratowski, où l'on utilise l'ensemble $\{a, \{a, b\}\}$ pour désigner (a, b). Notez que nous ne pouvons jamais avoir $a = \{a, b\}$, car ceci nous donnerait $a \in a$. Ainsi, l'ensemble $\{a, \{a, b\}\}$ a deux éléments distincts. De plus, les ensembles $\{a, \{a, b\}\}$

et $\{b, \{a, b\}\}$ sont distincts lorsque a et b le sont. De cette manière, les critères correspondant à nos attentes sont satisfaits, et nous pouvons définir $(a, b) = \{a, \{a, b\}\}$.

Maintenant, nous pouvons regrouper les paires en un ensemble comme suit :

Définition IX.1.1 (Produit cartésien)**.** Soient A, B des ensembles. Alors, le *produit cartésien* de A et B est l'ensemble

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

Quelques remarques : premièrement, le truc employé ci-haut n'est pas la seule possibilité pour définir une paire. Ce qui importe réellement est que les paires se comportent de la façon attendue, peu importe comment elles sont définies. Deuxièmement, nous devrions nous demander si $A \times B$, tel que défini ci-haut, existe ! Et bien, notez à priori que $\{a, \{a, b\}\}$ est un sous-ensemble de $A \cup \mathcal{P}(A \cup B)$. Donc, l'ensemble $A \times B$ de toutes ces paires est un sous-ensemble de $\mathcal{P}(A \cup \mathcal{P}(A \cup B))$. Ce dernier existe, donc nous pouvons obtenir $A \times B$ via la compréhension.[1]

Exemple IX.1.2. Supposons que $A = \{a, b\}$ et $B = \{b, c, d\}$. Alors,

$$A \times B = \{(a, b), (a, c), (a, d), (b, b), (b, c), (b, d)\}.$$

Lorsque nous voulons établir ce que ceci veut dire en termes de la définition de Kuratowski pour une paire (en principe, nous ne portons pas d'intérêt à cela, mais supposons que nous sommes intéressés à le faire), nous obtenons

$$A \times B = \{\{a, \{a, b\}\}, \{a, \{a, c\}\}, \{a, \{a, d\}\}, \{b, \{b\}\}, \{b, \{b, c\}\}, \{b, \{b, d\}\}\}.$$

L'opération de produit $\times$ se comporte un peu comme la multiplication de nombres ; par contre, pas tout à fait de la sorte : nous n'avons pas $A \times (B \times C) = (A \times B) \times C$ en général, ni même $A \times B = B \times A$. (Essayez de trouver les plus petits contre-exemples possibles !) Toutefois, nous pouvons obtenir une forme légèrement modifiée de l'associativité et de la commutativité — nous reviendrons à cette idée au cours de la leçon XII.

IX.2 Coproduits

Nous nous tournons maintenant vers l'opération « duale » au produit, à savoir, les sommes (aussi appelées coproduits). Étant donné deux ensembles A et B, nous voulons les combiner de telle manière que l'ensemble résultant satisfassent deux critères : (1) il possède à la fois les éléments de A et les éléments de B, et (2) il a la propriété que nous pouvons toujours distinguer entre les éléments de A et les éléments de B. Prendre l'union $A \cup B$ n'est pas tout à fait adéquat : lorsque A et B ne sont pas disjoints (i.e. $A \cap B \neq \emptyset$), nous perdons le sens de la provenance des éléments (de A ou de B) à l'endroit où A et B se chevauchent.

La solution est de s'arranger pour que A et B soient disjoints en marquant les éléments avec des étiquettes uniques pour identifier leurs provenances. Par exemple, nous pouvons donner une étiquette de 0 aux éléments de A et nous pouvons donner une étiquette de 1 aux éléments de B. (Les noms des étiquettes sont sans importance, tant qu'ils sont distincts.) Nous pouvons utiliser $0 = \emptyset$ et $1 = \{\emptyset\}$, par exemple.

[1] Tout de même, il y a des mathématiciens (particulièrement ceux qui doutent de l'existence des ensembles de parties) qui ne font qu'introduire un axiome de plus pour énoncé que les produits d'ensembles existent toujours.

Définition IX.2.1. Étant donné des ensembles A et B, on définit l'ensemble

$$A + B = A \times \{0\} \cup B \times \{1\}.$$

Voici des exemples concrets :

Exemples IX.2.2.

1. Soient $A = \{a, b\}$ et $B = \{b, c, d\}$. Alors,

   $$A + B = \{(a, 0), (b, 0), (b, 1), (c, 1), (d, 1)\}.$$

   Observez que l'élément b est représenté deux fois dans la somme : une fois avec l'étiquette 0, et une fois avec l'étiquette 1.

2. Même lorsque A et B sont disjoints, le coproduit diffère de l'union. Par exemple, lorsque $A = \{a, b\}$ et $B = \{c, d\}$, nous avons $A+B = \{(a, 0), (b, 0), (c, 1), (d, 1)\}$. Donc, nous nous arrangeons toujours pour étiqueter tous les éléments, même lorsque cela n'est pas nécessaire.

3. $\mathbb{N} + \emptyset = \{(x, 0)|x \in \mathbb{N}\}$.

4. $\{\emptyset\} + \{\emptyset\} = \{(\emptyset, 0), (\emptyset, 1)\}$.

Encore une fois, il y a un sens par lequel l'opération + se comporte comme l'addition de nombres, mais nous donnerons un sens précis à cela au cours de la leçon XII.

IX.3 Sommaire

Deux nouvelles constructions ont été définies :

- *Produit cartésien* d'ensembles $A \times B = \{(a, b)|a \in A, b \in B\}$.
- *Somme* d'ensembles $A + B = A \times \{0\} \cup B \times \{1\}$.

La première est définie en termes de la *définition de paire de Kuratowski* : $(a, b) = \{a, \{a, b\}\}$. La seconde est définie en rendant les ensembles disjoints à priori, puis en prenant leur union.

IX.4 Exercices

Exercice 94. Calculez $\{\emptyset\} \times \{\emptyset\}$.

Exercice 95. L'ensemble $\{\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$ est-il un produit de deux autres ensembles ?

Exercice 96. Pour $A = \{a, b, \{a\}\}, B = \{\{a, b\}, b\}$, donnez $A \times B$.

Exercice 97. Donnez des exemples (aussi simples que possible) pour démontrer, en général, que $A \neq A \times A$, que $A \times B \neq B \times A$ et que $A \times (B \times C) \neq (A \times B) \times C$. Aussi, trouvez des exceptions à ces énoncés.

Exercice 98. Calculez $\{\emptyset, \{\emptyset\}\} + \{\emptyset\}$.

Exercice 99. Est-il vrai que $A + B = B + A$? $A + (B + C) = (A + B) + C$? $A + \emptyset = A$?

Exercice 100. Calculez $A \times (B + C)$, où $A = \{a, b\}$, $B = \{a, c\}$, $C = \{b, c\}$.

Exercice 101. Prouvez que si $A \subseteq A'$ et $B \subseteq B'$, alors $A \times B \subseteq A' \times B'$.

Exercice 102. Prouvez que si $A \subseteq A'$ et $B \subseteq B'$, alors $A + B \subseteq A' + B'$.

Exercice 103. Enquêtez sur la validité des énoncés suivants :

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

(c) $A + (B \cup C) = (A + B) \cup (A + C)$

(d) $A + (B \cap C) = (A + B) \cap (A + C)$

(e) $(A + B) \cup C = (A \cup C) + (B \cup C)$

(f) $(A \times B) \cap C = (A \cap C) \times (B \cap C)$.

Exercice 104. Est-il possible que $A + B = A \times B$? Trouvez tous les exemples possibles, et démontrez que votre liste est exhaustive.

LEÇON X

RELATIONS

Dans cette leçon, nous entreprenons l'étude des *relations* entre des ensembles. La première étape est de définir ce qu'est une relation, de comprendre quels types de relations existent et de concevoir comment celles-ci peuvent être combinées.

X.1 DÉFINITION DE BASE

Supposons que nous avons deux ensembles A et B.

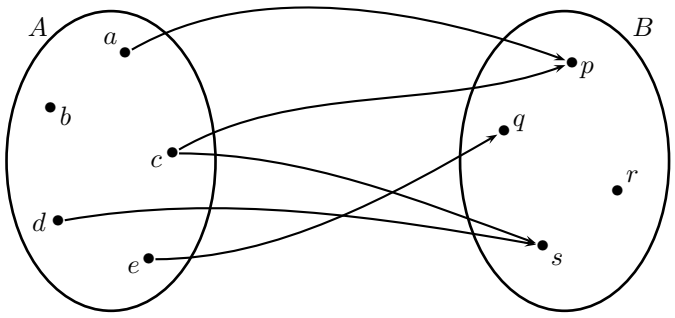
Définition X.1.1. Une *relation (binaire*[1]*)* d'un ensemble A vers un ensemble B est un sous-ensemble R de $A \times B$.

Il y a une multitude de notations utilisées en rapport avec les relations ; lorsque $(a, b) \in R$, on écrit souvent $R(a, b)$ ou $a\,R\,b$ à la place. Dans ce cas, on dit que « a est en relation avec b par R » (ou simplement, que « a est en relation avec b » lorsque la relation R est sous-entendue). Pour indiquer que $(a, b) \notin R$, on écrit aussi $\neg R(a, b)$ ou $\neg aRb$. De plus, certains textes emploient une flèche spéciale comme $\nrightarrow$ pour indiquer une relation ; plus précisément, la notation $R : A \nrightarrow B$ est utilisé pour dire que R est une relation de A vers B. Dans ce cas, on dit que A est le *domaine* de R, et que B est le *codomaine* de R.

Remarquez deux choses :

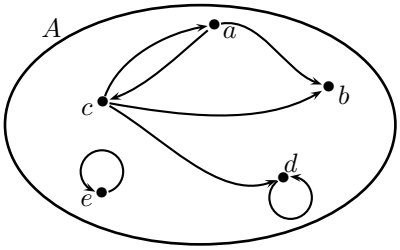
1. Une relation est un objet mathématique d'ordre très général : *tout* sous-ensemble de $A \times B$ est une relation de A vers B, peu importe comment étrange cela peut sembler. Ainsi, il y a généralement beaucoup de différentes relations d'un ensemble à un autre.

[1] Plus généralement, on peut définir des relations n-aire pour n'importe quel $n \in \mathbb{N}$; une relation ternaire est un sous-ensemble de $A_1 \times A_2 \times A_3$, et ainsi de suite. Un cas particulier survient pour $n = 1$: une relation unaire est simplement un sous-ensemble de A_1 dans ce cas. Vous voudriez peut-être réfléchir à ce que pourrait être une relation nullaire !



Une relation
$R \subseteq A \times B$ avec
$R = \{(a,p),(c,p),$
$(c,s),(d,s),(e,q)\}$

FIGURE X.1 – Exemple de relation R, de A vers B



Une relation $R \subseteq A \times A$ avec
$R = \{(a,b),(a,c),(c,a),(c,b),$
$(c,d),(d,d),(e,e)\}$

FIGURE X.2 – Exemple de relation R, de A vers A

2. Une relation de A vers B n'est pas la même chose qu'une relation de B vers A. Les relations de A vers B et celles de B vers A sont reliées (dans un sens que nous explorerons plus en détails plus tard), mais elles sont manifestement différentes et nous devons faire la distinction. Bien entendu, rien ne nous empêche de considérer le cas spécial où $A = B$; dans ce cas, une relation $R \subseteq A \times A$ est appelée une relation (binaire) sur A, ou une relation de A vers lui-même.

Les relations peuvent également avoir une représentation schématique : la figure X.1 donne un exemple, et la figure X.2 aussi, mais avec une relation d'un ensemble vers lui-même. Notez la directionalité des connexions, laquelle est nécessaire pour éliminer toute ambiguïté.

Notez qu'il n'y a rien qui empêche un élément quelconque d'être relié à plusieurs autres éléments, incluant lui-même. Notez également que certains éléments pourraient n'être reliés à aucun élément. En effet, nous avons les exemples extrêmes suivants :

Exemple X.1.2. Étant donné des ensembles A, B, l'ensemble vide (lequel est un sous-ensemble de $A \times B$) est une relation de A vers B. On l'appelle la *relation vide*. À l'autre extrême, $A \times B$ est lui-même un sous-ensemble de $A \times B$, et ainsi, c'est une relation de A vers B. On l'appelle la *relation maximale*.

Dans la relation vide, il n'y a aucun élément de A qui est relié à quelque élément de B que ce soit, tandis que dans la relation maximale, tous les éléments de A sont reliés à *tous* les éléments de B.

Dans les circonstances particulières où $A = B = \emptyset$, les deux extrêmes se rejoignent : nous obtenons $A \times B = \emptyset$, et l'ensemble vide a exatement un sous-ensemble, qui est lui-même.

Exemple X.1.3. Pour n'importe quel ensemble A, considérez la relation

$$\Delta_A \subseteq A \times A; \qquad \Delta_A = \{\, (x,x) \,|\, x \in A \,\}.$$

La relation Δ_A porte plusieurs noms : elle est souvent appelée *relation identité* sur A ; elle est aussi appelée *relation diagonale* sur A.

L'exemple suivant est un cas particulier d'*ordre* sur un ensemble ; nous explorerons ces derniers plus en détails lors d'une leçon subséquente. Pour l'instant, il est important de reconnaître que les relations d'ordre standards (avec lesquelles vous êtes familiers) sont effectivement des exemples de relations.

Exemple X.1.4. Employons $\leq$ pour dénoter l'ordre usuel sur $\mathbb{N}$. Puis, considérons le sous-ensemble

$$\{\,(n,m) \in \mathbb{N} \times \mathbb{N} \,|\, n \leq m\,\} \subseteq \mathbb{N} \times \mathbb{N}.$$

Ceci est une relation de $\mathbb{N}$ vers lui-même.

Pour une variante, nous pouvons considérer le sous-ensemble

$$\{\,(n,m) \in \mathbb{N} \times \mathbb{N} \,|\, n < m\,\} \subseteq \mathbb{N} \times \mathbb{N}.$$

Ceci est également une relation de $\mathbb{N}$ vers lui-même.

De manière similaire, l'ordre standard sur les entiers, les rationnels ou les réels peut être considéré comme une relation.

L'exemple suivant est de nature un peu différente :

Exemple X.1.5. Définissons

$$R \subseteq \mathbb{Z} \times \mathbb{Z}; \qquad n\,R\,m \Leftrightarrow_{\text{déf}} n \text{ divise } m.$$

Ceci est une relation sur $\mathbb{Z}$, appelée *relation de divisibilité*.

Et une de plus :

Exemple X.1.6. Soit X un ensemble, et considérons $A = \mathcal{P}(X)$. Alors,

$$\{\,(U,V) \in \mathcal{P}(X) \times \mathcal{P}(X) \,|\, U \subseteq V\,\}$$

est la *relation de sous-ensemble* sur l'ensemble des parties de X.

Procédure de preuve

Pour prouver que deux relations R et S sont égales, vous devez :

- prendre des éléments arbitraires x, y avec xRy, puis démontrer que xSy, **ET**
- prendre des éléments arbitraires x, y avec xSy, puis démontrer que xRy.

X.2 Le calcul des relations

Puisque les relations sont définies comme des sous-ensembles, alors tout ce que nous pouvons faire avec des sous-ensembles, nous pouvons également le faire avec des relations. En particulier, nous pouvons comparer des relations :

Définition X.2.1. Soient A, B des ensembles, et soient R, S deux relations de A vers B. On dit alors que R est une relation *plus petite* que S (ou que S est une relation *plus grande* que R) si $R \subseteq S$.

Une autre façon d'exprimer ceci : R est plus petit que S lorsque $a\,R\,b$ implique $a\,S\,b$ pour tout a, b. Par exemple, pour les relations $\leq$ et $<$ sur $\mathbb{N}$, nous avons que $<$ est plus petit que $\leq$, car $a < b$ implique $a \leq b$ pour tout a, b.

Exercice 105. Vérifiez que la relation vide de A vers B est plus petite que toute autre relation de A vers B, et que la relation maximale est plus grande que n'importe quelle autre relation de A vers B.

Nous pouvons aussi former l'intersection, l'union, le complément et la différence de relations (consultez les exercices pour des exemples et des applications).

> Procédure de preuve
>
> Pour prouver qu'une relation R est plus petite qu'une autre S (i.e. que $R \subseteq S$), vous devez :
>
> - Prendre des éléments arbitraires x, y avec xRy, puis démontrer que xSy.

Plus tôt, nous avons insisté sur le fait qu'une relation de A vers B n'est pas la même chose qu'une relation de B vers A. Tout de même, il y a une construction qui nous permet de faire une conversion d'un type de relation à l'autre :

Définition X.2.2 (Relation inverse)**.** Soit R une relation de A vers B, i.e. $R \subseteq A \times B$. On définit une relation R° de B vers A par

$$b\,R^\circ\,a \Leftrightarrow_{\text{déf}} a\,R\,b.$$

De manière équivalente, $R^\circ = \{\,(b,a) \in B \times A \mid (a,b) \in R\,\}$. La relation R° est appelée la *relation inverse* de R (aussi : la *réciproque* de R, ou l'*opposée* de R).

Au niveau de la repésentation schématique d'une relation, tout ce que nous devons faire pour obtenir R° à partir de R, c'est inverser l'orientation des flèches.

Par exemple, considérons l'ordre $\leq$ sur $\mathbb{N}$. La réciproque de cette relation, dénotée $\leq^\circ$, est simplement la relation $\geq$. Ainsi, nous pourrions écrire $\leq^\circ = \geq$, mais on évite de le faire la plupart du temps car on ne ferait qu'affecter la lisibilité. (Tout de même, ceci est techniquement correct car les deux côtés de l'équation sont des sous-ensembles de $\mathbb{N} \times \mathbb{N}$ et, ainsi, l'équation ne fait qu'exprimer que deux relations sur $\mathbb{N}$ sont égales.) Similairement, la réciproque de $<$ est $>$.

L'énoncé suivant est une conséquence directe de la définition de réciproque.

Lemme X.2.3. *Étant donné une relation $R \subseteq A \times B$, nous avons $(R^\circ)^\circ = R$.*

Exercice 106. Vérifiez cet énoncé.

Ensuite, considérons une façon de combiner deux relations en une nouvelle : la *composition*.

Définition X.2.4 (Composition de relations)**.** Soient $R \subseteq A \times B$ et $S \subseteq B \times C$ des relations. On définit la *composée* de R et S, $S \circ R \subseteq A \times C$, comme étant la relation

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

En d'autres mots : dans la relation composée $S \circ R$, un élément $a \in A$ est relié à un élément $c \in C$ lorsqu'il existe un élément $b \in B$ tel que $a\,R\,b$ et $b\,S\,c$. Dans la figure X.3, nous avons une représentation schématique de ceci ; notez que vous pouvez simplement suivre le tracé des flèches pour savoir quels éléments de A sont reliés à quels éléments de C.

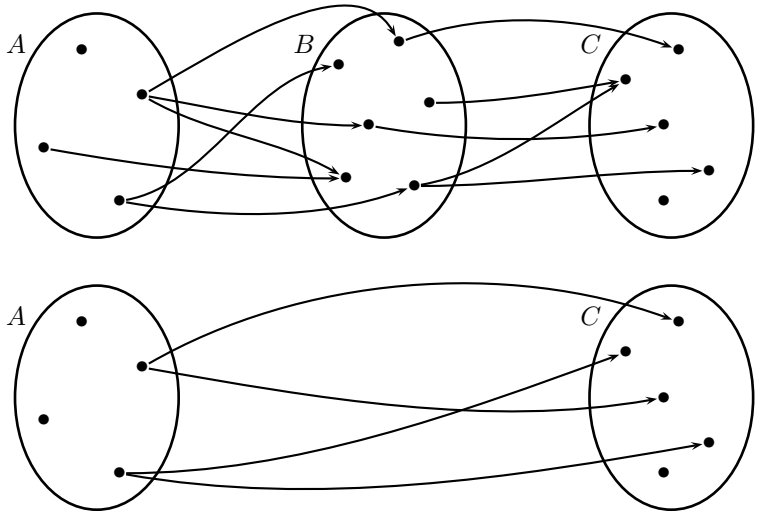


FIGURE X.3 – Deux relations et leur composée

Voici quelques exemples concrets où nous calculons une composée de relations :

Exemples X.2.5.

1. Soient $A = \{a, b\}$, $B = \{c, d, e\}$, $C = \{f, g, h\}$, et considérons les relations $R = \{(a, c), (a, d), (b, d), (b, e)\}$ et $S = \{(c, f), (d, f)\}$. Alors $S \circ R$ est la relation $S \circ R = \{(a, f), (b, f)\}$.
2. Soit $X = \{x, y, z\}$, et soit $R = \{(x, y), (y, x), (x, z)\}$. Nous obtenons $R \circ R = \{(x, x), (y, y), (y, z)\}$.
3. Considérez la relation d'ordre standard $\leq$ sur $\mathbb{N}$. Nous avons que $\leq \circ \leq$ est la même relation que $\leq$: D'une part, supposons que $a \,(\leq \circ \leq)\, c$. Par définition de la composée, il y a un $b \in \mathbb{N}$ tel que $a \leq b$ et $b \leq c$. Il s'ensuit que $a \leq c$ (c'est une conséquence de la *transitivité de la relation d'ordre*). D'autre part, si $a \leq c$, alors il existe $b \in \mathbb{N}$ tel que $a \leq b$ et $b \leq c$ (nous pouvons prendre $b = a$, par exemple), et donc $a \,(\leq \circ \leq)\, c$.
4. Avec la même notation que dans l'exemple précédent, nous avons que $\leq \circ \leq^{\circ}$ est la relation maximale sur $\mathbb{N}$. (Vérifiez ceci par vous-même !)

D'autres exemples de ce genre sont donnés à travers les exercices à la fin de cette leçon.

X.3 Propriétés

Dans cette section, nous établissons quelques résultats à propos de la réciproque et de la composée de relations. Nous faisons quelques preuves en détails ici, mais nous allons laisser la majorité en exercices.

Proposition X.3.1. *Les opérations* $(-)^{\circ}$ *et* $- \circ -$ *sur les relations satisfont les propriétés suivantes :*

1. $R \subseteq R'$ *implique* $R^{\circ} \subseteq (R')^{\circ}$
2. $T \circ (S \circ R) = (T \circ S) \circ R$

3. $\Delta_B \circ R = R = R \circ \Delta_A$ *(où* $R \subseteq A \times B$*)*
4. $(S \circ R)^\circ = R^\circ \circ S^\circ$
5. $R \subseteq R'$ *et* $S \subseteq S'$ *implique* $S \circ R \subseteq S' \circ R'$.

Démonstration. Pour la 1^{re} partie, supposons que $R \subseteq R'$. Nous devons montrer que $R^\circ \subseteq (R')^\circ$. Ainsi, prenons x, y avec $x\, R^\circ\, y$; ceci veut dire (par définition de la relation réciproque) que $y\, R\, x$. Puisque $R \subseteq R'$, il s'ensuit que $y\, R'\, x$ également. Finalement, en appliquant la définition de la réciproque à nouveau, nous obtenons $x\, (R')^\circ\, y$, tel que voulu.

Pour la 3^e partie, nous démontrons que $\Delta_B \circ R = R$. Premièrement, considérons x, y arbitraires tels que $x\, R\, y$. Puis, par la définition de Δ_B, nous avons $y \Delta_B y$. Ainsi, $x\, (\Delta_B \circ R)\, y$ est vrai également. Inversement, si $x\, (\Delta_B \circ R)\, y$, alors par la définition de la composée, il y a un élément z avec $x\, R\, z$ et $z\, \Delta_B\, y$. Mais, par la définition de Δ_B, nous obtenons $z = y$, et donc $x\, R\, y$.

Finalement, nous prouvons la moitié de la 4^e partie. Premièrement, considérons x, z tels que $z\, (S \circ R)^\circ\, x$. Par définition de la réciproque, ceci veut dire que $x\, (S \circ R)\, z$; par définition de la composée, il existe un élément y tel que $x\, R\, y$ et $y\, S\, z$. En employant la définition de la réciproque à deux reprises, nous obtenons $y\, R^\circ\, x$ et $z\, S^\circ\, y$. Ceci démontre que $z\, (R^\circ \circ S^\circ)\, x$. □

La première partie de la proposition énonce que l'opération $(-)^\circ$ est monotone. La deuxième partie énonce que la composition est associative, et la troisième, que la relation identité est un élément neutre de la composition (i.e. composer avec la relation identité ne change rien). La quatrième partie décrit comment les opérations de composition et de réciproque interagissent : la réciproque de la composée est la composée des réciproques (vous voudriez peut-être faire un dessin ici). Finalement, la cinquième partie énonce que la composition est monotone.

Exercice 107. Complétez les preuves de la proposition X.3.1 ci-haut.

X.4 Sommaire

Cette leçon introduit la notion de *relation* R de A vers B comme étant un sous-ensemble du produit cartésien $A \times B$. Trois relations spéciales sont souvent considérées :

- La relation vide $R = \emptyset$
- La relation maximale $R = A \times B$
- La relation diagonale (ou relation identité) $\Delta_A = \{\, (a, a) \mid a \in A \,\} \subseteq A \times A$

Deux opérations fondamentales sur les relations sont possibles :

- Composition
- Réciproque

Le *calcul des relations* (dont les propriétés les plus importantes sont listées dans la proposition X.3.1) décrit comment ces opérations se comportent.

X.5 Exercices

Exercice 108. Soient $A = \{a, b, c, d\}$ et $B = \{p, q, r\}$. Soit $R \subseteq A \times A$, la relation définie par $R = \{(a, b), (c, d), (a, d)\}$, et soit $S \subseteq A \times B$, la relation définie par $S = \{(a, p), (b, p), (c, p), (d, p), (d, r), (a, q)\}$. Déterminez les relations suivantes :

(a) R°

(b) $R \circ R$

(c) $R \circ R^\circ$

(d) $R^\circ \circ R$

(e) $S \circ R$

(f) $S \circ R^\circ$

(g) $S \circ S^\circ$

(h) $S^\circ \circ S$

(i) $S \circ R \circ S^\circ$

Exercice 109. Soit $C = \{0, 1\}$. Déterminez toutes les relations R sur C pour lesquelles $R = R^\circ$. Aussi, déterminez celles pour lesquelles $R = R \circ R$.

Exercice 110. Prouvez que si R ou S est une relation vide, alors $S \circ R$ est également vide. Aussi, démontrez que si R est vide, alors R° également.

Exercice 111. Démontrez que lorsque R et S sont toutes les deux maximales, alors $S \circ R$ l'est également. Aussi, démontrez que si R est maximale, alors R° également.

Exercice 112. Peut-il y avoir des relations R, S telles que ni R, ni S sont vides, mais avec $S \circ R$ vide ? Donnez un exemple, ou bien donnez une preuve si cela ne peut se produire.

Exercice 113. Peut-il y avoir des relations R, S telles que ni R, ni S sont maximales, mais avec $S \circ R$ maximale ? Donnez un exemple, ou bien donnez une preuve si cela ne peut se produire.

Exercice 114. Étant donné une relation $R \subseteq A \times B$, nous pouvons considérer son complément

$$R^c = \{\, (a, b) \mid (a, b) \notin R \,\}.$$

Menez une investigation sur le comportement du complément vis-à-vis des autres opérations. Par exemple, déterminez si $(S \circ R)^c = (S^c \circ R^c)$, et si $(R^\circ)^c = (R^c)^\circ$.

Exercice 115. Considérez la relation d'ordre $<$ sur $\mathbb{N}$. Qu'est-ce que $< \circ <$? Qu'est-ce que $< \circ <^\circ$? Et $<^\circ \circ <$?

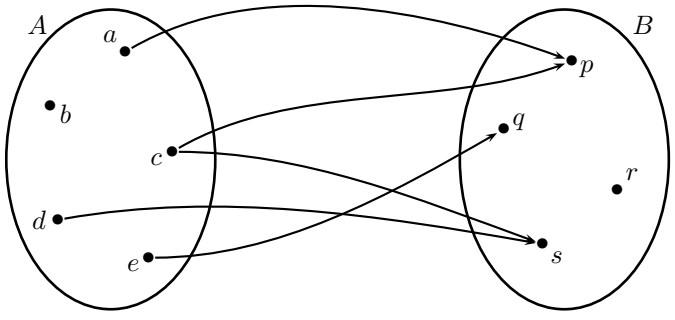
LEÇON XI

FONCTIONS

Comme nous l'avons vu, les relations sont d'une nature particulièrement générale dans l'univers des mathématiques. Il y a certaines classes singulières de relations que nous allons étudier plus en profondeur : les fonctions, les relations d'équivalence, les relations d'ordre. Cette leçon introduit les fonctions entre des ensembles.

XI.1 DÉFINITION

L'objet de cette section est de définir les fonctions en termes de relations. Ceci est peut-être inhabituel étant donné que la plupart d'entre nous ont appris ce qu'était une fonction avant même d'avoir entendu parler de relations. Néanmoins, pour rester en ligne avec notre objectif de concevoir comment les mathématiques se réduisent ultimement à la théorie des ensembles, nous ne voulons pas présenter le concept de fonction comme notion primitive ; nous voulons définir celle-ci à partir d'ensembles.



Une relation
$R \subseteq A \times B$ avec
$R = \{(a,p),(c,p),$
$(c,s),(d,s),(e,q)\}$

FIGURE XI.1 – Exemple de relation R de A vers B

Considérons à nouveau un exemple typique de relation comme celle donnée dans la figure XI.1. Cette relation pourrait nous rappeler quelque chose ayant des ressemblance avec une fonction : elle associe à des éléments de l'ensemble A (sur la gauche), des éléments de l'ensemble B (sur la droite).[1] Mais il y a deux raisons pour lesquelles elle ne l'est pas : premièrement, ce ne sont pas tous les éléments de A qui sont reliés à un élément de B (les fonctions doivent associer quelque chose à chaque élément de l'ensemble de départ, et R n'assigne rien à b) ; deuxièmement, certains éléments sont associés à plus d'un élément (les fonctions doivent être non ambiguës, et associer exactement une valeur de l'ensemble d'arrivée à chaque élément de l'ensemble de départ, mais R associe deux valeurs à c).

Ceci nous mène à la définition suivante :

Définition XI.1.1 (Fonction)**.** Soient A, B des ensembles et $R \subseteq A \times B$ une relation.

1. R est dite *totale* si pour chaque $x \in A$, il existe au moins un $y \in B$ tel que $x\,R\,y$.
2. R est dite *univaluée* si pour chaque $x \in A$, il y a au plus un $y \in B$ tel que $x\,R\,y$.
3. Lorsque R est à la fois totale et univaluée, R est appelée une *fonction* (ou *relation fonctionnelle*).

On désigne couramment des relations fonctionnelles par les symboles f, g, h, et ainsi de suite. Aussi, pour indiquer que f est une fonction de A vers B, on utilise la notation standard $f : A \to B$. Finalement, étant donné une fonction $f : A \to B$ et un élément $x \in A$, nous écrivons $f(x) = y$ pour désigner que y est l'élément (nécessairement unique !) de B pour lequel $(x, y) \in f$.

Pour saisir en quoi consiste ces définitions : prenons $A = \{a, b, c, d\}$ et $B = \{p, q, r, s\}$, et considérons les relations

$$\begin{aligned} R &= \{(a,q),(b,q),(b,s),(c,p),(d,p)\} \\ S &= \{(a,q),(c,r),(d,p)\} \\ T &= \{(a,q),(b,q),(c,r),(d,p)\} \end{aligned}$$

La relation R est totale, mais elle n'est pas univaluée (car l'élément b est relié à deux éléments distincts) ; la relation S est univaluée, mais elle n'est pas totale (car l'élément b n'est relié à aucun élément) ; la relation T est une fonction.

Voici quelques exemples extrêmes :

Exemple XI.1.2. Soient A, B des ensembles. Alors, la relation vide de A vers B est univaluée. Pourquoi ? Ceci est un autre exemple de vérité vide : nous devons vérifier que, si $x\,R\,y$ et $x\,R\,y'$, alors $y = y'$. Mais l'antécédent est toujours faux, donc l'implication est toujours vraie.

Procédure de preuve

Pour prouver que $R \subseteq A \times B$ est totale, vous devez :

- Prendre un élément arbitraire $x \in A$, puis démontrer qu'il existe $y \in B$ tel que xRy.

Pour prouver que $R \subseteq A \times B$ n'est pas totale, vous devez :

- Démontrer l'existence d'un $x \in A$ pour lequel il n'y pas de $y \in B$ tel que xRy.

Procédure de preuve

Pour prouver que $R \subseteq A \times B$ est univaluée, vous devez :

- Démontrer que *si* $x\,R\,y$ et $x\,R\,y'$, *alors* $y = y'$.

Pour prouver que $R \subseteq A \times B$ n'est pas univaluée, vous devez :

- Démontrer qu'il existe $x \in A$ et $y, y' \in B$ tels que $x\,R\,y$, $x\,R\,y'$ et $y \neq y'$.

[1] Vraisemblablement, la « définition » de fonction qu'on vous a enseignée était quelque chose comme : une fonction $f : A \to B$ est une règle qui associe à chaque élément de A, un et un seul élément de B.

Exemple XI.1.3. Soient A, B des ensembles. Alors, la relation vide de A vers B est totale précisément lorsque $A = \emptyset$:

Pour l'une des directions, supposons que $A = \emptyset$. Alors, la relation vide R est totale : nous devons vérifier que si $x \in A$, alors il existe $y \in B$ tel que $x\,R\,y$. Mais $x \in A$ est faux, donc l'implication est vraie.

Réciproquement, supposons que la relation vide R est totale. Alors, nous savons que pour tout $x \in A$, il existe $y \in B$ tel que $x\,R\,y$. Mais si R est vide, alors l'énoncé $x\,R\,y$ est toujours faux. Ainsi, le conséquent de l'implication est faux, et donc l'antécédent est également faux.

Comme exercices, vous voudriez peut-être trouver les plus petits[2] exemples possibles pour les types de relations suivantes :

- une relation qui est totale, mais pas univaluée
- une relation qui est univaluée, mais pas totale
- une relation qui n'est ni univaluée, ni totale.

Finalement, essayons de comprendre comment les fonctions courantes peuvent être représentées comme des relations. Considérons la fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$. Alors, le *graphe* de f est la relation

$$Gr(f) = \{\, (x, x^2) \mid x \in \mathbb{R} \,\}.$$

Ceci est une relation de $\mathbb{R}$ vers lui-même. Généralement, étant donné une fonction $f : A \to B$, on définit le graphe de f comme étant la relation

$$Gr(f) = \{\, (x, f(x)) \mid x \in A \,\} \subseteq A \times B.$$

Ainsi, ce que nous appellons habituellement le graphe d'une fonction (en calcul infinitésimal, disons) est véritablement ce qui constitue la fonction ici.

L'exercice important suivant énonce que les propriétés d'être totale, univaluée et fonctionnelle sont fermées sous la composition.

Exercice 116. Soient $R \subseteq A \times B$ et $S \subseteq B \times C$ des relations.

(1) Prouvez :

(i) Si R et S sont totales, alors $S \circ R$ aussi.

(ii) Si R et S sont univaluées, alors $S \circ R$ aussi.

(iii) Si R et S sont fonctionnelles, alors $S \circ R$ aussi.

(2) Concluez que la composée de relations fonctionnelles donne effectivement la composée habituelle de fonctions $(g \circ f)(x) = g(f(x))$.

[2] Chercher le plus petit (ou plus simple) exemple possible pour quelque chose constitue un excellent exercice pour maîtriser les définitions et établir des connexions entre elles.

XI.2 Fonctions et produits

En calcul infinitésimal, il est courant de considérer non seulement des fonctions $\mathbb{R} \to \mathbb{R}$, mais aussi des fonctions plus générales avec plusieurs variables $\mathbb{R}^n \to \mathbb{R}$, ou même des fonctions à valeurs vectorielles $\mathbb{R}^n \to \mathbb{R}^m$. Dans cette section, nous expliquons brièvement en quoi consistent les fonctions entre des produits cartésiens, et comment travailler avec elles.

Tout d'abord, considérons une fonction $f : A \to B \times C$. Une telle fonction prend comme entrée un élément de A, et donne un élément de $B \times C$ en sortie. Les élément produits en sortie sont des paires ; donc, étant donné $a \in A$, nous obtenons $f(a) \in B \times C$ avec $f(a) = (f_B(a), f_C(a))$. Ainsi, nous pouvons observer que f fait appel à deux fonctions : $f_B : A \to B$ et $f_B : A \to C$, lesquelles sont employées comme une paire. De plus, ces deux fonctions sont complètement déterminées par f.

Ceci prouve :

Lemme XI.2.1. *Étant donné des fonctions $p : A \to B$ et $q : A \to C$, il existe une fonction unique $\langle p, q\rangle : A \to B \times C$ telle que $\langle p, q\rangle(a) = (p(a), q(a))$. Toute fonction $A \to B \times C$ survient uniquement de cette façon.*

En termes plus succincts : une fonction dans un produit est une paire de fonctions. Une formulation un peu plus rigoureuse de cet énoncé est présentée à la leçon XII. Vous pouvez aussi consulter les exercices de la leçon actuelle pour davantage d'exemples.

Le lemme ci-haut explique de quelle manière se présentent les fonctions dont le codomaine est un produit d'ensembles. Qu'en est-il des fonctions dont le domaine est un produit ? Généralement, il y a peu de choses qu'on peut dire à leur sujet. Une fonction $f : A \times B \to C$ ne fait qu'envoyer des paires $(a, b) \in A \times B$ sur des éléments $f(a, b) \in C$. Tout de même, il y a une situation particulière qui revient souvent en pratique : Étant donné des fonctions $p : A \to C$ et $g : B \to D$, nous pouvons combiner ces dernières pour former une nouvelle fonction $f \times g : A \times B \to C \times D$, définie par

$$(f \times g)(a, b) = (f(a), g(b)) \in C \times D.$$

La vérification que cette dernière est effectivement une fonction est laissée comme exercice. Notez que nous abusons légèrement de la notation : $f \times g$ est un nom pour cette nouvelle fonction, mais celle-ci ne représente pas le produit cartésien des relations fonctionnelles f et g (vues comme des ensembles).

XI.3 Trois types de fonctions particuliéres

Cette section introduit trois classes de fonctions prévalentes en mathématiques.

Définition XI.3.1 (Injective, surjective, bijective)**.** Soit $f : A \to B$ une fonction.

1. f est dite *injective* lorsque pour tout $x, x' \in A$, $f(x) = f(x')$ implique $x = x'$. Notation logique : $\forall x, x' \in A.(f(x) = f(x') \to x = x')$.
2. f est dite *surjective* lorsque pour tout $y \in B$, il existe au moins un $x \in A$ tel que $f(x) = y$. Notation logique : $\forall y \in B\, \exists x \in A.f(x) = y$.
3. f est dite *bijective* lorsqu'elle est à la fois injective et surjective.

Souvent, une fonction bijective est appelée une *correspondance bijective*, ou bien une *correspondence un à un*, parce qu'elle relie chaque élément de l'ensemble de départ (le domaine) à un unique élément de l'ensemble d'arrivée (le codomaine), et vice-versa.[3]

Comme d'habitude, nous commençons avec quelques exemples pour illustrer ces concepts.

Exemples XI.3.2.

1. Soient $A = \{a, b, c\}$ et $B = \{p, q, r, s\}$. Considérons les fonctions f, $g : A \to B$ telles que

$$\begin{array}{ll} f(a) = p & g(a) = p \\ f(b) = p & g(b) = r \\ f(c) = q & g(c) = s \end{array}$$

   Alors, f n'est pas injective, car nous avons $f(a) = f(b)$ et $a \neq b$. Aussi, f n'est pas surjective, car il n'y a pas de $x \in A$ tel que $f(x) = s$. La fonction g est injective, mais elle n'est pas surjective.

2. Soient $A = \{a, b, c, d\}$ et $B = \{p, q, r\}$. Considérons les fonctions $f, g : A \to B$ telles que

$$\begin{array}{ll} f(a) = p & g(a) = p \\ f(b) = p & g(b) = r \\ f(c) = q & g(c) = r \\ f(d) = r & g(d) = r \end{array}$$

   Alors, f est surjective, mais n'est pas injective, et g n'est pas injective ni surjective.

3. Soient $A = \{a, b, c, d\}$ et $B = \{p, q, r, s\}$. Considérons les fonctions $f, g : A \to B$ telles que

$$f(a) = p,\ f(b) = s,\ f(c) = r,\ f(d) = q.$$

   Alors, f est à la fois injective et surjective, et donc bijective.

> PROCÉDURE DE PREUVE
>
> Pour prouver que $f : A \to B$ est injective, vous devez
>
> - prendre arbitrairement $x, x' \in A$ tels que $f(x) = f(x')$, puis démontrer que $x = x'$.
>
> Pour prouver que $f : A \to B$ n'est pas injective, vous devez
>
> - trouver des éléments $x, x' \in A$ tels que $f(x) = f(x')$ et $x \neq x'$.
>
> Pour prouver que $f : A \to B$ est surjective, vous devez
>
> - prendre arbitrairement $y \in B$, puis démontrer qu'il existe un $x \in A$ tel que $f(x) = y$.
>
> Pour prouver que $f : A \to B$ n'est pas surjective, vous devez
>
> - trouver un élément $y \in B$ tel que $f(x) \neq y$ pour tout $x \in A$.

Exemple XI.3.3. Rappelons-nous que pour tout ensemble A, il y a une relation Δ_A, la relation identité. Cette relation est fonctionnelle, et elle est en fait bijective. Une notation plus courante pour Δ_A, lorsque nous considérons cette dernière comme une fonction, est $1_A : A \to A$. Avec la notation pour les fonctions, nous avons $1_A(x) = x$ pour tout $x \in A$, et nous appelons 1_A la *fonction identité* sur A.

[3] Et si vous voulez faire démonstration de votre compréhension du fondement des mathématiques et de votre niveau de sophistication mathématique, vous devriez les appeler des *isomorphismes*, car c'est ce qu'elles sont en réalité.

Voici quelques exemples avec des fonctions courantes du calcul infinitésimal :

Exemples XI.3.4.

1. La fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$ n'est ni injective ni surjective. Elle n'est pas injective[4] car, par exemple, nous avons $f(-2) = 4 = f(2)$ et $2 \neq -2$. Elle n'est pas surjective, car il n'y a pas de $x \in \mathbb{R}$ tel que $f(x) = -1$, par exemple.
2. La fonction $g : \mathbb{R} \to \mathbb{R}$ définie par $g(x) = 2x-5$ est injective : si $g(x) = g(x')$, alors $2x-5 = 2x'-5$, ce qui donne $2x = 2x'$, et donc $x = x'$. Elle est également surjective : étant donné $y \in \mathbb{R}$, pour trouver x avec $g(x) = y$, nous devons résoudre $2x - 5 = y$. Nous trouvons que $x = \frac{y+5}{2}$ est un candidat approprié. Donc, g est bijective.
3. Considérons la fonction tangente $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$. (Notez que le domaine a été restreint à une seule période de la fonction.) La fonction tan est bijective dans ce cas.

Pour le cas particulier où $f : A \to A$ est une bijection de A vers lui-même, nous appelons parfois f une *permutation* de A, car une telle fonction ne fait que permuter les éléments de A.

Nous terminons cette section avec un résultat utile à propos des fonctions bijectives.

Lemme XI.3.5. *Soit $f : A \to B$ une fonction. Alors f est bijective si et seulement si il existe une fonction $g : B \to A$ telle que $g \circ f = 1_A$ et $f \circ g = 1_B$.*

Démonstration. Pour commencer, supposons que f est une fonction bijective. Ensuite, définissons une fonction $g : B \to A$ comme suit :

$$g(y) = \text{ l'unique élément } x \in A \text{ tel que } f(x) = y.$$

Ceci est bien défini parce que f est une bijection : par la surjectivité, un tel x existe, et par l'injectivité, il est unique. (Comme alternative, vous pouvez employer $g(y) = x \Leftrightarrow f(x) = y$.) Maintenant,

$$g(f(x)) = \text{ l'unique élément } x \in A \text{ tel que } f(x) = f(x).$$

Mais, clairement, ceci donne $g(f(x)) = x$ (encore une fois, parce que f est injective). Ainsi, $g \circ f = 1_A$. De plus, nous avons

$$f(g(y)) = f(x), \text{ où } x \in A \text{ est l'unique élément avec } f(x) = y.$$

Ainsi, $f(g(y)) = y$, et nous obtenons $f \circ g = 1_B$.

Réciproquement, supposons qu'il existe une fonction g telle que $g \circ f = 1_A$ et $f \circ g = 1_B$. Pour démontrer que f est injective, supposons que nous avons x, $x' \in A$ tels que $f(x) = f(x')$. Il s'ensuit que

$$x = g(f(x)) = g(f(x')) = x'.$$

Pour démontrer que f est surjective, considérons $y \in B$. Alors, pour $x = g(y) \in A$, nous avons $f(x) = f(g(y)) = y$. □

Une fonction g avec les propriétés $g \circ f = 1_A$ et $f \circ g = 1_B$ est appelée un *inverse* de f. Il n'est pas difficile de prouver que si g et g' sont toutes les deux des inverses de f, alors elles doivent être égales :

$$g(y) = g(f(g'(y))) = g'(y)$$

où la première étape utilise $f(g'(y)) = y$, et la seconde utilise $g(f(x)) = x$. Ainsi, il est justifié de parler de l'inverse de f (plutôt que d'un inverse), et nous lui donnons la notation spéciale f^{-1}.

[4] En calcul infinitésimal, vous avez peut être vu le *test de la droite horizontale* pour l'injectivité. Prenez le temps de vérifier qu'il s'agit bien là d'une façon visuelle de déterminer notre concept d'injectivité.

XI.4 Ensembles de fonctions

Étant donné deux ensembles A et B, nous pouvons considérer la collection de toutes les relations de A vers B. Dénotons cet ensemble par $\mathsf{Rel}(A, B)$. Ainsi, par définition, nous avons

$$\mathsf{Rel}(A, B) = \{\, R \mid R \text{ est une relation de } A \text{ vers } B \,\} = \mathcal{P}(A \times B).$$

Dans la section précédente, nous avons appris que les fonctions sont des formes particulières de relations. Conséquemment, en gardant A et B fixés, nous pouvons considérer l'ensemble de toutes les fonctions de A vers B. Nous dénotons cet ensemble par $\mathsf{Fun}(A, B)$. Par définition, nous avons

$$\mathsf{Fun}(A, B) = \{\, R \in \mathsf{Rel}(A, B) \mid R \text{ est fonctionnelle} \,\}.$$

Une façon un peu plus élégante d'écrire ceci serait $\mathsf{Fun}(A, B) = \{\, f \mid f : A \to B \,\}$. Nous allons également utiliser la notation d'« exponentiation » B^A pour désigner cet ensemble. Cette dernière sera justifiée plus tard par l'observation que les ensembles de fonctions se comportent un peu comme les exponentielles.

Nous pouvons maintenant jouer à un jeu : Je vous donne un ensemble (qui comporte des fonctions et peut-être des produits), puis vous me donnez un élément qui appartient à cet ensemble.[5]

Commençons avec un cas simple : A^A. C'est l'ensemble de toutes les fonctions de A vers A. (Souvenez-vous, je ne vous ai rien dit à propos de A lui-même !) Pouvez-vous trouver un élément dans cet ensemble ? Oui : parmi toutes les fonctions de A dans A, nous pouvons considérer la fonction identité $Id_A \in A^A$. Même si nous ne connaissons rien à propos de A, nous savons que cette fonction existe toujours.

Maintenant, considérons $A^{A\times A}$, l'ensemble de toutes les fonctions de $A \times A$ vers A. Pouvez-vous trouver un élément dans cet ensemble ? Pour ce faire, vous devez définir une fonction $A \times A \to A$. En fait, il y a deux solutions possibles au problème : la première fonction est

$$\pi_1 : A \times A \to A; \qquad \pi_1(a, b) = a.$$

et la seconde est

$$\pi_2 : A \times A \to A; \qquad \pi_2(a, b) = b.$$

Ces fonctions sont parfois appelées *projections*. Consultez les exercices à la fin de cette leçon pour plus d'exemples.

Ensuite, considérons $(A^A)^A$. Un élément de cet ensemble est une fonction de A vers A^A. Pouvez-vous me donner une fonction de ce genre ? En fait, ce problème est un peu comme le précédent, et il y a de nouveau deux solutions. Pour la première, considérons la fonction $\eta : A \to A^A$ qui envoie $a \in A$ vers la fonction $c_a \in A^A$ définie par $c_a(x) = a$. Pour la deuxième, prenons la fonction $\iota : A \to A^A$ qui envoie tout $a \in A$ vers la fonction identité sur A.

Un dernier cas : trouvez un élément de $\mathsf{Fun}(A^A \times A, A)$. C'est-à-dire, trouvez une fonction de $A^A \times A$ vers A. Encore une fois, il y a exactement deux réponses possibles. La première est de prendre la fonction $\pi : A^A \times A \to A$ définie par $\pi(f, a) = a$. (C'est à nouveau une projection.) La deuxième est plus intéressante :

$$\epsilon : A^A \times A \to A; \qquad \epsilon(f, a) = f(a).$$

[5] On peut attribuer un sens très précis à ce genre de jeu (dans le cadre de la théorie des jeux) pour des ensembles construits de cette façon ; et ceci est dû à James Dolan.

Cette dernière est appelée la *fonction d'évaluation* : elle prend une fonction f comme premier paramètre et un élément a du domaine de cette fonction comme deuxième paramètre, puis elle donne $f(a)$ comme valeur de sortie, i.e. l'évaluation de f en a.

Nous allons revisiter ces idées dans la prochaine leçon. Pour le moment, notons qu'il y a des jeux que nous ne pouvons pas gagner : par exemple, supposons que je vous donne l'ensemble $\mathsf{Fun}(A^A, A)$. Vous êtes supposé de me donner une fonction de A^A vers A, mais que pourriez-vous faire ? En effet, vous verrez que vous ne pouvez pas gagner, à moins que vous ayez connaissance d'un élément spécifique de A à priori. Donc, si $A = \emptyset$, vous perdez automatiquement.

Exercice 117. Pouvez-vous gagner le jeu avec $\mathsf{Fun}(A^A, A^A)$? De combien de façons pouvez-vous gagner ?

XI.5 Sommaire

Les relations fonctionnelles (fonctions) sont définies comme des relations satisfaisant deux propriétés :

- Totalité
- Univaluée

La notion usuelle de composition de fonctions peut être représentée à travers la composition relationnelle de relations fonctionnelles.

Étant donné des fonctions $f : A \to B$ et $g : A \to C$, nous obtenons une fonction unique $\langle f, g\rangle : A \to B \times C$ telle que $\langle f, g\rangle(a) = (f(a), g(a))$. Toute fonction dont le codomaine est un ensemble-produit a une représentation unique de cette forme. De plus, étant donné des fonctions $f : A \to C$ et $g : B \to D$, nous définissons $f \times g : A \times B \to C \times D$ par $(f \times g)(a, b) = (f(a), g(b))$.

Parmi les fonctions, il y a trois classes particulières qui présentent un intérêt :

- Injections (aussi appelées : *une-à-une*)
- Surjections
- Bijections (aussi appelées : *correspondances bijectives*)

Toute fonction bijective $f : A \to B$ possède un unique *inverse*, c'est-à-dire, une fonction $g : B \to A$ pour laquelle $g \circ f = 1_A$ et $f \circ g = 1_B$. Cet inverse est désigné par f^{-1}.

Nous écrivons $\mathsf{Rel}(A, B)$ pour l'ensemble des relations de A vers B, et $\mathsf{Fun}(A, B)$ (ou B^A) pour l'ensemble des fonctions de A vers B.

XI.6 Exercices

Exercice 118. Considérons une relation $R \subseteq A \times B$.

(i) Si R est totale, avons-nous que R° est totale également ?

(ii) Si R est univaluée, avons-nous que R° est univaluée également ?

(iii) Si R est fonctionnelle, avons-nous que R° est fonctionnelle également ?

Exercice 119. Considérons la relation suivante de $\mathbb{R}$ vers lui-même :

$$R = \{\, (x^2, x) \mid x \in \mathbb{R} \,\}.$$

Cette relation est-elle fonctionnelle ?

Exercice 120. Considérons la relation $S = \{\, (x, x^3) \mid x \in \mathbb{R} \,\}$ de $\mathbb{R}$ vers lui-même. Cette relation est-elle fonctionnelle ? Qu'en est-il de S° ?

Exercice 121. Trouvez toutes les fonctions de $\{0, 1\}$ vers $\{0, 1\}$. (C'est-à-dire, décrivez tous les éléments de l'ensemble $\mathsf{Fun}(\{0, 1\}, \{0, 1\})$.)

Exercice 122. Démontrez que si $f : A \to \emptyset$ est une fonction, alors $A = \emptyset$.

Exercice 123. Démontrez que toute fonction $f : \emptyset \to B$ est injective.

Exercice 124. Démontrez que si B a exactement un élément, alors pour n'importe quel ensemble A, il existe exactement une fonction $f : A \to B$.

Exercice 125. Posons $f : \mathbb{R} \to \mathbb{R}$ comme étant la fonction $f(x) = x^3$. Cette fonction est-elle injective ? surjective ? bijective ?

Exercice 126. Même question, mais avec la fonction de valeur absolue

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

Exercice 127. Considérez la fonction affine $f(x) = ax + b$ (comme une fonction de $\mathbb{R}$ vers $\mathbb{R}$). Pour quelles valeurs a, b cette fonction est-elle injective ? surjective ? bijective ?

Exercice 128. Démontrez que si $f : A \to B$ et $g : B \to C$ sont toutes deux surjectives, alors $g \circ f$ aussi. (On exprime ceci en disant que les fonctions surjectives sont *fermées sous la composition.*)

Exercice 129. Démontrez que si $f : A \to B$ et $g : B \to C$ sont toutes deux injectives, alors $g \circ f$ aussi. (On exprime ceci en disant que les fonctions injectives sont *fermées sous la composition.*)

Exercice 130. Démontrez que si $f : A \to B$ et $g : B \to C$ sont toutes deux bijectives, alors $g \circ f$ aussi. (On exprime ceci en disant que les fonctions bijectives sont *fermées sous la composition.*)

Exercice 131. Est-il possible que ni f ni g soient injectives, mais que $g \circ f$ le soit ? Même question pour la surjectivité et la bijectivité.

Exercice 132. Démontrez que si f est bijective avec inverse f^{-1}, alors f^{-1} est également bijective, et $(f^{-1})^{-1} = f$.

Exercice 133. Démontrez que pour n'importe quel ensemble A, la fonction identité 1_A sur A est bijective. Quelle est son inverse ?

Exercice 134. Démontrez que si f et g sont bijectives, alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Exercice 135. Trouvez toutes les permutations de l'ensemble $A = \{a, b, c\}$.

Exercice 136. Même question, mais pour l'ensemble $B = \{a, b, c, d\}$.

Exercice 137. Supposons que A contient n éléments. Combien de permutations pensez-vous qu'il y a de A vers A ? (Notez : ceci est une question de combinatoire surtout.)

Exercice 138. Trouvez toutes les fonctions injectives de l'ensemble $A = \{a, b\}$ vers l'ensemble $B = \{p, q, r, s\}$.

Exercice 139. Trouvez toutes les fonctions surjectives de l'ensemble $A = \{a, b, c, d\}$ vers l'ensemble $B = \{p, q\}$.

Exercice 140. Est-il possible qu'une fonction $f : X \to X$ soit injective mais pas surjective ? Peut-elle être surjective mais pas injective ? Donnez des exemples.

Exercice 141. Soient A, B des ensembles. Démontrez qu'il existe une fonction $\pi_A : A \times B \to A$ qui envoie (x, y) sur x, et similairement, $\pi_B : A \times B \to B$ qui envoie (x, y) sur y. Ces fonctions sont appelées les *projections de produits*.

Exercice 142. Soient $f : A \to B$ et $g : A \to C$ des fonctions. Démontrez qu'il existe une fonction $\langle f, g\rangle : A \to B \times C$ donnée par $\langle f, g\rangle(x) = (f(x), g(x))$. Démontrez également que $\pi_B \circ \langle f, g\rangle = f$ et que $\pi_C \circ \langle f, g\rangle = g$.

Exercice 143. Démontrez que, pour $f : A \to B$ et $g : C \to D$, il existe une fonction $f \times g : A \times C \to B \times D$ qui envoie (x, y) sur $(f(x), g(y))$.

Exercice 144. Supposons que A contient n éléments, et que B contient m éléments. Combien d'éléments pensez-vous qu'il y a dans B^A ?

LEÇON XII

Correspondances bijectives

On rencontre souvent des ensembles qui semblent très différents les uns des autres à priori, mais qui sont étroitement reliés. En mathématiques, plusieurs résultats de profondeur substantielle énoncent que deux ensembles paraissant différents sont en fait « les mêmes ». Les correspondances bijectives sont employées pour donner un sens précis à ces énoncés. En affirmant qu'il existe une correspondance bijective entre deux ensembles A et B, on veut simplement dire qu'il existe une fonction bijective $f : A \to B$.

Dans cette leçon, nous étudions quelques correspondances bijectives non triviales. Nous introduisons la notation suivante pour caractériser l'existence d'une bijection entre deux ensembles A et B :

$$A \cong B \Leftrightarrow_{\text{déf}} \text{ il existe une bijection } f : A \to B.$$

Intuitivement, deux ensembles reliés par une correspondance bijective sont en fait le même ensemble, *mis à part que leurs éléments portent des noms différents*. En particulier, les deux ensembles contiennent la même quantité d'information, car nous pouvons faire l'aller-retour entre les deux sans perdre d'information.

> Procédure de preuve
>
> Démontrer que $A \cong B$ peut être beaucoup plus difficile que de simplement démontrer qu'une fonction donnée $f : A \to B$ est une bijection, car trouver une bijection candidate requiert parfois de la perspicacité et (ou) de la créativité. Généralement, la meilleure approche est de regarder attentivement en quoi consiste les éléments de A, et ceux de B, puis de chercher à établir un lien entre ceux-ci.

À partir des exercices de la leçon précédente, nous avons le résultat suivant en ce qui a trait aux correspondances bijectives :

Proposition XII.0.1. *La relation $\cong$ a les propriétés suivantes :*

1. $A \cong A$
2. $A \cong B$ *implique* $B \cong A$
3. $A \cong B$ *et* $B \cong C$ *implique* $A \cong C$

Gardez à l'esprit qu'il pourrait y avoir plusieurs bijections différentes de A à B.

Attention : le matériel présenté dans cette leçon rejoint un niveau d'abstraction plus élevé que celui rencontré jusqu'ici.

XII.1 Produits

Dans une leçon précédente, nous avons prouvé qu'il y a exactement un ensemble vide. Mais qu'en est-il des ensembles avec un seul élément ? (Un ensemble avec un seul élément est appelé un *singleton*.) Ceux-ci ne sont certainement pas uniques (il suffit d'employer l'extensionalité) : $\{\emptyset\}, \{\{\emptyset\}\}$ et $\{\mathbb{N}\}$ sont tous des singletons, mais ils diffèrent les uns des autres car leurs éléments diffèrent. Tout de même, les singletons sont en correspondance bijective, et en ce sens, il y a un unique ensemble avec un seul élément.

Lemme XII.1.1. *Supposons que A et B sont tous les deux des singletons. Alors, $A \cong B$.*

Démonstration. Dénotons l'unique élément de A par a, et l'unique élément de B par b. Il n'y a pas grand choix à faire maintenant : il n'y a qu'une seule fonction $f : A \to B$; notamment, celle définie par $f(a) = b$. Réciproquement, il n'y a qu'une seule fonction $g : B \to A$; notamment, celle définie par $g(b) = a$. Clairement, f et g sont des inverses l'une de l'autre. (Voir les exercices pour une preuve plus élégante.) □

La façon courante de référer au résultat ci-haut est de dire que les singletons sont uniques *à isomorphisme près*.[1] Il est coutumier d'écrire 1 pour désigner un singleton lorsqu'il importe peu en quoi consiste l'unique élément de cet ensemble.

Proposition XII.1.2. *Soit A un ensemble. Alors, $A \times 1 \cong A \cong 1 \times A$.*

Démonstration. Nous prouvons que $A \times 1 \cong A$, et le reste est laissé en exercice. Pour faciliter les choses, nous dénotons l'unique élément de 1 par $*$. Ensuite, notons que

$$A \times 1 = \{(a, *) | a \in A\}.$$

Ainsi, $A \times 1$ est pratiquement[2] la même chose que A ; la seule différence est que les éléments de $A \times 1$ ont une étiquette « $*$ ». Donc, la bijection de $A \times 1$ vers A devrait simplement « enlever l'étiquette ».

Pour faire une preuve plus concrète, posons

$$\pi_A : A \times 1 \to A; \qquad \pi_A(a, *) = a.$$

Alors, la projection π_A est une bijection ; son inverse est $\pi_A^{-1}(a) = (a, *)$. □

[1] « Iso » provient du grec et signifie « égal », tandis que « morphè » veut dire « forme ». Ainsi, tous les ensembles à un élément ont une forme égale.

[2] Vous entendrez souvent des mathématiciens dire des choses comme : « Pratiquement parlant, ces deux ensembles sont les mêmes. » En général, ils veulent dire : ces ensembles pourraient ne pas être identiques, techniquement, mais ils se comportent de manière similaire dans les circonstances où nous les considérons.

Notons que ceci pourrait ne pas être la seule bijection de $A \times 1$ vers A. (Si σ est une permutation de A, alors $\sigma \circ \pi_A$ est aussi une bijection $A \times 1 \to A$.) Tout de même, la bijection π_A donnée est *canonique*.

Ensuite, rappelons-nous qu'il a été indiqué plus tôt que $A \times B$ est généralement différent de $B \times A$. Mais, certainement, ces derniers sont étroitement reliés l'un à l'autre ! En effet :

Proposition XII.1.3. *Pour tous ensembles A, B nous avons $A \times B \cong B \times A$.*

Démonstration. Encore une fois, il est assez évident en quoi devrait consister la bijection :

$$\tau : A \times B \to B \times A; \qquad \tau(x, y) = (y, x).$$

Vous devriez maintenant vérifier les propriétés suivantes :

(i) τ est en effet une fonction bien définie.

(ii) τ est injective.

(iii) τ est surjective.

Comme alternative, vous pouvez donner directement un inverse $\sigma : B \times A \to A \times B$ de τ. □

Pour une dernière correspondance avec des produits : Supposons que $f : A \to B$ et $g : C \to D$ sont des fonctions. Comme discuté plus tôt dans la leçon IX, nous obtenons une fonction

$$f \times g : A \times C \to B \times D; \qquad (f \times g)(a, c) = (f(a), g(c)).$$

Nous voulons démontrer que si f et g sont toutes les deux bijectives, alors $f \times g$ aussi. Ceci démontrera :

Proposition XII.1.4. *Si $A \cong B$ et $C \cong D$, alors $A \times C \cong B \times D$.*

Démonstration. Nous démontrons que $f \times g$ est injective et surjective.

Injectivité : supposons que nous avons deux éléments (x, y) et (x', y') de $A \times C$ tels que $(f \times g)(x, y) = (f \times g)(x', y')$. Par définition de $f \times g$, ceci veut dire que $(f(x), g(y)) = (f(x'), g(y'))$. Ceci, en revanche, revient à dire $f(x) = f(x')$ et $g(y) = g(y')$ (pourquoi ?). Puisque f et g sont toutes les deux injectives, ceci force $x = x'$ et $y = y'$. Ainsi, nous obtenons $(x, y) = (x', y')$, tel que voulu.

Surjectivité : considérons un élément $(u, v) \in B \times D$. Puisque f est surjective, il existe un $x \in A$ tel que $f(x) = u$. Puis, g est surjective, donc il existe un $y \in C$ tel que $g(y) = v$. Nous obtenons $(f \times g)(x, y) = (f(x), g(y)) = (u, v)$, tel que voulu. □

Exercice 145. Donnez une preuve alternative en démontrant que $f^{-1} \times g^{-1}$ est l'inverse de $f \times g$.

Exercice 146. Démontrez que pour n'importe quels ensembles A, B, C, nous avons $A \times (B \times C) \cong (A \times B) \times C$.

Finalement, étudions un exemple d'une nature un peu différente. Nous allons démontrer (de manière un peu informelle, car nous revisiterons cette matière dans une leçon ultérieure) que $\mathbb{N} \cong P$, où P est l'ensemble des nombres premiers positifs. Pour ce faire, nous allons employer le théorème d'Euclide, lequel postule l'existence de nombres premiers arbitrairement grands.

Nous devons construire une fonction bijective $f : \mathbb{N} \to P$. L'idée est d'envoyer n sur le n^e nombre premier. Ceci a du sens car nous pouvons énumérer tous les nombres premiers par ordre croissant : p_0, p_1, p_2, ... Nous pouvons supposer qu'il n'y a pas de répétition dans cette liste. Par le théorème d'Euclide, nous savons que cette liste n'arrête pas. La fonction est donnée par $f(n) = p_n$ est la bijection désirée.

XII.2 Fonctions caractéristiques

Dans cette section, nous abordons un exemple un peu plus sophistiqué de correspondance bijective. Le point de départ est l'ensemble $\{0,1\}$, qui porte parfois le nom de 2 (car il a deux éléments). Parfois, les éléments de cet ensemble sont dénotés $\top, \bot$, ou V, F, pour *vrai* et *faux*. Nous allons nous en tenir à $\{0,1\}$.

Comme exercice de réchauffement, considérons l'ensemble $A = \{a,b,c\}$. Dirigeons notre attention sur les fonctions $A \to \{0,1\}$, c'est-à-dire, sur les éléments de l'ensemble $\mathsf{Fun}(A,\{0,1\})$. Étant donné que A est très petit, nous pouvons faire la liste de toutes les fonctions en question (nous leur attribuons des noms aléatoires pour le moment) :

$$\begin{array}{lll} f(a)=f(b)=f(c)=0 & g(a)=g(b)=0,\ g(c)=1 & h(a)=h(c)=0,\ h(b)=1 \\ i(a)=0,\ i(b)=i(c)=1 & j(a)=1,\ j(b)=j(c)=0 & k(1)=k(1)=0,\ k(b)=0 \\ l(a)=l(b)=1,\ l(c)=0 & m(a)=m(b)=m(c)=1 & \end{array}$$

Ainsi, il y a 8 fonctions $A \to \{0,1\}$ au total, ce qui veut que $\mathsf{Fun}(A,\{0,1\})$ a 8 éléments.

Maintenant, ces fonctions peuvent être interprétées de manière différente. Étant donné que les éléments $\{0,1\}$ peuvent jouer le rôle de valeurs de vérité, une fonction $p : A \to \{0,1\}$ peut être vue comme décidant, pour chaque élément de A, si ce dernier est envoyé sur vrai (i.e sur 1) ou sur faux (i.e. sur 0). Ainsi, l'ensemble de tous les éléments qui sont envoyés sur vrai peuvent former un sous-ensemble de A. Par exemple, la fonction i envoie b et c sur 1, et a sur 0, donc l'ensemble de tous les éléments qui sont envoyés sur « vrai » est $\{b,c\}$.

Nous pouvons faire cela pour chaque fonction $A \to \{0,1\}$, et ainsi, chacune de ces fonctions détermine un sous-ensemble de A. Nous obtenons

$$\begin{array}{ll} f \rightsquigarrow \emptyset & j \rightsquigarrow \{a\} \\ g \rightsquigarrow \{c\} & k \rightsquigarrow \{a,c\} \\ h \rightsquigarrow \{b\} & l \rightsquigarrow \{a,b\} \\ i \rightsquigarrow \{b,c\} & m \rightsquigarrow \{a,b,c\} \end{array}$$

Ceci caractérise une fonction $\mathsf{Fun}(A,\{0,1\}) \to \mathcal{P}(A)$. Notez que, non seulement chaque fonction $A \to \{0,1\}$ détermine un sous-ensemble de A, mais *chaque* sous-ensemble de A est déterminé de cette manière. De plus, des fonctions distinctes donnent des sous-ensembles distincts. Par conséquent, nous avons une correspondance bijective

$$\mathsf{Fun}(A,\{0,1\}) \cong \mathcal{P}(A).$$

Nous avons abordé cet exemple en termes de la façon dont les fonctions $A \to \{0,1\}$ donnent lieu à des sous-ensembles de A. Mais la direction opposée est tout aussi importante. Comment les sous-ensembles de A donnent-ils lieu à des fonctions ? Supposons que nous avons un sous-ensemble $U \subseteq A$. Nous voulons représenter celui-ci par une fonction $A \to \{0,1\}$. En imaginant que 1 joue le rôle de vrai, et 0 le rôle de faux, nous voulons que cette fonction génère un « vrai » en sortie lorsqu'un élément appartient effectivement à U, et un « faux » lorsque ce n'est pas le cas. Cette fonction est appelée la *fonction caractéristique*[3] du sous-ensemble U. Formellement :

$$\chi_U(x) = \begin{cases} 1 & \text{si } x \in U \\ 0 & \text{si } x \notin U \end{cases}.$$

[3] Certains textes la dénomme *fonction indicatrice*.

Par exemple, si $U = \{a, c\}$, alors $\chi_U(a) = \chi_U(c) = 1$ et $\chi_U(b) = 0$.

La représentation de sous-ensembles via des fonctions caractéristiques n'est pas aussi ésotérique que l'on pourrait imaginer : Les ordinateurs ne reconnaissent que des 0 et des 1 ; donc, lorsque l'on veut encoder un sous-ensemble dans un ordinateur, c'est précisément les fonctions caractéristiques que l'on utilise.

Nous procédons maintenant à une généralisation de l'exemple précédent. L'idée de la preuve est la même que celle dans le cas étudié, mais nous écrirons une preuve détaillée cette fois. La difficulté principale ne réside pas dans l'appréhension de l'idée générale de la preuve ici (après tout, je vous ai déjà expliqué en quoi elle consistait), mais dans le fait que nous devons procéder de manière particulièrement systématique à l'égard de ce qui doit être fait. Étant donné que nous ne travaillons pas avec des fonctions entre des ensembles d'ensembles et des ensembles de fonctions, nous pouvons facilement nous égarer.

Proposition XII.2.1. *Soit X un ensemble. Alors, il y a une correspondance bijective $\mathcal{P}(X) \cong \mathsf{Fun}(X, \{0,1\})$.*

Démonstration. L'objectif est de construire une fonction bijective de $\mathcal{P}(X)$ vers $\mathsf{Fun}(X, \{0,1\})$. Appelons cette fonction (que nous devons spécifier) ϕ. Donc, pour chaque sous-ensemble U de X, nous devons définir un élément $\phi(U) \in \mathsf{Fun}(X, \{0,1\})$. C'est-à-dire, $\phi(U)$ est une fonction $X \to \{0,1\}$. Nous définissons, étant donné $U \subseteq X$, $\phi(U)$ comme étant la fonction caractéristique de U :

$$\phi(U) = \chi_U : X \to \{0,1\}; \qquad \chi_U(x) = \begin{cases} 1 & \text{si } x \in U \\ 0 & \text{si } x \notin U \end{cases}$$

Ceci définit une fonction $\phi : \mathcal{P}(X) \to \mathsf{Fun}(X, \{0,1\})$. Il reste à vérifier que c'est une bijection. Nous allons exhiber l'inverse de ϕ. (Comme alternative, vous pourriez tenter de prouver que ϕ est injective et surjective, ce qui nécessiterait à peu près les mêmes idées.)

Donc, essayons de définir $\phi^{-1} : \mathsf{Fun}(X, \{0,1\}) \to \mathcal{P}(X)$ par

$$\phi^{-1}(f) = \{\, x \in X \mid f(x) = 1 \,\}.$$

En d'autres termes, ϕ^{-1} envoie un élément $f : X \to \{0,1\}$ sur l'ensemble des x pour lesquels $f(x) = 1$. (Notez que ϕ^{-1} prend une fonction comme entrée, et donne un sous-ensemble comme sortie.)

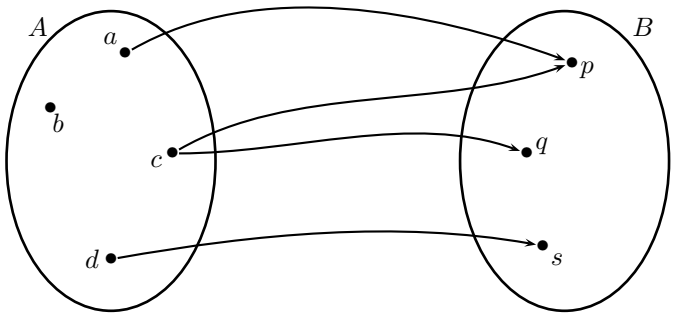
Finalement, nous devons montrer que ϕ^{-1} est effectivement l'inverse de ϕ. Pour démontrer $\phi^{-1} \circ \phi = 1_{\mathcal{P}(X)}$, considérons $U \in \mathcal{P}(X)$ et calculons

$$\phi^{-1}(\phi(U)) = \phi^{-1}(\chi_U) = \{\, x \in X \mid \chi_U(x) = 1 \,\} = U.$$

Et pour démontrer $\phi \circ \phi^{-1} = 1_{\mathsf{Fun}(X,\{0,1\})}$, prenons $f : X \to \{0,1\}$; nous voulons maintenant prouver que $\phi(\phi^{-1}(f)) = f$. Étant donné qu'il s'agit là de fonctions, nous démontrons qu'elles sont égales en démontrant qu'elles sont en accord sur toutes les entrées possibles. Donc, considérons une valeur d'entrée arbitraire $x \in X$. Alors,

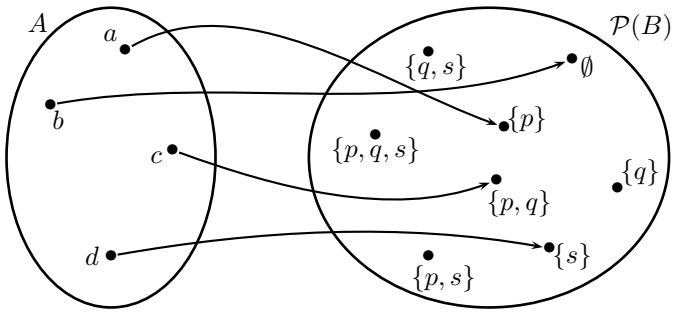
$$\begin{aligned} \phi(\phi^{-1}(f))(x) &= \phi(\{\, x \in X \mid f(x) = 1 \,\})(x) \\ &= \chi_{\{\, x \in X \mid f(x) = 1 \,\}}(x) \\ &= \begin{cases} 1 & \text{si } f(x) = 1 \\ 0 & \text{si } f(x) = 0 \end{cases} \\ &= f(x) \end{aligned}$$

□



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

FIGURE XII.1 – Relation R de A vers B



... et la
fonction
correspondante

FIGURE XII.2 – Fonction de A vers $\mathcal{P}(B)$

XII.3 RELATIONS

Le dernier exemple de correspondance bijective (pour l'instant) est entre les relations de A vers B et les fonctions $A \to \mathcal{P}(B)$. Pour se faire une idée de cette correspondance, considérons la relation donnée à la figure XII.1. Comment pouvons-nous interpréter cette relation comme une fonction de A vers $\mathcal{P}(B)$? Une telle fonction devrait associer à chaque élément de A un sous-ensemble de B. Quel devrait être le sous-ensemble associé à l'élément c ? La relation R relie c aux éléments p et q. Ainsi, il est sensé que nous associons c au sous-ensemble $\{p, q\}$. Généralement, un élément $x \in A$ est associé à l'ensemble de tous les éléments dans B qui sont reliés à x par R. En dénotant la fonction recherchée par $r : A \to \mathcal{P}(B)$, nous obtenons ainsi

$$r(a) = \{p\},\ r(b) = \emptyset,\ r(c) = \{p, q\},\ r(d) = \{s\}.$$

La figure XII.2 dépeint la fonction correspondante.

De cette façon, les relations peuvent être représentées comme des fonctions dont les valeurs sont des ensembles. Et maintenant, nous formulons l'énoncé général :

Proposition XII.3.1. *Pour tous ensembles A, B, nous avons la correspondance bijective*

$$\mathsf{Rel}(A, B) \cong \mathsf{Fun}(A, \mathcal{P}(B)).$$

En se rappelant que l'ensemble des relations de A vers B est $\mathcal{P}(A \times B)$, et que l'ensemble des fonctions de A vers $\mathcal{P}(B)$ est $\mathcal{P}(B)^A$, nous pouvons écrire ceci comme

$$\mathcal{P}(A \times B) \cong \mathcal{P}(B)^A.$$

Démonstration. Nous allons définir une fonction bijective $\phi : \mathsf{Rel}(A, B) \to \mathsf{Fun}(A, \mathcal{P}(B))$. Considérons un élément $R \in \mathsf{Rel}(A, B)$, i.e. une relation $R \subseteq A \times B$. Nous devons définir $\phi(R)$ pour qu'il soit un élément de $\mathcal{P}(B)^A$, soit une fonction $A \to \mathcal{P}(B)$. Définissons cette fonction comme suit :

$$\phi(R) : A \to \mathcal{P}(B); \qquad \phi(R)(x) = \{\, y \in B \mid xRy \,\}.$$

Ainsi, $\phi(R)$ est une fonction qui envoie x sur l'ensemble des éléments reliés à lui.

Maintenant, définissons une fonction (soyons optimiste et appelons la ϕ^{-1}) dans l'autre direction. Cette fonction ϕ^{-1} prend un élément de $\mathsf{Fun}(A, \mathcal{P}(B))$ comme entrée (c'est-à-dire, une fonction $A \to \mathcal{P}(B)$) et donne une relation de A vers B comme sortie. Étant donné $r : A \to \mathcal{P}(B)$, définissons

$$\phi^{-1}(r) \subseteq A \times B; \qquad \phi^{-1}(r) = \{\, (x, y) \mid y \in r(x) \,\}.$$

La vérification que ϕ^{-1} est effectivement un inverse de ϕ est laissée en exercice. □

Exercice 147. Complétez la preuve ci-haut.

XII.4 Sommaire

Cette leçon cherchait essentiellement à établir quelques exemples importants de *correspondances bijectives* entre des ensembles.

- Deux ensembles sont en correspondance bijective lorsqu'il existe une bijection allant de l'un vers l'autre (et donc, dans l'autre direction également).
- Lorsque deux ensembles sont en correspondance bijective, il est courant de concevoir que leurs éléments respectifs contiennent la même information, quoique décrite d'une manière différente.
- Lorsque $A \cong B$, ceci veut dire que nous pouvons faire l'aller-retour entre A et B sans perdre d'information.

Les correspondances bijectives surviennent constamment en mathématiques. Nous nous sommes limités à établir les suivantes :

- les correspondances bijectives dans le contexte de produits cartésiens d'ensembles,
- les correspondances bijectives entre les sous-ensembles et les fonctions dans $\{0, 1\}$,
- les correspondances bijectives entre les relations et les fonctions dans des ensembles de parties.

En cherchant à établir $A \cong B$, la stratégie suivante est habituellement recommandable :

- Premièrement, obtenez une description à l'écrit de ce qu'un élément typique de l'ensemble A représente ; similairement, faites-vous une image claire de ce en quoi consistent les éléments de B.
- Demandez-vous quelle information est contenue dans un élément de A, et comment cette information peut être utilisée pour spécifier un élément de B.

- Transformez ceci en une définition de fonction $f : A \to B$.
- Prouvez que f est une bijection.

Si vous éprouvez des difficultés à concevoir comment un élément de A peut être transformé en un élément de B, la meilleure chose à faire est souvent de commencer par étudier un exemple concret ; ensuite, il devient plus facile d'établir le cas général.

XII.5 Exercices

Exercice 148. Listez toutes les fonctions bijectives de $A = \{a, b, c\}$ vers $B = \{0, 1, 2\}$.

Exercice 149. Vrai ou faux ? (Donnez une preuve ou un contre-exemple.) Si une fonction $f : A \to A$ est bijective, alors elle est la fonction identité.

Exercice 150. Considérez l'ensemble $A = \{\text{Jean, Marie, Karine}\}$, et le sous-ensemble $B = \{\text{Marie, Karine}\}$. Déterminez la fonction caractéristique de ce sous-ensemble.

Exercice 151. Considérez l'ensemble $A = \{0, 1, 2, 3\}$, de même que les fonctions suivantes de A vers $\{0, 1\}$:

$$f(0) = f(2) = 0,\ f(1) = f(3) = 1 \quad g(0) = 0,\ g(1) = g(2) = g(3) = 1$$

Trouvez les sous-ensembles de A correspondant à ces fonctions.

Exercice 152. Considérez l'ensemble des nombres naturels $\mathbb{N}$, et le sous-ensemble $P \subseteq \mathbb{N}$ des nombres premiers. Décrivez la fonction caractéristique de ce sous-ensemble.

Exercice 153. Considérez la fonction $\max : \{0, 1\} \times \{0, 1\} \to \{0, 1\}$. Quel est le sous-ensemble de $\{0, 1\} \times \{0, 1\}$ correspondant à cette fonction ?

Exercice 154. Soient U, V des sous-ensembles de A avec les fonctions caractéristiques χ_U et χ_V, respectivement. Démontrez que $\chi_{U \cap V}$ est la fonction

$$\chi_{U \cap V}(x) = \chi_U(x) \cdot \chi_V(x)$$

(i.e. multipliez les deux fonctions caractéristiques). Trouvez des formules similaires pour $\chi_{U \cup V}$, χ_{U^c} et $\chi_{U - V}$.

Exercice 155. Considérez l'ensemble $B = \{\text{Jean, Marie, Karine}\}$. Supposez que Jean aime Marie et Karine, Marie aime Jean, et Karine aime seulement elle-même. Déterminez la fonction $B \to \mathcal{P}(B)$ correspondant à cette relation.

Exercice 156. En employant la corresponsdance entre les relations $R \subseteq A \times A$ et les fonctions $r : A \to \mathcal{P}(A)$, déterminez quelle fonction correspond à la relation vide ? la relation maximale ? et la relation identité ?

Exercice 157. Supposez que la relation $R \subseteq A \times B$ est totale. Démontrez que la fonction correspondante $r : A \to \mathcal{P}(B)$ n'est pas surjective.

Exercice 158. Pour tout ensemble X, il y a une fonction $\eta_X : X \to \mathcal{P}(X)$ définie par

$$\eta_X(x) = \{x\}.$$

À quelle relation $X \to X$ correspond cette fonction ?

Exercice 159. Prouvez les correspondances bijectives suivantes. (Nous écrivons 0 pour désigner l'ensemble vide.)

1. $A + 0 \cong A \cong 0 + A$
2. $A + B \cong B + A$
3. $A + (B + C) \cong (A + B) + C$
4. $A \times 0 \cong 0 \cong 0 \times A$

Exercice 160. Prouvez la *loi de distributivité* $A \times (B + C) \cong (A \times B) + (A \times C)$.

Exercice 161. Rappelez-vous que Y^X est l'ensemble de toutes les fonctions $X \to Y$. Prouvez :

(a) $A^1 \cong A$

(b) $1^A \cong 1$

(c) $A^0 \cong 1$

(d) $(A \times B)^C \cong A^C \times B^C$

(e) $A^{B+C} \cong A^B \times A^C$

(f) $A^{B \times C} \cong (A^B)^C$

Exercice 162. Est-il vrai que $0^A \cong 0$?

Exercice 163. Rappelez-vous que $\mathsf{Rel}(A, B)$ dénote l'ensemble des relations de A vers B. Prouvez : $\mathsf{Rel}(A, B) \cong \mathsf{Rel}(B, A)$. Indice : lemme X.2.3.

Exercice 164. Prouvez : $\mathsf{Rel}(A \times B, C) \cong \mathsf{Rel}(A, B \times C)$.

LEÇON XIII

RELATIONS D'ÉQUIVALENCE

Nous avons étudié une classe particulière de relations, c'est-à-dire les fonctions. Cette leçon est consacrée à l'étude d'une classe de relations différentes, quoique toutes aussi importantes, notamment, les *relations d'équivalence*.

XIII.1 DÉFINITIONS

Nous commençons par lister une variété de propriétés que les relations peuvent avoir. Nous insistons sur le fait que les propriétés en question peuvent être définies seulement pour une relation d'un ensemble vers lui-même.

Définition XIII.1.1. Soit A un ensemble et $R \subseteq A \times A$ une relation sur A. On dit que R est

1. *réflexive* lorsque $\forall x \in A. xRx$
2. *irréflexive* lorsque $\forall x \in A. \neg xRx$
3. *symétrique* lorsque $\forall x, y \in A. [xRy \to yRx]$
4. *antisymétrique* lorsque $\forall x, y \in A. [xRy \wedge yRx \to x = y]$[1]
5. *transitive* lorsque $\forall x, y, z \in A. [xRy \wedge yRz \to xRz]$.

À titre d'exemple, considérons les relations R, S, V et W de la figure XIII.1.

Premièrement, vérifions lesquelles de ces relations satisfont la réflexivité. Schématiquement parlant, ceci veut dire de vérifier que chaque élément a une boucle qui lui est rattachée. La relation R sur A satisfait certainement ce critère, mais ce n'est pas le cas des autres relations.

[1] Parfois, on rencontre une définition plus forte $\forall x, y \in A. \neg(xRy \wedge yRx)$; cette dernière exclut la possibilité que xRx. Nous allons employer la version plus faible.

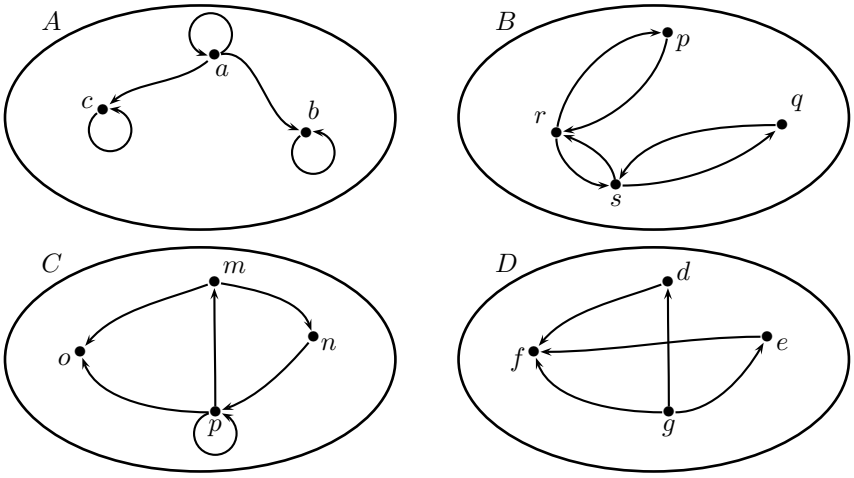


FIGURE XIII.1 – Les relations $R \subseteq A \times A$, $S \subseteq B \times B$, $V \subseteq C \times C$, $W \subseteq D \times D$

Afin de tester l'irréflexivité d'une relation, on doit vérifier qu'il n'y a pas d'élément avec une boucle. Les relations S et W ont cette propriété, tandis que R et V ne l'ont pas. Notons que la relation V n'est ni irréflexive, ni réflexive, car certains éléments ont une boucle, alors que d'autres non.

Ensuite, la symétrie : ceci veut dire que *s'il* y a une flèche d'un élément vers un autre, *alors* il doit y avoir une flèche dans l'autre sens. La seule relation qui est symétrique est S.

Pour l'antisymétrie, nous vérifions plutôt : *s'il* y a une flèche d'un élément vers un autre, *alors* il ne peut y avoir de flèche dans l'autre sens (à moins que les deux éléments soient égaux). Or, S n'est pas antisymétrique car sSq et qSs, mais il est faux que $s = q$. Toutes les autres relations sont antisymétriques.

Finalement, la transitivité : nous devons vérifier que *s'il* existe une flèche de x vers y et une flèche de y vers z, *alors* il doit y avoir une flèche de x vers z. La relation R satisfait ce critère : chaque chemin à deux pas peut également se faire en un seul pas. La relation S ne l'est pas : par exemple, nous pouvons aller de p vers r et de r vers p, mais nous ne pouvons pas aller de p vers p directement. Aussi, V n'est pas transitive : nous pouvons aller de p vers m et de m vers n, mais pas de p vers n directement. Finalement, W est transitive. L'ensemble des résultats est résumé au tableau XIII.1.

Relation	**Réflexive**	**Irréflexive**	**Symétrique**	**Antisymétrique**	**Transitive**
$R \subseteq A \times A$	Oui	Non	Non	Oui	Oui
$S \subseteq B \times B$	Non	Oui	Oui	Non	Non
$V \subseteq C \times C$	Non	Non	Non	Oui	Non
$W \subseteq D \times D$	Non	Oui	Non	Oui	Oui

Tableau XIII.1 – Propriétés de R, S, V, W

Voici quelques exemples plus courants en mathématiques :

Exemples XIII.1.2.

1. La relation d'ordre $\leq$ sur $\mathbb{N}$ est réflexive : pour tout $x \in \mathbb{N}$, nous avons $x \leq x$. Elle n'est pas irréflexive car, par exemple, nous avons $3 \leq 3$. Elle n'est pas symétrique : nous avons, par exemple, $2 \leq 6$, mais pas $6 \leq 2$. Elle est antisymétrique : si $x \leq y$ et $y \leq x$, alors $x = y$. Elle est transitive : si $x \leq y$ et $y \leq z$, alors $x \leq z$ aussi.
2. L'ordre strict $<$ sur $\mathbb{N}$ n'est pas réflexif, ni symétrique, mais il est irréflexif, antisymétrique et transitif. Assurez-vous de comprendre pourquoi il est antisymétrique !
3. La relation de sous-ensemble sur $\mathcal{P}(X)$ est réflexive, antisymétrique et transitive, mais elle n'est pas irréflexive, ni symétrique (vérifiez ceci).

La partie difficile (selon la majorité des étudiants !) est que certaines relations peuvent statisfaire certaines ou toutes ces propriétés comme des vérités vides. Par exemple, considérons l'ensemble $A = \{a, b\}$ et la relation $R = \{(a, b)\}$. Cette relation est transitive comme vérité vide : il n'y pas d'éléments x, y, z tels que xRy et yRz en même temps, donc l'antécédent de l'implication dans la définition est toujours faux.

Voici les exercices importants que vous devriez faire : pour chaque paire de propriétés, trouvez : (a) une relation qui satisfait les deux propriétés, (b) une relation qui n'en satisfait aucune, (c) une relation qui satisfait la première propriété, mais pas la deuxième, puis (d) une relation qui satisfait la deuxième propriété, mais pas la première. Trouvez les exemples les plus petits possibles ! Vous ne pouvez prétendre que vous comprenez les définitions si vous n'avez pas bien complété ces exercices.

Aspects logiques

Garder à l'esprit qu'un énoncé tel que

$$\forall xyz.(xRy \wedge yRz \to xRz)$$

est vrai dans le cas où, pour chaque x, y, z, nous avons

si xRy et yRz, *alors* xRz.

Ainsi, vous devez vérifier cette implication pour tous choix possibles de x, y, z, incluant des choix où $x = y$, $y = z$, ou $x = z$. Pour chaque choix, souvenez-vous que si l'antécédent est faux, alors l'implication est vraie.

XIII.2 Relations d'équivalence

Les définitions précédentes n'étaient qu'une étape préparatoire ; le concept qui est véritablement d'intérêt dans cette leçon est le suivant :

Définition XIII.2.1 (Relation d'équivalence)**.** Une relation $R \subseteq A \times A$ est une *relation d'équivalence* lorsqu'elle est réflexive, symétrique et transitive.

Bien souvent, une relation d'équivalence est dénotée par un symbole tel que $\sim$. Nous abordons un certain nombre d'exemples pour illustrer ce concept. Pour chacun d'entre eux, vous devriez vérifier les détails.

Exemples XIII.2.2.

1. Pour $A = \{*\}$ (c'est-à-dire, A est un singleton), il y a une seule relation d'équivalence, notamment $\{(*, *)\}$. (L'autre relation sur A, notamment l'ensemble vide, n'est pas réflexive.)

2. Pour un ensemble arbitraire A, la relation identité $\Delta_A = \{(x, x) | x \in A\}$ est une relation d'équivalence. Il s'agit de la plus petite relation d'équivalence sur A, au sens que pour n'importe quelle relation d'équivalence R sur A, nous avons $\Delta_A \subseteq R$. (Δ_A est également la plus petite relation réflexive sur A.)

3. Pour un ensemble arbitraire A, la relation maximale $A \times A$ est une relation d'équivalence. Il s'agit de la plus grande relation d'équivalence sur A.

4. Voici un exemple de relation d'équivalence sur $\mathbb{R}$: posons

$$x \sim y \Leftrightarrow |x| = |y|.$$

   C'est-à-dire, nous déclarons que x et y sont équivalents s'ils ont la même valeur absolue.

5. Une autre relation d'équivalence sur $\mathbb{R}$: posons

$$x \sim y \Leftrightarrow |x - y| \in \mathbb{N}.$$

   C'est-à-dire, x et y sont équivalents lorsque la distance entre les deux est un entier.

6. Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction. Définissons

$$x \sim y \Leftrightarrow f(x) = f(y).$$

   (l'exemple 4 est un cas particulier de ceci, avec $f(x) = |x|$.)

7. Voici une relation d'équivalence sur l'ensemble $\mathbb{R} \times \mathbb{R}$: posons

$$(u, v) \sim (x, y) \Leftrightarrow u^2 + v^2 = x^2 + y^2.$$

   C'est-à-dire, deux points dans le plan sont équivalents lorsqu'ils ont la même distance par rapport à l'origine.

8. Finalement, considérons une relation d'équivalence sur $\mathbb{Z}$ comme suit : Premièrement, fixons un nombre naturel $n > 0$. Puis, définissons

$$x \sim_n y \Leftrightarrow x - y \text{ est divisible par } n.$$

   Cette dernière est réflexive : pour tout $x \in \mathbb{N}$, nous avons $x - x = 0$, lequel est certainement divisible par n. Elle est également symétrique : si $x - y$ est divisible par n, alors $y - x = -(x - y)$ aussi. Et finalement, elle est transitive : si $x - y = kn$ et $y - z = ln$ pour des entiers k, l, alors

$$x - z = x - y + y - z = kn + ln = (k + l)n,$$

   donc $x - z$ est divisible par n aussi.

   Notez que nous avons une relation d'équivalence de ce genre pour chaque choix de n.

XIII.3 Classes d'équivalence

Lorsque $\sim$ est une relation d'équivalence sur un ensemble A et $x \sim y$, on dit que x et y sont *équivalents*. Souvent, nous voulons identifier des éléments équivalents, car il convient parfois, selon le contexte dans lequel nous travaillons, de les considérer comme égaux. À titre d'exemple pratique, considérez un jeu de cartes. Si on vous remet une main et que l'ordre des cartes ne vous intéresse pas, vous pouvez considérer que deux mains sont égales lorsqu'elles contiennent les mêmes cartes. Ainsi, il y a une relation d'équivalence sur les mains possibles : deux mains sont équivalentes si vous pouvez obtenir l'une à partir de l'autre en permutant les cartes.

L'idée de « considérez des éléments équivalents comme étant égaux » acquiert un sens formel comme suit : Premièrement, fixons un élément $x \in A$. Étant donné un tel élément, nous pouvons évoquer l'ensemble de tous les éléments qui sont équivalents à x. Dénotons l'ensemble en question par $[x]_\sim$, ou simplement par $[x]$ lorsque nous savons implicitement en quoi consiste la relation d'équivalence dans un contexte donné[2]. Ainsi,

$$[x]_\sim =_{\text{déf}} \{\, y \in A \mid x \sim y \,\}.$$

L'ensemble $[x]_\sim$ (lequel est, par définition, un sous-ensemble de A) est appelé la *classe d'équivalence* de x.

Pour revenir à l'exemple du jeu de cartes, supposons que lors d'une certaine partie, on vous remet trois cartes. Alors, A pourrait être l'ensemble de toutes les façons dont on peut recevoir trois cartes (où $A\clubsuit\, K\spadesuit\, Q\heartsuit$ serait un élément différent de $K\spadesuit\, Q\heartsuit\, A\clubsuit$, disons) ; étant donné une main particulière x, par exemple $A\clubsuit\, K\spadesuit\, Q\heartsuit$, la classe d'équivalence serait alors

$$[A\clubsuit\, K\spadesuit\, Q\heartsuit] = \{A\clubsuit\, K\spadesuit\, Q\heartsuit,\ A\clubsuit\, Q\heartsuit\, K\spadesuit,\ K\spadesuit\, A\clubsuit\, Q\heartsuit,\ K\spadesuit\, Q\heartsuit\, A\clubsuit,\ Q\heartsuit\, A\clubsuit\, K\spadesuit,\ Q\heartsuit\, K\spadesuit\, A\clubsuit\,\}.$$

Ainsi, la classe d'équivalence correspond à l'ensemble de toutes les permutations de la main $A\clubsuit\, K\spadesuit\, Q\heartsuit$.

Voici un autre exemple : soit $A = \{a, b, c, d, e, f\}$, et considérons la relation d'équivalence

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

Nous avons alors

$$[a] = [b] = \{a, b\}, \qquad [c] = [d] = [e] = \{c, d, e\}, \qquad [f] = \{f\}.$$

Plusieurs autres exemples seront abordés dans la section suivante.

XIII.4 La fonction quotient canonique

Maintenant que nous avons défini les classes d'équivalence, nous pouvons les regrouper en un seul tout :

Définition XIII.4.1. Soit $\sim$ une relation d'équivalence sur l'ensemble A. Le *quotient* de A par $\sim$ est l'ensemble

$$A/{\sim} =_{\text{déf}} \{\, [x] \mid x \in A \,\}.$$

[2] Dans certains contextes, d'autres notations sont courantes ; en l'arithmétique modulaire, par exemple, la classe d'équivalence d'un entier n modulo p est dénotée $\overline{n}$.

En d'autres termes : $A/\sim$ est l'ensemble de toutes les classes d'équivalence de $\sim$. Notez qu'il s'agit d'un sous-ensemble de $\mathcal{P}(A)$, car tous les $[x]$ sont des sous-ensembles de A.

De quelle manière les ensembles A et $A/\sim$ sont-ils reliés l'un à l'autre ? À chaque élément $x \in A$, nous pouvons associer un élément $[x] \in A/\sim$. En fait, nous avons simplement une fonction

$$\pi : A \to A/\sim; \qquad \pi(x) = [x].$$

Cette fonction est appelée la *fonction quotient canonique* associée à la relation d'équivalence $\sim$. Cette terminologie est justifiée du fait que π est une fonction surjective : chaque $[x] \in A/\sim$ est de la forme $\pi(x)$. Aussi, cette fonction quotient donne un sens précis par lequel nous identifions les éléments équivalents de A.

Pour la dernière partie de cette section, nous revisitons les exemples de relations d'équivalence et nous expliquons en quoi consiste la fonction quotient dans chaque cas.

Exemples XIII.4.2.

1. Pour $A = \{*\}$, il n'y a rien à identifier : $[*] = \{*\}$, et $A/\sim = \{[*]\} = \{\{*\}\}$, lequel est à nouveau un ensemble avec un seul élément (un singleton). En termes informels, lorsque nous avons un singleton, il n'y a rien à identifier, et la fonction quotient devient une bijection.

2. Pour un ensemble arbitraire A et la relation identité $\Delta_A = \{(x, x) | x \in A\}$, nous avons $[x] = \{x\}$. Puis, $A/\sim = \{\{x\} | x \in A\}$, et la fonction quotient $\pi(x) = \{x\}$ est non seulement surjective, mais aussi injective.

3. Pour un ensemble arbitraire A et la relation maximale $\sim = A \times A$, nous avons $[x] = A$ pour tout $x \in A$. Ainsi, $A/\sim = \{A\}$, et la fonction quotient est $\pi(x) = A$ pour tout x.

4. Lorsque $\sim$ est la relation d'équivalence sur $\mathbb{R}$ donnée par

   $$x \sim y \Leftrightarrow |x| = |y|,$$

   nous obtenons $[x] = \{x, -x\}$. Ainsi, chaque classe (à l'exception de celle de 0) a précisément deux éléments.

5. Pour la relation d'équivalence sur $\mathbb{R}$ donnée par

   $$x \sim y \Leftrightarrow |x - y| \in \mathbb{N},$$

   nous obtenons $[x] = \{x + n | n \in \mathbb{Z}\}$. Ainsi, chaque classe d'équivalence contient une infinité d'éléments.

6. Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction. Définissons

   $$x \sim y \Leftrightarrow f(x) = f(y).$$

   Alors, $[x] = \{y \in \mathbb{R} | f(x) = f(y)\}$. Ainsi, la classe de x est l'ensemble de tous les éléments qui sont envoyés sur la même valeur que x en appliquant f.

7. Pour la relation d'équivalence sur l'ensemble $\mathbb{R} \times \mathbb{R}$ donnée par

   $$(u, v) \sim (x, y) \Leftrightarrow u^2 + v^2 = x^2 + y^2,$$

   la classe d'un point (x, y) est l'ensemble de tous les points qui se trouvent sur le même cercle (centré à l'origine) que (x, y). Ainsi, $(\mathbb{R} \times \mathbb{R})/\sim$ est l'ensemble de tous les cercles centrés à l'origine.

8. Finalement, considérons la relation d'équivalence sur $\mathbb{Z}$ donnée par

$$x \sim_n y \Leftrightarrow x - y \text{ est divisible par } n.$$

Alors, $[x] = \{x + kn | k \in \mathbb{Z}\}$. Il y a n classes d'équivalence : $[0]$, $[1]$, ..., $[n-1]$. (Vérifiez par vous-même que toutes ces classes sont distinctes, et que $[0] = [n]$, de telle sorte qu'il ne peut y avoir d'autres classes.) Travailler avec ces classes s'appelle *l'arithmétique modulo n*.

XIII.5 Sommaire

Nous avons introduit les *relations d'équivalence* comme étant des relations qui sont, à la fois, réflexives, symétriques et transitives. Étant donné une relation d'équivalence $\sim$ sur A, les constructions suivantes constituent les points focaux de notre attention :

- les *classes d'équivalence*, définies par $[x]_\sim = \{y | y \sim x\} \subseteq A$ pour $x \in A$, et
- la *fonction quotient canonique* de A vers l'ensemble $A/\sim = \{[x]_\sim | x \in A\}$.

La fonction quotient, laquelle est toujours surjective, nous permet d'identifier les éléments équivalents.

XIII.6 Exercices

Exercice 165. Soit A un ensemble non-vide, et R une relation univaluée sur A. La relation R peut-elle être réflexive ? irréflexive ? symétrique ? antisymétrique ? transitive ? Peut-elle être une relation d'équivalence ? Dans chaque cas, donnez un exemple aussi simple que possible, ou bien expliquez pourquoi c'est impossible.

Exercice 166. Même question, mais pour une relation totale.

Exercice 167. Même question, mais pour une relation fonctionnelle.

Exercice 168. Soit A l'ensemble de toutes les personnes. Quelles propriétés la relation « est un frère de » a-t-elle ? Qu'en est-il de « est un ancêtre de », et « est un enfant qui a un parent en commun avec » ?

Exercice 169. Soit $R \subseteq A \times A$ une relation sur A. Prouvez :

(a) R est réflexive si et seulement si $\Delta_A \subseteq R$.

(b) R est irréflexive si et seulement si $\Delta_A \cap R = \emptyset$.

(c) R est symétrique si et seulement si $R^\circ \subseteq R$ si et seulement si $R \subseteq R^\circ$ si et seulement si $R = R^\circ$.

(d) R est antisymétrique si et seulement si $R \cap R^\circ \subseteq \Delta_A$.

(e) R est transitive si et seulement si $R \circ R \subseteq R$.

Exercice 170. Les relations transitives satisfont-elles nécessairement $R \circ R = R$? Donnez une preuve ou bien un contre-exemple. Qu'en est-il des relations d'équivalence ?

Exercice 171. Soit $A = \{a, b, c, d, e\}$ et considérez la relation

$$R = \Delta_A \cup \{(a, e), (e, a), (c, b), (b, c)\}.$$

Vérifiez que R est une relation d'équivalence. Décrivez toutes les classes d'équivalence. Combien y a-t-il de classes d'équivalence distinctes ? Décrivez la fonction quotient.

Exercice 172. Même question, mais pour la relation

$$S = R \cup \{(a, b), (b, a), (a, c), (c, a), (c, e), (e, c), (b, e), (e, b)\}.$$

Exercice 173. Supposons que j'ai un ensemble avec une relation d'équivalence dessus. Je vous dis ensuite qu'il y a précisément une classe d'équivalence pour celle-ci. Que pouvez-vous conclure à propos de cette relation d'équivalence ?

Exercice 174. Considérez la relation suivante sur $A = \mathbb{Z} \times \mathbb{Z}$:

$$(x, y) \sim (u, v) \Leftrightarrow x + y = u + v.$$

Prouvez qu'il s'agit d'une relation d'équivalence. Décrivez toutes les classes d'équivalence.

Exercice 175. Soit $p : \mathbb{N} \to \{0, 1\}$ la fonction caractéristique des nombres pairs, i.e. $p(x) = 1$ si x est pair et $p(x) = 0$ si x est impair. Posons

$$x \sim y \Leftrightarrow p(x) = p(y).$$

Prouvez que $\sim$ est une relation d'équivalence. Décrivez toutes les classes d'équivalence. Quel est l'ensemble $\mathbb{N}/\sim$?

Exercice 176. Posons $\mathsf{sng} : \mathbb{Z} \to \{1, 0, -1\}$ comme étant la fonction signe, i.e. la fonction qui donne 1 si l'entrée est un nombre positif, 0 si l'entrée est 0 et -1 si l'entrée est un nombre négatif. Définissons une relation d'équivalence sur $\mathbb{Z}$ par $x \sim y \Leftrightarrow \mathsf{sgn}(x) = \mathsf{sgn}(y)$.

Prouvez qu'il s'agit bien d'une relation d'équivalence. Décrivez toutes les classes d'équivalence. Quel est le quotient $\mathbb{Z}/\sim$?

Exercice 177. Supposons que R et S sont deux relations d'équivalence sur un ensemble A.

1. Prouvez que $R \cap S$ est également une relation d'équivalence.
2. Prouvez que $R \cup S$ n'est pas toujours une relation d'équivalence.
3. $R \circ S$ est-elle une relation d'équivalence ?
4. Supposons que $R \circ S = S \circ R$. Prouvez que $R \circ S$ est une relation d'équivalence.

Exercice 178. Supposons que R et S sont toutes les deux des relations d'équivalence sur A et que $R \subseteq S$. Prouvez qu'il existe une fonction unique $\phi : A/R \to A/S$ telle que la composée $A \to A/R \to A/S$ est égale à la fonction quotient $A \to A/S$.

Exercice 179. Considérons l'ensemble $\mathsf{Fun}(\mathbb{N}, \mathbb{N})$ des fonctions allant de l'ensemble des nombres naturels vers lui-même. Définissons une relation R sur cet ensemble par

$$f R g \iff_{\text{déf}} f(x) \neq g(x) \text{ pour au plus un } x \in \mathbb{N}.$$

C'est-à-dire, deux fonctions sont équivalentes lorsqu'elles diffèrent en au plus un argument. S'agit-il d'une relation d'équivalence ?

LEÇON XIV

PARTITIONS

Nous avons appris qu'une relation d'équivalence $\sim$ sur un ensemble A donne lieu à des classes d'équivalence $[x] = \{\, y \,|\, y \sim x \,\}$. De plus, ces classes d'équivalence sont des sous-ensembles de A, lesquels constituent les éléments de l'ensemble quotient $A/\!\sim$. Dans cette leçon, nous investiguons de plus près les ensembles de la forme $A/\!\sim$. Nous allons démontrer, comme résultat principal, que les relations d'équivalence sur un ensemble A correspondent, en vérité, aux partitions de A.

XIV.1 DÉFINITION

Nous débutons avec un petit exemple pour illustrer le concept de partition. Considérons l'ensemble A tel que représenté sur la gauche dans la figure XIV.1, et la relation d'équivalence $\sim$ qui lui est associée.

Il est clair, d'après l'image, que les éléments de A qui font partie de la même classe d'équivalence sont connectés par des flèches ; ceux qui ne sont pas équivalents (i.e. qui appartiennent à des classes

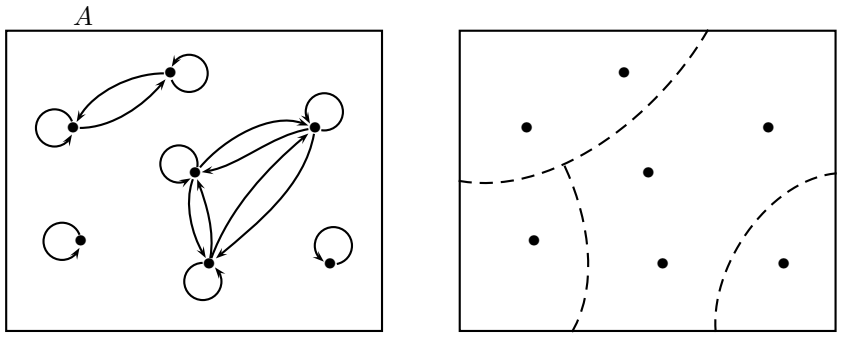


FIGURE XIV.1 – Une relation d'équivalence et la partition correspondante

d'équivalence distinctes) ne sont pas connectés. Sur la droite, il est indiqué comment les classes d'équivalence partitionnent l'ensemble en quatre sous-ensembles. Notez que les deux images en question contiennent la même information, mais la représentent d'une manière différente.

La collection des quatre sous-ensembles dans l'image de droite a trois caractéristiques importantes : premièrement, aucun des sous-ensembles n'est vide. Deuxièmement, aucun des sous-ensembles ne se chevauchent, i.e. les sous-ensembles sont *deux à deux disjoints*. Et troisièmement, chaque élément de A se trouve dans un de ces sous-ensembles : on exprime ceci en disant que les sous-ensembles forment un *recouvrement* de l'ensemble A. Nous formalisons maintenant ces propriétés en une définition :

Définition XIV.1.1. Soit A un ensemble et soit $\mathcal{U}$ une collection de sous-ensembles de A (i.e. $\mathcal{U} \subseteq \mathcal{P}(A)$). On dit que $\mathcal{U}$ est une *partition* de A lorsque :

- Chaque $U \in \mathcal{U}$ est non vide.
- Pour tout $U, V \in \mathcal{U}$: $U \neq V$ implique $U \cap V = \emptyset$ (les éléments de $\mathcal{U}$ sont deux à deux disjoints).
- Pour tout $x \in A$, il existe un $U \in \mathcal{U}$ tel que $x \in U$ (les éléments de $\mathcal{U}$ recouvrent A).

Intuitivement, une partition de A divise A en « compartiments ». Tout d'abord, nous étudions quelques exemples de partitions ; nous reviendrons sur la connexion que ces dernières partagent avec les relations d'équivalence dans la prochaine section.

Exemples XIV.1.2.

1. Pour n'importe quel ensemble A, nous avons que la collection $\mathcal{U} = \{\, \{x\} \mid x \in A \,\}$ est une partition de A. C'est la partition la *plus fine* de A.
2. À l'extrême opposé, nous avons la partition $\mathcal{U} = \{A\}$ de A. Il s'agit de la partition la *moins fine* de A.
3. La collection $\{\text{pair}, \text{impaire}\}$ est une partition de $\mathbb{Z}$.
4. La collection d'ensembles $\{\, C_r \mid r \geq 0 \,\}$, où $C_r = \{\, (x, y) \mid x^2 + y^2 = r \,\}$ est une partition de $\mathbb{R}^2$. (Elle partitionne le plan réel en cercles concentriques.)

XIV.2 Des relations d'équivalence vers les partitions

L'exemple donné au début de cette leçon illustre comment une relation d'équivalence donne lieu à une partition. En fait, nous avons déjà vu en quoi consiste cette partition, car celle-ci n'est nulle autre que l'ensemble $A/\!\sim$, le quotient de A par la relation d'équivalence $\sim$. La proposition suivante formalise cette idée.

Proposition XIV.2.1. *Soit $\sim$ une relation d'équivalence sur un ensemble A. Alors, $A/\!\sim$ est une partition de A.*

Démonstration. Nous devons montrer que $\{ [x]_\sim \mid x \in A \}$ est une partition de A.

Premièrement, notons que $x \in [x]$ (car $\sim$ est réflexive). Donc, tout $[x]$ est non vide.

Deuxièmement, supposons que nous avons $[x], [y]$ avec $[x] \neq [y]$. Nous avons alors $x \not\sim y$ (sinon $x \sim y$ nous donne $[x] = [y]$). Maintenant, si nous avions $z \in [x] \cap [y]$, nous aurions $z \sim x$ et $z \sim y$. Mais puisque $\sim$ est symétrique et transitive, ceci forcerait $x \sim y$. Contradiction. Ainsi, $[x] \cap [y] = \emptyset$.

Finalement, les ensembles $[x]$ recouvrent A car, pour tout $x \in A$, nous avons $x \in [x]$. □

XIV.3 Des partitions vers les relations d'équivalence

Supposons maintenant que nous commençons avec une partition $\mathcal{U}$ de l'ensemble A. Nous voulons transformer cette dernière en une relation d'équivalence sur A. Quelle devrait être cette relation ? La partition nous dit : deux éléments de A devraient être équivalents lorsqu'ils appartiennent à la même partie de la partition. Essayons cela :

$$x \sim_{\mathcal{U}} y \Leftrightarrow \exists U \in \mathcal{U}. x \in U \wedge y \in U.$$

Nous appelons ceci la relation d'équivalence *induite* par la partition $\mathcal{U}$. Bien entendu, nous devons démontrer qu'il s'agit effectivement d'une relation d'équivalence.

Proposition XIV.3.1. *Lorsque $\mathcal{U}$ est une partition de A, la relation $\sim_{\mathcal{U}}$ induite sur A est une relation d'équivalence.*

Démonstration. Premièrement, démontrons que $\sim_{\mathcal{U}}$ est réflexive. Donc, considérons un $x \in A$ arbitraire. Pour démontrer que $x \sim_{\mathcal{U}} x$, nous devons trouver un $U \in \mathcal{U}$ tel que $x \in U$. Mais puisque $\mathcal{U}$ recouvre A, l'existence d'un tel U est garantie.

Deuxièmement, nous devons démontrer que $\sim_{\mathcal{U}}$ est symétrique. Ceci est trivial : s'il existe un $U \in \mathcal{U}$ tel que $x \in U$ et $y \in U$, alors nous avons $y \in U$ et $x \in U$ pour ce même U.

Finalement, pour prouver que $\sim_{\mathcal{U}}$ est transitive, supposons que nous avons $x \sim_{\mathcal{U}} y$ et $y \sim_{\mathcal{U}} z$. Alors, il existe un $U \in \mathcal{U}$ tel que $x, y \in U$, et il existe un $V \in \mathcal{U}$ tel que $y, z \in V$. Ceci veut dire que $z \in U \cap V$. Puisque les éléments de $\mathcal{U}$ sont deux à deux disjoints, il s'ensuit que $U = V$. Ainsi, nous avons $x, z \in U$, et donc $x \sim_{\mathcal{U}} z$. □

Pour conclure les discussions menées jusqu'ici : chaque relation d'équivalence sur A donne lieu à une partition de A, et réciproquement, toute partition de A donne lieu à une relation d'équivalence sur A. Nous sommes maintenant dans une position où nous pouvons prouver le résultat important suivant :

Théorème XIV.3.2. *Il y a une correspondance bijective entre l'ensemble des relations d'équivalence sur A et l'ensemble des partitions sur A.*

Pour effectuer la preuve, nous utilisons la notation suivante : nous écrivons $\mathbf{EqRel}(A)$ pour dénoter l'ensemble des relations d'équivalence sur A ; tandis que $\mathbf{Part}(A)$ dénotera l'ensemble des partitions sur A

Démonstration. Nous devons maintenant montrer que $\mathbf{EqRel}(A) \cong \mathbf{Part}(A)$. Ainsi, nous devons construire une bijection entre ces ensembles. Nous avons déjà défini, dans les deux sections antécédentes, les fonctions que nous avons à l'esprit :

$$\Phi : \mathbf{EqRel}(A) \to \mathbf{Part}(A); \qquad \Phi(R) = \{\, [x]_R \mid x \in A \,\}$$

et

$$\Psi : \mathbf{Part}(A) \to \mathbf{EqRel}(A); \qquad \Psi(\mathcal{U}) = \sim_{\mathcal{U}} .$$

Il ne reste qu'à démontrer que les fonctions en question sont des inverses l'une de l'autre.

Premièrement, pour démontrer $\Phi \circ \Psi = 1_{\mathbf{Part}(A)}$, considérons une partition $\mathcal{U}$ de A. Nous avons que $\Psi(\mathcal{U})$ est la relation $\sim_{\mathcal{U}}$, donc $\Phi(\Psi(\mathcal{U}))$ est la partition associée à $\sim_{\mathcal{U}}$. Mais alors,

$$[x]_{\sim_{\mathcal{U}}} = \{\, y \mid y \sim_{\mathcal{U}} x \,\} = \{\, y \mid \exists U \in \mathcal{U}.y, x \in U \,\} = U.$$

Ainsi, chaque classe $[x]_{\sim_{\mathcal{U}}}$ est un membre de $\mathcal{U}$. Réciproquement, étant donné $U \in \mathcal{U}$, prenons un $x \in U$; puis, un raisonnement similaire nous donne $U = [x]_{\sim_{\mathcal{U}}}$. Ainsi, $\mathcal{U} = \{\, [x]_{\sim_{\mathcal{U}}} \mid x \in A \,\} = \Phi(\Psi(\mathcal{U}))$.

Deuxièmement, pour démontrer $\Psi \circ \Phi = 1_{\mathbf{EqRel}(A)}$, considérons une relation d'équivalence $\sim$ sur A. Alors, la relation d'équivalence $\Psi(\Phi(\sim))$ a la propriété que

$$(x, y) \in \Psi(\Phi(\sim)) \quad \Leftrightarrow \quad \exists U \in \Phi(\sim).(x, y \in U) \quad \Leftrightarrow \quad \exists [z] \in A/\sim .(x, y \in [z]) \quad \Leftrightarrow \quad x \sim y$$

La dernière étape découle du fait que $x, y \in [z]$ implique $x \sim z$ et $y \sim z$. □

XIV.4 Sommaire

Nous avons introduit une *partition* comme étant une collection de sous-ensembles non vides qui sont deux à deux disjoints et qui forment un recouvrement. La correspondance entre les partitions et les relations d'équivalence comporte deux aspects :

- Toute relation d'équivalence $\sim$ sur A donne lieu à une partition sur l'ensemble A, c'est-à-dire $A/\sim$.
- Toute partition $\mathcal{U}$ sur A donne lieu à une relation d'équivalence sur A, laquelle est régie par $x \sim_{\mathcal{U}} y \Leftrightarrow \exists U \in \mathcal{U}.(x, y \in U)$.

Ces deux constructions sont des inverses mutuels au sens que, pour un ensemble A fixé, elles définissent une correspondance bijective entre l'ensemble des relations d'équivalence sur A et l'ensemble des partitions sur A.

XIV.5 Exercices

Exercice 180. Soit $A = \{a, b, c, d\}$. Trouvez toutes les partitions possibles de A.

Exercice 181. Pour chaque partition de l'ensemble $A = \{a, b, c, d\}$, trouvez la relation d'équivalence sur A correspondante.

Exercice 182. Démontrez que la collection $\{[n, n+1) | n \in \mathbb{Z}\}$ est une partition de $\mathbb{R}$.

Exercice 183. La collection $\{(-n, n) | n \in \mathbb{N}\}$ est-elle une partition de $\mathbb{R}$?

Exercice 184. Démontrez que pour tout ensemble A et tout sous-ensemble (strict) $U \subset A$, l'ensemble $\{U, U^c\}$ est une partition de A.

Exercice 185. Supposons que $f : \mathbb{R} \to \mathbb{R}$ est une fonction, et définissons

$$x \sim y \Leftrightarrow f(x) = f(y).$$

Donnez une description géométrique de la partition associée à cette relation en termes du graphe de f.

Exercice 186. Trouvez la partition associée à la relation d'équivalence sur $\mathbb{R}$ suivante :

$$x \sim y \Leftrightarrow |x - y| \in \mathbb{N}.$$

Exercice 187. En quoi consiste l'ensemble $\mathsf{Part}(\emptyset)$?

Exercice 188. Soit S, l'ensemble de tous les mots de longueur 4 qui emploient seulement des 0 et des 1. C'est-à-dire,

$$S = \{abcd | a, b, c, d \in \{0, 1\}\}.$$

(a) Listez tous les éléments de S.

(b) Considérez la relation sur S définie par $s \sim t$ si et seulement si s est une permutation de t. Démontrez que cette dernière est une relation d'équivalence sur S.

(c) Décrivez toutes les classes d'équivalence de $\sim$, et donnez la partition sur S qui lui est associée.

LEÇON XV

FAMILLES

Souvent, nous ne nous intéressons pas seulement à un ensemble spécifique, mais à une collection d'ensembles prise comme un tout. Dans ce cas, il est avantageux de formuler ce tout explicitement en employant des *familles d'ensembles*. Cette leçon introduit l'idée de base en ce qui a trait aux familles d'ensembles, et elle établit également des connexions avec les concepts étudiés lors de leçons antécédentes.

XV.1 INDEXATION

Nous débutons avec un exemple usuel de famille d'ensembles. Considérons l'intervalle fermé $[a, a+1] = \{\, x \in \mathbb{R} \mid a \leq x \leq a+1 \,\} \subseteq \mathbb{R}$, où $a \in \mathbb{Z}$ est un entier. Puisque nous pouvons considérer plusieurs valeurs pour a, nous avons en fait plusieurs ensembles, soit un pour chaque $a \in \mathbb{Z}$. On exprime ceci en disant que $[a, a+1]_{a\in\mathbb{Z}}$ est une *famille d'ensembles indexés par* $a \in \mathbb{Z}$, ou simplement par $\mathbb{Z}$.

Généralement, une famille d'ensembles est présentée comme une paire de données : premièrement, un ensemble I (appelé l'*ensemble d'indexation*, ou *index*) ; deuxièment, pour chaque $i \in I$, un ensemble A_i. Souvent, la notation $\mathcal{A} = (A_i)_{i\in I}$ est employée pour dénoter une telle famille. Il est important de remarquer que les ensembles A_i ne sont pas forcément tous distincts. De ce fait, une famille d'ensembles n'est pas la même chose qu'un ensemble d'ensembles !

Une intuition utile est qu'une famille d'ensembles s'apparente à un système d'archivage de dossiers : les éléments de l'index I agissent comme des étiquettes, et à chaque étiquette i est associé un ensemble A_i « entreposé sous cette étiquette ».

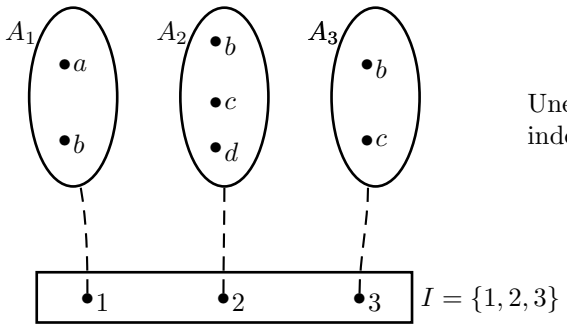


FIGURE XV.1 – Exemple de famille d'ensembles

Voici quelques exemples :

Exemples XV.1.1.

1. Considérez l'ensemble $I = \{1, 2, 3\}$ et les ensembles $A_1 = \{a, b\}, A_2 = \{b, c, d\}, A_3 = \{b, c\}$. Dans ce cas, la famille a trois membres. Notez que ceux-ci s'adonnent à être tous distincts, mais qu'ils se chevauchent. Une représentation imagée est donnée à la figure XV.1.

2. Dans notre terminologie, une famille d'ensembles indexée par $I = \{1, 2, \ldots, n\}$ consiste en n ensembles. En particulier, pour $n = 1$, la famille a un seul membre, tandis que pour $n = 0$, la famille est vide. (Ce qui n'est pas la même chose que la famille dont le seul membre est l'ensemble vide !)

3. Une *chaîne de bits* est une séquence finie de 0 et de 1. Par exemple, 101101000 est une chaîne de bits, de même que 0010. Chaque chaîne de bits a une *longueur*, c'est-à-dire le nombre de bits dans celle-ci. Écrivons B_n pour dénoter l'ensemble des chaînes de bits de longueur n. Nous obtenons une famille d'ensembles (indexée par $\mathbb{N}$) : $(B_n)_{n\in\mathbb{N}}$.

4. Lorsque a est un nombre positif réel, nous pouvons considérer le cercle de rayon a, centré autour de l'origine, comme suit :
$$C_a = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = a^2\}.$$
Nous avons un tel cercle pour chaque a, et de fait, nous avons une famille $(C_a)_{a\in\mathbb{R}^+}$.

5. Lorsque I est un ensemble, et X un autre ensemble, nous pouvons considérer la famille $(X_i)_{i\in I}$, avec $X_i = X$ tout simplement. Ainsi, tous les membres de cette famille sont identiques. Une famille de ce genre est parfois dite *constante*.

6. Autre exemple extrême : pour n'importe quel ensemble I, nous avons la famille d'éléments de I donnée par $\{i\}_{i\in I}$.

Remarque XV.1.2. Techniquement, nous avons été un peu négligeant ici. Comment pouvons-nous inférer, à partir des axiomes de la théorie des ensembles, que les familles d'ensembles existent ? En portant plus d'attention à la façon dont nous avons introduit ces familles. Lorsque I est un ensemble d'indexation, et A un autre ensemble, alors nous pouvons considérer une fonction $I \to \mathcal{P}(A)$. Ceci revient à donner une famille (de sous-ensembles de A) indexée par I. Maintenant, pour garantir qu'une famille $(A_i)_{i\in I}$ (indexée par I) existe au sens général (c'est-à-dire que nous pouvons prouver son existence à partir des axiomes de la théorie des ensembles), il suffit de vérifier que chaque ensemble A_i peut être considéré comme un sous-ensemble de l'ensemble A (dont l'existence a été démontrée à priori).

XV.2 Unions et intersections

Nous avons considéré, antérieurement, les opérations booléennes sur des ensembles, et en particulier, l'union $A \cup B$ et l'intersection $A \cap B$. Nous avons également indiqué qu'au sens plus général, nous pouvons établir des unions n-aires $A_1 \cup \cdots \cup A_n$ et des intersections n-aires $A_1 \cap \cdots \cap A_n$. Il est maintenant possible de généraliser ces opérations finies á des opérations sur des familles arbitraires d'ensembles.

Définition XV.2.1. Soit $\mathcal{A} = (A_i)_{i \in I}$, une famille d'ensembles. Nous définissons l'*union* de $\mathcal{A}$ comme étant l'ensemble

$$\bigcup \mathcal{A} = \{\, x \mid \exists i \in I . x \in A_i \,\}$$

et l'*intersection* de $\mathcal{A}$ comme étant l'ensemble

$$\bigcap \mathcal{A} = \{\, x \mid \forall i \in I . x \in A_i \,\}.$$

En d'autres mots, un élément x est dans l'union de $\mathcal{A}$ précisément lorsqu'il appartient à au moins un des membres A_i. Un élément x est dans l'intersection de $\mathcal{A}$ précisément lorsqu'il appartient à tous les membres A_i. Remarquez que $\mathcal{A}$ est une *famille* d'ensembles, alors que $\bigcup \mathcal{A}$ (tout comme $\bigcap \mathcal{A}$) est un ensemble ordinaire.

Nous pouvons aussi employer les notations $\bigcup_{i \in I} A_i$ et $\bigcap_{i \in I} A_i$ pour désigner, respectivement, l'union et l'intersection de $\mathcal{A}$.

Exemples XV.2.2.

1. Considérez l'ensemble $I = \{1, 2, 3\}$ et les ensembles $A_1 = \{a, b\}, A_2 = \{b, c, d\}, A_3 = \{b, c\}$. Alors, $\bigcup_{i \in I} A_i = \{a, b, c, d\}$ et $\bigcap_{i \in I} A_i = \{b\}$.
2. Considérez la famille $(A_n)_{n \in \mathbb{N}}$ de sous-ensembles de la ligne des réels avec $A_n = [-n, n]$. Alors, $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{R}$ et $\bigcap_{n \in \mathbb{N}} A_n = \{0\}$.
3. Lorsque $X_i = X$ est une famille constante sur I, nous avons $\bigcup_{i \in I} X_i = X = \bigcap_{i \in I} X_i$.

Le lemme qui suit met en valeur, pour les unions et les intersections, quelques propriétés auxquelles nous allons faire appel dans la section suivante.

Lemme XV.2.3. *Soit $(A_i)_{i \in I}$, une famille d'ensembles.*

- $\bigcap_{i \in I} A_i \subseteq A_i$ *pour tout* $i \in I$.
- *Lorsque B est un ensemble tel que $B \subseteq A_i$ pour tout i, alors $B \subseteq \bigcap_{i \in I} A_i$.*
- $A_i \subseteq \bigcup_{i \in I} A_i$ *pour tout* $i \in I$.
- *Lorsque B est un ensemble tel que $A_i \subseteq B$ pour tout $i \in I$, alors $\bigcup_{i \in I} A_i \subseteq B$.*

Exercice 189. Prouvez ces énoncés.

Les unions et les intersections satisfont des propriétés algébriques en commun avec leur contreparties finies. Pour la plupart, ces propriétés sont telles que nous les aurions imaginées, mais il y a tout de même quelques différences. Un des faits importants est que nous pouvons toujours appliquer une version de la loi de distributivité :

Lemme XV.2.4. *Lorsque $(A_i)_{i\in I}$ est une famille d'ensembles, et B un ensemble, nous avons*

$$B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I} (B \cap A_i).$$

Démonstration. Nous effectuons une preuve en employant la logique des prédicats :

$$\begin{aligned} x \in B \cap \bigcup_{i\in I} A_i &\leftrightarrow x \in B \wedge x \in \bigcup_{i\in I} A_i \\ &\leftrightarrow x \in B \wedge \exists i. x \in A_i \\ &\leftrightarrow \exists i. x \in B \wedge x \in A_i \\ &\leftrightarrow x \in \bigcup_{i\in I} (B \cap A_i) \end{aligned}$$

où la troisième étape fait appel à l'équivalence (de la logique des prédicats) $\exists i.(B \wedge A(i)) \equiv B \wedge \exists i.A(i)$ (cette dernière est permise lorsque i n'appartient pas à B). □

XV.3 Fermeture

Nous présentons une application de l'union et de l'intersection de familles à la théorie des relations d'équivalence. Comme vous le savez, le fait d'être une relation d'équivalence a quelque chose de particulier ; la plupart des relations ne sont certainement pas des relations d'équivalence. Supposons que nous ayons une relation R sur A qui n'est pas une relation d'équivalence. Y a-t-il une façon de forcer les choses et de modifier R pour que celle-ci en devienne une ? (Préférablement, de telle sorte que R demeure aussi intacte que possible.)

Ce que nous avons à l'esprit est illustré à la figure XV.2 : Sur la gauche, nous avons une relation R qui n'atteint pas le statut de relation d'équivalence (celle-ci n'est ni réflexive, ni symétrique, ni transitive). Et sur la droite, nous avons « fixé » R, puis ajouté toutes les flèches nécessaires pour obtenir une relation d'équivalence.

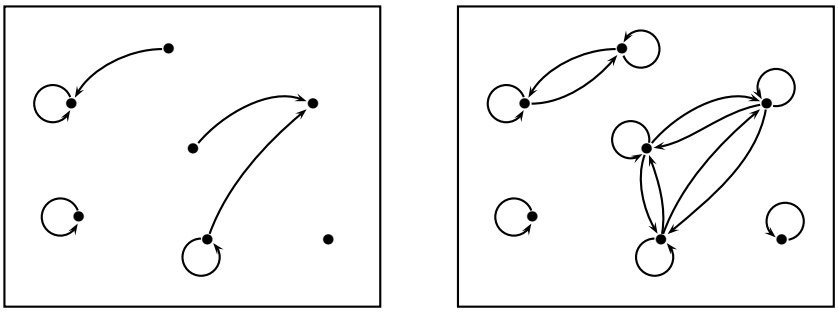


Figure XV.2 – Une relation R, et la relation d'équivalence qu'elle génère

Comment avons-nous procédé ? Étape 1 : pour rendre la relation réflexive, nous avons ajouté une boucle à chaque élément qui n'en a pas déjà. Étape 2 : pour la rendre symétrique, nous avons ajouté

une flèche de y vers x chaque fois qu'il y en a une de x vers y. Étape 3 : pour la rendre transitive, nous avons ajouté une flèche de x vers z chaque fois qu'il y en a une de x vers y et une de y vers z pour un certain y.

Une des complications avec cette procédure est que l'ajout de certaines flèches peut briser la transitivité et (ou) la symétrie. Ainsi, il ne suffit pas de rendre la relation symétrique pour commencer, puis de rendre la relation résultante transitive par la suite ; le résultat pourrait ne pas être symétrique une fois de plus ! De même, en retournant à l'étape 2, il se pourrait que vous n'arriviez pas à une relation transitive, car l'ajout de flèches crée de nouveaux problèmes. Mais si cela se produisait, il suffirait de répéter les étapes 2 et 3, en alternant, jusqu'à ce que vous obteniez une relation à la fois symétrique et transitive (fort heureusement, la réflexivité n'est jamais perturbée).

Comment savons-nous si ce processus s'arrête éventuellement ? Et bien, dans l'exemple précédent, ceci se produit car il y a seulement un nombre fini d'éléments et, conséquemment, il ne peut y avoir qu'un nombre fini de flèches à rajouter. Or, généralement parlant, nous ne pouvons garantir que ce processus a une fin. Par exemple, considérons l'ensemble $\mathbb{N}$, et la relation $R = \{(x, x+1) | x \in \mathbb{N}\}$. En répétant l'étape 3, nous ajoutons toujours plus de flèches : tout d'abord $(x, x+2)$, puis $(x, x+3)$, et ainsi de suite. Ce processus se poursuit indéfiniment.

Voici le moment où les familles entrent en jeu. En premier lieu, remarquez que, si la seule chose qui nous préoccupait était de trouver une relation d'équivalence contenant R, alors la réponse serait simple : il suffirait de prendre la relation maximale. Or, nous voulons faire mieux que cela : nous voulons trouver la *plus petite* relation d'équivalence contenant R. Il convient de formaliser cette idée en une définition :

Définition XV.3.1. Étant donné une relation R sur A, la relation d'équivalence *générée par* R est définie comme étant la relation $\overline{R}$ sur A telle que

- $\overline{R}$ est une relation d'équivalence
- $R \subseteq \overline{R}$
- Pour toute relation d'équivalence S (sur A) contenant R, nous avons $\overline{R} \subseteq S$.

Ceci donne un sens précis à notre objectif de mettre en évidence une solution minimale ; les solutions paresseuses tel que la relation d'équivalence maximale sont exclues.

Proposition XV.3.2. *Pour toute relation R sur A, il existe une relation minimale (et nécessairement unique) générée par R.*

Démonstration. Premièrement, considérons la famille $\mathcal{A}$ de toutes les relations d'équivalence possibles sur A qui contiennent R. (Il s'agit effectivement d'une famille d'ensembles car toute relation d'équivalence sur A est un sous-ensemble de $A \times A$.)

Maintenant, considérons l'intersection de cette famille :

$$\overline{R} =_{\text{déf}} \bigcap \mathcal{A} = \bigcap \{\, S \mid S \text{ est une rel. d'équiv. telle que } R \subseteq S \,\}.$$

Observez que la famille $\mathcal{A}$ est non vide, car elle contient au moins la relation d'équivalence maximale $A \times A$. (Il semblerait que la solution paresseuse ait une utilité en fin de compte.)

Ensuite, nous avançons que ce $\overline{R}$ est effectivement la relation d'équivalence générée par R. Nous devons tout d'abord démontrer que $\overline{R}$ est bel et bien une relation d'équivalence :

- Réflexivité : étant donné $x \in A$, nous savons que $(x, x) \in S$ pour tout $S \in \mathcal{A}$, car tout $S \in \mathcal{A}$ est réflexif. Ainsi, $(x, x) \in \overline{R}$ également.
- Symétrie : supposons que $(x, y) \in \overline{R}$. Alors, $(x, y) \in S$ pour tout $S \in \mathcal{A}$. Il s'ensuit que $(y, x) \in S$ pour tout $S \in \mathcal{A}$ (car tout $S \in \mathcal{A}$ est symétrique). Ainsi, $(y, x) \in \mathcal{R}$ également.
- Transitivité : supposons que $(x, y) \in \overline{R}$ et que $(y, z) \in \overline{R}$. Alors, $(x, y) \in S$ et $(y, z) \in S$ pour tout $S \in \mathcal{A}$. Ceci nous donne $(x, z) \in S$ pour tout $S \in \mathcal{A}$ (par transitivité des S), et donc $(x, z) \in \overline{R}$.

Deuxièmement, nous devons démontrer que $R \subseteq \overline{R}$. Mais ceci découle simplement du lemme XV.2.3.

Et troisièmement, nous devons démontrer que, si S est une relation d'équivalence contenant R, alors $\overline{R} \subseteq S$. Mais si S est en effet une relation d'équivalence contenant R, alors $S \in \mathcal{A}$ par définition. Ainsi, (en appliquant le lemme XV.2.3 à nouveau) nous obtenons $\overline{R} \subseteq S$. □

XV.4 Sommaire

La raison principale pour laquelle nous étudions les *familles d'ensembles* est que, bien souvent, nous voulons considérer plusieurs ensembles en même temps ; et un grand nombre de constructions naturelles mènent à des ensembles indexés par d'autres ensembles. Lorsque $\mathcal{A} = (A_i)_{i \in I}$ est une famille d'ensembles, nous appelons I l'*ensemble d'indexation* (ou *index*). Il y a deux opérations importantes sur les familles :

- Union : $\bigcup_{i \in I} A_i = \{\, x \mid \exists i \in I . x \in A_i \,\}$
- Intersection : $\bigcap_{i \in I} A_i = \{\, x \mid \forall i \in I . x \in A_i \,\}$.

Les intersections peuvent être employées pour démontrer que, pour toute relation d'équivalence R sur A, il existe une *plus petite* relation d'équivalence contenant R, i.e. celle *générée par* R. Celle-ci peut être construite en prenant l'intersection de la famille de toutes les relations d'équivalence contenant R.

XV.5 Exercices

Exercice 190. Considérez la famille d'ensembles A_i, $i \in \{1, 2, 3\}$, donnée par

$$A_1 = \{1, 3, 5, 7, \ldots\}, \quad A_2 = \{\, n \in \mathbb{N} \mid n \text{ divise } 99 \,\}, \quad A_3 = \{\, p \in \mathbb{N} \mid p \text{ est premier} \,\}.$$

Trouvez $\bigcap_i A_i$ et $\bigcup_i A_i$.

Exercice 191. Quelles sont l'union et l'intersection de la famille $(-a, a)_{a \in \mathbb{N}}$? (Ici, (a, b) dénote un intervalle réel ouvert.)

Exercice 192. Même question, mais pour la famille $(a, a + 1)_{a \in \mathbb{Z}}$.

Exercice 193. Considérez la famille d'intervalles ouverts $(-1/n, 1/n)_{n \in \mathbb{N} - \{0\}}$. Quelle est l'union de cette famille ? Quelle est l'intersection ?

Exercice 194. Considérez la famille d'intervalles semi-ouverts $[0, \log_2 n)_{n\in\mathbb{N}-\{0\}}$. Quelle est l'union ? Et quelle est l'intersection ?

Exercice 195. Considérez la famille de relations $(R_c)_{n\in\mathbb{N}}$ sur $\mathbb{Z}$, définies par $a\,R_c\,b \Leftrightarrow a + c \leq b$. Décrivez quelques-uns des membres R_c appartenant à cette famille. Aussi, trouvez l'union et l'intersection.

Exercice 196. Considérez la relation $R \subseteq \mathbb{Z} \times \mathbb{Z}$ définie par $R(x, y) \Leftrightarrow y = x + 2012$. Trouvez la plus petite relation d'équivalence contenant R.

Exercice 197. Quelle est la plus petite relation d'équivalence sur $\mathbb{R}^2$ qui contient la relation $(x, y) \sim (u, v) \Leftrightarrow x^2 + y^2 \leq u^2 + v^2$?

Exercice 198. Trouvez la plus petite relation d'équivalence sur $\mathbb{R}$ qui contient la relation $x \sim y \Leftrightarrow x = -y$.

Exercice 199. Une *famille d'ensembles doublement indexée* consiste en des ensembles I, J et une famille d'ensembles $(A_{i,j})_{i\in I, j\in J}$ indexée par $I \times J$. Démontrez que pour une telle famille, nous avons

$$\bigcup_{i\in I}\bigcup_{j\in J} A_{i,j} = \bigcup_{j\in J}\bigcup_{i\in I} A_{i,j}.$$

Prouvez une formule similaire pour l'intersection.

Exercice 200. Considérez les ensembles $I = J = \mathbb{N} - \{0\}$ et la famille doublement indexée $A_{i,j} = \{\, x \in \mathbb{R} \mid \frac{1}{i} < x < j^2 \,\}$. Déterminez que

$$\bigcup_{i\in I}\bigcap_{j\in J} A_{i,j}, \qquad \text{et} \qquad \bigcap_{i\in I}\bigcup_{j\in j} A_{i,j}.$$

LEÇON XVI

FIBRES

Cette leçon étudie une approche particulièrement importante pour obtenir des familles d'ensembles, notamment par l'intermédiaire des fonctions.

XVI.1 IMAGE DIRECTE ET IMAGE INVERSE

Avant d'expliquer en quoi consiste les fibres, nous commençons par étudier un phénomène plus général en ce qui a trait aux fonctions. Fixons une fonction $f : A \to B$. Comme vous le savez, f relie les éléments de A aux éléments de B. Mais, est-il également possible de relier les sous-ensembles de A aux sous-ensembles de B en employant f ?

Supposons que $U \subseteq A$ est un sous-ensemble de A. Nous pouvons appliquer f sur chacun des éléments de U ; ceci nous donne un ensemble d'éléments de B. (Voir la figure XVI.1 pour un exemple.)

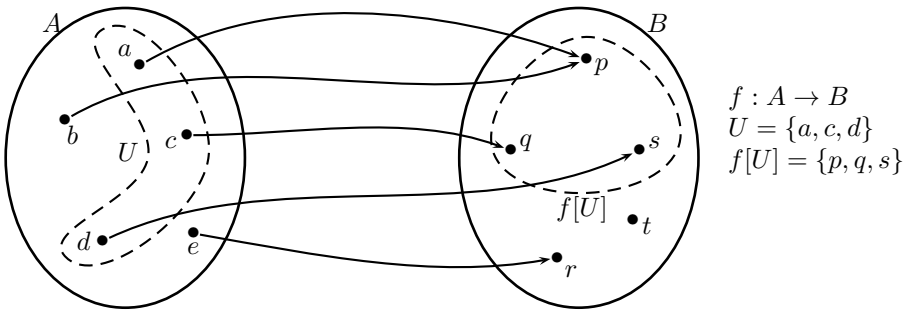


FIGURE XVI.1 – Image directe de U par f

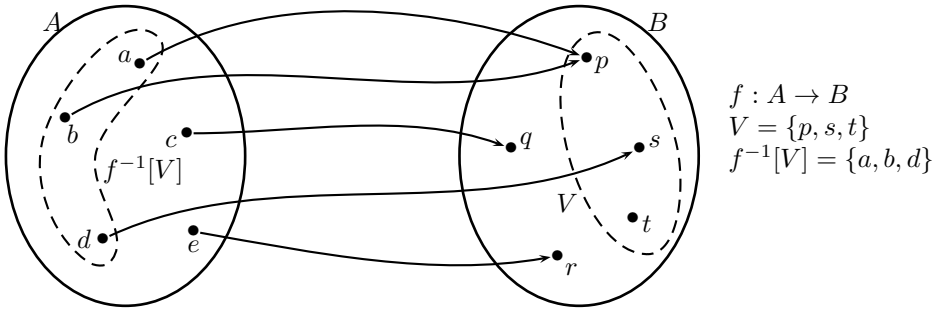


FIGURE XVI.2 – Image inverse de V par f

Définition XVI.1.1 (Image directe)**.** Étant donné $f : A \to B$ et un sous-ensemble $U \subseteq A$, l'*image directe* de U par f est

$$f[U] =_{\text{déf}} \{\, f(x) \,|\, x \in U \,\} \subseteq B.$$

Par exemple, pour $f : \mathbb{R} \to \mathbb{R}$ avec $f(x) = x^2 + 1$ et U, l'intervalle fermé $[-2, 1]$, nous avons $f[U] = [1, 5]$.

Nous pouvons également aller dans l'autre direction : étant donné un sous-ensemble V de B, nous pouvons considérer tous les éléments de A qui sont associés à des éléments de V à travers f. Ceci est illustré à la figure XVI.2

Définition XVI.1.2 (Image inverse)**.** Étant donné $f : A \to B$ et un sous-ensemble $V \subseteq B$, l'*image inverse* de V par f est

$$f^{-1}[V] = \{\, x \in A \,|\, f(x) \in V \,\}.$$

Par exemple, pour $f : \mathbb{R} \to \mathbb{R}$ avec $f(x) = x^2 + 1$ et $V = \{0, 1\}$, nous avons $f^{-1}[V] = \{0\}$, car il n'y a que $f(0) = 1$ (avec $f(x) = 1$) et il n'y pas de $x \in \mathbb{R}$ tel que $f(x) = 0$. Lorsque W est l'intervalle fermé $[-2, 3]$, nous avons $f^{-1}[W] = [-\sqrt{2}, \sqrt{2}]$.

Avertissement : La notation $f^{-1}[V]$ n'est *pas* employée ici pour sous-entendre l'existence d'un inverse (une fonction inverse) de f ! Les constructions de l'image directe et de l'image inverse sont admissibles, peu importe la fonction f considérée (pas seulement pour les bijections).

XVI.2 Fibres d'une fonction

Le concept d'image inverse d'un sous-ensemble par une fonction comporte un cas important à considérer :

Définition XVI.2.1 (Fibre)**.** Soit $f : A \to B$ une fonction et $b \in B$. La *fibre* de f en b est

$$f^{-1}(b) = f^{-1}[\{b\}] = \{x \in A | f(x) = b\}.$$

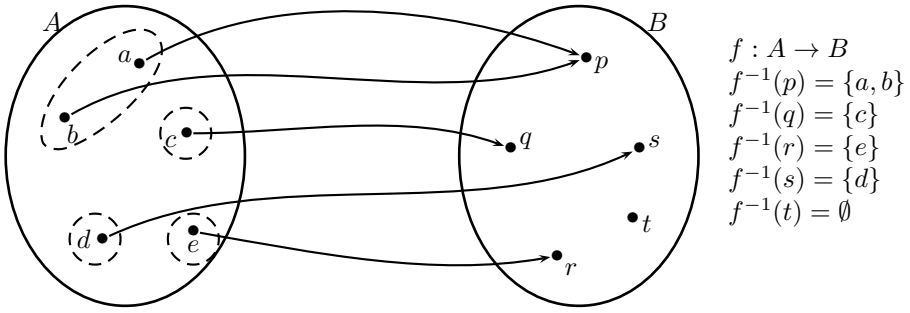


FIGURE XVI.3 – Les fibres d'une fonction f.

Ceci est illustré à la figure XVI.3. Notez que la fibre d'un élément peut être vide. Notez aussi que deux éléments $x, x' \in A$ appartiennent à la même fibre précisément lorsque $f(x) = f(x')$. Ceci veut dire qu' « appartenir à la même fibre de f » est une relation d'équivalence sur A.[1]

L'exercice suivant nous indique comment certaines propriétés d'une fonction f peuvent être traduites en des propriétés sur les fibres de f.

Exercice 201. Soit $f : A \to B$ une fonction. Alors,

1. f est injective si et seulement si chaque fibre a au plus un élément.
2. f est surjective si et seulement si chaque fibre a au moins un élément.
3. f est bijective si et seulement si chaque fibre a précisément un élément.

Nous pouvons organiser les choses un peu différemment. Pour chaque élément $y \in B$, nous avons un ensemble $f^{-1}(b)$. Ainsi, nous avons une famille d'ensembles $(f^{-1}(y))_{y \in B}$. La première observation à faire est la suivante :

Proposition XVI.2.2. *Lorsque $f : A \to B$ est surjective, la famille $(f^{-1}(y))_{y \in B}$ constitue une partition de A.*

Démonstration. Premièrement, en raison de l'exercice précédent, les fonctions surjectives ont des fibres non vides. Deuxièmement, étant donné deux fibres $f^{-1}(y)$ et $f^{-1}(y')$, si $z \in f^{-1}(y)$ et $z \in f^{-1}(y')$, alors $f(z) = y$ et $f(z) = y'$, et donc $y = y'$. Ceci veut dire que les fibres sont disjointes. Troisièmement, étant donné $x \in A$, nous avons $x \in f^{-1}(f(x))$, donc les fibres recouvrent A. □

XVI.3 Représentation de familles avec des fibres

Dans la section précédente, nous avons commencer avec une fonction, puis nous avons démontré comment cette information peut être interprétée pour donner une famille d'ensembles, notamment, à travers les fibres d'une fonction. Dans cette section, nous procédons dans l'autre sens : en commençant

[1] En fait, nous avons déjà vu que toute fonction $f : A \to B$ donne lieu à une relation d'équivalence sur A définie par $x \sim x' \Leftrightarrow f(x) = f(x')$.

avec une famille d'ensembles, nous voulons démontrer qu'une telle famille peut être interprétée comme une fonction.

Tout d'abord, posons $(A_i)_{i\in I}$, une famille d'ensembles. Nous voulons remballer cette information sous la forme d'une fonction $f : A \to B$, où A, B sont des ensembles convenablement choisis. En nous référant à la représentation (d'ordre général) d'une famille d'ensembles de la figure XV.1, nous pouvons concevoir que $B = I$ est sans doute un bon choix. Qu'en est-il de A à présent ? Nous devons regrouper tous les ensembles A_i en un grand ensemble A formant un seul tout. S'agit-il de $\bigcup_{i\in I}(A_i)$? Le problème est que les ensembles A_i pourraient se chevaucher, ou que certains d'entre eux pourraient être vides. Dans ce cas, nous perdons de l'information en formant l'union.

Le truc est d'opter pour le *coproduit* (somme) des A_i à la place. Ceci s'accomplit (comme dans le cas particulier de la somme de deux ensembles $X + Y$) en attachant des étiquettes aux éléments, pour nous rappeler à quel ensemble chacun appartenait originellement. Ceci nous mène à :

Définition XVI.3.1 (Coproduit d'une famille)**.** Soit $(A_i)_{i\in I}$ une famille d'ensembles. Le *coproduit* de la famille est

$$\coprod_{i\in I} A_i =_{\text{déf}} \{\, (x, i) \,|\, x \in A_i \,\}.$$

Maintenant, en présence d'un élément (x, i) du coproduit, nous pouvons immédiatement dire de quel ensemble A_i il provient.

Exemple XVI.3.2. (Cf. figure XV.1.) Le coproduit de la famille avec $A_1 = \{a, b\}, A_2 = \{b, c, d\}, A_3 = \{b, c\}$ est l'ensemble

$$\coprod_{i\in\{1,2,3\}} A_i = \{(a, 1), (b, 1), (b, 2), (c, 2), (d, 2), (b, 3), (c, 3)\}.$$

Avec les ensembles $A = \coprod_{i\in I} A_i$ et $B = I$ en main, il ne reste qu'à préciser une fonction de $A \to I$. Mais ceci est évident à ce stade : nous posons $f(x, i) = i$, i.e. nous envoyons un élément sur l'étiquette de l'ensemble auquel il appartient.

Et finalement, en quoi consistent les fibres de cette nouvelle fonction f ? Pour un élément $i \in I$, nous avons $f(x, j) = i \Leftrightarrow i = j$, donc $f^{-1}(i) = \{\, (x, i) \,|\, x \in A_i \,\}$. Ce dernier n'est pas littéralement le même ensemble que A_i, car nous y avons attaché des étiquettes. Toutefois, il y a une bijection évidente entre les deux :

$$\phi : A_i \to f^{-1}(i); \qquad \phi(x) = (x, i).$$

Ceci démontre :

Proposition XVI.3.3. *Toute famille $(A_i)_{i\in I}$ donne lieu à une fonction f pour laquelle $f^{-1}(i) \cong A_i$ pour tout $i \in I$.*

Je vous laisse le soin de réfléchir à la façon dont cette construction est reliée à celle de la section précédente.

XVI.4 Sommaire

À chaque fonction $f : A \to B$, nous pouvons associer deux opérations :

- *Image directe* : elle envoie un sous-ensemble $U \subseteq A$ sur $f[U] = \{f(x) | x \in A\}$
- *Image inverse* : elle envoie un sous-ensemble $V \subseteq B$ sur $f^{-1}[V] = \{x \in A | f(x) \in V\}$.

Un cas particulier survient lorsque $V = \{y\}$: nous obtenons la *fibre* de f en y, c'est-à-dire

- $f^{-1}(y) = \{\, x \in A \mid f(x) = y \,\}$.

Les faits importants sont les suivants :

- Les fibres $(f^{-1}(y))_{y \in B}$ forment une famille d'ensembles indexée par B.
- Lorsque f est une fonction surjective, cette famille forme une partition de A (sinon, les fibres non vides forment une partition).
- Étant donné une famille $(A_i)_{i \in I}$, il y a une fonction $f : \coprod_{i \in I} A_i \to I$ telle que $f^{-1}(i) \cong A_i$.

Le dernier fait énonce qu'*à isomorphisme près*, toute famille d'ensembles est la famille de fibres d'une certaine fonction.

XVI.5 Exercices

Exercice 202. Soient $A = \{0, 1, 2, 3, 4\}, B = \{5, 6, 7, 8\}$ et posons f définie par $f(0) = 7, f(1) = f(4) = 6, f(2) = f(3) = 8$. Trouvez l'image directe par f des ensembles $U_0 = \emptyset, U_1 = \{0\}, U_2 = \{0, 1\}, U_3 = \{0, 1, 2\}, U_4 = \{1, 4\}, U_5 = \{0, 1, 2, 3, 4\}$. Aussi, trouvez l'image inverse par f des ensembles $V_0 = \emptyset, V_1 = \{5\}, V_2 = \{5, 6\}, V_3 = \{6, 7\}, V_4 = \{7, 8\}, V_5 = \{6, 7, 8\}$.

Exercice 203. Considérez la fonction $f(x) = x^2$ allant des réels vers les réels. Décrivez les fibres de cette fonction. Déterminez également l'image inverse de l'ensemble $(-2, 1]$. Idem pour $[-1, 2)$.

Exercice 204. Pour une fonction $f : A \to B$, démontrez que $U \subseteq U'$ implique $f[U] \subseteq f[U']$.

Exercice 205. Pour une fonction $f : A \to B$, démontrez que $V \subseteq V'$ implique $f^{-1}[V] \subseteq f^{-1}[V']$.

Exercice 206. Donnez un exemple de fonction $f : \mathbb{R} \to \mathbb{R}$ pour laquelle toutes les fibres sont infinies.

Exercice 207. Considérez une fonction $f : \mathbb{Z} \to \mathbb{Z}$ définie par $f(x) = x + 2$. Trouvez tous les sous-ensembles $U \subseteq \mathbb{Z}$ pour lesquels $f[U] = U$.

Exercice 208. Supposons que $f : A \to B$ est une fonction constante (au sens que $f(x) = f(y)$ pour tout $x, y \in A$). Prouvez que f a au plus une fibre non vide. La réciproque est-elle vraie ?

Exercice 209. Soit $f : A \to B$ une fonction. Prouvez ou réfutez : $f[U^c] = f[U]^c$.

Exercice 210. Soit $f : A \to B$ une fonction. Prouvez ou réfutez : $f[U \cap U'] = f[U] \cap f[U']$.

Exercice 211. Soit $f : A \to B$ une fonction. Prouvez ou réfutez : $f[U \cup U'] = f[U] \cup f[U']$.

Exercice 212. Soit $f : A \to B$ une fonction. Prouvez ou réfutez : $f^{-1}[V^c] = f[V]^c$.

Exercice 213. Soit $f : A \to B$ une fonction. Prouvez ou réfutez : $f^{-1}[V \cap V'] = f^{-1}[V] \cap f^{-1}[V']$.

Exercice 214. Soit $f : A \to B$ une fonction. Prouvez ou réfutez : $f^{-1}[V \cup V'] = f^{-1}[V] \cup f^{-1}[V']$.

Exercice 215. Considérez la fonction $f : X \to Y$ avec $X = \{a, b, c\}, Y = \{p, q\}$ et $f(a) = f(b) = p, f(c) = q$. Combien de fibres y a-t-il ? Quelles sont-elles ? Quelle est la partition de X qui leur est associée ?

Exercice 216. Décrivez les fibres de la fonction identité sur un ensemble A.

Exercice 217. Rappelez-vous que, pour des ensembles A, B, il existe une *fonction de projection* $\pi_A : A \times B \to A$ définie par $\pi_A(a, b) = a$. Prouvez que, pour tout élément $a \in A$, nous avons $\pi_A^{-1}(a) \cong B$; c'est-à-dire, que toutes les fibres de π_A sont isomorphes à B.

Exercice 218. Considérez l'ensemble $I = \{1, 2, 3\}$ et les ensembles $A_1 = \{a, b\}, A_2 = \{b, c, d\}, A_3 = \{c\}$. Déterminez en quoi consiste l'ensemble $A = \{(a, i) | a \in A_i\}$ dans ce cas, et quelle est la fonction associée $f : A \to I$. Combien de fibres cette fonction a-t-elle ? Quelles sont ces fibres ?

Exercice 219. Considérez la famille $\{\{n - 1, n, n + 1\} | n \in \mathbb{Z}\}$ indexée par $\mathbb{Z}$. (Ainsi, tout membre a trois éléments.) Déterminez en quoi consiste la fonction correspondante. Quelles sont les fibres de cette dernière ?

Exercice 220. Trouvez une fonction $f : \mathbb{N} \to \mathbb{N}$ telle que, pour tout $n \in \mathbb{N}$, il existe une fibre de f avec exactement n éléments.

Exercice 221. Considérez la fonction quotient $\pi : \mathbb{Z} \to \mathbb{Z}/3$ pour la relation d'équivalence $x \sim_3 y \Leftrightarrow x - y$ est divisible par 3. Combien de fibres cette fonction a-t-elle ? Quelles sont ces fibres ?

Exercice 222. Soient $f : A \to B$ et $g : B \to C$ des fonctions. Démontrez que, pour tout $c \in C$, nous avons $(g \circ f)^{-1}(c) = \bigcup_{g(x)=c} f^{-1}(x)$.

LEÇON XVII

L'AXIOME DU CHOIX

Il y a plusieurs situations en mathématiques où nous savons qu'un certain ensemble est non vide, mais obtenir un élément concret de cet ensemble n'est pas toujours évident. Par exemple, considérez l'ensemble A des solutions à l'équation polynomiale $x^5 - 4x^4 - 2x^3 + x^2 - 8$. Nous savons que cet ensemble est non vide, mais trouver un élément de ce dernier s'avère plutôt compliqué.

Dans certains cas, il y a des solutions évidentes à ce type de « problème ». Par exemple, pour $A = \mathbb{N}$, nous pouvons certainement prendre un nombre naturel. Il y a en fait un choix *canonique* : il suffit de prendre 0 tout simplement, le premier nombre. Dans d'autres cas, il est nécessaire de mettre un peu plus de créativité à l'oeuvre. Si A est l'ensemble des nombres irrationnels entre 5 et 6, il n'y a pas de choix évident. Mais nous pourrions tout de même, par exemple, prendre le nombre $\pi + 2$. En général, toutefois, il se pourrait que nous n'ayons pas une description concrète des éléments de l'ensemble A, et ceci rendrait difficile la tâche d'arriver à un choix particulier d'élément.

Or, dans bien des cas, vous verrez des phrases telles que : « L'ensemble A est non vide ; soit x un élément de $A\ldots$ » Habituellement, le texte enchaînera avec une preuve d'un énoncé qui dépend de l'existence d'un tel x, mais sans exhiber une instance conrète de ce dernier. Le pire dans tout ça est que, dans bien des cas, la preuve ne fera pas uniquement un seul choix d'élément, mais une infinité de tels choix à la fois. Ceci soulève un questionnement : pouvons-nous supposer que de tels choix peuvent toujours être effectués sans conséquences, ou devrions-nous douter des preuves qui font appel à ces choix ?

L'axiome du choix (AC) aborde précisément ce problème : pouvons-nous toujours choisir des éléments dans des ensembles non vides, peu importe ce que nous savons à propos de ces ensembles ou de la façon dont ils nous sont présentés ?

XVII.1 Fonctions de choix

En fait, nous pouvons formuler un problème plus général : Étant donné un ensemble A, est-il possible, pour chaque sous-ensemble non vide U de A, de choisir un élément de U ? Une solution à ce problème est appelée une *fonction de choix* pour l'ensemble A. Techniquement, il s'agit d'une fonction

$$s : \mathcal{P}_+(A) \to A$$

assujettie à la condition que $s(U) \in U$ pour tout U. Ici, $\mathcal{P}_+(A)$ dénote l'ensemble des parties (sous-ensembles) non vides de A. La condition est là pour assurer que l'élément choisi pour U soit effectivement un élément de U.

Pour illustrer le concept d'une fonction de choix, considérez l'ensemble $A = \{a, b, c\}$. Alors,

$$\mathcal{P}_+(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Pour établir une fonction de choix pour A, nous devons choisir, pour chaque sous-ensemble non vide $U \in \mathcal{P}_+(A)$, un élément de ce sous-ensemble. Pour le sous-ensemble $\{a\}$, il n'y a pas grand choix à faire, car il y a un seul élément à choisir. Donc, nous devons poser $s(\{a\}) = a$. Similairement, nous devons poser $s(\{b\}) = b$ et $s(\{c\}) = c$. Ensuite, que pourrions-nous choisir pour $s(\{a, b\})$? Nous devons choisir soit a, soit b ici. Similairement, $s(\{b, c\})$ peut être égal à b ou à c. Et nous procédons ainsi pour le reste. Donc, un exemple de choix de fonction s pour A pourrait être

$$\begin{array}{lll} s(\{a\}) = a, & s(\{b\}) = b, & s(\{c\}) = c, \\ s(\{a, b\}) = a, & s(\{a, c\}) = c, & s(\{b, c\}) = c, \\ s(\{a, b, c\}) = c. & & \end{array}$$

Comme exercice, vous pourriez essayer de trouver une autre fonction de choix pour l'ensemble A (il y en a 24 au total).

Exercice 223. Essayez de trouver des fonctions de choix pour les ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$. (Indice : ne perdez pas trop de temps sur le dernier ensemble !)

Nous pouvons maintenant énoncé une version de l'axiome du choix :

Axiome du choix (première formulation) :
Tout ensemble non vide admet au moins une fonction de choix.

L'impact de cet axiome semble peu significatif lorsque nous considérons des petits ensembles, car nous pouvons toujours effectuer un « choix à la main » dans ces cas-là. Toutefois, pour des ensembles comme les nombres réels, l'axiome nous dit que nous pouvons accomplir quelque chose de particulièrement incroyable : choisir un élément de chaque sous-ensemble non vide des nombres réels, peu importe comment compliqués ces sous-ensembles pourraient être.

Avant d'étudier les différents aspects et formulations de ce principe puissant, nous devrions indiquer que, parmi tous les axiomes de la théorie formelle des ensembles, l'axiome du choix est de loin le plus

controversé. Quoique les autres axiomes semblent capturer des aspects intuitivement plausibles de la théorie naïve des ensembles, l'axiome du choix postule l'existence de fonctions que personne n'arrive à saisir intuitivement. En effet, lorsque David Hilbert a employé une version de l'axiome dans sa preuve pour le fameux théorème de la base (en 1888), son travail a été critiqué par ses collègues comme appartenant à la théologie plutôt qu'aux mathématiques.[1]

Donc, devrions-nous accepter l'axiome du choix ? C'est un problème de nature profondément philosophique, mais une chose est certaine : plusieurs théorèmes que nous choyons en mathématiques en dépendent de manière cruciale. Par exemple, il nous faut cet axiome pour prouver que tout espace vectoriel admet une base, ou que tout corps admet une fermeture algébrique.[2]

D'une autre part, l'axiome nous permet aussi de prouver plusieurs résultats contre-intuitifs, tel que le fameux paradoxe de Banach–Tarksi, lequel énonce que nous pouvons prendre une sphère, la briser en morceaux, puis réarranger ces morceaux de manière à obtenir deux sphères dont chacune a le même volume que la sphère initiale.

Quoique la plupart des mathématiciens se contentent d'accepter l'axiome du choix comme partie intègral aux fondements des mathématiques, plusieurs font le choix de l'omettre, ou d'adopter une version plus faible tel que l'axiome du choix dénombrable (celui-ci postule seulement l'existence de fonctions de choix pour les ensembles dénombrables).

XVII.2 Choix et familles d'ensembles

Comme définie dans la section précédente, une fonction de choix a la forme $\mathcal{P}_+(A) \to A$; elle choisit, pour chaque sous-ensemble non vide $U \subseteq A$, un élément $a \in U$. Or, $\mathcal{P}_+(A)$ est une famille d'ensembles en particulier (on rappelle que tout ensemble d'ensembles peut être interprété comme une famille d'ensembles). Ceci nous mène a une formulation plus générale de fonctions de choix pour des familles arbitraires d'ensembles.

Considérez une famille d'ensembles $(A_i)_{i\in I}$, telle que chaque A_i est non vide (sinon, nous ne pouvons rien choisir dans celle-ci). Une fonction de choix pour cette famille est, intuitivement, une fonction s qui donne, pour chaque $i \in I$, un élément de A_i. En symboles : $s(i) \in A_i$. La seule chose qui semble peu évidente à l'égard de f est : en quoi devrait consister son codomaine ? Entre autres, celui-ci devrait contenir les éléments de tous les A_i. En fait, il suffit de considérer l'ensemble $\bigcup_{i\in I} A_i$, et de prendre $s : I \to \bigcup_{i\in I} A_i$. De cette manière, il est possible de forcer $s(i)$ à être un élément de A_i, pour tout i. L'idée se formalise comme suit :

Définition XVII.2.1. Une *fonction de choix* pour une famille d'ensembles $(A_i)_{i\in I}$ est une fonction

$$s : I \to \bigcup_{i\in I} A_i$$

telle que $s(i) \in A_i$ pour tout $i \in I$.

Et nous avons la version correspondante de l'axiome du choix :

[1] Toutefois, ces mêmes collègues ont admis par la suite que, même si l'axiome faisait appel à un certain acte de foi, il y avait des avantages indéniables à permettre un peu de contenu religieux dans les mathématiques.

[2] Des livres ont été écrits à propos de la multitude de résultats mathématiques qui dépendent de l'axiome du choix (dont plusieurs sont équivalents à celui-ci en fait). Consultez, par exemple, le livre à deux parties de Rubin & Rubin, intitulé ≪ Equivalents of the Axiom of Choice ≫.

Axiome du choix (deuxième formulation) :
Toute famille d'ensembles non vides a au moins une fonction de choix.

À titre d'exemple, considérez à nouveau la famille d'ensembles donnée par $I = \{1, 2, 3\}$ et $A_1 = \{a, b\}, A_2 = \{b, c, d\}, A_3 = \{c\}$. Nous avons dès lors $\bigcup A_i = \{a, b, c, d\}$. Une fonction de choix pour cette famille devrait prendre la forme $s : \{1, 2, 3\} \to \{a, b, c, d\}$ telle que $s(1) \in \{a, b\}$, $s(2) \in \{b, c, d\}$ et $s(3) \in \{c\}$. Notez que ceci force $s(3) = c$, mais qu'il reste plusieurs options pour $s(1)$ et $s(2)$.

Exercice 224. Construisez toutes les fonctions de choix possibles pour l'exemple ci-haut.

XVII.3 Sections

Nous nous préparons maintenant en vue d'une troisième formulation de AC. Rappelez-vous que, en présence d'une famille d'ensembles A_i indexée par I, il existe une fonction $f : A \to I$ dont les fibres sont précisément les ensembles A_i. Ainsi, notre idée est de formuler l'axiome du choix en termes de la fonction f, plutôt qu'en termes de la famille $(A_i)_{i \in I}$.

Définition XVII.3.1. Soit $f : A \to I$ une fonction. Une *section* de f est une fonction $s : I \to A$ telle que $fs = 1_I$.

Clairement, ce ne sont pas toutes les fonctions qui admettent des sections. Par exemple, si nous prenons $A = \{0\}$ et $I = \{0, 1\}$ et $f(0) = 0$, alors il existe une fonction $s : I \to A$ (laquelle envoie $0, 1$ sur 0). Mais celle-ci donne $fs(1) = 0$, et ainsi, elle ne satisfait pas la condition $fs = 1_I$. Le problème ici est que, pour avoir une section de f, il est nécessaire que f soit surjectif.

Exercice 225. Prouvez que si f a une section s, alors f est surjective et s est injective.

Conséquemment, nous pouvons seulement exiger des sections pour des fonctions surjectives.

Axiome du choix (troisième formulation) :
Toute fonction surjective a une section.

Afin d'illustrer comment les sections sont reliées au choix, considérez la surjection $f : \{a, b, c, d\} \to \{1, 2\}$ définie par $f(a) = f(d) = 1, f(b) = f(c) = 2$. Pour spécifier une section s de f, nous devons donner $s(1)$ et $s(2)$. Mais il est requis que $fs(1) = 1$ et $fs(2) = 2$. Ceci veut dire que $s(1) \in \{a, d\}$ et $s(2) \in \{b, c\}$. Ceci nous donne quatre possibilités de sections. Notez que le choix d'une section revient précisément à effectuer un choix d'un élément dans chaque fibre de f, i.e. de prendre une fonction de choix pour la famille de fibres de f.

Exercice 226. Trouvez quelques sections pour la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/3$.

Rappelez-vous que, étant donné des ensembles A, B, nous pouvons définir leur produit cartésien : $A \times B = \{(a, b) | a \in A, b \in B\}$. Nous démontrons maintenant comment le concept de section peut être employé pour définir le produit d'une famille infinie d'ensembles également. Nous allons nous servir du fait que toute famille d'ensembles $(A_i)_{i\in I}$ donne lieu à une fonction de projection $f : \coprod_{i\in I} A_i \to I$.

Définition XVII.3.2. Soit $(A_i)_{i\in I}$ une famille d'ensembles. Le *produit cartésien* de $(A_i)_{i\in I}$ est l'ensemble

$$\prod_{i\in I} A_i = \{\, s : I \to \coprod_{i\in I} A_i \mid fs = 1_I \,\}.$$

Ainsi, le produit des ensembles A_i est l'ensemble des sections de la projection $f : \coprod_{i\in I} A_i \to I$. Concrètement parlant, une telle section s effectue un choix d'un élément de A_i pour chaque $i \in I$. Il s'ensuit que de donner une section de f est la même chose que de donner une fonction de choix pour la famille $(A_i)_{i\in I}$. Ceci donne lieu à une formulation de plus pour l'axiome du choix :

Axiome du choix (quatrième formulation) :
Si $(A_i)_{i\in I}$ est une famille d'ensembles non vides,
alors le produit $\prod_{i\in I} A_i$ est non vide.

XVII.4 Toutes les formulations sont équivalentes

Nous allons maintenant prouver que les quatre formulations présentées pour l'axiome du choix sont équivalentes.

Tout d'abord, considérons la première formulation. Celle-ci énonce que tout ensemble non vide admet une fonction de choix. Nous voulons démontrer que ceci implique la deuxième formulation, laquelle énonce que toute famille d'ensembles non vides admet une fonction de choix. Ainsi, supposons que la première formulation est vraie. Considérons une famille d'ensembles non vides $(A_i)_{i\in I}$ et démontrons que cette famille admet une fonction de choix. Une telle fonction devrait être de la forme

$$s : I \to \bigcup_{i\in I} A_i$$

et devrait satisfaire $s(i) \in A_i$ pour tout $i \in I$. Maintenant, pour employer la supposition que la première formulation est vraie, nous devons trouver un ensemble A nous permettant d'appliquer l'AC. Mais, notez que tous les ensembles A_i (ceux dans lesquels nous devons choisir des éléments) sont des sous-ensembles de leur union $\bigcup_{i\in I} A_i$. Ceci suggère que nous devrions employer $A = \bigcup_{i\in I} A_i$. En posant A ainsi, nous avons $A_i \in \mathcal{P}_+(A)$. Maintenant, selon notre hypothèse, nous pouvons déclarer une fonction de choix

$$v : \mathcal{P}_+(A) \to A,$$

et celle-ci satisfait $v(U) \in U$ pour tout $U \subseteq A$. En particulier, elle nous donne $v(A_i) \in A_i$. Or, nous voulons une fonction dont le domaine est I, pas $\mathcal{P}_+(A)$. Si nous pouvions trouver une fonction adéquate de $I \to \mathcal{P}_+(A)$, alors nous pourrions composer celle-ci avec v, et peut-être obtenir une fonction $I \to A$ avec la propriété cherchée. En fait, il y a un candidat évident : prenons $r(i) = A_i$. Ceci nous donne

$$vr(i) = v(A_i) \in A_i$$

et la composée vr est une fonction de choix pour la famille $(A_i)_{i \in I}$.

Ensuite, cherchons à savoir comment la deuxième formulation implique la troisième. Donc, supposons que toute famille d'ensembles non vides a une fonction de choix, et supposons qu'une fonction surjective $f : X \to I$ nous est donnée. Nous devons trouver une section de f, i.e. une fonction $s : I \to X$ telle que $fs = 1_I$. Pour employer notre supposition, nous devons mettre en évidence une famille d'ensembles. Mais nous savons qu'une fonction avec codomaine I peut être interprétée, à travers ses fibres, comme une famille d'ensembles indexée par I. Ainsi, considérons la famille $\{ f^{-1}(i) \,|\, i \in I \}$ indexée par I. Chaque membre est non vide, car nous avons fait l'hypothèse que f est surjective. Il existe donc une fonction de choix

$$v : I \to \bigcup_{i \in I} f^{-1}(i)$$

qui satisfait $v(i) \in f^{-1}(i)$ pour tout $i \in I$. Cette fonction est la section que nous cherchions : elle choisit effectivement, pour chaque $i \in I$, un élément de la fibre $f^{-1}(i)$ (c'est là un des rôles joués par une section). Le seul problème est qu'il nous faut une fonction $s : I \to X$ et nous avons une fonction $v : I \to \bigcup_{i \in I} f^{-1}(I)$. Mais, nous avons démontré plus tôt que $X = \bigcup_{i \in I} f^{-1}(i)$, donc nous avons terminé.

Nous procédons à la démonstration que la troisième formulation implique la première. Pour ce faire, supposons que toute surjection admet une section, et démontrons que tout ensemble admet une fonction de choix. Considérons un ensemble A. Nous voulons définir une fonction surjective de telle sorte qu'une section de cette fonction nous donne le choix désiré, i.e. le choix d'un élément de chaque sous-ensemble non vide de A. Il faut préparer une surjection en employant A et ses sous-ensembles d'une façon ou d'une autre. Voici une telle possiblité : posons

$$X = \{(a, U) | a \in U \subseteq A\}; \qquad f : X \to \mathcal{P}_+(A); \qquad f(a, U) = U$$

Selon notre hypothèse, cette surjection a une section $s : \mathcal{P}_+(A) \to X$. Par définition d'une section, cette dernière satisfait $fs(U) = U$, ce qui veut dire que $s(U)$ doit être de la forme (a, U) avec $a \in U$. Il s'ensuit, effectivement, que s choisit un élément $a \in U$ pour tout U. C'est ce que nous voulions, quoiqu'il nous faille une fonction $\mathcal{P}_+(A) \to A$, et pas une de $\mathcal{P}_+(A) \to X$. Toutefois, nous pouvons arrangez cela en composant avec une fonction appropriée $X \to A$, et dans ce cas, $g(a, U) = a$ fait l'affaire. Nous avons dès lors que $gs(U) \in U$, comme voulu.

Finalement, il est évident que les troisième et quatrième formulations sont équivalentes : étant donné une surjection $f : A \to I$, nous pouvons interprétée celle-ci comme une famille d'ensembles indexée par I. Ainsi, un élément du produit de cette famille est simplement une section de f.

Nous venons tout juste de prouver :

Théorème XVII.4.1. *Les quatre formulations de l'axiome du choix sont équivalentes.*

XVII.5 Sommaire

Dans cette leçon, nous avons étudié l'*axiome du choix*, lequel énonce, informellement parlant, que pour toute fois où nous sommes en présence d'une collection d'ensembles non vides, nous pouvons choisir un élément de chacun de ces ensembles. Les notions suivantes sont employées pour les diverses formulations :

- Une *fonction de choix* pour un ensemble A est une fonction $c : \mathcal{P}_+(A) \to A$ telle que $c(U) \in U$ pour tout $U \subseteq A$ (et U non vide).
- Une *fonction de choix* pour une famille d'ensembles $(A_i)_{i\in I}$ est une fonction $c : I \to \bigcup_{i\in I} A_i$ telle que $c(i) \in A_i$ pour tout $i \in I$.
- Une *section* d'une fonction $f : A \to B$ est une fonction $s : B \to A$ pour laquelle $fs = 1_B$.
- Le *produit* d'une famille d'ensembles $(A_i)_{i\in I}$ est l'ensemble de toutes les sections de la projection $\coprod_{i\in I} A_i \to I$.

Les quatre formulations de l'axiome du choix correspondent alors à :

1. Tout ensemble non vide admet une fonction de choix.
2. Toute famille d'ensembles non vides admet une fonction de choix.
3. Toute surjection admet une section.
4. Le produit d'ensembles non vides est lui-même non vide.

Le résultat principal est que toutes ces formulations sont équivalentes.

XVII.6 Exercices

Exercice 227. Trouvez toutes les fonctions de choix pour l'ensemble $\{0, 1\}$.

Exercice 228. Essayez de trouver des fonctions de choix pour les ensembles suivants :

(a) $\emptyset$

(b) $\{\emptyset\}$

(c) $\{\mathbb{N}\}$

(d) $\mathbb{N}$

(e) $\{\, x \in \mathbb{Z} \mid x \text{ est premier} \,\}$

(f) $\{\, x \in \mathbb{Q} \mid 0 < x < 1 \,\}$

Exercice 229. Supposons qu'un ensemble A contient n éléments. Combien de fonctions de choix l'ensemble A admet-il ? (Notez : ceci requiert un peu de combinatoire.)

Exercice 230. Considérez la fonction $f : \{a, b, c, d, e\} \to \{p, q, r\}$ donnée par $f(a) = f(c) = q, f(b) = f(d) = r, f(e) = p$. Trouvez toutes les sections possibles de f.

Exercice 231. Soit $f : A \to B$ une fonction bijective. Combien de sections f peut-elle avoir ?

Exercice 232. Considérez la famille d'ensembles indexée par $I = \{1, 2, 3\}$ avec $A_1 = \{a, b, c\}, A_2 = \{b, c, d\}, A_3 = \{c, e\}$. Trouvez trois fonctions de choix pour cette famille. Combien de fonctions de choix y a-t-il au total ?

Exercice 233. Construisez des fonctions de choix pour la famille $\{\{n-1, n, n+1\} | n \in \mathbb{Z}\}$ indexée par $\mathbb{Z}$.

Exercice 234. Considérez un ensemble I et la famille indexée par I avec $A_i = \{i\}$. Trouvez toutes les fonctions de choix pour cette famille.

Exercice 235. Considérez un ensemble I et la famille indexée par I avec $A_i = I$. Trouvez toutes les fonctions de choix possibles pour cette famille.

Exercice 236. Supposons que $R \subseteq A \times B$ est une relation totale (mais pas nécessairement univaluée). Démontrez que R contient une fonction (i.e. qu'il y a un sous-ensemble de R qui est une fonction). (Indice : utilisez l'AC.)

Exercice 237. Considérez la relation d'ordre stricte $<$ sur $\mathbb{R}$. Trouvez une fonction contenue dans cette relation. Avez-vous eu besoin de l'AC ?

Exercice 238. Considérez la fonction $f : \mathbb{R} \to [-1, 1]$ donnée par $f(x) = \sin(x)$. Trouvez au moins deux différentes sections de f.

Exercice 239. Supposons que $f : A \to B$ et $g : B \to C$ sont surjectives, et que s est une section de f, et t une section de g. Démontrez que st est une section de gf.

Exercice 240. Considérez la famille d'ensembles $(A_i)_{i \in I}$ où $I = \{1, 2, 3, 4\}$,

$$A_1 = \{a, b, c\}, A_2 = \{p, q\}, A_3 = \{c\}, A_4 = \{p, a\}.$$

Décrivez explicitement le domaine de la fonction surjective correspondante $e : X \to I$, puis la fonction surjective elle-même. Décrivez aussi la fonction correspondante $X \to \bigcup_{i \in I} A_i$. Finalement, construisez une fonction de choix explicite pour $(A_i)_{i \in I}$, et expliquez comment cette fonction correspond à la section de e.

Exercice 241. Considérez la relation d'équivalence sur $\mathbb{R}$ définie par $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$. Trouvez quelques exemples de sections pour la fonction quotient $\pi : \mathbb{R} \to \mathbb{R}/\sim$.

Exercice 242. Considérez la famille d'ensembles $\{(n-1, n+1) \subseteq \mathbb{R} | n \in \mathbb{Z}\}$. Trouvez quelques exemples de fonctions de choix pour cette famille. Construisez les surjections associées et démontrez comment les fonctions de choix donnent lieu a des sections pour ces surjections.

Exercice 243. Posons $X = \{\, U \subseteq \mathbb{R} \,|\, U \text{ est fini} \,\}$. Pouvez-vous trouver une fonction de choix pour X ?

LEÇON XVIII

CARDINALITÉ

Qu'est-ce que les ensembles $A = \{0, 1, 2\}, B = \{\text{Jean, Marie, Karine}\}$ et $C = \{\mathbb{N}, \mathbb{Z}, \mathbb{R}\}$ ont en commun ? Ils ont chacun trois éléments. Ceci veut dire qu'ils sont en correspondance bijective : $A \cong B \cong C$. Au sens général, deux ensembles finis X, Y ayant le même nombre d'éléments sont en correspondance bijective. Mais que pouvons-nous dire à propos de deux ensembles infinis ? Quel sens pouvons-nous accordé à « le même nombre d'éléments » ? Les ensembles $\mathbb{N}$ et $\mathbb{Z}$ partagent-ils le même nombre d'éléments ? Qu'en est-il de $\mathbb{Q}$ et $\mathbb{R}$?

Cette leçon apporte une réponse à ces questions.

XVIII.1 GRANDEUR

Comme indiqué, on peut concevoir que deux ensembles « ont la même grandeur » lorsque ceux-ci sont en correspondance bijective. La terminologie employée à cet effet est la suivante :

Définition XVIII.1.1 (Cardinalité)**.** Deux ensembles X et Y *ont la même cardinalité* lorsque $X \cong Y$. Dans ce cas, on dit aussi que X et Y sont *équipotents*.

Rappelons-nous que la relation $\cong$ a les propriétés suivantes :

- $A \cong A$ pour tout ensemble A
- $A \cong B$ implique $B \cong A$
- $A \cong B$ et $B \cong C$ implique $A \cong C$

Conséquemment, la notion d'« avoir la même cardinalité » peut être vue comme une relation d'équivalence sur la collection[1] de tous les ensembles. La classe d'équivalence d'un ensemble A est dénotée $|A|$; les éléments de cette classe sont tous les ensembles en correspondance bijective avec A.

[1] Comme nous le savons, il n'existe pas de telle chose qu'un ensemble de tous les ensembles !

Remarque XVIII.1.2 (que vous pouvez ignorer). Une question se pose naturellement à savoir si la classe $|A|$ admet un représentant canonique comme élément. En d'autres termes, est-il possible, pour tout choix de « grandeur » pour un ensemble, d'obtenir un ensemble canonique avec cette grandeur ? La réponse est oui, mais elle requiert un peu de théorie. Les représentants canoniques sont appelés les *nombres cardinaux*, et ils généralisent les nombres naturels (lesquels sont employés pour compter le nombre d'éléments pour des ensembles finis). Vous pouvez en lire davantage à ce sujet dans n'importe quel manuel sur la théorie des ensembles ; par exemple, dans le livre d'Halmos intitulé *Naive Set Theory*.

XVIII.2 Exemples

Nous établissons maintenant quelques résultats positifs : nous allons démontrer que certains ensembles admettent la même cardinalité.

Exemples XVIII.2.1.

1. Soit $A = \mathbb{N}$ et $B = \mathbb{N} - \{0\}$. Nous avançons que $|A| = |B|$. Définissons $\phi : A \to B$ par $\phi(n) = n+1$. Alors, clairement, ϕ est injective et surjective, i.e. bijective. Ceci prouve que $\mathbb{N} \cong \mathbb{N} - \{0\}$.

2. Soit $A = \mathbb{N}$ et $B = \mathbb{N} + \mathbb{N}$ (i.e. B consiste en deux copies disjointes des nombres naturels). Alors, $|A| = |B|$. Posons $\psi : B \to A$ avec $\psi(x, 0) = 2x$ et $\psi(y, 1) = 2y + 1$. Il s'ensuit que ψ est bijective, donc $\mathbb{N} \cong \mathbb{N} + \mathbb{N}$.

3. $|\mathbb{N}| = |\mathbb{Z}|$: définissons $f : \mathbb{Z} \to \mathbb{N}$ par $f(x) = 2x$ si $x \geq 0$, et $f(x) = -2x - 1$ si $x < 0$. Il s'ensuit que f est bijective.

Ces exemples démontrent, en particulier, qu'un ensemble peut être en correspondance bijective avec un sous-ensemble propre (strict) de lui-même. Clairement, pour des ensembles finis, cela est impossible. Ainsi, nous pouvons employer cette idée pour *définir* ce qu'est un ensemble infini :

Définition XVIII.2.2 (Infinité)**.** Un ensemble X est *infini* s'il existe un sous-ensemble $Y \subseteq X$ tel que $Y \neq X$, mais avec $|X| = |Y|$. Un ensemble est *fini* s'il n'est pas infini.

En fait, il suffit d'exiger l'existence d'un sous-ensemble propre Y de X et d'une fonction surjective $Y \to X$.

Il s'ensuit, de la définition, que les ensembles finis ont la propriété suivante (vous pouvez vérifiez cette dernière directement pour des petits exemples) :

Lemme XVIII.2.3. *Soit X un ensemble fini. Alors, pour une fonction $f : X \to X$, les énoncés suivants sont équivalents :*

- *f est injective*
- *f est surjective*
- *f est bijective*

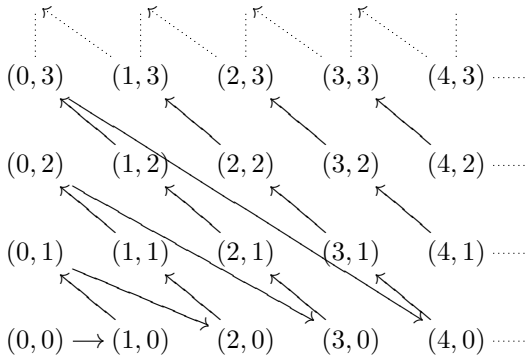


FIGURE XVIII.1 – Un encodage du plan

Démonstration. Il suffit de démontrer que l'injectivité implique la surjectivité, et vice-versa. Supposons que f est injective. Nous avons alors $X \cong f[X]$, car f est injective et chaque $y \in f[X]$ est dans l'image de f. Mais $f[X]$ est un sous-ensemble de X, et donc, il doit être égal à X si X est fini. Nous obtenons $f[X] = X$ ainsi, et ceci revient à dire que f est surjective.

Réciproquement, si f est surjective, alors supposons que $f(x) = f(x')$, mais que $x \neq x'$. Il s'ensuit que $X - \{x'\}$ est un sous-ensemble propre de X, et donc, il existe une surjection $X - \{x'\} \to X$ (laquelle est simplement f restreinte à ce sous-ensemble). Mais ceci est impossible si X est fini. □

Parfois, nous voulons exprimer qu'un ensemble est plus grand qu'un autre ; la définition suivante donne un sens précis à cette idée :

Définition XVIII.2.4. Pour des ensembles X, Y, on écrit $|X| \leq |Y|$ s'il existe une injection de X vers Y. On écrit $|X| < |Y|$ si $|X| \leq |Y|$, mais $|X| \neq |Y|$.

Par exemple, il s'ensuit trivialement que, si $X \subseteq Y$, alors $|X| \leq |Y|$. De plus, si $f : Y \to X$ est une surjection, alors il s'ensuit que $|X| \leq |Y|$. (Il suffit de prendre une section !)

L'exemple suivant est un peu plus engagé :

Exemple XVIII.2.5. L'ensemble $\mathbb{N}$ est équipotent à $\mathbb{N} \times \mathbb{N}$. (C'est-à-dire : $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.)

Pour prouver ceci, nous devons construire une fonction bijective de $\mathbb{N} \times \mathbb{N}$ vers $\mathbb{N}$. La figure XVIII.1 illustre l'idée derrière l'élaboration de cette bijection.

Comme vous pouvez le constater, nous dénombrons systématiquement des antidiagonales $y + x = c$. Il est évident que ceci établit une bijection $C : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (C pour « couplage »).

Il y a aussi deux fonctions de « décodage » $C_0, C_1 : \mathbb{N} \to \mathbb{N}$, avec les propriétés suivantes :

$$C_0(C(n, m)) = n, \qquad C_1(C(n, m)) = m, \qquad C(C_0(x), C_1(x)) = x.$$

Ainsi, la fonction $C^{-1}(x) = (C_0(x), C_1(x))$ est l'inverse de C. Les équations ci-haut sont souvent appelées *équations de couplage*.

Or, la fonction C satisfait

$$C(x, y) = \frac{1}{2}(x + y)(x + y + 1) + y.$$

En fait, il est possible de démontrer (en supposant l'axiome du choix) que *tout* ensemble infini X satisfait $|X| = |X \times X|$. D'ailleurs, il s'agit d'un des énoncés équivalents à l'AC. Pour une preuve de cet énoncé, nous référons le lecteur aux manuels standards de la théorie des ensembles.

Une conséquence de l'exemple antécédent est la suivante :

Exemple XVIII.2.6. Nous avons $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$.

La première égalité a déjà été prouvée plus haut. Il est clair que $|\mathbb{Z}| \leq |\mathbb{Q}|$, et donc, il ne reste qu'à savoir si $|\mathbb{Q}| \leq |\mathbb{Z}|$. Pour construire l'injection témoin, rappelons-nous qu'un élément q de $\mathbb{Q}$ peut être representé par $\frac{a}{b}$, où $a \in \mathbb{Z}, b \in \mathbb{N}$ et a, b sont relativement premiers. Appelons ceci la *représentation minimale* de q, et notons qu'elle est unique. Maintenant, considérons

$$f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}; \qquad f(q) = (a, b) \text{ où } q = \frac{a}{b} \text{ est la repr. min. de } q.$$

Puis, f est fonctionnelle, car la représentation minimale est unique, et f est injective, car des nombres rationnels distincts ont des représentations distinctes. La preuve se conclue ainsi.

Un exemple important de plus : pour toute paire de nombres réels a, b avec $a < b$, nous avons $|\mathbb{R}| = |(a, b)|$. Je vais démontrer ceci pour l'intervalle $(-\pi/2, \pi/2)$ et laisser en exercice la démonstration que n'importe quelles deux intervalles ouverts bornés (a, b) ont la même cardinalité. Tout simplement, la fonction arctan : $\mathbb{R} \to (-\pi/2, \pi/2)$ est bijective (avec inverse tan). Ceci prouve l'assertion en question. Dans les exercices, vous allez également démontrer que tous intervalles $[a, b]$ ont la même cardinalité que $\mathbb{R}$.

Nous avons introduit la notation $|A| \leq |B|$, mais nous ne l'avons pas justifiée. Une question importante est la suivante : si $|A| \leq |B|$ et $|B| \leq |A|$, s'ensuit-il que $|A| = |B|$? En déballant la définition, ceci devient : s'il y a des fonctions injectives $f : A \to B$ et $g : B \to A$, alors y a-t-il une bijection $A \cong B$?

Théorème XVIII.2.7 (Cantor–Bernstein)**.** *Si* $|A| \leq |B|$ *et* $|B| \leq |A|$*, alors* $|A| = |B|$.

Nous ne verrons pas la preuve ici ; il est possible de déduire ce résultat à partir de l'axiome du choix, mais ce dernier n'est pas nécessaire. Pour une preuve élégante de « va-et-vient », nous réferrons le lecteur aux lectures recommandées (annexe A).

XVIII.3 Argument de la diagonale de Cantor

Au cours de la section précédente, nous avons étudié plusieurs exemples d'ensembles de mêmes cardinalités. Dans cette section, nous introduisons une technique pour démontrer que deux ensembles ont une cardinalité différente.

Définition XVIII.3.1. Un ensemble A est *dénombrable* lorsque $|A| \leq |\mathbb{N}|$. Si A n'est pas dénombrable, alors on dit aussi que A est *non dénombrable*.

Notez que, selon cette définition, les ensembles finis sont dénombrables. Un ensemble infini qui est dénombrable est qualifié d'*infini dénombrable*. Intuitivement, si un ensemble est dénombrable, alors il est possible d'« énumérer ses éléments » : on peut écrire $A = \{a_0, a_1, a_2, \ldots\}$. Techniquement, ceci veut dire que nous choisissons une injection $s : A \to \mathbb{N}$, puis une fonction $e : \mathbb{N} \to A$ pour laquelle s est une

section. Nous pouvons concevoir que la fonction e (qui doit être surjective !) énumère les éléments de A (possiblement avec des répétitions).

Notre objectif est de démontrer : $\mathbb{R}$ est non dénombrable. Clairement, il suffit de prouver qu'il existe un sous-ensemble de $\mathbb{R}$ qui est non dénombrable. Nous allons entreprendre cela pour l'intervalle ouvert $(0,1)$. La preuve est due à Georg Cantor, le père de la théorie des ensembles ; sa technique est appelée l'*argument de la diagonale*.

Théorème XVIII.3.2. *L'ensemble* $(0,1)$ *est non dénombrable.*

Démonstration. Supposons, afin d'obtenir une contradiction, que $(0,1)$ est dénombrable. Ceci veut dire que nous pouvons trouver une énumération $e : \mathbb{N} \to (0,1)$. Cette fonction nous permet de faire la liste de tous les éléments de $(0,1)$, un à un. Par exemple, les quelques premiers éléments pourraient avoir la forme suivante :

$$\begin{array}{lcccccccccccc}
e(0): & \mathbf{3} & 4 & 1 & 0 & 0 & 0 & 2 & 9 & 9 & 2 & 5 & \cdots \\
e(1): & 2 & \mathbf{5} & 5 & 5 & 5 & 3 & 2 & 9 & 7 & 1 & 0 & \cdots \\
e(2): & 2 & 4 & \mathbf{5} & 3 & 5 & 0 & 0 & 4 & 4 & 4 & 7 & \cdots \\
e(3): & 5 & 2 & 0 & \mathbf{7} & 1 & 6 & 1 & 9 & 7 & 1 & 7 & \cdots \\
e(4): & 1 & 2 & 0 & 8 & \mathbf{3} & 0 & 3 & 3 & 8 & 8 & 5 & \cdots \\
e(5): & 2 & 5 & 4 & 2 & 3 & \mathbf{6} & 2 & 9 & 7 & 5 & 8 & \cdots \\
e(6): & 8 & 8 & 8 & 9 & 9 & 7 & \mathbf{0} & 8 & 1 & 0 & 1 & \cdots \\
e(7): & 3 & 3 & 2 & 1 & 1 & 0 & 7 & \mathbf{3} & 6 & 9 & 0 & \cdots \\
e(8): & 3 & 5 & 2 & 6 & 8 & 0 & 0 & 2 & \mathbf{3} & 3 & 0 & \cdots \\
e(9): & 8 & 5 & 1 & 7 & 4 & 0 & 0 & 6 & 6 & \mathbf{0} & 2 & \cdots \\
\vdots &&&&&&&&&&&&
\end{array}$$

Ceci veut dire que le premier nombre dans la liste est un nombre réel dont le développement décimal commence avec 0,34100029925…, et ainsi de suite. La seule chose que nous devons garder à l'esprit est que, par hypothèse, *tout* élément de $(0,1)$ se trouve dans cette liste quelque part.

Nous allons dégager une contradiction en trouvant un nombre réel dans $(0,1)$ qui ne peut être dans cette liste. La façon de construire ce nombre est la suivante : Considérons la diagonale de la liste, i.e. la i-ème position décimale du i-ème élément de la liste, pour chaque $i \in \mathbb{N}$. Cette diagonale est représentée par les chiffres à caractère gras dans le diagramme.

Maintenant, considérons le nombre réel dont le développement décimal est le suivant :

$$c = 0{,}4668471441\ldots$$

En d'autres mots, prenons les entrées le long de la diagonale et additionnons 1 à chacune. (Si une entrée est 9, remplacez-la par 0.) Assertion : $c \neq e(i)$ pour tout $i \in \mathbb{N}$. Preuve : supposons que $c = e(i)$. Le i-ème chiffre de c est différent du i-ème chiffre de $e(i)$ (car nous avons construit c de cette façon). Contradiction. □

Une technique similaire (ou une variation de cette dernière) peut être employée pour établir une variété d'autres résultats. Par exemple :

Théorème XVIII.3.3. *L'ensemble* $\mathcal{P}(\mathbb{N})$ *est non dénombrable.*

Démonstration. Supposons que nous avons une énumération $e : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. Un sous-ensemble U de $\mathbb{N}$ peut être représenté à travers sa fonction caractéristique $\chi_U : \mathbb{N} \to \{0,1\}$. Nous pouvons visualiser χ_U

comme une séquence de 0 et de 1 : $\chi_U(0), \chi_U(1), \chi_U(2), \chi_U(3)$, et ainsi de suite. Les quelques premiers éléments de l'énumération prennent la forme suivante :

$$\begin{array}{lcccccccccccc}
e(0): & \mathbf{1} & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & \cdots \\
e(1): & 1 & \mathbf{0} & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & \cdots \\
e(2): & 1 & 1 & \mathbf{1} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \cdots \\
e(3): & 0 & 1 & 0 & \mathbf{1} & 1 & 0 & 1 & 1 & 1 & 1 & 0 & \cdots \\
e(4): & 1 & 1 & 0 & 1 & \mathbf{1} & 0 & 1 & 1 & 0 & 0 & 1 & \cdots \\
e(5): & 0 & 0 & 0 & 1 & 1 & \mathbf{0} & 1 & 1 & 0 & 0 & 1 & \cdots \\
e(6): & 0 & 1 & 0 & 1 & 1 & 1 & \mathbf{0} & 1 & 1 & 0 & 1 & \cdots \\
e(7): & 0 & 1 & 0 & 1 & 1 & 0 & 1 & \mathbf{0} & 1 & 1 & 0 & \cdots \\
e(8): & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{0} & 0 & 0 & \cdots \\
e(9): & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & \mathbf{0} & 0 & \cdots \\
\vdots &&&&&&&&&&&&
\end{array}$$

Maintenant, définissons une fonction $\chi : \mathbb{N} \to \{0, 1\}$ en prenant les valeurs de la diagonale, puis inversons les valeurs (i.e. remplaçons les 0 par des 1, et vice-versa) :

$$\chi(i) = \begin{cases} 1 & \text{si le } i\text{-ème élément de } e(i) \text{ est } 0 \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, χ est différent de tous les $e(i)$, et donc, il correspond à un sous-ensemble qui n'est pas dans l'énumération. Contradiction. □

Le théorème suivant est similaire, et il est laissé en exercice :

Théorème XVIII.3.4. *L'ensemble $\mathbb{N}^{\mathbb{N}}$ est non dénombrable.*

En vérité, tous les résultats précédents admettent une généralisation comme suit :

Théorème XVIII.3.5. *Pour tout ensemble A avec $|A| > 1$, nous avons $|A| < |\mathcal{P}(A)|$ et $|A| < |A^A|$.*

La preuve fait de nouveau appel à la diagonalisation : si $|A| = |A^A|$, alors il y a une surjection $e : A \to A^A$. Ainsi, pour chaque $a \in A$, $e(a)$ est une fonction de A vers A. Écrivons $e_{a,b}$ pour l'élément $e(a)(b)$. Aussi, fixons deux éléments distincts a_0, a_1 de A. Maintenant, définissons une fonction $f : A \to A$ par

$$f(a) = \begin{cases} a_0 & \text{si } e_{a,a} \neq a_0 \\ a_1 & \text{sinon.} \end{cases}$$

Cette fonction n'est pas un élément de $e[A]$. Contradiction.

XVIII.4 Sommaire

On dit que deux ensembles A, B ont la même *cardinalité* lorsqu'ils sont en correspondance bijective. Notation : $|A| = |B|$.

Nous avons découvert que $|\mathbb{N}| = |\mathbb{N} + \mathbb{N}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$. Tout ensemble dont la cardinalité est moindre ou identique à celle de $\mathbb{N}$ est appelé *dénombrable*. Les ensembles qui ne sont pas

dénombrables sont appelées *non dénombrables*. Un ensemble A est dénombrable si et seulement s'il existe une *énumération* de A, c'est-à-dire une fonction surjective $\mathbb{N} \to A$.

L'*argument de la diagonale* de Cantor peut être appliqué pour démontrer les énoncés suivants :

- $|\mathbb{N}| < |(0,1)^{\mathbb{N}}|$ (et donc $|\mathbb{N}| < |\mathbb{R}|$)
- $|A| < |\mathcal{P}(A)|$ pour tout ensemble A
- $|A| < |A^A|$ pour tout ensemble A avec plus d'un élément.

Finalement, le théorème de Cantor–Bernstein énonce que $|A| \leq |B|$ et $|B| \leq |A|$ implique $|A| = |B|$.

XVIII.5 Exercices

Exercice 244. Prouvez les énoncés suivants portant sur les cardinalités :

(a) Si $|A| = |A'|$ et $|B| = |B'|$, alors $|A \times B| = |A' \times B'|$.

(b) Si $|A| = |A'|$ et $|B| = |B'|$, alors $|A + B| = |A' + B'|$.

(c) Si $|A| = |A'|$ et $|B| = |B'|$, alors $|A^B| = |A'^{B'}|$.

(d) Si $|A| = |A'|$, alors $|\mathcal{P}(A)| = |\mathcal{P}(A')|$.

Exercice 245. Prouvez que tous les ensembles suivants ont la même cardinalité :

- $\mathbb{N}$
- $\mathbb{N} + 1$
- $\mathbb{N} + k$, où k est un ensemble avec k éléments
- $\mathbb{N} + \mathbb{N} + \mathbb{N}$
- $\mathbb{Z} + \mathbb{Z}$
- $\mathbb{Z} \times \mathbb{Z}$
- $\mathbb{Z}^k$
- $\mathbb{Z} + (\mathbb{Q} \times \mathbb{N})^k$
- L'ensemble des nombres premiers (comme sous-ensemble de $\mathbb{Z}$)
- L'ensemble des nombres pairs (comme sous-ensemble de $\mathbb{Z}$)

Exercice 246. Supposons que $a < b$ et $c < d$ sont des nombres réels. Démontrez que $(a, b) \cong (c, d)$ et que $[a, b] \cong [c, d]$. Finalement, démontrez que $(a, b) \cong [a, b]$. (Indice : prenez $c < a, d > b$ et servez-vous du théorème de Cantor–Schröder–Bernstein.)

Exercice 247. Supposons que A est infini. Servez-vous de $|A| = |A \times A|$ pour démontrer que $|A| = |A + A|$.

Exercice 248. Supposons que A est non dénombrable, et que $B \subseteq A$ est dénombrable. Démontrez que $A - B$ est non dénombrable également.

Exercice 249. Démontrez que l'ensemble des nombres irrationnels est non dénombrable.

Exercice 250. Considérez l'ensemble L des fonctions affines $\mathbb{R} \to \mathbb{R}$. (Une fonction affine est de la forme $f(x) = ax + b$ avec $a, b \in \mathbb{R}$ fixés.) Prouvez que $|L| = |\mathbb{R}|$.

Exercice 251. Soit A l'ensemble de toutes les chaînes de caractères (de longueur arbitraire, mais finie) employant l'alphabet $\{a, b, \ldots, z\}$. Est-ce un ensemble dénombrable ?

Exercice 252. Prouvez que l'ensemble des sous-ensembles finis de $\mathbb{N}$ est dénombrable. (Indice : essayez de trouver une énumération systématique pour de tels sous-ensembles.)

Exercice 253. Un sous-ensemble $A \subseteq \mathbb{N}$ est appelé *cofini* si $\mathbb{N} - A$ est fini. Prouvez que l'ensemble des sous-ensembles cofinis de $\mathbb{N}$ est dénombrable.

Exercice 254. Considérez l'ensemble des sous-ensembles infinis de $\mathbb{N}$. S'agit-il d'un ensemble dénombrable ?

Exercice 255. Démontrez que s'il existe une surjection $A \to \mathbb{N}$, alors A est infini. Vous pouvez faire appel à l'AC.

Exercice 256. Soit $\mathbb{Q}_n[x]$ l'ensemble de tous les polynômes de degré n (à une variable) avec coefficients dans $\mathbb{Q}$. Ainsi, un élément de cet ensemble prend la forme $a_n x^n + \ldots + a_1 x + a_0$ où les $a_i \in \mathbb{Q}$. Démontrez que $\mathbb{Q}_n[x]$ est dénombrable. Généralisez au cas des polynômes à plusieurs variables.

Exercice 257. Écrivez $\mathbb{R}_n[x]$ pour l'ensemble des polynômes de degré n à une variable sur $\mathbb{R}$ (voir l'exercice précédent). Prouvez que $|\mathbb{R}_n[x]| = |\mathbb{R}|$. Vous pouvez employer le fait que $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Exercice 258. Démontrez que $|\mathbb{C}| = |\mathbb{R}|$.

Exercice 259. Considérez la relation d'équivalence sur $\mathbb{R}$ donnée par

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}$$

et l'ensemble quotient $\mathbb{R}/\!\sim$. Démontrez que chaque classe d'équivalence est dénombrable. Aussi, démontrez que l'ensemble quotient est non dénombrable en élaborant une bijection avec un ensemble dont la non-dénombrabilité est connue.

Exercice 260. Soit $(A_i)_{i \in I}$ une famille d'ensembles telle que I est dénombrable, et telle que chaque A_i est dénombrable. Démontrez que $\coprod_{i \in I} A_i$ et $\bigcup_{i \in I} A_i$ sont également dénombrables.

Exercice 261. Un *point fixe* pour une fonction $f : A \to A$ est un élément $a \in A$ pour lequel $f(a) = a$. On dit que f est *sans points fixes* si f n'a pas de point fixe, i.e. $f(a) \neq a$ pour tout $a \in A$. Vérifiez que, pour chaque fois où nous avons employé l'argument de la diagonale, nous avons élaboré une fonction sans points fixes.

LEÇON XIX

Ensembles ordonnés

Lors des leçons antécédentes, nous avons étudié des relations avec des propriétés spéciales. Parmi les cas les plus importants, nous avons considéré les fonctions (et entre autres, des classes particulières de fonctions, comme les bijections) et les relations d'équivalence. Nous abordons maintenant l'étude d'une troisième classe importante de relations appelées *relations d'ordre* (ou *ordres* tout simplement).

XIX.1 Définition et exemples

Nous avons déjà rencontré plusieurs exemples standards de relations d'ordre : les relations de « plus petit ou égal à » sur $\mathbb{N}$ (ou sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$), et la relation de sous-ensemble (sur $\mathcal{P}(A)$ pour un ensemble quelconque A). La définition suivante dégage les aspects en commun de ces exemples.

Définition XIX.1.1 (Ordre)**.** Soient A un ensemble et R une relation sur A. On dit que R est une *relation de préordre* (ou un *préordre*) lorsque R est réflexive et transitive. Lorsque R est également antisymétrique, on dit qu'il s'agit d'une *relation d'ordre* (ou d'un *ordre*).

Typiquement, nous employons des symboles tel que $\leq$ ou $\preceq$ pour dénoter des relations d'ordre. Lorsque A est un ensemble, et $\leq$ un ordre sur A, on dit que $(A, \leq)$ est un *ensemble (partiellement) ordonné*.

Exemple XIX.1.2. Posons $A = \{a, b, c, d\}$, et considérons les relations suivantes :

- $R_1 = \{(a,a), (b,b), (c,c), (d,d), (a,c)\}$
- $R_2 = \{(a,a), (b,b), (c,c), (d,d), (a,c), (a,d)\}$
- $R_3 = \{(a,a), (b,b), (c,c), (d,d), (a,c), (c,d)\}$
- $R_4 = \{(a,a), (b,b), (c,c), (d,d), (a,b), (a,c), (a,d)\}$

- $R_5 = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,c),(c,d),(b,c),(b,d),(a,d)\}$
- $R_6 = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,a),(a,d),(b,d)\}$

La relation R_1 est un ordre, et R_2 aussi. Par contre, R_3 ne l'est pas, car elle n'est pas transitive. La relation R_4 est un ordre, et R_5 également. Finalement, R_6 est un préordre, mais pas un ordre (elle n'est pas antisymétrique).

Une chose à retenir de cet exemple élémentaire est qu'un ensemble donné peut avoir plusieurs ordres différents (même si parfois, il y en a un en particulier qui est « évident », comme pour les nombres naturels !). Voici quelques exemples de plus, mais de nature légèrement plus abstraite cette fois.

Exemples XIX.1.3.

1. Soit A un ensemble arbitraire. Alors la relation diagonale Δ_A est un ordre.
2. La relation maximale sur un ensemble A n'est pas un ordre lorsque A a plus d'un élément ; dans ce cas, la relation maximale n'est pas antisymétrique. Toutefois, elle est toujours un préordre.
3. Lorsque $(A, \leq)$ est un ensemble ordonné, nous pouvons considérer la relation opposée $\leq^{op}$. Par définition, nous avons $x \leq^{op} y$ si et seulement si $y \leq x$. Alors, $\leq^{op}$ est également une relation d'ordre.

Parfois, nous nous intéressons davantage à la relation « strictement plus petit que » qu'à la relation « plus petit ou égal à » (lister toutes les paires (x,x) dans une relation est parfois encombrant). Nous adressons cette idée comme suit :

Définition XIX.1.4 (Ordre strict)**.** Une relation R sur un ensemble A est un *ordre strict* lorsqu'elle est antiréflexive, transitive et antisymétrique.

Par exemple, la relation $R = \{(a,b),(a,c),(d,c)\}$ est un ordre strict sur $\{a,b,c,d,e\}$. Le prochain lemme démontre que les concepts d'ordre strict et d'ordre général sont interchangeables :

Lemme XIX.1.5. *Il y a une correspondance bijective entre les relations d'ordre sur A et les relations d'ordre strict sur A.*

Démonstration. Supposons tout d'abord que $<$ est une relation d'ordre strict sur A. Puis, définissons $\leq$ par la relation suivante sur A :

$$a \leq b \Leftrightarrow a < b \text{ ou } a = b.$$

(De manière équivalente, $\leq$ est l'union de $<$ et de la relation diagonale.) Nous pouvons constater sans difficulté que $\leq$ est une relation d'ordre. Réciproquement, si $\leq$ est un ordre, définissons $<$ par

$$a < b \Leftrightarrow a \leq b \text{ et } a \neq b.$$

Alors, $<$ est un ordre strict. Les constructions de $<$ à partir de $\leq$, et vice-versa, sont des inverses mutuels. □

Pour conclure cette section, nous donnons quelques exemples additionnels, que l'on retrouve couramment dans la pratique des mathématiques.

Exemples XIX.1.6.

1. Définissons une relation sur $\mathbb{Z}$ par
$$x \preceq y \Leftrightarrow_{\text{déf}} x \text{ divise } y.$$
Il s'agit d'un ordre.

2. Considérons l'ensemble $\mathbb{N}^{\mathbb{N}}$ des fonctions de $\mathbb{N}$ vers $\mathbb{N}$. On peut définir un ordre sur cet ensemble par
$$f \leq g \Leftrightarrow_{\text{déf}} f(x) \leq g(x) \text{ pour tout } x \in \mathbb{N}.$$
Notez que le $\leq$ sur la gauche est celui que nous définissons, tandis que celui sur la droite est l'ordre standard sur $\mathbb{N}$. (On appelle cet emploi à double sens pour une notation, la surcharge d'une notation, ce qui peut mener à de la confusion, mais c'est une pratique courante.)

3. En généralisant les exemples précédents : Étant donné un ensemble X et un ensemble ordonné $(A, \leq)$, on peut définir un ordre sur A^X par
$$f \leq g \Leftrightarrow_{\text{déf}} f(x) \leq g(x) \text{ pour tout } x \in X.$$
Encore une fois, le symbole $\leq$ est employé à double sens, pour désigner deux ordres distincts.

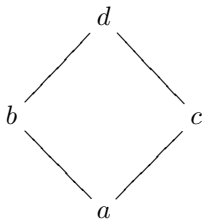
4. Lorsque A est un ensemble quelconque, l'ensemble des parties $\mathcal{P}(A)$ est ordonné par l'inclusion (i.e. la relation de sous-ensemble). Lorsque $(A, \leq)$ est un ensemble ordonné, nous pouvons employer l'ordre sur A pour définir une autre relation sur $\mathcal{P}(A)$, notamment
$$U \leq V \Leftrightarrow_{\text{déf}} \forall x \in U \exists y \in V. x \leq y.$$
Cette dernière définit un préordre, lequel n'est pas antisymétrique en général. (Essayez de trouver un exemple qui l'est.)

XIX.2 Diagrammes de Hasse

Les diagrammes de Hasse sont un outil pour visualiser les ensembles ordonnés. Bien entendu, nous savons déjà comment faire le dessin d'une relation, et en principe, nous pourrions en faire de même pour les ensembles ordonnés. Toutefois, la notion de diagramme de Hasse est plus facile et plus intuitive lorsque nous considérons des relations d'ordre.

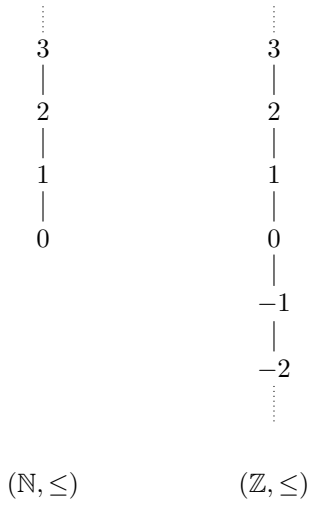
Dans un diagramme de Hasse, nous dessinons les éléments de la façon habituelle, mais avec la différence que, lorsque $a \leq b$, nous dessinons a en-dessous de b. L'exemple suivant illustre cette approche :

Exemple XIX.2.1. Soit $A = \{a, b, c, d\}$ et soit R une relation d'ordre spécifiée par $\{(a, b), (a, c), (a, d), (b, d), (c, d)\}$. Le diagramme de Hasse correspondant est



Notez que nous ne dessinons pas d'arête allant de a vers d, même si $a \leq d$. Ceci n'est pas nécessaire, car nous pouvons voir dans l'image que d est au-dessus de a. Aussi, nous ne représentons pas la réflexivité de cette relation. Lorsque deux éléments se trouvent à la même hauteur dans un diagramme de Hasse (comme b et c dans l'exemple), ceci veut dire qu'ils sont *incomparables*, au sens que nous n'avons ni $b \leq c$, ni $c \leq b$.

Voici un autre exemple où l'on représente (en partie) les diagrammes de Hasse pour l'ordre usuel sur $\mathbb{N}$ et pour l'ordre usuel sur $\mathbb{Z}$.



$(\mathbb{N}, \leq)$ $(\mathbb{Z}, \leq)$

XIX.3 Constructions

Dans cette section, nous abordons diverses méthodes pour construire de nouvelles relations d'ordre à partir d'anciennes.

Pour commencer, nous considérons les sommes (ou coproduits). Soient $(A, \leq)$ et $(B, \leq)$ des ensembles ordonnés. On définit un ordre sur $A + B$ par

$$(x, i) \leq (y, j) \Leftrightarrow_{\text{déf}} i = j \text{ et } x \leq y.$$

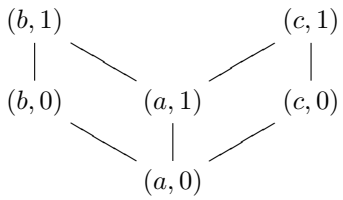
En termes de diagrammes de Hasse, ceci veut simplement dire que nous plaçons les diagrammes de $(A, \leq)$ et de $(B, \leq)$ côte à côte ; tous les éléments de A sont incomparables à tous les éléments de B.

Ensuite, nous considérons les produits d'ensembles ordonnés. Supposons que $(A, \leq)$ et $(B, \leq)$ sont des ensembles ordonnés. On définit un ordre sur $A \times B$ par

$$(a, b) \leq (a', b') \Leftrightarrow_{\text{déf}} a \leq a' \text{ et } b \leq b'.$$

Ceci est appelé l'*ordre produit*. Par exemple, supposons que $A = \{a, b, c\}$ est donné avec $a \leq b$ et $a \leq c$, et que $B = \{0, 1\}$ est donné avec $0 \leq 1$. Alors, le diagramme de Hasse suivant représente l'ordre produit

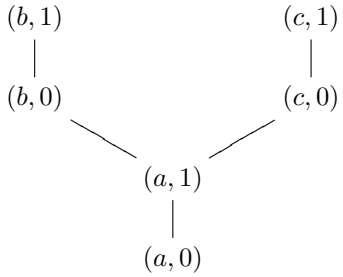
sur $A \times B$:



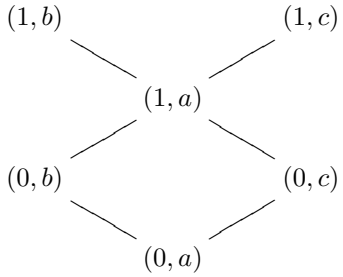
Il y a une autre façon de construire un ordre sur le produit $A \times B$; il s'agit de l'*ordre lexicographique*. On le définit comme suit :

$$(x, y) \leq_l (x', y') \Leftrightarrow_{\text{déf}} \begin{cases} x < x' & \text{ou} \\ x = x' \text{ et } y \leq y' \end{cases}$$

En reprenant l'exemple précédent, l'ordre lexicographique sur $A \times B$ est



Nous pouvons également calculer l'ordre lexicographique sur $B \times A$:



Notez que ces ordres lexicographiques sont très différents !

XIX.4 Sommaire

Une *relation d'ordre* sur un ensemble est une relation réflexive, transitive et antisymétrique. Un ordre est souvent représenté par son *diagramme de Hasse*, dans lequel $x \leq y$ est exprimé en dessinant y au-dessus de x.

Il est important de garder à l'esprit qu'un ensemble peut être ordonné de bien des façons différentes.

Les relations d'ordre peuvent être combinées de plusieurs manières :

- Somme : étant donné deux ensembles ordonnés $(A, \leq)$ et $(B, \leq)$, nous pouvons construire un ordre sur $A + B$ via la relation $(x, i) \leq (y, j)$ ssi $i = j$ et $x \leq y$.
- Ordre produit : c'est l'ordre sur $A \times B$ donné par $(x, y) \leq (x', y')$ ssi $x \leq x'$ et $y \leq y'$.
- Ordre lexicographique : il s'agit d'un autre ordre sur $A \times B$ et il est donné par $(x, x') \leq (y, y')$ ssi $x < x'$ ou ($x = x'$ et $y \leq y'$).

XIX.5 Exercices

Exercice 262. Listez tous les ordres possibles sur les ensembles suivants et dessinez les diagrammes de Hasse correspondants :

(a) $\emptyset$

(b) 1 (un singleton)

(c) $\{a, b\}$

(d) $\{a, b, c\}$

(e) $\{a, b, c, d\}$

Exercice 263. Dessinez le diagramme de Hasse pour l'ordre d'inclusion (de sous-ensemble) sur $\mathcal{P}(A)$, où $A = \{1, 2, 3\}$.

Exercice 264. Donnez au moins trois relations d'ordre différentes sur l'ensemble $\mathbb{Z}$.

Exercice 265. Dessinez le diagramme de Hasse pour la relation de divisibilité sur $\mathbb{N}$, puis sur $\mathbb{Z}$ également.

Exercice 266. Dénotons l'ensemble de toutes les propositions par PROP. La relation $\vdash$ définie par

$$\phi \vdash \psi \Leftrightarrow (\phi \to \psi) \text{ est une tautologie}$$

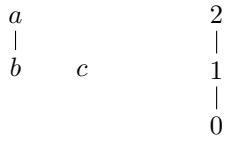
est-elle une relation d'ordre ?

Exercice 267. Soit $(A, \leq)$ un ensemble ordonné et soit $U \subseteq A$ un sous-ensemble de A. Considérez la relation $\leq \cap (U \times U)$ sur U. Démontrez qu'il s'agit d'une relation d'ordre. (Il s'agit de la *restriction* de l'ordre $\leq$ à U.)

Exercice 268. Soient $A = \{a, b, c\}$ et $B = \{0, 1, 2\}$. Considérez les relations suivantes sur A et sur B :

Déterminez les ordres produits sur $A \times B$ et sur $B \times A$. Déterminez également les ordres lexicographiques sur $A \times B$ et sur $B \times A$.

Exercice 269. Même question, mais pour



Exercice 270. Même question, mais pour

Exercice 271. Soit $A = \{1, 2, \ldots, 24\}$, et considérons la relation de divisibilité sur cet ensemble. Dessinez le diagramme de Hasse.

Exercice 272. Dessinez (en partie) le diagramme de Hasse pour l'ordre lexicographique sur $\mathbb{N} \times \mathbb{N}$. Même question, mais pour $\mathbb{N} \times \mathbb{Z}$.

Exercice 273. Soit $f : A \to B$ une fonction, et supposons que $\leq$ est un ordre sur B. Définissons une relation sur A par

$$x \leq y \Leftrightarrow_{\text{déf}} f(x) \leq f(y).$$

Démontrez que cette relation est un préordre.

Exercice 274. Soit A un ensemble, et considérons $\mathcal{P}(A)/\cong$, le quotient de $\mathcal{P}(A)$ par la relation $\cong$. Démontrez que l'inégalité $|U| \leq |V|$ pour les cardinalités est un ordre sur cet ensemble quotient.

Exercice 275. Soit A un ensemble, et considérons $\mathsf{Par}(A, B)$, l'ensemble des fonctions partielles de A vers B. (Il s'agit de relations univaluées tout simplement.) Écrivons $dom(f) = \{\, x \in A \mid \exists y. f(x) = y \,\}$, et définissons

$$f \leq g \Leftrightarrow \forall x \in dom(f). f(x) = g(x).$$

Démontrez que $\leq$ est un ordre sur l'ensemble des fonctions partielles.

Exercice 276. Soit R un préordre sur un ensemble A. Définissons une nouvelle relation $\sim$ sur A par $x \sim y \Leftrightarrow xRy \wedge yRx$. Démontrez qu'il s'agit là d'une relation d'équivalence, et que le quotient $A/\sim$ est muni d'une relation d'ordre induite par R.

LEÇON XX

Plus de théorie

Dans cette leçon, nous étudions quelques propriétés particulières que les ensembles ordonnés peuvent avoir. Entre autres, nous étudions les ensembles linéairement ordonnés et les ordres complets. Nous considérons également les chaînes dans les ensembles ordonnés.

XX.1 Linéarité

Il y a une différence notable entre l'ensemble ordonné par inclusion $\mathcal{P}(A)$ et l'ensemble ordonné $\mathbb{Z}$ avec l'ordre standard. Dans le premier cas, nous pouvons trouver des éléments U, V tels que U et V sont *incomparables*, au sens qu'aucun d'entre eux n'est inclu dans l'autre. Pour $\mathbb{Z}$ (ou même $\mathbb{N}, \mathbb{Q}$ ou $\mathbb{R}$, à cet effet), ceci est impossible : deux éléments sont toujours comparables. On formalise cette idée à travers la définition suivante :

Définition XX.1.1 (Linéarité)**.** Soit $(A, \leq)$ un ensemble ordonné. On dit que $(A, \leq)$ est *linéaire* si pour tout $x, y \in A$, nous avons $x \leq y$ ou $y \leq x$.

Les ensembles linéairement ordonnés sont également appelés des *ordres linéaires* ; certains textes emploient la terminologie *ordre total*, mais notez que ceci est en conflit avec le qualificatif « total » pour les relations.

Je vous ai déjà présenté les exemples standards d'ordres linéaires : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$. Voici un exemple un peu plus hors contexte de quelque chose qui est presque linéaire, mais pas tout à fait.

Exemple XX.1.2 (Droite avec deux origines)**.** Considérons l'ensemble $A = \mathbb{R} + \mathbb{R}$, constitué de deux copies de la droite réelle. Définissons une relation d'équivalence sur A par

$$(x, 0) \sim (y, 1) \Leftrightarrow_{\text{déf}} x = y \neq 0.$$

En d'autres termes, nous identifions les éléments de la forme $(a, 0)$ et $(a, 1)$, mais nous gardons les origines séparées. (Vous voudriez peut-être prouver qu'il s'agit effectivement d'une relation d'équivalence.)

Maintenant, considérons le quotient $A/\sim$. Cet ensemble hérite d'un ordre sur $\mathbb{R}$ qui n'est pas linéaire, car les deux origines sont incomparables entre elles. (Vérifiez les détails !)

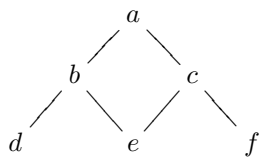
XX.2 Supremum et infimum

Définition XX.2.1 (Supremum)**.** Étant donné un ensemble ordonné $(A, \leq)$ et un sous-ensemble $U \subseteq A$, un *supremum* de U est un élément $a \in A$ tel que (1) $u \leq a$ pour tout $u \in U$, et (2) lorsque y est un élément de A avec $u \leq y$ pour tout $u \in U$, alors $a \leq y$.

Un supremum est également appelé une *plus petite borne supérieure* (ou *plus petit majorant*) : le supremum est une *borne supérieure* (ou *majorant*) au sens qu'il est au-dessus de tous les éléments de U, et il est le plus petit avec cette propriété. Puisqu'un ensemble U peut avoir au plus un supremum dans $(A, \leq)$ (vérifiez cela), nous pouvons écrire $\bigvee U$ pour désigner le supremum de U, dans la mesure où ce dernier existe. Si l'ensemble U a précisément deux éléments, disons $U = \{p, q\}$, alors nous écrivons $p \vee q$ pour désigner $\bigvee\{p, q\}$. Un supremum de cette forme est appelé un *supremum binaire*.

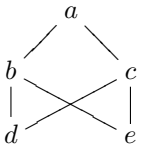
Exemples XX.2.2.

1. Considérez le diagramme de Hasse



   Nous avons $a = b \vee c$, $b = d \vee e$, $c = e \vee f$, $a = d \vee f = \bigvee\{d, e, f\} = \bigvee\{d, c, f\}$.

2. Dans le diagramme de Hasse



   l'ensemble $\{d, e\}$ n'a pas de supremum, mais il admet trois bornes supérieures (notamment a, b et c) et aucune n'est *la* plus petite.

3. Dans l'intervalle unité fermé, avec l'ordre usuel, nous avons $\bigvee\{1 - \frac{1}{n+1} | n \in \mathbb{N}\} = 1$. En effet, nous avons que 1 est une borne supérieure pour cet ensemble, car $1 - \frac{1}{n+1} < 1$ pour tout $n \in \mathbb{N}$. De plus, il est le plus petit avec cette propriété : si $y < 1$ était une borne supérieure, on pourrait prendre un n suffisamment grand pour obtenir $1 - \frac{1}{n+1} > y$. Contradiction.

4. Dans $\mathcal{P}(A)$, le supremum d'un ensemble de sous-ensembles est simplement leur union.

5. Certains ensembles n'admettent pas de supremum, simplement parce qu'ils ne sont pas majorés (i.e. n'admettent pas de borne supérieure). Par exemple, l'ensemble des nombres premiers (interprété comme un sous-ensemble de $\mathbb{N}$) n'admet pas de borne supérieure et, conséquemment, certainement pas une plus petite borne supérieure.

6. Même si un ensemble admet une borne supéreure, il n'existe pas nécessairement de plus petite borne supérieure. Considérez les nombres rationnels, et le sous-ensemble $U = \{ x \in \mathbb{Q} \mid x < \pi \}$. Cet ensemble admet une borne supérieure, mais il n'admet pas de plus petite borne supérieure, car π n'est pas un élément de $\mathbb{Q}$.

Si nous remplaçons $\leq$ par $\geq$, nous obtenons :

Définition XX.2.3 (Infimum)**.** Étant donné un ensemble ordonné $(A, \leq)$ et un sous-ensemble $U \subseteq A$, un *infimum* de U est un élément $a \in A$ tel que (1) $u \geq a$ pour tout $u \in U$, et (2) lorsque y est un élément de A avec $u \geq y$ pour tout $u \in U$, alors $a \geq y$.

Un infimum est également appelé une *plus grande borne inférieure* (ou *plus grand minorant*), et il est unique dans la mesure où il existe pour un sous-ensemble donné. Nous dénotons l'infimum de U par $\bigwedge U$. Les infimums dans $(A, \leq)$ sont simplement des supremums dans l'ordre opposé $(A, \leq^{op})$.

Un cas particulier pour les supremums et infimums vaut la peine d'être mentionné : Lorsque dans un ensemble ordonné $(A, \leq)$ le supremum $\bigvee A$ existe, on l'appelle le *maximum* de A (ou *plus grand élément* de A). Par dualité, $\bigwedge A$ est appelé le *minimum* de A (ou *plus petit élément* de A).

Par exemple, 0 est le plus petit élément de $\mathbb{N}$, et il n'y a pas de plus grand élément. Les entiers n'ont pas de minimum, ni de maximum. Dans $\mathcal{P}(X)$ avec l'ordre des sous-ensembles, l'ensemble vide est le plus petit élément, tandis que X lui-même est le plus grand élément.

Le lemme suivant constitue un exercice un peu trivial, mais tout de même utile.

Lemme XX.2.4. *Dans un ensemble ordonné $(A, \leq)$ avec un plus petit élément $\bot$, nous avons $\bigvee \emptyset = \bot = \bigwedge A$. Par dualité, si $\top$ est un plus grand élément, nous avons $\bigwedge \emptyset = \top = \bigvee A$.*

Démonstration. Supposons que $\bot$ est un plus petit élément. Nous devons démontrer qu'il est un supremum de l'ensemble vide, et un infimum de l'ensemble A. Le deuxième cas est évident. Pour le premier, considérons un élément arbitraire $a \in A$. Trivialement, a est un majorant pour l'ensemble vide. Ainsi, tous les éléments de A sont des majorants pour $\emptyset$. Un supremum pour $\emptyset$ est le plus petit de ces derniers ; donc, il s'agit du plus petit élément de A. L'énoncé dual admet une preuve similaire. □

Définition XX.2.5. Lorsqu'un ensemble ordonné $(A, \leq)$ admet un supremum et un infimum pour chaque sous-ensemble, on dit que son ordre est *complet*.

Les deux exemples canoniques d'ordres complets sont les suivants :

Exemple XX.2.6. L'ensemble des parties $\mathcal{P}(X)$ avec l'ordre d'inclusion est complet : les supremums sont les unions, et les infimums sont les intersections.

Exemple XX.2.7. L'intervalle unité fermé $[0, 1]$ est complet.

Les ensembles ordonnés suivants ne sont pas complets :

Exemples XX.2.8.

1. L'ensemble ordonné $\mathbb{Q} \cap [0, 1]$ avec l'ordre usuel n'est pas complet.

2. L'ensemble ordonné $\mathcal{P}_f(X)$ des sous-ensembles finis de X n'est pas complet lorsque X est un ensemble infini.

3. Étant donné qu'un ensemble ordonné complet admet un plus petit élément et un plus grand élément (voir le lemme XX.2.4), les ensembles ordonnés tel que $\mathbb{N}$, $\mathbb{Z}$, , $\mathbb{Q}$, $\mathbb{R}$ ne sont pas complets.

On ne soulignera jamais assez l'importance de la complétude de $[0,1]$ (ou de n'importe quel sous-ensemble fermé et borné de $\mathbb{R}$). Il s'agit en fait d'une propriété clé pour la définition des nombres réels, et c'est ce qui les distingue des nombres rationnels.[1]

Quoique les supremums et les infimums diffèrent, techniquement parlant, ils entretiennent tout de même un rapport entre eux. Le lemme suivant explique en quoi consiste ce rapport.

Lemme XX.2.9. *Si un ensemble ordonné a tous les infimums, alors il a tous les supremums. (La réciproque est également vraie.)*

Démonstration. Supposons que $(A, \leq)$ a tous les infimums. En particulier, par le lemme XX.2.4, il a un plus grand élément. Ainsi, tout sous-ensemble $U \subseteq A$ admet une borne supérieure. Or, pour un sous-ensemble U de A, considérons l'ensemble

$$V = \{\, x \in A \,|\, x \text{ est une borne sup. de } U \,\}$$

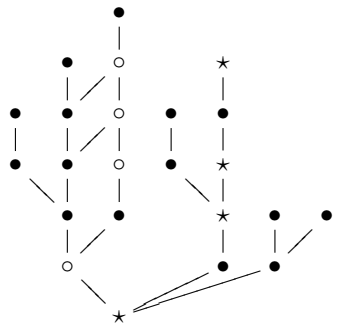
et posons $b = \bigwedge V$. À vérifier : b est un supremum de U. Premièrement, notez que si $u \in U$, alors $u \leq b$, car u est une borne inférieure de V et b est la plus grande borne inférieure de V. Ainsi, b est une borne supérieure de U. Maintenant, considérons une borne supérieure arbitraire x de U. Nous avons donc $x \in V$. Mais, $b \leq x$ par définition de b, et nous avons terminé la preuve. □

XX.3 Chaînes

Les chaînes sont des sous-ensembles particuliers d'ensembles ordonnés qui jouent un rôle important en pratique.

Définition XX.3.1 (Chaîne)**.** Une *chaîne* dans un ensemble ordonné $(A, \leq)$ est un sous-ensemble U de A qui est linéairement ordonné (avec l'ordre de A restreint à U).

L'image suivante illustre deux chaînes : l'une donnée par le sous-ensemble des éléments dénotés $\circ$, l'autre par le sous-ensemble des éléments dénotés $\star$.



[1] Techniquement, les nombres réels sont définis en termes des nombres rationnels ; $\mathbb{R}$ est ce que nous obtenons lorsque nous « ajoutons les supremums manquants dans $\mathbb{Q}$ ». Dans votre cours d'analyse, cette construction est entreprise de manière plus précise.

Nous pouvons constater, à travers l'exemple précédent, qu'une chaîne peut « sauter » des éléments.

Exemple XX.3.2. Si $A = \mathcal{P}(\mathbb{N})$, alors le sous-ensemble

$$U = \{\, \{0, \ldots, n\} \mid n \in \mathbb{N} \,\}$$

est une chaîne. Une autre chaîne dans cet ensemble ordonné est l'ensemble $\{\, \mathbb{N} - \{0, \ldots, n\} \mid n \in \mathbb{N} \,\}$.

Un concept un peu plus raffiné est celui d'une suite croissante ou décroissante. Lorsque A est un ensemble, une *suite* d'éléments dans A est simplement une fonction $f : \mathbb{N} \to A$. Nous écrivons parfois a_0, a_1, a_2, ... pour désigner une suite $f(0)$, $f(1)$, $f(2)$, ... Par exemple, la fonction $f(n) = \frac{1}{n+1}$ définit une suite dans $\mathbb{R}$, et celle-ci peut également s'écrire sous la forme 1, $\frac{1}{2}$, $\frac{1}{3}$, ...

Lorsque A est un ensemble avec un ordre, nous pouvons donner un sens à cette classe de suites qui prennent cet ordre en considération ; c'est là l'objet de la définition suivante :

Définition XX.3.3 (Suite croissante)**.** Soit $(A, \leq)$ un ensemble ordonné, et $f : \mathbb{N} \to A$ une suite dans A. On dit que f est une *suite croissante* lorsque $i \leq j$ implique $f(i) \leq f(j)$. Si $i < j$ implique $f(i) < f(j)$, alors f est dite *strictement croissante*.

Il y a un concept dual évident pour définir une suite décroissante, et nous vous laissons le soin de donner un sens précis à cette définition. Une suite croissante est parfois dite *monotone*.

Exemples XX.3.4.

1. La suite 0, $\frac{1}{2}$, $\frac{2}{3}$, $\frac{3}{4}$, ... est strictement croissante dans $\mathbb{Q}$.
2. La fonction identité sur $\mathbb{N}$ est une suite strictement croissante.
3. La fonction $f(x) = \lfloor \frac{x}{2} \rfloor$ est une suite croissante dans $\mathbb{N}$. (Notez qu'elle répète des éléments ; ceci est permis dans la définition d'une suite croissante, mais nous n'obtenons pas une suite stricte dans ce cas.)
4. La suite $a_n = -2^n$ est strictement décroissante dans $\mathbb{Z}$.
5. Toute fonction constante est croissante, de même que décroissante (mais pas stricte).
6. La suite $\{0\}, \{0, 2\}, \{0, 2, 4\}, \{0, 2, 4, 6\}$, ... est strictement croissante dans $\mathcal{P}(\mathbb{N})$.
7. La fonction $f : \mathbb{N} \to \mathbb{R}$ donnée par $f(n) = 2^{-n}$ est une suite strictement décroissante dans $\mathbb{R}$.

Plus tôt, nous avons énoncé que l'intervalle unité fermé $[0, 1]$ est complet, au sens qu'il a tous les infimums et les supremums. Nous pouvons maintenant présenter une variante de cette idée :

Proposition XX.3.5. *Considérons une suite a_0, a_1, ... dans $\mathbb{R}$ qui est bornée supérieurement, au sens qu'il existe $q \in \mathbb{R}$ tel que $a_i \leq q$ pour tout $i \in \mathbb{N}$. Alors, la chaîne $\{\, a_i \mid i \in \mathbb{N} \,\}$ admet un supremum.*

Démonstration. Prenons une borne supérieure q pour cette suite. Les valeurs a_i ne sont pas nécessairement contenues dans un intervalle borné et fermé $[p, q]$, car la suite peut admettre des éléments arbitrairement petits. Posons $p = a_0$, et considérons le sous-ensemble U de $\{\, a_i \mid i \in \mathbb{N} \,\}$ qui contient les a_i pour lesquels $p \leq a_i$. Il s'agit d'un sous-ensemble non vide, et il est contenu dans l'intervalle borné et fermé $[p, q]$, lequel est complet. Donc, $\bigvee U$ est le supremum de $\{\, a_i \mid i \in \mathbb{N} \,\}$. □

La complétude des intervalles fermés dans $\mathbb{R}$ a une autre conséquence d'intérêt :

Propriété d'Archimède :
Il n'existe pas de nombres réels positifs x, y tels que, pour tout $n \in \mathbb{N}$, nous avons $nx < y$.

La démonstration procède comme suit : Tout d'abord, on dit qu'un élément x est *infinitésimal* par rapport à un élément y lorsque pour tout $n \in \mathbb{N}$, nous avons $nx < y$. Considérons un y positif arbitraire, et posons I comme étant l'ensemble de tous ces infinitésimaux positifs x par rapport à ce y. Maintenant, faisons quelques observations à propos de I. Pour commencer, notons que pour $x \in I$, nous avons $nx \in I$ pour tout nombre naturel positif n. De plus, notons que si $x \in I$, alors $\frac{x}{n} \in I$ pour tout nombre naturel positif n. Finalement, si $0 < x' < x$ et $x \in I$, alors $x' \in I$ également. Supposons maintenant que I n'est pas vide. Alors, nous avons $I \subseteq (0, 1)$ car, clairement, un nombre $x \geq 1$ ne peut pas être infinitésimal. Posons $a = \bigvee I$. Donc, a est positif. Question : a est-il lui-même infinitésimal ? Si c'est le cas, alors $2a$ est aussi infinitésimal. Ceci est une contradiction, car $2a > a$ et a est le supremum de I. Donc, a n'est pas infinitésimal. Mais alors, $\frac{a}{2}$ ne peut pas être infinitésimal non plus. Ceci nous donne encore une contradiction, car ce dernier nous donnerait un supremum de I sinon. La seule possibilité est d'admettre que $I = \emptyset$.

XX.4 Sommaire

Nous avons considéré deux types d'ordres : les ordres *linéaires* (dans lesquels deux éléments sont toujours comparables) et les ordres *complets* (dans lesquels tout sous-ensemble admet un infimum et un supremum).

- Pour un sous-ensemble ordonné A, le *supremum* (plus petite borne supérieure) $\bigvee U$ d'un sous-ensemble U de A est un élément satisfaisant

$$\forall x \in U.x \leq \bigvee U \quad \wedge \quad \forall y \in A[\forall x \in U.x \leq y \rightarrow \bigvee U \leq y].$$

- Pour un sous-ensemble ordonné A, l'*infimum* (plus grande borne inférieure) $\bigwedge U$ d'un sous-ensemble U de A est un élément satisfaisant

$$\forall x \in U.x \geq \bigwedge U \quad \wedge \quad \forall y \in A[\forall x \in U.x \geq y \rightarrow \bigwedge U \geq y].$$

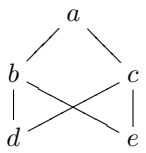
Finalement, nous avons étudié les *suites croissantes* (de même que le concept dual des suites décroissantes) : il s'agit de fonctions $f : \mathbb{N} \rightarrow A$ satisfaisant $x \leq y \Rightarrow f(x) \leq f(y)$.

La *propriété d'Archimède* (que les nombres réels admettent) énonce qu'il n'y a pas de nombres positifs x, y tels que, pour tout nombre naturel $n \in \mathbb{N}$, nous avons $nx < y$.

XX.5 Exercices

Exercice 277. Considérez l'ensemble $A = \{a, b, c, d\}$. Trouvez tous les ordres linéaires sur A.

Exercice 278. Considérez le diagramme de Hasse



$\{d, c, a\}$ est-il une chaîne ? Qu'en est-il de $\{d, a\}$? Et de $\{d, b, c\}$?

Exercice 279. Prouvez qu'un ordre linéaire fini admet un plus petit élément et un plus grand élément.

Exercice 280. Démontrez que pour un ordre linéaire, tout sous-ensemble fini admet un supremum et un infimum.

Exercice 281. Considérez la fonction $a : \mathbb{N} \to \mathbb{R}$ définie par $a(n) = \sin(2\pi n(1 + \frac{1}{10^{100}})$. S'agit-il d'une suite croissante ?

Exercice 282. Démontrez que si $(A, \leq)$ est un ordre linéaire, alors, pour tout $U \subseteq A$, l'ordre de A restreint à U est également linéaire.

Exercice 283. Démontrez qu'il existe des suites croissantes dans $\mathbb{Q}$ dont le supremum est dans $\mathbb{R}$, mais pas dans $\mathbb{Q}$.

Exercice 284. Expliquez la différence, en ce qui a trait à l'existence des supremums et des infimums, entre l'intervalle unité ouvert $(0, 1)$ et l'intervalle unité fermé $[0, 1]$.

Exercice 285. Supposons que $(A, \leq)$ et $(B, \leq)$ sont des ensembles ordonnés. Pour chaque cas suivant, donnez une preuve ou un contre-exemple.

(a) Si A et B ont chacun un plus petit élément, alors l'ordre produit sur $A \times B$ également.

(b) Si A et B ont chacun un plus petit élément, alors l'ordre lexicographique sur $A \times B$ également.

(c) Si A et B sont linéaires, alors l'ordre produit sur $A \times B$ aussi.

(d) Si A et B sont linéaires, alors l'ordre lexicographique sur $A \times B$ aussi.

Exercice 286. Prouvez (en détails) l'assertion faite à propos de l'ensemble I des nombres infinitésimaux.

Exercice 287. Démontrez que la propriété d'Archimède est équivalente à l'énoncé que, pour tout nombre positif réel x, il existe $n \in \mathbb{N}$ tel que $\frac{1}{n} < x$.

Exercice 288. Dans un ensemble ordonné avec tous les supremums, démontrez que $U \subseteq V$ implique $\bigvee U \leq \bigvee V$. La réciproque est-elle vraie ?

Exercice 289. Considérons $\mathbb{N} + \{\infty\}$, ordonné à la façon standard, mais en rajoutant : $x \leq \infty$ pour tout x. Démontrez que cet ensemble ordonné est complet.

Exercice 290. Démontrez que, si un ensemble ordonné satisfait $\{a \wedge b, a \vee b\} = \{a, b\}$ (pour tous éléments a, b), alors il est linéaire. La réciproque est-elle vraie ?

Exercice 291. Donnez un exemple d'ensemble ordonné qui est complet, mais qui ne satisfait pas la loi de distributivité

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Indice : vous avez besoin de seulement 5 éléments.

Exercice 292. La loi de distributivité infinie est

$$a \wedge \bigvee U = \bigvee \{a \wedge u | u \in U\}.$$

Prouvez que $\mathcal{P}(X)$ satisfait cette loi. Quelle principe de la logique des prédicats est analogue à cette loi ?

LEÇON XXI

Ensembles bien ordonnés

Lorsque nous avons étudié l'axiome du choix, nous avons découvert que pour certains ensembles munis d'un ordre, la tâche de choisir un élément dans un ensemble non vide était facile. Souvent, étant donné un sous-ensemble non vide, on choisissait le plus petit élément de ce sous-ensemble.

Bien entendu, ceci ne fonctionne pas toujours : $\mathbb{R}$ est muni d'un ordre, mais ce ne sont pas tous les sous-ensembles non vides qui ont un plus petit élément. Le problème est que l'ordre en question n'est pas « assez bon » (même s'il est linéaire). Dans cette leçon, nous étudions les *bons ordres*, qui sont les ordres pour lesquels nous pouvons toujours résoudre notre problème d'effectuer un choix. Nous discutons également de certaines applications que l'ont rencontre souvent en pratique, notamment le lemme de Zorn.

XXI.1 Bon ordre

Nous commençons avec une définition :

Définition XXI.1.1 (Bon ordre)**.** Un ensemble ordonné $(A, \leq)$ est dit *bien ordonné* lorsque tout sous-ensemble non vide de A admet un plus petit élément. Dans ce cas, on dit aussi que $\leq$ est un *bon ordre*.

Quelques exemples ont déjà été présentés, mais voici un compte-rendu plus précis :

Exemples XXI.1.2.

1. Les nombres naturels $\mathbb{N}$ avec l'ordre usuel constituent l'exemple archétype de bon ordre.
2. Les entiers $\mathbb{Z}$ avec l'ordre usuel ne sont *pas* bien ordonnés. Par exemple, le sous-ensemble $\mathbb{Z}$ n'a pas de plus petit élément. Même problème avec $\mathbb{Q}$ et $\mathbb{R}$.

3. L'intervalle unité rationnel fermé $\{\, x \in \mathbb{Q} \mid 0 \leq x \leq 1 \,\}$ n'est pas bien ordonné : le sous-ensemble $\{\frac{1}{n+1} | n \in \mathbb{N}\}$ est non vide, mais n'admet pas de plus petit élément. Il en est de même pour l'intervalle unité réel fermé.

4. Tout ordre linéaire fini est un bon ordre.

5. Considérez $A = \{0, 1\} \times \mathbb{N}$ avec l'ordre lexicographique (lequel ressemble, dans ce cas, à deux copies de $\mathbb{N}$ empilées l'une par dessus l'autre). Il s'agit d'un bon ordre : Étant donné un sous-ensemble non vide U de A, demandez-vous tout d'abord si U contient un élément de la forme $(0, n)$. Si oui, il existe un plus petit n avec une étiquette 0. Sinon, tous les éléments sont de la forme $(1, m)$, et il doit y avoir un plus petit m avec une étiquette 1.

Le lemme suivant, dont la preuve est laissée en exercice (recommandé), établit quelques-unes des propriétés de base des bons ordres.

Lemme XXI.1.3. *Si $(A, \leq)$ est un bon ordre, alors*

- *il admet un plus petit élément,*
- *il est linéaire,*
- *tout sous-ensemble $Y \subseteq A$ est à nouveau un bon ordre avec l'ordre restreint à Y.*

Les ensembles bien ordonnés peuvent également être caractérisés en termes de suites décroissantes. Nous employons la terminologie suivante : une suite décroissante a_0, a_1, a_2, ... *devient stationnaire* lorsqu'il existe un $N \in \mathbb{N}$ tel que $a_i = a_N$ pour tout $i \geq N$.

Proposition XXI.1.4. *Un ordre linéaire $(A, \leq)$ est un bon ordre si et seulement si toute suite décroissante dans A devient stationnaire.*

Démonstration. Supposons que A est bien ordonné et que a_0, a_1, ... est une suite décroissante. Alors, l'ensemble $\{a_i | i \in \mathbb{N}\}$ a un plus petit élément, disons a_N. Puisque la suite est décroissante, nous avons que $a_i \leq a_N$ pour tout $i \geq N$. Mais, avec $a_N \leq a_i$ pour tout $i \in \mathbb{N}$, nous pouvons aisément constater que la suite devient stationnaire à partir du N-ième pas.

Réciproquement, supposons que toute suite décroissante dans A devient stationnaire, et considérons un sous-ensemble non vide $U \subseteq A$. Considérons un élément a_0 dans U. S'il existe un élément strictement plus petit que a_0 dans U, dénotons le a_1 et poursuivons ; sinon, posons $a_1 = a_0$. Nous continuons de cette façon pour obtenir une suite décroissante a_0, a_1, a_2, ... Étant donné que cette suite devient stationnaire après N pas, pour un certain N, ceci veut dire qu'il n'y a pas d'élément dans U qui est strictement plus petit que a_N. Donc, ce a_N est le plus petit élément de U. [Notez : cette dernière étape emploie la linéarité de $(A, \leq)$.] □

XXI.2 Choix, ordre et lemme de Zorn

Tel qu'énoncé antécédemment, nous accordons un intérêt particulier à l'étude des ensembles bien ordonnés, principalement parce qu'ils nous permettent de définir explicitement une fonction de choix.[1]

[1] Un autre aspect important est que les ensembles bien ordonnés admettent un principe d'induction qui généralise le principe d'induction habituel sur les nombres naturels.

Ceci nous mène au questionnement suivant : un ensemble arbitraire peut-il toujours être muni d'un bon ordre ? Par exemple, est-il possible d'établir un bon ordre sur les nombres réels ?

Définition XXI.2.1 (Axiome du bon ordre)**.** Tout ensemble peut être bien ordonné. C'est-à-dire, pour tout ensemble X, il existe un ordre $\leq$ sur X qui est un bon ordre.

Proposition XXI.2.2. *L'axiome du bon ordre implique l'axiome du choix.*

Démonstration. Nous démontrons que si X peut être bien ordonné, alors une fonction de choix existe pour X. Donc, supposons que $(X, \leq)$ est un bon ordre pour X. Nous devons définir une fonction de choix $s : \mathcal{P}_+(X) \to X$. Posons, pour un sous-ensemble non vide $U \subseteq X$,

$$s(U) = \text{le plus petit élément de } U.$$

Cette opération est sensée car, par la définition d'un bon ordre, U admet un plus petit élément (lequel est nécessairement unique). De toute évidence, nous avons $s(U) \in U$, donc s est une fonction de choix. □

En fait, l'implication réciproque est également vraie, et nous allons voir cela dans un instant. Toutefois, à cette étape, il convient d'introduire un troisième principe, appelé le lemme de Zorn. Avant que nous le présentions, il nous faut un peu de terminologie :

Définition XXI.2.3 (Élément maximal)**.** Un élément a dans un ensemble ordonné $(A, \leq)$ est *maximal* lorsqu'il n'y a pas de $b \in A$ tel que $a < b$.

Un maximum (plus grand élément) est un élément maximal, mais la réciproque n'est pas vraie. Un contre-exemple est donné par l'ordre Δ_A sur un ensemble A, où chaque élément est maximal, mais aucun n'est le maximum. Notez aussi, en général, qu'un ensemble ordonné peut avoir plus d'un élément maximal.

Le lemme de Zorn se pose alors comme suit :

Lemme de Zorn :
Si $(A, \leq)$ est un ensemble ordonné dans lequel toute chaîne admet une borne supérieure, alors $(A, \leq)$ admet un élément maximal.

Avant de prouver le lemme de Zorn, considérons une application typique de celui-ci. Supposons que nous voulons montrer que tout espace vectoriel V admet une base. Intuitivement, nous commençons par choisir n'importe quel vecteur non nul a_0 dans V ; et si ce dernier génère V, alors nous avons terminé. Sinon, nous pouvons choisir un vecteur a_1 qui est linéairement indépendant de a_0. Si $\{a_0, a_1\}$ génère V, alors nous avons terminé ; sinon, nous continuons ainsi. Si V est de dimension finie, ce processus s'arrête après un nombre fini d'étapes. Mais qu'arrive-t-il si V est vraiment très grand ? Par exemple, V pourrait être l'espace des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Dans ce cas, une base de V est non dénombrable, et ajouter des éléments un à un prendra un certain temps...

Le lemme de Zorn « résout » ce problème. Considérons l'ensemble ordonné P dont les éléments sont les paires (U, A) pour lesquelles U est un sous-espace de V, et A est une base de U. L'ordre est donné

par $(U, A) \leq (V, B)$ ssi $U \subseteq V$ et $A \subseteq B$. Si nous avons une chaîne $K = \{(U_i, A_i) | i \in I\}$ dans P, alors il existe une borne supérieure pour celle-ci : il suffit de prendre le plus petit sous-espace de V qui est généré par l'union $U = \bigcup_{i \in I} U_i$. Aussi, l'ensemble $A = \bigcup_{i \in I} A_i$ donne une base de U, et donc (U, A) est une borne supérieure de la chaîne. Le lemme de Zorn affirme que P admet un élément maximal (W, C). À vérifier : $U = W$, et le C en question nous donne la base cherchée. Preuve : Supposons que $W \neq V$. Alors, il existe un vecteur $v \in V$ qui n'est pas dans W (et ainsi, il n'est pas une combinaison linéaire de vecteurs dans W). Considérons le sous-espace de V défini par $W' = span(W \cup \{v\})$. Nous obtenons que $C' = C \cup \{v\}$ est une base pour W'. Mais ceci veut dire que $(W, C) < (W', C')$, ce qui contredit la maximalité de (W, C).

Plusieurs applications mathématiques suivent ce patron : ils invoquent le lemme de Zorn pour démontrer l'existence d'un certain objet mathématique, plutôt que d'employer l'axiome du choix directement.

Maintenant, nous énonçons le résultat principal :

Théorème XXI.2.4. *L'axiome du choix, l'axiome du bon ordre et le lemme de Zorn sont équivalents.*

Démonstration. Nous avons déjà expliqué que l'axiome du choix découle de l'axiome du bon ordre. Il suffit, dès lors, de prouver que l'AC implique le lemme de Zorn, et que le lemme de Zorn implique l'axiome du bon ordre.

Une preuve rigoureuse que AC implique Zorn fait appel à la récurrence transfinie (ou induction transfinie), mais l'idée générale est relativement plus simple. Supposons que nous avons un ensemble ordonné $(A, \leq)$ dans lequel toute chaîne admet une borne supérieure. Supposons qu'il n'existe pas d'élément maximal. Maintenant, étant donné une chaîne C dans A, nous pouvons trouver une borne supérieure a_C pour C, puis un élément strictement plus grand $f(C) > a_C$. Choisissons, pour chaque chaîne C, un tel élément $f(C)$. Ensuite, définissons (par induction) une chaîne en prenant a_0 arbitrairement, puis en prenant $a_k = f\{a_i | i < k\}$. Ceci nous donne une contradiction car, passé un certain point, la chaîne devient « trop grande » : sa cardinalité ne devrait jamais excéder celle de A.

Finalement, nous prouvons que le lemme de Zorn implique l'axiome du bon ordre. Considérons un ensemble A (pour lequel nous cherchons à établir un bon ordre). Considérons l'ensemble ordonné P dont les éléments sont les paires $(U, \leq_U)$, où U est un sous-ensemble de A et $\leq_U$ est un bon ordre sur U. L'ordre se définit comme suit : $(U, \leq_U) \leq (V, \leq_V)$ ssi $U \subseteq V$ et $\leq_U$ est la restriction de $\leq_V$ à U. Considérons une chaîne $C = \{ (U_i, \leq_{U_i}) \,|\, i \in I \}$ dans P. Alors, pour $U = \bigcup_{i \in I} U_i$ avec l'ordre évident $\leq_U$, nous obtenons que $(U, \leq_U)$ est une borne supérieure de C. Ainsi, la condition pour le lemme de Zorn est satisfaite, et il existe un élément maximal $(W, \leq_W)$ dans P. À vérifier : $W = A$. Supposons que $W \neq A$. Alors, il existe $a \in A$ avec $a \notin W$. Construisons une extension de $(W, \leq_W)$ en plaçant a en-dessous de tous les éléments de W. Ainsi, nous avons un bon ordre sur $W \cup \{a\}$, ce qui contredit la maximalité de W. □

XXI.3 Sommaire

Un *ensemble bien ordonné* est un ensemble ordonné dans lequel tout sous-ensemble non vide admet un plus petit élément. Un bon ordre est linéaire et admet un plus petit élément, mais la réciproque est fausse. Un bon ordre sur un ensemble nous donne une fonction de choix pour cet ensemble.

L'*axiome du bon ordre* énonce que tout ensemble peut être bien ordonné. (Notez : ceci ne veut pas dire que tout ordre est un bon ordre.)

Le *lemme de Zorn* énonce que, si toute chaîne dans un ensemble ordonné admet une borne supérieure, alors cet ensemble admet au moins un élément maximal. Le lemme de Zorn, l'axiome du choix et l'axiome du bon ordre sont équivalents.

Le lemme de Zorn est la forme (de l'axiome du choix) qui est la plus fréquemment employée en mathématiques. En particulier, ce lemme est employé pour démontrer que tout espace vectoriel admet une base, et aussi, pour démontrer que tout corps admet une fermeture algébrique.

XXI.4 Exercices

Exercice 293. Démontrez que tout ordre linéaire fini est un bon ordre.

Exercice 294. Donnez un exemple pour démontrer qu'un ensemble ordonné sans maximum peut avoir la propriété que toute chaîne admet une borne supérieure. Un tel ensemble peut-il être infini ?

Exercice 295. Considérons l'ensemble ordonné $\mathsf{Par}(A, B)$ des fonctions partielles de A vers B (ordonné par $f \leq g$ ssi $f(x) = g(x)$ pour tout $x \in dom(f)$). Démontrez que toute chaîne dans cet ensemble ordonné admet une borne supérieure. À quoi ressemblent les éléments maximaux ? Y a-t-il un maximum ?

Exercice 296. Considérons l'ensemble ordonné $\mathsf{Rel}(A, B)$ des relations de A vers B, ordonné par l'inclusion. Démontrez que toute chaîne admet une borne supérieure. Quels sont les éléments maximaux ? Y a-t-il un maximum ?

Exercice 297. Dans un ensemble ordonné $(X, \leq)$, on dit qu'un élément y est un *successeur* d'un élément x si $x < y$, et si, de plus, $x \leq z \leq y$ implique $x = z$ ou $x = y$. Intuitivement, y est au-dessus de x, mais il n'y a rien entre les deux.

(a) Dans l'ensemble ordonné $(\mathbb{N}, \leq)$, quel est le successeur d'un élément n ?

(b) Dans l'ensemble ordonné $(\mathbb{Q}, \leq)$, l'élément 3 a-t-il un successeur ?

(c) Démontrez que, dans un ensemble ordonné fini, tout élément est maximal (n'a pas d'élément au-dessus de lui) ou a un successeur.

(d) Donnez un exemple d'ordre dans lequel il y a un élément avec plus d'un successeur.

(e) Démontrez que si x n'est pas un élément maximal dans un ensemble bien ordonné, alors il admet un successeur unique.

(f) Donnez un exemple d'ensemble bien ordonné avec un élément qui n'est pas le plus petit élément, et qui n'est pas le successeur de quoi que ce soit non plus.

LEÇON XXII

INDUCTION

Dans cette dernière leçon, nous allons explorer une stratégie importante de preuve appelée l'induction. Dans sa forme la plus simple, l'induction est utilisée pour prouver des énoncés à propos des nombres naturels, et c'est ce sur quoi nous portons notre attention dans cette leçon. Toutefois, il est à noter qu'il existe bien d'autres circonstances dans lesquelles l'induction peut être employée de manière profitable.

XXII.1 PRINCIPE DE BASE

Supposons que nous devons prouver que tous les éléments d'un ensemble donné X ont une certaine propriété P, c'est-à-dire que $\forall x \in X.P(x)$. Si l'ensemble X est fini et petit, nous pouvons faire la vérification pour tous les éléments un à un. Mais que faire lorsque X est infini ? La logique des prédicats suggère de prendre un élément arbitraire x dans X, puis de démontrer que $P(x)$ est vrai. Parfois, ceci fonctionnera, mais dans d'autres cas, effectuer une preuve ainsi s'avérera difficile.

L'idée qui sous-tend l'induction (aussi appelée induction mathématique) est d'exploiter le fait que, dans certains cas, nous en savons un peu plus sur la façon dont X est érigé. Les nombres naturels ne sont pas qu'une antiquité agissant comme un ensemble infini. Chose certaine, nous savons que $\mathbb{N}$ est un ensemble bien ordonné et, ainsi, qu'il a un plus petit élément, que tout élément a un successeur unique et que tout élément non égal à zéro admet un prédécesseur unique. Une façon légèrement différente de voir les choses est la suivante : si nous voulons « générer » systématiquement l'ensemble $\mathbb{N}$ des nombres naturels, il suffit de commencer avec 0, puis d'ajouter $n+1$ chaque fois que n est présent. Plus formellement, $\mathbb{N}$ est un ensemble A avec les propriétés suivantes :

- $0 \in A$
- $n \in A$ implique $n + 1 \in A$.

Un ensemble A avec ces deux propriétés est appelé *inductif*. Bien entendu, $\mathbb{N}$ n'est pas le seul ensemble avec ces propriétés. Par exemple, les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et ainsi de suite, sont inductifs. Toutefois, et ceci est le point crucial, $\mathbb{N}$ est le *plus petit* ensemble avec ces propriétés. Ceci veut dire que pour tout ensemble inductif A, nous avons $\mathbb{N} \subseteq A$.

Théorème XXII.1.1. *Si $A \subseteq \mathbb{N}$ est un ensemble inductif, alors $A = \mathbb{N}$.*

Démonstration. Supposons que $A \neq \mathbb{N}$. Alors, l'ensemble $\mathbb{N} - A$ est non vide. Étant donné que $\mathbb{N}$ est bien ordonné, il existe un plus petit élément de $\mathbb{N} - A$, disons k. On ne peut pas avoir $k = 0$, car $0 \in A$. Et puisque k est le plus petit élément de $\mathbb{N} - A$, l'élément $k - 1$ doit être dans A. Mais A est inductif, donc $k \in A$. Contradiction. □

En quoi ceci nous permettrait-il de prouver des choses à propos des nombres naturels ? Et bien, supposons que nous voulons vérifier que tous les nombres naturels ont une certaine propriété P. Considérons l'ensemble

$$A = \{x \in \mathbb{N} \mid P(x)\},$$

c'est-à-dire, l'ensemble de tous les nombres qui ont cette propriété. Nous voulons démontrer que $A = \mathbb{N}$ — mais le théorème nous dit qu'il suffit de démontrer que A est inductif. En déballant cette définition, nous obtenons un principe bien connu, le principe d'induction mathématique :

Induction mathématique :
Supposons que P est une propriété sur les nombres naturels. Pour prouver $\forall x \in \mathbb{N}.P(x)$, il suffit de prouver les deux énoncés suivants :

- $P(0)$ est vrai.
- Pour tout k, si $P(k)$ est vrai, alors $P(k+1)$ aussi.

Une façon courante d'imaginer les choses est de penser à une séquence de dominos : pour faire tomber tous les dominos, il suffit de faire tomber le premier (correspondant au nombre 0), puis de s'assurer que tout domino qui tombe fera aussi tomber celui qui vient juste après.

Quelques remarques sont de mise. Premièrement, prouver $P(0)$ constitue habituellement ce qu'on appelle l'*étape de base* de l'induction (ou *cas de base* de l'induction). L'étape suivante (prouver que $P(k)$ implique $P(k+1)$ pour un k arbitraire) est appelée l'*étape inductive* (ou *cas inductif*). Deuxièmement, lorsque vous effectuez la preuve de l'étape inductive, vous êtes confrontés à un énoncé de la forme

$$\forall k.[P(k) \to P(k+1)].$$

Ceci veut dire que vous devez considérer un k arbitraire, supposer que $P(k)$ est vrai, puis démontrer que $P(k+1)$ est également vrai. Lorsqu'on émet l'hypothèse $P(k)$ dans une telle preuve, on l'appelle habituellement *hypothèse d'induction* (abrév. H.I.). Il est de bonne pratique de clairement identifier tous les ingrédients dans votre preuve. Finalement, il arrive souvent que nous voulons prouver que tous les nombres, à l'exception de quelques-uns, satisfont la propriété P. Par exemple, si nous voulons prouver que tous les nombres plus grands que 2 ont cette propriété, nous devons considérer $P(3)$ comme étant le cas de base, puis prouver le cas inductif $\forall k \geq 3.[P(k) \to P(k+1)]$. Les exemples de la section suivante illustrent plus en détails cette procédure.

XXII.2 Exemples

Nous abordons maintenant un certain nombre d'exemples de preuves par induction.

Exemple XXII.2.1. Employez l'induction mathématique pour prouver que tout nombre naturel est soit pair, soit impair.

Démonstration. Nous voulons démontrer l'énoncé $\forall x \in \mathbb{N}.P(x)$, où la propriété en question est donnée par :

$$P(n) : n \text{ est pair ou } n \text{ est impair}$$

ou, en déballant les définitions utilisées, par :

$$P(n) : n = 2k \text{ pour un } k \in \mathbb{N} \text{ ou } n = 2k + 1 \text{ pour un } k \in \mathbb{N}.$$

Cas de base : $n = 0$. Nous devons montrer que $P(0)$ est vrai, i.e. que 0 est soit pair, soit impair. Mais $0 = 2 \cdot 0$, et donc 0 est pair. Ainsi, 0 a la propriété P, tel que voulu.

Étape inductive : Considérons un nombre $k \in \mathbb{N}$ arbitraire, et supposons que $P(k)$ est vrai. Ceci veut dire :

$$P(k) : k \text{ est pair ou impair.} \qquad \text{(H.I.)}$$

Nous démontrons à présent que $P(k+1)$ est vrai, i.e. que $k+1$ est soit pair, soit impair. Pour ce faire, considérons les deux cas suivants (selon notre hypothèse, ceux-ci sont mutuellement exhaustifs). Cas 1 : k est pair. Donc, $k = 2m$ pour un nombre naturel m. Puis, $k + 1 = 2m + 1$, ce qui démontre que $k + 1$ est impair. Nous obtenons que $P(k + 1)$ est vrai dans ce cas. Cas 2 : k est impair. Donc, $k = 2m + 1$ pour un nombre naturel quelconque m. Puis, $k + 1 = 2m + 2 = 2(m + 1)$, ce qui démontre que $k + 1$ est pair. Nous obtenons que $P(k + 1)$ est vrai dans ce cas également. Puisque $P(k + 1)$ est vrai dans tous les cas, ceci complète l'étape inductive.

Étant donné que $P(0)$ est vrai et que $P(k)$ implique $P(k + 1)$ pour tout k, nous pouvons conclure, par le principe d'induction mathématique, que $\forall n \in \mathbb{N}.P(n)$ est vrai. □

Dans l'exemple précédent, notez que nous

- énonçons la propriété P que nous cherchons à établir.
- énonçons le cas de base (et expliquons en quoi il consiste).
- énonçons l'étape inductive.
- énonçons l'hypothèse d'induction.
- concluons en disant que le résultat cherché découle de l'application du principe d'induction mathématique.

Toute preuve par induction que vous écrivez devrait contenir ces ingrédients. Certes, dans certains textes, vous verrez des preuves qui gardent certains de ces détails implicites ; mais, pour apprendre comment faire l'induction correctement, il est préférable d'être explicite à ce niveau.

Exemple XXII.2.2. Démontrez que pour tout nombre naturel $n > 0$, nous avons

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Démonstration. La propriété en question est

$$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Notez que le plus petit nombre pour lequel nous devons établir P est $n = 1$. Ainsi, notre induction commence à 1.

Cas de base : $n = 1$. Nous devons montrer que $P(1)$ est vrai, ce qui se traduit par : $1 = \frac{1(1+1)}{2}$. Ceci est clairement vrai.

Étape inductive : Considérons un nombre $k \in \mathbb{N}$ arbitraire tel que $k \geq 1$, et supposons que $P(k)$ est vrai. Ceci veut dire que :

$$P(k) : 1 + 2 + \cdots + k = \frac{k(k+1)}{2} \qquad \text{(H.I.)}$$

Nous devons montrer que $P(k+1)$ est vrai à présent. Explicitement, $P(k+1)$ se traduit par :

$$P(k+1) : 1 + 2 + \cdots + (k+1) = \frac{(k+1)((k+1)+1)}{2}.$$

Nous observons que le membre de gauche de cette équation peut être réécrit sous la forme :

$$(1 + 2 + \cdots + k) + (k+1).$$

Par l'H.I., nous savons que $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$, et ainsi, nous obtenons

$$\begin{aligned}(1 + 2 + \cdots + k) + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+2)(k+1)}{2}\end{aligned}$$

Ceci établit que $P(k+1)$ est vrai.

Étant donné que $P(1)$ est vrai et que $P(k)$ implique $P(k+1)$ pour tout $k \geq 1$, nous pouvons conclure, par le principe d'induction mathématique, que $\forall n \geq 1.P(n)$ est vrai. □

Ce qu'il faut retenir de l'exemple précédent : l'H.I. prend la forme d'une équation, et nous reconnaissons que son membre de gauche est étroitement lié au membre de gauche de l'équation que nous cherchons à démontrer. Par la suite, ce n'est qu'une question de manipulations algébriques.

Dans l'exemple qui suit, il faut effectuer un peu plus de travail pour manipuler l'énoncé objectif de telle manière à pouvoir employer l'H.I.

Exemple XXII.2.3. Démontrez que pour tout $n > 0$, le nombre $3^{2n+1} + 2n - 1$ est un multiple de 7.

Démonstration. La propriété en question est

$$P(n) : 7 \text{ divise } 3^{2n+1} + 2^{n-1}.$$

Cas de base : $n = 1$. Nous devons démontrer $P(1)$, lequel se traduit par : 7 divise $3^{2+1} + 2^0$. Ceci est clairement vrai car $3^{2+1} + 2^0 = 28 = 4 \cdot 7$.

Étape inductive : Considérons un $k \geq 1$ arbitraire et supposons que $P(k)$ est vrai, i.e.

$$P(k) : 7 \text{ divise } 3^{2k+1} + 2^{k-1} \qquad \text{(H.I.)}$$

Nous devons montrer que $P(k+1)$ est vrai, c'est-à-dire

$$P(k+1) : 7 \text{ divise } 3^{2(k+1)+1} + 2^{(k+1)-1}.$$

Pour simplifier un peu les choses, nous remarquons que ceci revient à dire

$$7 \text{ divise } 3^{2k+3} + 2^k.$$

Pour arriver à cette fin, nous manipulons $3^{2k+3} + 2^k$ jusqu'à ce que nous reconnaissions l'expression $3^{2k+1} + 2^{k-1}$, et nous serons en mesure d'appliquer l'H.I. à ce point. Nous procédons ainsi :

$$\begin{aligned} 3^{2k+3} + 2^k &= 3^2 \cdot 3^{2k+1} + 2 \cdot 2^{k-1} \\ &= 9 \cdot 3^{2k+1} + 2 \cdot 2^{k-1} \\ &= 7 \cdot 3^{2k+1} + 2 \cdot 3^{2k+1} + 2 \cdot 2^{k-1} \\ &= 7 \cdot 3^{2k+1} + 2(3^{2k+1} + 2^{k-1}) \end{aligned}$$

Le premier de ces deux termes est clairement un multiple de 7. Par l'H.I., $3^{2k+1}+2^{k-1}$ est un multiple de 7 également. Conséquemment, l'expression toute entière est un multiple de 7, ce qui démontre $P(k+1)$.

Étant donné que $P(1)$ est vrai et que $P(k)$ implique $P(k+1)$ pour tout $k \geq 1$, nous pouvons appliquer le principe d'induction mathématique et conclure que $\forall n \geq 1. P(n)$ est vrai.

□

Ensuite, considérons un exemple où nous prouvons une inégalité.

Exemple XXII.2.4. Soit h un nombre réel tel que $h > -1$. Démontrez que

$$1 + nh \leq (1 + h)^n \text{ pour tout } n \in \mathbb{N}.$$

(Ceci s'appelle l'*inégalité de Bernouilli*.)

Démonstration. La propriété que nous considérons est

$$P(n) : 1 + nh \leq (1 + h)^n.$$

Cas de base : $n = 0$. Nous devons montrer $P(0)$, lequel énonce que $1 + 0h \leq (1 + h)^0$. En simplifiant, ceci devient $1 \leq (1 + h)^0 = 1$, et cet énoncé est clairement vrai.

Étape inductive : Considérons un $k \geq 0$ arbitraire et supposons que $P(k)$ est vrai, i.e.

$$P(k) : 1 + kh \leq (1 + h)^k \qquad \text{(H.I.)}$$

Nous devons montrer que $P(k + 1)$ est également vrai, i.e.

$$P(k + 1) : 1 + (k + 1)h \leq (1 + h)^{(k+1)}.$$

Pour y parvenir, nous multiplions les deux côtés de l'équation dans l'H.I. par $(1 + h)$ et nous effectuons les manipulations suivantes :

$$\begin{aligned}(1 + h)^{k+1} &\geq (1 + kh)(1 + h)\\ &= 1 + h + kh + kh^2\\ &= 1 + (k + 1)h + kh^2\\ &\geq 1 + (k + 1)h\end{aligned}$$

où la dernière inégalité découle du fait que $kh^2 \geq 0$. Ceci prouve $P(k + 1)$.

Étant donné que $P(0)$ est vrai et que $P(k)$ implique $P(k+1)$ pour tout $k \in \mathbb{N}$, nous pouvons appliquer le principe d'induction mathématique et conclure que $\forall n.P(n)$ est vrai. □

Exercice 298. Dans la preuve ci-haut, où avons-nous employé l'hypothèse que $h > -1$?

Finalement, considérons un exemple pour lequel il n'est pas immédiatement évident de quelle manière l'induction fonctionne.

Exemple XXII.2.5. Démontrez que pour tout entier pair $n \geq 2$, nous avons

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots - n^2 = \frac{-n(n + 1)}{2}.$$

Démonstration. Le problème ici semble se rapporter au fait que nous ne prouvons pas quelque chose pour tous les entiers, mais seulement pour les entier pairs. Il y a plusieurs façons de contourner ce problème. Premièrement, nous pouvons le reformuler en prenant comme propriété P, le prédicat suivant :

$$P(n) : \text{si } n \text{ est pair, alors } 1^2 - 2^2 + 3^2 - 4^2 + \cdots - n^2 = \frac{-n(n + 1)}{2}.$$

Quoique ceci réduise notre problème à un problème de la forme « démontrer $P(n)$ pour tout n », l'induction ordinaire n'est pas tout à fait adéquate ici : nous ne pouvons pas nous servir de l'H.I. pour dégager quoi que ce soit d'utile à propos des nombres impairs. (Dans la section suivante, nous verrons que l'induction forte s'applique correctement ici.)

Une autre idée serait de formuler le principe d'induction pour les nombres pairs. Nous laissons ceci en exercice pour le lecteur.

Finalement, nous pouvons aussi reformuler l'énoncé comme suit :

$$P(n) : 1^2 - 2^2 + 3^2 - 4^2 + \cdots + (2n - 1)^2 - (2n)^2 = \frac{-2n(2n + 1)}{2}.$$

Ainsi, nous devons toujours prouver quelque chose à propos de tous les n, et nous évitons le problème où l'H.I. ne propose rien d'utile à propos des nombres impairs. Comme exercice, vous devriez compléter cette preuve. □

XXII.3 Induction forte

Souvent, il est difficile de prouver $P(k+1)$ lorsque la seule chose qui nous est donnée est que $P(k)$ est vrai. Voici un exemple :

Exemple XXII.3.1. Prouvez que tout $n \geq 2$ est un produit $p_1 \cdots p_m$ de nombres premiers.

Tentative de preuve : $P(2)$ est facile : 2 est déjà premier. Maintenant, supposons que $P(k)$ est vrai pour un certain $k \geq 2$, i.e. que k est un produit de nombres premiers. Nous devons montrer que $k+1$ est également un produit de nombres premiers. Or, si $k+1$ s'adonne à être premier, nous avons terminé. Mais si $k+1$ est un nombre composé, alors nous pouvons l'écrire $k+1 = ab$, avec $a \leq k$ et $b \leq k$.

Ce que nous voudrions faire par la suite, est d'écrire chacun de a et b sous la forme d'un produit de nombres premiers, disons $a = p_1 \cdots p_m$, $b = q_1 \cdots q_r$, puis de combiner ceux-ci pour obtenir $k+1 = ab = p_1 \cdots p_m q_1 \cdots q_r$. Ceci garantirait que $k+1$ est un produit de nombres premiers. Toutefois, l'H.I. habituelle énonce seulement que k est un produit de nombres premiers, et elle ne dit rien à propos de a et de b.

Notez que dans l'exemple ci-haut, nous voudrions savoir lors de l'étape inductive que non seulement $P(k)$ est vrai, mais qu'en fait $P(a)$ est vrai pour tout $1 \leq a \leq k$. Intuitivement, ceci a du sens, du moins avec l'analogie des dominos : si le domino k est tombé, alors tous les dominos précédents doivent être tombés aussi.

Voici comment nous pouvons préciser les choses : Nous disons qu'un sous-ensemble $A \subseteq \mathbb{N}$ est *fortement inductif* si

- $0 \in A$
- $\{0, \ldots, k\} \subseteq A$ implique $k+1 \in A$ pour tout k.

Puis, tel qu'attendu, nous obtenons :

Théorème XXII.3.2. *Si $A \subseteq \mathbb{N}$ est fortement inductif, alors $A = \mathbb{N}$.*

Démonstration. Un exercice à effectuer. □

À partir de cela, nous obtenons le principe d'induction forte :

Induction forte :
Supposons que P est une propriété sur les nombres naturels. Pour prouver que $\forall x \in \mathbb{N}.P(x)$, il suffit de prouver les deux énoncés suivants :

- $P(0)$ est vrai.
- Pour tout k, si $P(0), \ldots, P(k)$ sont vrais, alors $P(k+1)$ aussi.

La raison pour laquelle nous appelons ceci l'induction forte est que l'hypothèse d'induction contient plus d'information (est plus forte). En pratique, il se pourrait que vous n'ayez pas besoin de tous les $P(0), \ldots, P(k)$ pour prouver $P(k+1)$; peut-être que vous avez uniquement besoin d'un $P(i)$ spécifique, ou peut-être qu'il vous en faut deux (comme dans l'exemple au début de cette section). Des exemples d'induction forte sont présentés dans les exercices à la fin de ce chapitre. Pour l'instant, nous démontrons que l'induction forte, quoique plus forte en apparence, est en fait équivalente à l'induction ordinaire, au sens suivant :

Théorème XXII.3.3. *Tout énoncé qui peut être prouvé avec l'induction forte peut être prouvé en employant l'induction mathématique, et vice-versa.*

Démonstration. Une des directions est claire : si vous pouvez prouver que $P(k) \to P(k+1)$ est vrai, alors vous pouvez également prouvez que $P(0) \wedge \cdots \wedge P(k) \to P(k+1)$ est vrai. Ainsi, tout ce que nous pouvons prouver avec l'induction peut être prouvé avec l'induction forte.

Pour la réciproque, supposons que nous avons une preuve de $\forall n.P(n)$ qui emploie l'induction forte. Ceci veut dire que nous pouvons prouver :

- $P(0)$
- $P(0) \wedge \cdots \wedge P(k) \to P(k+1)$ pour tout k

Nous prouvons maintenant $\forall n.P(n)$ en employant l'induction mathématique. Voici le truc : Considérez la propriété

$$Q(n) =_{\text{déf}} P(0) \wedge \cdots \wedge P(n).$$

Alors, clairement, nous avons

$$\forall n.P(n) \equiv \forall n.Q(n).$$

Ainsi, nous pouvons prouver $\forall n.Q(n)$ par induction. Puisque $Q(0)$ est identique à $P(0)$ et puisque nous étions en mesure de prouver $P(0)$, le cas de base est terminé. Maintenant, prenons un k arbitraire, et supposons que $Q(k)$ est vrai. Alors, par définition, $P(0) \wedge \ldots \wedge P(k)$ est vrai, et puisque $P(k)$ est vrai, nous pouvons prouver $P(k+1)$. Ainsi, $P(0) \wedge \ldots \wedge P(k+1)$ est vrai, et ceci veut dire que $Q(k+1)$ est vrai. Nous pouvons donc conclure que $\forall n.Q(n)$ est vrai, par le principe d'induction. □

Exercice 299. Donnez une preuve différente du théorème ci-haut en démontrant qu'un sous-ensemble $A \subseteq \mathbb{N}$ est inductif si et seulement s'il est fortement inductif.

XXII.4 Sommaire

Étant donné que les nombres naturels sont bien ordonnés, il existe une technique, appelée *induction mathématique*, pour prouver des énoncés de la forme $\forall n \in \mathbb{N}.P(n)$ Celle-ci repose sur le fait que, si 0 a une certaine propriété et si cette propriété se propage (au sens que pour tout k, si k a la propriété, alors $k+1$ aussi), alors tous les nombres naturels doivent admettre cette propriété. Formellement :

$$[P(0) \wedge \forall k.(P(k) \to P(k+1))] \to \forall n.P(n).$$

Une variante qui est utile est l'*induction forte*. Formellement, il s'agit du principe suivant :

$$[P(0) \wedge \forall k.(P(0) \wedge \cdots \wedge P(k) \to P(k+1))] \to \forall n.P(n).$$

L'induction et l'induction forte sont équivalentes, au sens que tout ce que nous pouvons prouver avec l'une peut être prouvé avec l'autre (quoiqu'en pratique, il est plus commode d'employer l'induction forte).

XXII.5 Exercices

Exercice 300. Démontrez que $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{6}$ pour tout $n \geq 1$.

Exercice 301. Démontrez que $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$ pour tout $n \in \mathbb{N}$.

Exercice 302. Prouvez que pour tout entier $n \geq 1$, nous avons

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Exercice 303. Démontrez que pour tout entier $n \geq 3$, $n^2 \geq 2n + 3$

Exercice 304. Démontrez que $7^n - 2^n$ est divisible par 5 pour tout $n \in \mathbb{N}$.

Exercice 305. Démontrez que pour tout entier $n \geq 1$, 8 divise $n^2 - 1$.

Exercice 306. Démontrez que $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$ pour tout $n > 0$.

Exercice 307. Un étudiant écrit une preuve par induction lors d'un examen, et commence l'étape inductive de la manière suivante :

> **Étape inductive :** Supposons que $P(k)$ est vrai pour tout $k \in \mathbb{N}$. Nous devons montrer que $P(k+1)$ est vrai aussi.

Le professeur enlève une bonne quantité de points. Pourquoi ?

Exercice 308. Supposons que $A \subseteq \{2n \mid n \in \mathbb{N}\}$ est un sous-ensemble des nombres pairs, et que A a les propriétés : $0 \in A$ et, pour tout k, $k \in A$ implique $k + 2 \in A$. Démontrez que $A = \{2n \mid n \in \mathbb{N}\}$. Servez-vous de ce résultat pour formuler un principe d'induction sur les nombres pairs, puis résolvez le problème de l'exemple XXII.2.5.

Exercice 309. L'induction fonctionne-t-elle pour l'ensemble $\mathbb{Z}$? Essayez de formuler un principe d'induction cohérent.

Exercice 310. Même question, mais pour $\mathbb{Q}$ et $\mathbb{R}$.

ANNEXE A

Ressources et lectures recommandées

Il y a plusieurs manuels d'introduction à la logique et à la théorie des ensembles. Certains textes que vous voudriez peut-être considérer, suite à ce cours, incluent :

1. Un des manuels standards d'introduction à la théorie des ensembles est celui de P.R. Halmos : *Naive Set Theory* (Undergraduate Texts in Mathematics, Springer, 1998). Il explique plusieurs aspects de la théorie des ensembles en beaucoup plus de détails et avec finesse, en comparaison à ce que nous avons couvert dans ce cours.

2. Si vous êtes intéressé au développement de la théorie formelle des ensembles (i.e. le système formel ZFC et les systèmes apparentés), il y a le vieux texte (quoique utile) par P. Suppes : *Axiomatic Set Theory* (Dover Books, 1962).

3. Une discussion concise de bien des aspects intéressants de la logique et de la théorie des ensembles est le livre de P.T. Johnstone : *Notes on Logic and Sets* (Cambridge University Press, 1987). Il couvre la logique classique de premier ordre et culmine avec les fameux théorèmes d'incomplétude de Gödel.

4. Pour les étudiants sérieux en mathématiques qui cherchent à acquérir une perspective plus profonde et plus conceptuelle, en ce qui a[?] trait au matériel introduit dans ce cours (et à bien d'autres aspects des mathématiques en général), nous recommandons le livre *Sets for Mathematics*, par F.W. Lawvere et R. Rosebrugh (Cambridge University Press, 2003), voir

   `http://www.mta.ca/~rrosebru/setsformath/`

5. La page web de Eric Schechter qui aborde plusieurs erreurs courantes que l'on retrouve au niveau sous-gradué est

   `http://www.math.vanderbilt.edu/~schectex/commerrs/`

6. Et pour le simple plaisir de la chose, voici un court exposé à propos de l'axiome du choix, de la trichotomie et de l'hypothèse généralisée du continu :

   `http://www.maa.org/news/monthly544-553.pdf`

ANNEXE B

Guide pour l'écriture de preuves

Lorsque nous parlons d'une preuve dans la pratique des mathématiques au quotidien, nous parlons en fait d'une justification ou d'une démonstration de la vérité d'un énoncé mathématique. Il est important de réaliser que ce qui compte comme justification (ou démonstration) convaincante n'est pas absolu, mais dépend amplement du contexte social.[1] Par exemple, un expert dans une certaine branche des mathématiques pourrait être convaincu de la vérité d'une proposition après avoir lu l'idée clé de la preuve, mais un novice pourrait avoir besoin de vérifier plusieurs étapes intermédiaires, écrites dans le moindre détail, avant qu'il ou elle accepte que la preuve est correcte. Aussi, dans un cours, un professeur pourrait attribuer la totalité des points à un étudiant qui démontre une compréhension vis-à-vis suffisament de matière, même si la façon dont celui-ci écrit n'est pas impeccable. Tandis que dans un autre cours, le même professeur pourrait soustraire des points pour un manque de précision dans les preuves écrites. Ainsi, le niveau de détail et de précision dans une preuve doit être adapté en fonction du lecteur.

Pour les mathématiques en général (et dans la majorité de vos cours), le but est essentiellement d'écrire des preuves de façon à ce que votre auditoire puisse :

- les suivre avec facilité,
- atteindre la conviction que vous savez de quoi vous parlez,
- avoir l'impression que vous ne sautez pas par-dessus des choses requérant plus d'attention,
- avoir l'impression que vous ne vous attardez pas sur des détails que tout le monde reconnaît comme étant triviaux et impertinents vis-à-vis du problème en question.

En somme, une preuve devrait être précise, lisible, concise, et elle devrait toujours garder son objectif en vue.

Tout de même, il y a une branche des mathématiques appelée la *théorie des preuves*, dont l'objet est de donner un sens précis à ce qui compte comme une preuve, d'établir les limites de ce qui peut

[1] Le niveau le plus élevé de rigueur est obtenu dans la mesure où une vérification par ordinateur est possible.

être prouvé et comment nous pouvons justifier les diverses méthodes et techniques que nous employons lorsque nous prouvons des théorèmes. D'une part, il s'agit d'une entreprise au niveau du fondement des mathématiques, car cette théorie cherche à établir une fondation technique solide et une justification pour les mathématiques et le raisonnement. D'une autre part, nous pouvons aussi concevoir cette dernière comme de la *métamathématique*, parce que celle-ci étudie les propriétés des mathématiques en employant les méthodes des mathématiques elles-mêmes. Si vous êtes intéressés par ce genre de choses, inscrivez-vous à un cours de logique (comme MAT 3761).

Apprendre à bien écrire des preuves n'est pas facile. La meilleure façon est d'étudier attentivement des bons exemples de preuves, de vous engager à l'écriture vous-même et d'avoir quelqu'un d'experimenté pour commenter votre travail. Garder à l'esprit en tout temps que comprendre le fonctionnement d'une preuve est nécessaire, mais ne garantit pas que vous savez l'écrire correctement. De même, après l'écriture d'une preuve, essayez d'en faire l'analyse et la critique. Où et comment avez-vous utilisé vos hypothèses ? Quelle est l'étape clé de la preuve ? Quelle est sa structure logique dans l'ensemble ? Au cours des sections qui suivent, je vais discuter plusieurs aspects liés aux preuves et à leur écriture ; ceci devrait vous aider à mettre l'accent sur les choses importantes.

B.1 Que cherchons-nous à prouver ?

Les choses que nous cherchons à prouver peuvent prendre diverses formes. Toutefois, elles ont toutes deux traits en commun : elles doivent être dépourvues de toute ambiguïté, et avoir une valeur de vérité bien définie (soit vrai, soit faux). Vous ne pouvez pas prouvez le nombre 12, ou la fonction $\sin(x)$, car il n'y a rien de vrai ou de faux à leur égard ; ces derniers sont des *objets* mathématiques, pas des propositions. Voici quelques exemples de la forme que divers énoncés mathématiques peuvent prendre :

- $a = b$ (ici, l'énoncé est que : une chose est égale à une autre)
- aRb (une chose est en relation par R avec une autre)
- si p, alors q (quelque chose implique quelque chose d'autre)
- p si et seulement si q (quelque chose est équivalent à une autre chose)
- Il existe x tel que $P(x)$ (ici, P est une propriété).
- Il n'existe pas de x tel que $P(x)$ et $Q(x)$.
- Pour tout x, $P(x)$.
- Si $x \in A$ satisfait $P(x)$, alors il satisfait $Q(x)$ aussi.

Dans la section qui suit, nous expliquons comment la forme logique d'un énoncé peut vous donner des indications quant à une stratégie pour élaborer une preuve. Pour l'instant, nous faisons simplement la remarque que, d'un point de vue logique, un énoncé aussi simple que $a = b$ peut en fait être très difficile à prouver : a et b peuvent être des objets très compliqués, ou encore, leurs descriptions n'admettent peut-être pas de lignes de raisonnement faciles. Par exemple, lorsque a et b sont des ensembles, nous devons prouver qu'ils ont les mêmes éléments ; i.e. nous devons démontrer que $\forall x.(x \in a \leftrightarrow x \in b)$. Dans un cas concret comme

$$a = \{\, n \in \mathbb{N} \mid n > 2,\, x^n + y^n = z^n \,\}, \quad b = \emptyset$$

(où x, y, z sont des nombres naturels fixés), vous auriez de la difficulté à déterminer les éléments de l'ensemble a. Néanmoins, la première chose que vous devriez faire, face à la tâche de prouver quelque chose, est de réfléchir à la forme de l'énoncé.

B.2 Aspects logiques liés aux preuves

Prenons le temps de considérer quelques lignes directrices de base pour transformer la forme logique d'un énoncé en une stratégie pour prouver ce dernier. Il est également important de se questionner sur la façon dont nous pouvons exploiter la forme logique d'une information mise à notre disposition (que ce soit sous la forme d'axiomes, d'hypothèses ou de données). Pour chaque connectif possible ($\wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists$) nous allons aborder ces deux aspects. Nous allons aussi apprendre comment réfuter des énoncés selon leurs diverses formes. Dans chaque cas, un schéma représentant la stratégie de preuve nous est donné ; les ellipses ($\vdots$) indiquent que la tâche subséquente pour effectuer une preuve est de remplacer les points par d'autres étapes de raisonnement valide.

B.2.1 Implication

Prouver une implication

Schématiquement parlant, la preuve écrite pour une implication $p \rightarrow q$ prend la forme suivante :

Preuve de $p \rightarrow q$

Supposons que p est vrai.

$\vdots$

Il s'ensuit que q est également vrai.

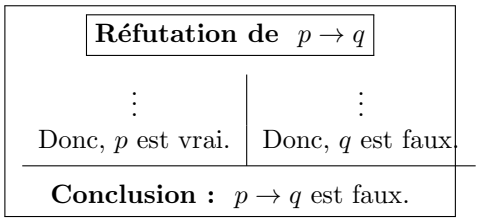
Conclusion : $p \rightarrow q$ est vrai.

Ainsi, la stratégie est de démontrer que *si* p est vrai, *alors* q est vrai aussi. Étant donné qu'une implication est toujours vraie lorsque l'antécédent est faux, ceci est suffisant : si p est faux, alors l'implication est une *vérité vide* (c'est-à-dire, l'implication est vraie car il n'y a rien à prouver). Il est également possible que vous n'ayez pas besoin de p pour prouver q. Par exemple, pour prouver « si n est impair, alors $2n + 1$ aussi », nous n'avons pas besoin de l'hypothèse que n est impair ; i.e. nous pouvons montrer directement que $2n + 1$ est impair.

Fréquemment, une implication $p \rightarrow q$ est démontrée en établissant une chaîne d'implications intermédiaires. Plus précisément, il se pourrait que vous ayez de la difficulté à prouver $p \rightarrow q$ directement, mais vous êtes peut-être en mesure d'établir $p \rightarrow r_1$, puis $r_1 \rightarrow r_2$, puis $r_2 \rightarrow r_3$, et ainsi de suite. Finalement, il se pourrait que vous obteniez $r_n \rightarrow q$. Ceci évoque une idée importante : essayez de décomposer une preuve difficile en étapes plus petites et abordables.

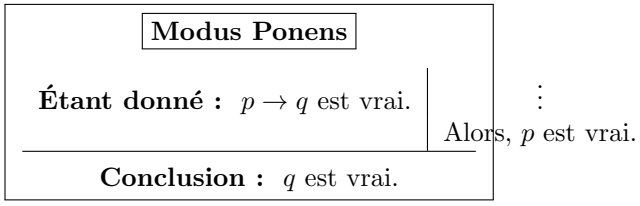
Réfuter une implication

Une implication $p \to q$ est fausse précisément lorsque p est vrai, et q faux. Ainsi, pour réfuter $p \to q$ vous devez établir deux choses :



Employer une implication

La manière la plus courante d'employer une implication (laquelle pourrait être donnée comme hypothèse, ou comme résultat établi à priori) est *Modus Ponens* :

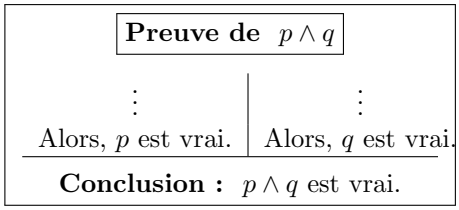


Ainsi, Modus Ponens nous permet d'inférer le conséquent q à partir de l'implication $p \to q$, si nous pouvons prouver l'antécédent p à priori.

B.2.2 Conjonction

Prouver une conjonction

Schématiquement parlant, une preuve de $p \wedge q$ prend la forme suivante :



Ainsi, pour prouver un énoncé de la forme $p \wedge q$, nous devons simplement démontrer p, et démontrer q aussi.

Réfuter une conjonction

Une conjonction $p \wedge q$ est fausse précisément lorsqu'au moins une des énoncés p et q est faux. De ce fait, il y a deux stratégies possibles :

Réfutation de $p \wedge q$	**Réfutation de** $p \wedge q$
⋮	⋮
Alors, p est faux.	Alors, q est faux.
Conclusion : $p \wedge q$ est faux.	**Conclusion :** $p \wedge q$ est faux.

Employer une conjonction

Étant donné une conjonction $p \wedge q$ (peut-être prouvée antécédemment), nous pouvons inférer p et nous pouvons inférer q.

Spécialisation	**Spécialisation**
Étant donné : $p \wedge q$ est vrai.	**Étant donné :** $p \wedge q$ est vrai.
Conclusion : p est vrai.	**Conclusion :** q est vrai.

B.2.3 Disjonction

Prouver une disjonction

Il y a deux façons de prouver $p \vee q$:

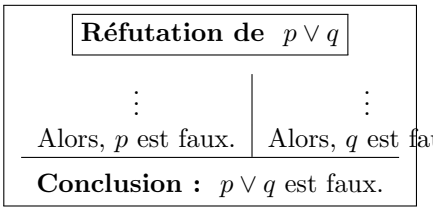
Preuve de $p \vee q$	**Preuve de** $p \vee q$
⋮	⋮
Alors, p est vrai.	Alors, q est vrai.
Conclusion : $p \vee q$ est vrai.	**Conclusion :** $p \vee q$ est vrai.

Ainsi, pour démontrer un énoncé de la forme $p \vee q$, nous devons simplement démontrer l'un de p ou q. Parfois, les choses ne se font pas aussi directement : il pourrait être impossible de démontrer p (ou q) pour tous les cas possibles. Par exemple, supposez que je vous demande de prouver qu'un certain entier positif n est soit premier, soit divisible par un nombre premier strictement plus petit que n. Le nombre n pourrait être trop grand pour que nous commençions à chercher un facteur premier, ou la façon dont le nombre nous est présenté pourrait rendre la tâche trop compliquée (par exemple, j'aurais pu vous dire que n est la racine d'une équation très complexe). Mais sûrement, l'énoncé est vrai ! Et la manière évidente d'effectuer la preuve est de considérer deux cas. Cas 1 : le nombre est premier, et nous avons fini. Cas 2 : le nombre n'est pas premier, mais par définition, il y a un diviseur premier m tel que $2 \leq m < n$. Ainsi, dans les deux cas, la disjonction est vraie.

Quoique cet exemple soit un peu dérisoire, il illustre néanmoins une stratégie importante : si vous ne pouvez pas prouver un énoncé directement, essayez de diviser la preuve en cas séparés. Si vous savez que les cas sont exhaustifs (au sens qu'au moins un de ces cas doit être vrai, même si vous ne savez pas lequel) et que l'énoncé en question est vrai dans tous les cas, alors vous pouvez conclure que l'énoncé est vrai tout simplement.

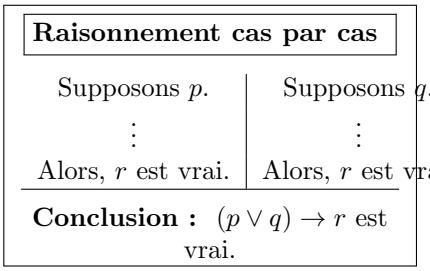
Réfuter une disjonction

Une disjonction $p \vee q$ est fausse précisément lorsque p et q sont toutes les deux faux. Ainsi :



Employer une disjonction

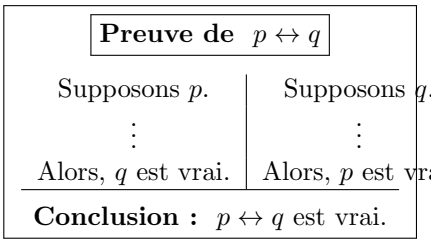
Étant donné une disjonction $p \vee q$ (peut-être prouvée antécédemment), nous pouvons raisonner cas par cas : pour tirer une conclusion r à partir de $p \vee q$, nous devons démontrer que p implique r et que q implique r.



Biconditionnel

Prouver un biconditionnel

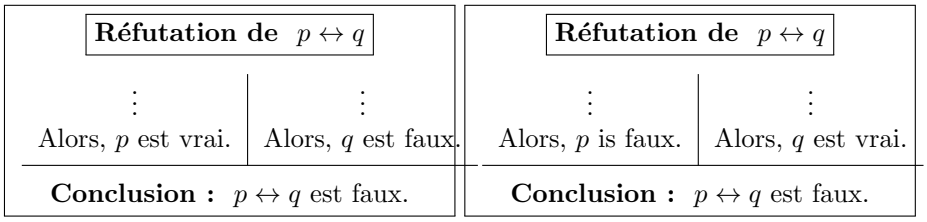
Schématiquement parlant, une preuve de $p \leftrightarrow q$ prend la forme suivante :



Ainsi, pour prouver un énoncé de la forme $p \leftrightarrow q$, vous devez prouver $p \to q$ et $q \to p$.

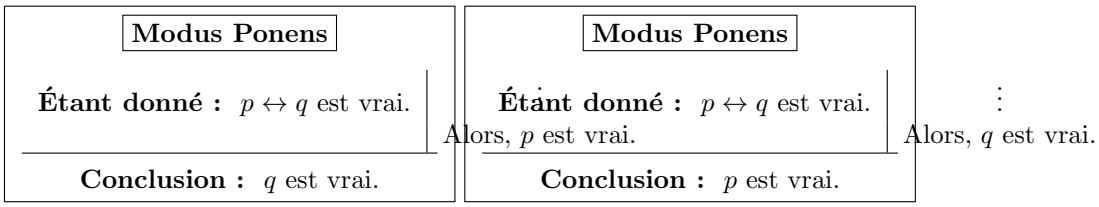
Réfuter un biconditionnel

Un biconditionnel $p \leftrightarrow q$ est faux précisément lorsque $p \to q$ est faux ou lorsque $q \to p$ est faux. De ce fait, il y a deux stratégies possibles :



Employer un biconditionnel

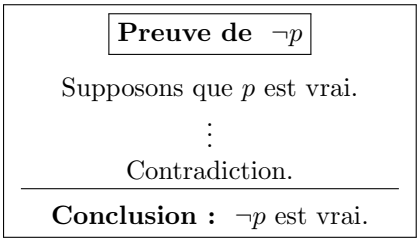
Étant donné un biconditionnel $p \leftrightarrow q$, nous pouvons nous en servir comme si nous nous servions des implications $p \to q$ et $q \to p$ individuellement.



B.2.4 Négation

Prouver une négation

Schématiquement parlant, une preuve de $\neg p$ prend la forme suivante :



Ainsi, la stratégie est de démontrer que *si* p est vrai, *alors* nous obtenons une contradiction. Effectivement, ceci démontre $p \to \bot$, lequel est logiquement équivalent à $\neg p$. Similairement, nous pouvons voir les choses comme suit : soit p est vrai, soit $\neg p$ est vrai. Si nous pouvons éliminer la première possiblité, alors la seule possibilité restante est celle que nous voulons prouver.

Réfuter une négation

Comment pouvons-nous prouver que $\neg p$ est faux ? Bien entendu, une approche est de prouver que p est vrai.

Réfutation de $\neg p$

$\vdots$

Alors, p est vrai.

Conclusion : $\neg p$ est faux.

Une autre approche est de supposer que $\neg p$ est vrai, puis de dégager une contradiction (voir l'objet suivant).

Employer la négation

Étant donné un énoncé $\neg p$, nous pouvons souvent tirer des conclusions à partir de ce dernier en dégageant une contradiction.

Ex Falso

$\vdots$	$\vdots$
Alors, p est vrai.	Alors, $\neg p$ est vrai.

Conclusion : r est vrai.

Ici, r peut être n'importe quel énoncé que vous voulez. Au sens propre, cette règle dit que si nous pouvons dériver une contradiction, alors nous pouvons conclure tout ce que nous voulons. La raison pour laquelle ceci est valide découle du fait que l'implication est vraie lorsque l'antécédent est faux ; clairement, les énoncés p et $\neg p$ pris ensemble nous donnent un énoncé faux.

Bien entendu, ce type de raisonnement survient typiquement pour une partie d'une preuve plus large dans laquelle nous avons fait des suppositions initialement. Sans suppositions, nous ne pourrions jamais prouver une contradition !

B.2.5 Quantification universelle

Prouver un énoncé avec une quantification universelle

Schématiquement parlant, une preuve de $\forall x \in A.\phi(x)$ prend la forme suivante :

Preuve de $\forall x.\phi(x)$

Soit $x \in A$, considéré arbitrairement.

$\vdots$

Alors, $\phi(x)$ est vrai.

Conclusion : $\forall x.\phi(x)$ est vrai.

Il est important de noter que, dans cette preuve, vous ne pouvez faire aucune supposition à propos de l'élément x initialement (à l'exception que celui-ci est un élément de A) ; autrement, vous ne seriez pas en train de prouver que ϕ est vrai pour *tout* élément $x \in A$.

Réfuter un énoncé avec une quantification universelle

Comment pouvons-nous prouver que $\forall x \in A.\phi(x)$ est faux ? En trouvant un contre-exemple. (Ainsi, nous devons spécifier un élément concret a dans A pour lequel $\phi(a)$ est faux.)

Réfutation de $\forall x.\phi(x)$

Considérons $a \in A$.

$\vdots$

Alors, $\phi(a)$ est faux.

Conclusion : $\forall x.\phi(x)$ est faux.

Employer un énoncé avec une quantification universelle

Étant donné un énoncé $\forall x \in A.\phi(x)$, vous pouvez l'instancier pour démontrer que n'importe quel élément $a \in A$ satisfait ϕ.

Instanciation

Étant donné : $\forall x \in A.\phi(x)$ | $a \in A$

Conclusion : $\phi(a)$ est vrai.

B.2.6 Quantification existentielle

Prouver un énoncé avec une quantification existentielle

Schématiquement parlant, une preuve de $\exists x.\phi(x)$ prend la forme suivante :

Preuve de $\exists x \in A.\phi(x)$

Considérons l'élément $a \in A$ suivant :

$\vdots$

Alors, $\phi(a)$ est vrai.

Conclusion : $\exists x \in A.\phi(x)$ est vrai.

Ainsi, pour prouver $\exists x \in A.\phi(x)$, il suffit de donner un exemple concret d'un élément $a \in A$ tel que $\phi(a)$. (Bien souvent, il est difficile de trouver un tel exemple. Dans ce cas, le raisonnement indirect est parfois nécessaire. Par exemple, vous pouvez commencer la preuve en supposant que l'énoncé est faux, puis en dégager une contradiction.)

Réfuter un énoncé avec une quantification existentielle

Comment pouvons-nous prouver que $\exists x \in A.\phi(x)$ est faux ? En démontrant que tous les éléments de A ne satisfont pas ϕ.

Réfutation de $\exists x.\phi(x)$

Soit $x \in A$ arbitraire.

$\vdots$

Alors, $\phi(x)$ est faux.

Conclusion : $\exists x \in A.\phi(x)$ est faux.

Essentiellement, ceci démontre $\forall x \in A.\neg\phi(x)$, lequel est logiquement équivalent à $\neg\exists x \in A.\phi(x)$.

Employer un énoncé avec une quantification existentielle

Étant donné un énoncé $\exists x \in A.\phi(x)$, si nous voulons tirer une conclusion r, nous faisons face au problème que nous ne savons pas nécessairement pour quel $a \in A$ en particulier l'énoncé ϕ est vrai. La patron de raisonnement s'établit comme suit : nous supposons qu'un élément $x \in A$ nous est donné, pour lequel $\phi(x)$ est vrai (même si nous ne savons pas précisément en quoi consiste cet élément) ; nous essayons ensuite de tirer la conclusion r. Si r n'emploie pas l'inconnu x, alors nous avons démontré que $\exists x.\phi(x)$ implique r. Nous devrions comparer ceci avec la règle pour employer la disjonction (raisonnement cas par cas). Effectivement, de savoir que $\exists x.\phi(x)$ est vrai revient à dire que l'un des cas $\phi(a)$, $\phi(b)$, $\phi(c)$, ... est vrai.

Élimination de la quantification existentielle

Soit $x \in A$ tel que $\phi(x)$.

$\vdots$

Alors, r est vrai.

Conclusion : $\exists x \in A.\phi(x) \to r$ est vrai.

Il y a une condition importante ici, notamment, que la conclusion r ne doit pas mentionner l'élément inconnu x comme variable libre.

Exemple B.2.1. Étant donné : $\forall x.(A(x) \to B(x))$ et $\exists x.(A(x) \wedge C(x))$. À prouver : $\exists x.(B(x) \wedge C(x))$.

Solution. Prenons un élément a pour lequel $A(a) \wedge C(a)$ est vrai. Nous pouvons employer l'instanciation : à partir de $\forall x.(A(x) \to B(x))$ nous concluons que $A(a) \to B(a)$.

Or, $A(a) \wedge C(a)$ implique $A(a)$, et en employant Modus Ponens avec $A(a) \to B(a)$, nous obtenons $B(a)$. Aussi, $A(a) \wedge C(a)$ donne $C(a)$, et donc $B(a) \wedge C(a)$. Ceci prouve que $\exists.(B(a) \wedge C(a))$ est vrai.

B.3 En quoi consiste une bonne preuve ?

Maintenant que nous avons abordé les diverses facettes logiques liées aux preuves, il est temps de se tourner vers les aspects plus pratiques de l'écriture de preuves.

Premièrement, une preuve devrait avoir une *structure claire*. À chaque étape de la preuve, le lecteur devrait être en mesure de comprendre où il se situe dans le développement, et pourquoi. Au niveau de la structure d'ensemble, une preuve prend la forme suivante :

Commencement :	Établit la liste des suppositions et des données employées, de même que les définitions pertinentes.
Développement :	Consiste en une série d'énoncés, dont chacun découle logiquement des énoncés antécédents. Une justification doit être fournie pour chaque étape.
Conclusion :	Conclut avec l'énoncé qui doit être prouvé.

Ainsi, une preuve devrait être un peu comme un essai, au sens que tout le travail se fait en réalité dans la partie du développement ; mais c'est l'introduction qui prépare la scène, et c'est la conclusion qui emballe le tout. Il semblerait que ceci soit plutôt évident, mais bien effectuer le développement constitue souvent la moitié du travail (et ce travail vous rapportera une partie des points). En revanche, si vous faites mal les choses à ce niveau, vous en arriverez certainement à un résultat désastreux. Une des raisons pour lesquelles plusieurs personnes commettent des erreurs à ce niveau est que la façon dont ces personnes conçoivent initialement cette partie diffère souvent de la façon dont ils la présentent. Bien souvent, vous procéderez à rebours en partant de la conclusion, en cherchant à remplacer l'objectif final par des sous-objectifs plus simples, jusqu'à ce que vous en arriviez au point où le passage entre les sous-objectifs et les suppositions initiales devient évident. Tout de même, ceci ne constitue pas l'ordre dans lequel la preuve devrait être présentée. Votre preuve écrite ne devrait pas être une projection directe de votre chaîne de pensées, mais une reconstruction de celle-ci.

Deuxièmement, pour écrire des preuves mathématiques, il est nécessaire d'employer un *langage précis et sans ambiguïtés*. À l'exception des preuves formelles (pour lesquelles l'intention est de permettre une vérification par ordinateur), les preuves mathématiques sont une combinaison de symbolisme mathématique (formules, équations, diagrammes) et de langage naturel (de français). Il est évident que les formules devraient être clairement présentées, et sans fautes, et que le simple changement d'un x pour un y pourrait avoir des conséquences dévastatrices. D'une autre part, l'emploi incorrect du langage peut avoir des conséquences tout aussi néfastes, car celui-ci relie les diverses formules ensemble. La fonction principale du français dans une preuve est d'expliquer comment les diverses formules mathématiques, équations, et cetera, sont reliées entre elles. L'équation 1 découle-t-elle de l'équation 2 suite à une manipulation algébrique ? Ou bien, l'équation 2 est-elle une instance d'une supposition qui n'a rien à voir avec avec l'équation 1 ? Ou même, faisons nous la supposition que l'équation 2 est vraie, avec l'intention de dégager une contradiction lorsque nous la combinons avec l'équation 1 ? En quelque part, nous pouvons concevoir une analogie entre l'écriture de preuves et l'art de cuisiner : vous avez peut-être les bons ingrédients (équations), mais vous ne pouvez pas simplement les mettre sur la table tels quels ; vous devez les combiner dans le bon ordre et en utilisant les bonnes techniques.

Plusieurs étudiants tendent à être timides quant il s'agit de rédiger du texte à l'intérieur de leurs preuves. Ceci découle du fait qu'ils découvrent des exigences très strictes en ce qui a trait à ce texte. « Si je n'écris rien, à l'exception d'équations vraies, il n'y a rien pour lequel le professeur pourrait me pénaliser », pensent-ils. Malheureusement, ceci n'est pas la façon dont ça fonctionne. Votre travail est de me convaincre que vous comprenez comment assembler les pièces du casse-tête. Et dans la plupart

des cas, la seule façon d'entreprendre cela est d'expliquer en quoi consiste la situation avec des mots, et pourquoi vous écrivez les formules que vous écrivez. Voici un exemple d'une « preuve » qui emploie seulement des symboles, et aucun texte.

Exemple Démontrez que le carré d'un nombre impair est impair.

« **Preuve** ». $(2p+1)^2 = 4p^2+4p+1$, $4p^2+4p = 4(p^2+p)$. CQFD.

Critique : L'idée importante est là, mais le lecteur n'est aucunement dirigé et il n'y a pas de mots pour indiquer en quoi consiste la structure de la preuve.[2] Voici comment nous devrions reprendre l'idée de cette preuve et l'habiller adéquatement, de telle manière qu'elle devienne comme une histoire que l'on raconte :

Preuve. Supposons que n est un nombre impair. Par définition, ceci veut dire que nous pouvons l'écrire sous la forme $n = 2p+1$ pour un certain p. Nous obtenons dès lors

$$n^2 = (2p+1)^2 = 4p^2+4p+1 = 2(2p^2+2p)+1.$$

La dernière étape ne fait que mettre un facteur de 2 en évidence. Ces équations démontrent que n^2 peut être écrit sous la forme $2m+1$, et ceci veut dire qu'il est impair. □

(Incidemment, certaines personnes tendent à fournir trop de texte ; habituellement, il s'agit d'une façon de compenser pour un manque de compréhension vis-à-vis du fonctionnement de la preuve. Une preuve claire aura toujours un bon équilibre entre le symbolisme et le texte.)

B.4 Exemples

Quelques exemples de preuves sont présentés ici. J'ai indiqué explicitement l'emplacement du commencement, du développement et de la conclusion, mais ce n'est qu'à des fins de clarification. En pratique, vous n'avez pas besoin de donner ces indications (la division en parties devrait être assez claire simplement en lisant le texte). Gardez également à l'esprit qu'il y a parfois plusieurs façons de prouver un résultat, et que les exemples donnés présentent seulement une des preuves possibles pour chaque cas.

Exemple B.4.1. Démontrez que pour tous ensembles A, B, si $A \subseteq \mathcal{P}(B)$, alors $\bigcup A \subseteq B$.

Preuve.

[Commencement] On nous donne deux ensembles arbitraires A, B, et la supposition est que $A \subseteq \mathcal{P}(B)$. Les définitions pertinentes sont : l'ensemble des parties, $\mathcal{P}(X) = \{\, U \mid U \subseteq X \,\}$, ainsi que l'union, $\bigcup A = \{\, u \in x \mid x \in A \,\}$.

[Développement] Nous commençons par faire étalage de nos hypothèses. Par définition d'un sous-ensemble, chaque $x \in A$ satisfait $x \in \mathcal{P}(B)$. En utilisant la définition d'un ensemble de parties, ceci revient à dire :

$$\text{Si } x \in A, \text{ alors } x \subseteq B. \tag{B.1}$$

[2] Pour cet exemple en particulier, les mathématiques sont plutôt simples, donc il se pourrait que l'on vous pardonne d'avoir été aussi concis. Tout de même, pour des cas plus complexes, ceci n'est pas acceptable.

Nous démontrons maintenant l'inclusion $\bigcup A \subseteq B$; c'est-à-dire, nous prenons un $u \in \bigcup A$ arbitraire et nous montrons que $u \in B$. Puisque $\bigcup A = \{\, u \in x \mid x \in A \,\}$, nous pouvons prendre un $x \in A$ tel que $u \in x$. Par l'équation (B.1), ceci nous donne $x \subseteq B$. De ce fait, $u \in x$ implique $u \in B$.

[Conclusion] Ainsi, $u \in \bigcup A$ implique $u \in B$, et ceci veut dire que $\bigcup A \subseteq B$. Ceci complète la preuve. □

L'exemple ci-haut présente une preuve dont le développement est relativement direct, au sens que, dans la mesure où nous déballons les suppositions et mettons sur papier l'énoncé à prouver, il y a peu de travail à faire pour établir la connexion entre les deux. Notez toutefois qu'une preuve comme celle-ci devient beaucoup plus difficile à suivre dans la mesure où vous n'établissez pas de façon précise la différence entre les éléments d'un ensemble et les sous-ensembles d'un ensemble.

Exemple B.4.2. Démontrez qu'il existe une infinité de nombres premiers. Vous pouvez vous servir du fait que tout entier positif admet une factorisation unique (à réorganisation près des facteurs) en un produit de nombres premiers.

Preuve.

[Commencement] Définition pertinente : un nombre premier est un nombre qui a précisément deux diviseurs, lesquels sont 1 et lui-même. Théorème admis : tout entier positif admet une factorisation unique en nombres premiers.

[Développement] Supposons que nous avons un ensemble fini de nombres premiers $\{p_1, \ldots, p_k\}$. Nous allons démontrer que nous pouvons trouver un nombre premier q qui ne fait pas partie de cet ensemble. Pour arriver à cette fin, considérons $a = p_1 \cdots p_k + 1$. Si ce nombre est premier, alors il est certainement différent de tous les p_i, et nous avons terminé. S'il n'est pas premier, alors nous pouvons nous servir du fait que tout entier positif admet une factorisation en nombres premiers pour écrire $a = q_1 \cdots q_l$, où tous les q_i sont des nombres premiers. Or, aucun des nombres premiers $p_1, \ldots, p_k$ ne peut diviser a, car le reste de a divisé par n'importe quel p_i est 1. Ainsi, aucun des p_i n'est un facteur premier de a, et conséquemment, les facteurs premiers q_j de a doivent tous être différents des p_i.

[Conclusion] Nous avons démontré que peu importe l'ensemble fini de nombres premiers que nous considérons, nous pouvons toujours agrandir ce dernier. Ainsi, il doit y avoir une infinité de nombres premiers.

Au cas où vous ne le sauriez pas, ce résultat est appelé le théorème d'Euclide. La première chose à noter à propos de cette preuve est qu'elle commence par reformuler le problème « Il existe une infinité de nombres premiers. » sous la forme « Tout ensemble fini de nombres premiers peut être agrandi. » C'est une reformulation utile, car elle suggère une stratégie de preuve : prenez arbitrairement un ensemble fini de nombres premiers, puis trouvez un nombre premier qui n'en fait pas partie. De plus, notez que la deuxième partie de la preuve (trouver un nombre premier en dehors de l'ensemble considéré) fait appel à une distinction entre deux cas possibles.

Exemple B.4.3. En employant les axiomes pour les applications linéaires, démontrez qu'il n'existe pas d'application linéaire $\mathbb{R} \to \mathbb{R}$ dont l'image est précisément l'ensemble des nombres rationnels.

Preuve.

[Commencement] Les axiomes pour une application linéaire $f : \mathbb{R} \to \mathbb{R}$ sont :

$$f(x + y) = f(x) + f(y) \qquad f(ax) = af(x) \qquad \text{pour tout } a, x, y \in \mathbb{R}.$$

L'image d'une fonction f est l'ensemble $\{\, y \mid \exists x. f(x) = y \,\}$.

[Développement] Nous supposons, avec l'intention d'arriver à une contradiction, qu'il existe une application linéaire f dont l'image est égale à $\mathbb{Q}$. Par définition d'une image, ceci implique que pour tout nombre rationnel $q \in \mathbb{Q}$, il existe $x \in \mathbb{R}$ tel que $f(x) = q$. En particulier, il existe $x \in \mathbb{R}$ tel que $f(x) = 1$, car $1 \in \mathbb{Q}$.

En utilisant le deuxième axiome pour les applications linéaires, nous pouvons établir que pour tout $a \in \mathbb{R}$, $f(ax) = af(x) = a1 = a$. Ainsi, tout $a \in \mathbb{R}$ est de la forme $f(y)$ pour un $y \in \mathbb{R}$. Ceci démontre que l'image de f égale $\mathbb{R}$, et nous obtenons une contradiction avec la supposition initiale que l'image de f ne contenait que les nombres rationnels.

[Conclusion] Pour conclure, notre supposition mène à une contradiction, et donc il ne peut y avoir d'application linéaire dont l'image est $\mathbb{Q}$. □.

Ici, on nous demandait de prouver que quelque chose n'existe pas. Pour ce faire, nous avons supposé l'existence d'un f avec les propriétés en question, et nous avons dégagé une contradiction. En particulier, nous n'avons pas eu besoin du premier axiome de linéarité, mais seulement de la partie avec la multiplication scalaire. Pour une situation tel que ci-haut, où une preuve n'emploie pas toutes les suppositions faites initialement, soyez sur le qui-vive : ceci veut dire que soit vous avez fait un travail particulièrement efficace, soit vous avez manqué une partie de la preuve ! Notez aussi que nous avons employé à deux reprises la supposition initiale à propos de l'image de f comme étant $\mathbb{Q}$: premièrement, pour trouver un x tel que $f(x) = 1$, et deuxièmement, pour dégager la contradiction avec $f(y) = a$.

Exemple B.4.4. En employant les axiomes d'un corps, prouvez que $a(b - c) = ab - ac$ pour tous nombres réels a, b, c. Vous pouvez vous servir du fait que $x \cdot 0 = 0$ pour tout x.

Preuve. [Commencement] On nous donne des nombres réels arbitraires a, b, c. Aussi, nous pouvons employer le fait que $x \cdot 0 = 0$. La définition pour la soustraction est $x - y = x + (-y)$.

[Développement] Tout d'abord, nous manipulons l'expression $a(b - c)$:

$$\begin{array}{rcll} a(b-c) & = & a(b+(-c)) & \text{définition de soustraction} \\ & = & ab + a(-c) & \text{loi de distributivité (un des axiomes pour un corps)} \end{array}$$

Ensuite, nous démontrons que $a(-c)$ est l'inverse additif de ac :

$$\begin{array}{rcll} ac + a(-c) & = & a(c+(-c)) & \text{loi de distributivité} \\ & = & a \cdot 0 & \text{inverse additif} \\ & = & 0 & \text{donné} \end{array}$$

Ainsi :

$$\begin{array}{rcll} a(-c) & = & -(ac) & \text{définition de l'inverse additif} \end{array}$$

Nous obtenons dès lors :

$$ab + a(-c) = ab - ac$$

[Conclusion] Finalement, en combinant les seconde et dernière équations, nous obtenons $a(b-c) = ab-ac$ comme requis.

Dans ce cas, nous n'avons pas fait la liste de tous les axiomes d'un corps au commencement, car ceux-ci sont plutôt nombreux et nous ne savions pas à l'avance de quels axiomes nous avions besoin pour faire la preuve. Nous devions prouver que deux expressions étaient égales, et nous avons accompli cela en établissant une chaîne d'égalités, où chaque égalité était justifiée par un des axiome pour les corps, par une définition ou une égalité donnée.

Exemple B.4.5. Prouvez que $\sqrt{2}$ est irrationnel.

Preuve.

[Commencement] Définition d'un nombre rationnel : un nombre de la forme $\frac{p}{q}$, où $p, q \in \mathbb{Z}$. Définition d'un nombre irrationnel : un nombre qui n'est pas rationnel.

[Développement] Avec l'intention d'arriver à une contradiction, supposons que $\sqrt{2}$ est rationnel. Alors, par définition d'un nombre rationnel, nous pouvons écrire $\sqrt{2} = \frac{p}{q}$, pour des entiers p, q. En éliminant les facteurs en commun de p et q, nous pouvons faire la supposition que p et q ne sont pas tous les deux pairs. (Sinon, ils auraient un facteur de 2 en commun et nous ne ferions qu'éliminer ce facteur.) Maitenant, nous avons

$$2 = (\sqrt{2})^2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}.$$

Ceci démontre que $p^2 = 2q^2$, et donc p^2 est pair. Mais le carré d'un nombre impair est toujours impair, donc p lui-même doit être pair, i.e. nous avons $p = 2n$ pour un entier n. Ceci donne

$$2 = \frac{p^2}{q^2} = \frac{4n^2}{q^2}$$

de telle manière que $q^2 = 2n^2$. Ceci démontre que q^2 est pair, et donc q est pair aussi. Mais alors, p et q sont tous les deux pairs. Contradiction, car nous avons supposé qu'ils n'étaient pas tous les deux pairs.

[Conclusion] Ainsi, $\sqrt{2}$ n'est pas rationnel, et ceci veut dire qu'il est irrationnel. □.

Il s'agit là d'une preuve de manuel que vous devez connaître par coeur. Nous devons montrer que $\sqrt{2}$ n'est pas rationnel. Pour ce faire, nous supposons que celui-ci est rationnel, puis nous dégageons une contradiction. Au commencement, un truc ingénieux est employé, notamment, de s'assurer que nous éliminons les facteurs pairs communs de p et q, de telle manière que ces derniers ne soient pas tous les deux pairs. (Assurez-vous de comprendre pourquoi il est admissible de faire cela — il y a une différence majeure entre employer une supposition qui n'est pas donnée à priori (pas acceptable !) et démontrer que nous pouvons, sans perte de généralité, supposer que nous sommes dans une situation particulière.)

Exemple B.4.6. À partir de la définition de convergence, prouvez que la séquence $(1/n)_{n>0}$ converge.

Preuve.

[Commencement] Définition de convergence : une séquence (a_n) converge vers a lorsque pour tout $\epsilon > 0$, il existe N tel que $|a_n - a| < \epsilon$ pour tout $n \geq N$. La séquence $(1/n)_{n>0}$ est donnée.

[Développement] En inspectant quelques-uns des premiers termes $1/1, 1/2, 1/3, 1/4, 1/5, \ldots$ de la séquence, nous remarquons que cette dernière se rapproche de 0. Ainsi, nous allons prouver que la séquence converge vers 0. Pour arriver à cette fin, supposons qu'on nous donne un $\epsilon > 0$. Nous devons trouver un nombre N tel que, pour tout $n \geq N$, la distance entre $1/n$ et 0 est plus petite que ϵ. En d'autres mots, nous devons trouver N tel que $1/n < \epsilon$ pour tout $n \geq N$. La condition $1/n < \epsilon$ peut être réécrite comme $1/\epsilon < n$, étant donné que n et ϵ sont strictement positifs. Or, si nous prenons N comme étant $1 + 1/\epsilon$, nous obtenons pour tout $n \geq N$:

$$1/n \leq 1/N = \frac{1}{1 + 1/\epsilon} = \frac{1}{(1+\epsilon)/\epsilon} = \epsilon/(1+\epsilon) < \epsilon.$$

[Conclusion] Ceci démontre que la séquence $(1/n)$ converge vers 0. □.

Ce type d'énoncé est complexe car il contient trois quantificateurs.[3] Tout de même, une approche systématique peut aider ici. Nous supposons qu'un ϵ positif arbitraire nous est donné. Ensuite, nous devons trouver un N avec une certaine propriété, notamment, que pour tout $n \geq N$, $1/n < \epsilon$. Nous devons réfléchir un peu au sens de cette dernière inégalité avant de réaliser que $N = 1 + 1/\epsilon$ ferait l'affaire ; mais, une fois que nous constatons cela, le reste de la preuve est facile. (Notez que vous pourriez prendre un N différent ; par exemple, $N = 1 + 1/(2\epsilon)$.)

B.5 Erreurs courantes dans les preuves

Il y a plusieurs choses qui peuvent mal tourner lorsque nous écrivons des preuves, en passant des petites erreurs qui n'affectent pas la cohérence de la preuve, aux erreurs fondamentales qui rendent le tout invalide. Je fais la liste des problèmes les plus courants.

1. **Écrire la preuve à l'envers.** Ceci résulte habituellement de l'écriture des étapes en suivant l'ordre dans lequel vous avez pensé à celles-ci. Voici un exemple d'une « preuve » qui progresse à l'envers pour prouver l'énoncé : $A \subseteq \mathcal{P}(B)$ implique $\bigcup A \subseteq B$.

   Preuve incorrecte. Nous devons prouver que $\bigcup A \subseteq B$. En employant les définitions de l'union et de sous-ensemble, ceci veut dire que $\{\, u \in x \mid x \in A \,\}$ est un sous-ensemble de B ; i.e. pour chaque $u \in x$ tel que $x \in A$, nous avons $u \in B$. Ainsi, pour tout $x \in A$, nous avons $x \subseteq B$, car $u \in x$ implique $u \in B$ (tel que démontré à la ligne précédente). Mais ceci veut dire que $x \in A$ implique $x \in \mathcal{P}(B)$, ce qui revient à dire que $A \subseteq \mathcal{P}(B)$. Le dernier énoncé est vrai, par supposition, donc nous avons terminé. CQFD.

   Qu'y a-t-il d'incorrect avec cette preuve ? Toutes les définitions ont été déballées correctement, mais l'ordre du raisonnement s'effectue à l'envers. Au lieu de commencer avec les suppositions et de terminer avec la conclusion, nous avons commencé par effectuer un développement autour de la conclusion, puis nous avons démontré que les suppositions étaient vraies. Mais il n'y a aucun sens associé à la démontration de ce que nous avons supposé comme étant vrai à priori... Le remède est de séparer notre façon de penser initialement à la preuve, de la façon selon laquelle nous présentons celle-ci sur papier. De plus, nous devrions nous assurer que la preuve commence avec les suppositions et se termine avec la conclusion désirée.

   (Soit dit en passant, si vous observez attentivement, la preuve incorrecte ci-haut est pratiquement une preuve correcte d'un autre énoncé. Lequel ?)

2. **Erreurs de logique.** Les erreurs les plus courantes sont :

   (a) *Négation incorrecte d'un énoncé.* Lorsque vous entreprenez une preuve par contradiction (ou lorsque vous réfutez un énoncé), vous devez trouver la négation d'un énoncé. Des erreurs sont souvent commises lorsque nous travaillons avec des quantificateurs et des implications. Voici un exemple : Quelle est la négation de l'énoncé que, pour tout $x \in A$, il existe $y \in B$ tel que $x = y$?

   1. Il n'y pas de $x \in A$ tel que, si $y \in B$, alors $x = y$.
   2. Il y a un $x \in A$ tel que, pour tout $y \in B$, nous avons $x = y$.

[3] Les humains ont une difficulté notable lorsqu'il s'agit de raisonner avec plus de trois quantificateurs qui alternent, et vous devez vous forcer pour suivre attentivement les règles de raisonnement liées aux quantificateurs dans de tels cas.

3. Pour chaque $x \in A$, il existe $y \in B$ tel que $x \neq y$.
4. Il existe un $x \in A$ tel que, pour tout $y \in B$, nous avons $x \neq y$.

(La bonne réponse est 4.)

(b) *Preuve avec un exemple.* Ceci veut dire que vous prouvez un énoncé pour un cas particulier, alors que vous êtes supposé donner une preuve pour un énoncé d'ordre général, i.e. une preuve qui tient compte de tous les cas possibles. Par exemple, voici une « preuve » que, si n est divisible par 3, alors n^2 aussi.

Preuve incorrecte. Soit n un nombre arbitraire qui est divisible par 3, disons 12. Alors $n^2 = 12^2 = 144 = 3 \cdot 48$, et nous avons terminé.

Le problème est, bien entendu, que 12 est loin d'être arbitraire. La preuve démontre seulement que l'énoncé est vrai pour le cas de $n = 12$.

(c) *Confondre la réciproque, la négation et la contraposée d'une implication.* Supposons qu'on nous demande de prouver une implication « Si p, alors q ». Une erreur courante est de prouver la réciproque à la place (la réciproque de cette implication serait $q \to p$). La bonne chose à prouver serait en fait la contraposée, $\neg q \to \neg p$, car celle-ci est logiquement équivalente à l'énoncé initial $p \to q$. Tout de même, ne confondez pas la contraposée (ou la réciproque) de $p \to q$ avec sa négation, laquelle s'écrit $\neg(p \to q)$.

3. **Manipulations incorrectes.** Celles-ci incluent les manipulations de formules et d'équations qui ne sont pas permises, même si celles-ci pourraient accidentellement mener au résultat cherché. Par exemple, prouvons que $4/6 - 1/3 = 1/3$:

   Preuve incorrecte. Nous avons

$$\begin{aligned} \frac{4}{6} - \frac{1}{3} &= \frac{4-1}{6+3} \\ &= \frac{3}{9} \\ &= \frac{1}{3} \end{aligned}$$

   Chaque équation dans la preuve est vraie, et la conclusion est vraie aussi. Toutefois, la première étape emploie une manipulation invalide pour les fractions.

4. **Emploi des mauvaises définitions.** Ce titre est évocateur en soi. Si vous n'employez pas les bonnes définitions pour commencer, alors le reste de la preuve sera sans intérêt.

5. **Négligence et justifications insuffisantes dans les étapes intermédiaires.** Ceci inclut l'omission d'étapes intermédiaires qui ne sont pas évidentes, sauter aux conclusions, ou bien employer des résultats en cours de route qui sont corrects, mais qui n'ont pas encore été établis. D'autant plus inadéquat est l'emploi de résultats sans mentionner ceux-ci explicitement. Parfois, il convient aussi de donner des indications claires quant à la provenance de ces résultats.

   À titre d'exemple, cherchons à savoir ce qui cloche avec la preuve suivante de l'énoncé qu'il y a une infinité de nombres premiers :

   Preuve négligée. Pour prouver qu'il y a une infinité de nombres premiers, considérons un nombre premier arbitraire p. Or, nous pouvons toujours prendre un nombre premier q qui est strictement plus grand que p. Ceci démontre que nous pouvons construire une séquence de nombres premiers toujours plus grands, et donc, il doit y avoir une infinité de nombres premiers.

   Où est l'acte de foi ici ? Il se trouve dans la supposition que nous pouvons toujours trouver un nombre premier plus grand. Ceci est certainement vrai, mais en faire la démonstration constitue

la partie importante de la preuve, la seule qui ne soit pas évidente à prouver. (Comparez la preuve ci-haut avec la preuve correcte qui est donnée à la section précédente.)

Finalement, notez que cette tentative de preuve a quelque chose de suspect : elle consiste seulement en de la prose. Il pourrait s'agir là d'un signe que l'auteur n'a pas tout à fait identifié la clé du problème.

Considérons un autre exemple. En employant les axiomes d'un corps, prouvons que

$$a(b-c) = ab - ac$$

Preuve négligée.

$$\begin{aligned} a(b-c) &= ab + a(-c) \\ a(-c) &= -ac \quad \text{(car si vous additionnez } ac \text{ de chaque côté, vous obtenez } 0 = 0) \\ a(b-c) &= ab - ac \end{aligned}$$

Il y a plusieurs choses qui ne tournent pas rond avec cette preuve. Le premier problème est que celle-ci n'a aucune structure. L'intention était sans doute : les deux premières équations sont vraies dans n'importe quel corps, et si vous les combinez, vous obtenez la troisième. Le fait que la première équation est vraie n'est pas mis en doute, mais aucune justification n'est donnée (une omission mineure). Beaucoup plus sérieux est le cas de la deuxième équation. Il s'agit d'une équation vraie, mais ceci ne peut être établi de façon immédiate, et comprendre pourquoi celle-ci est vraie est ce qui importe vraiment ici. En effet, cette partie de la preuve constitue la seule étape non triviale et il faut y porter plus d'attention. La « justification » pour cette équation n'incorpore pas de faussetés, mais ne constitue pas une explication complète et ne me convainc pas que vous comprenez comment l'additif inverse fonctionne.[4] La dernière ligne est à nouveau une équation vraie, mais aucune explication n'est donnée. (Encore une fois, une omission mineure, étant donné qu'aucune étape n'a été sautée.)

B.6 Conseils pratiques

Nous avons discuté comment écrire des preuves et comment ne pas les écrire. Toutefois, nous n'avons pas expliqué comment aborder une preuve. Vous devez avoir quelques stratégies pour attaquer des preuves dont les solutions ne sont pas immédiates. Certaines de ces stratégies pourraient sembler évidentes, suite à nos discussions antécédentes, mais il est important de s'essayer avec les choses faciles et évidentes avant de passer beaucoup de temps sur les techniques plus sophistiquées.

1. Avant de commencer, assurez-vous de comprendre la forme logique de ce que vous cherchez à prouver. Cette forme est souvent un indicateur de la stratégie à adopter pour la preuve.

2. Les parties faciles de la preuve sont le commencement et la conclusion. Donc, commencez d'abord à mettre attentivement par écrit en quoi consistent les données et les suppositions, et à déballer les définitions associées. Faites de même pour l'énoncé à prouver, et déballez sa définition également.

[4] Les néerlandais diraient pour ceci « Entendre le son de la cloche, mais ne pas savoir où le battant est suspendu. »

Une fois passé cette étape, tout ce qu'il reste à faire, c'est d'établir un raccord entre le commencement et la conclusion en remplissant l'espace vide au centre. Parfois, cela vous sautera aux yeux. D'autres fois, vous aurez du travail à faire de chaque bord avant d'établir le passage. (Bien entendu, vous devrez vous assurer en fin de compte que tout cela est écrit dans le bon ordre.)

3. Une autre façon d'établir le passage entre le commencement et la conclusion est de chercher un énoncé intermédiaire, pour ensuite figurer comment arriver à celui-ci à partir du commencement et comment arriver à la fin à partir de cet énoncé. (Bien entendu, vous pouvez appliquer cette idée itérativement, en cherchant une séquence d'énoncés intermédiaires.)

4. S'il arrive qu'une approche directe soit (trop) difficile, il pourrait être utile de trouver une formule logiquement équivalente à l'énoncé. Par exemple, si vous cherchez à prouver une implication $p \to q$, vous auriez peut-être plus de facilité à prouver la formule équivalente $\neg q \to \neg p$.

5. Parfois, il vous faudra entreprendre une preuve par contradiction. Une preuve de ce genre fonctionne parfois mieux car elle vous donne une supposition de plus avec laquelle travailler.

6. Si votre intuition vous fait défaut, ou si vous ne parvenez pas à saisir la raison pour laquelle l'énoncé que vous cherchez à prouver est vrai (ou même s'il n'est tout simplement pas vrai), essayez d'abord de faire la preuve pour des cas particuliers. Vous développerez ainsi une meilleure perspective du problème.

7. Parfois, les techniques et idées employées dans certaines circonstances peuvent être réutilisées de manière inattendue dans d'autres circonstances. Soyez ouvert d'esprit quand il s'agit d'essayer diverses techniques, particulièrement lorsque vous sentez qu'il y a une similarité avec des problèmes rencontrés antécédemment.

8. Une fois que votre preuve est écrite, vérifiez attentivement les points suivants :

   - L'ordre dans lequel se fait le développement de la preuve est-il correct ?
   - Employez-vous uniquement les hypothèses données, et rien d'autre ?
   - Est-il possible de reconnaître la forme logique derrière chaque ligne écrite ? Les énoncés ainsi dégagés individuellement sont-ils corrects ?
   - Avez-vous justifié chaque étape ?
   - Y a-t-il un bon équilibre entre le symbolisme mathématique et le français écrit ?

9. Une fois que vous pensez avoir complété la preuve, ne vous précipitez pas sur la prochaine ; assurez-vous de comprendre ce que vous avez prouvé et d'en tirer une leçon. Comprenez-vous la structure de votre preuve ? Comment le résultat s'applique-t-il aux cas particuliers ? À quels emplacements avez-vous employé les suppositions, et de quelles manières ?

10. Essayez d'expliquer vos preuves aux autres, et cherchez à savoir si vous les comprenez suffisamment pour les communiquer avec clarté. Assurez-vous d'obtenir de la rétroinformation de la part de vos professeurs et de vos camarades de classe.

ANNEXE C

Solutions pour exercices sélectionnés

Leçon I

Exercice 1 :

(a) Oui (il s'agit d'une proposition simple).

(b) Oui (il s'agit d'une proposition complexe).

(c) Non (il s'agit d'une question, pas d'un énoncé).

(d) Non (il s'agit d'une phrase impérative).

(e) Oui.

(f) Non ; la première partie est une phrase impérative, la deuxième est une proposition.

(g) Oui.

(h) Non (encore une phrase impérative).

(i) Il s'agit d'une proposition, et elle fausse. (Et vous devriez vous méfier d'elle, étant donné qu'elle comporte une référence à elle-même.)

Exercice 2 : *Définitivement pas* bien formées pour (c), (d), (g), (i) et (j). Par convention, nous acceptons (b). Notez que (d) n'adhère pas à la convention car $(p \leftrightarrow q) \leftrightarrow r$ n'est pas équivalent à $p \leftrightarrow (q \leftrightarrow r)$. (La plupart du temps, les gens écrivent $p \leftrightarrow q \leftrightarrow r$ pour dire $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$.)

Exercice 5 :

(a) $\neg q \rightarrow \neg r$

(b) $r \rightarrow q$

(c) $p \wedge q$ (le « quand même » suggère un contraste, mais n'a pas d'apport au niveau logique)

(d) $\neg q \wedge (\neg p \to \neg q)$ (également possible : $(p \to \neg q) \wedge (\neg p \to \neg q)$)

(e) $r \to (\neg p \wedge \neg\neg q)$

(f) $(\neg q \vee p) \to \neg r$

Leçon II

Exercice 9 :

(a) $v(p \wedge (q \vee r)) = \mathsf{F}$ car $v(q \vee r) = \mathsf{F}$.

(b) $v(p \to (\neg q \to \neg r)) = \mathsf{V}$ car $v(\neg q) = v(\neg r) = \mathsf{V}$, d'où $v(\neg q \to \neg r) = \mathsf{V}$.

(c) $v(\neg p \to \bot) = \mathsf{V}$ car $v(\neg p) = \mathsf{F}$.

(d) $v(p \vee (q \wedge (\neg r \to q))) = \mathsf{V}$ car $v(p) = \mathsf{V}$.

Exercice 10 : Considérons tout d'abord la possiblité que $v(p) = \mathsf{F}$. Dans ce cas, le troisième énoncé donne $v(q \vee r) = \mathsf{F}$, d'où $v(q) = \mathsf{F} = v(r)$. L'affectation $v(p) = \mathsf{F}$ rend donc les trois énoncés faux.

Considérons maintenant la possibilité que $v(p) = \mathsf{V}$. Alors, $v(\neg q \to r) = \mathsf{F}$, et donc $v(q) = v(r) = \mathsf{F}$. Ainsi nous concluons, d'une manière ou d'une autre, que $v(q) = v(r) = \mathsf{F}$, et $v(p)$ peut prendre n'importe quelle valeur.

Exercice 11 :

(a) La solution la plus directe est $(\neg p \wedge q) \vee (p \wedge \neg q)$. Également possible : $p \leftrightarrow \neg q$.

(b) Nous employons les lois de l'algèbre booléenne pour transformer la formule comme suit :

$$(\neg p \wedge q) \vee (p \wedge \neg q) \equiv (\neg p \wedge \neg\neg q) \vee (\neg\neg p \wedge \neg q) \equiv \neg(p \vee \neg q) \vee \neg(\neg p \vee q).$$

(c) Avec un peu plus de manipulations, nous obtenons $\neg(\neg(\neg p \to \neg q)) \to \neg(\neg\neg p \to q)$. Ce qui peut être simplifier pour aboutir à $\neg(\neg(q \to p)) \to \neg(p \to q)$.

Exercice 15 : Nous employons le lexique suivant :

p – Nous supportons la candidate.

q – Elle sera élue.

r – Les taxes augmenteront.

s – Nous pourrons nous permettre d'acheter une nouvelle voiture.

La traduction devient alors :

$$\frac{\begin{array}{c} p \to q \\ q \to r \\ \neg r \to s \end{array}}{\neg p \to s}$$

Cet argument n'est pas valide. Lorsque $v(p) = v(s) = v(q) = \mathsf{F}$ et $v(r) = \mathsf{V}$, toutes les suppositions sont vraies, mais la conclusion est fausse.

Exercice 18 : Nous avons

$$\begin{aligned}(\neg p \to q) \to r &\equiv (\neg\neg p \vee q) \to r \\ &\equiv (p \vee q) \to r \\ &\equiv \neg(p \vee q) \vee r \\ &\equiv (\neg p \wedge \neg q) \vee r \\ &\equiv r \vee (\neg p \wedge \neg q) \\ &\equiv (r \vee \neg p) \wedge (r \vee \neg q) \\ &\equiv (\neg p \vee r) \wedge (\neg q \vee r) \\ &\equiv (p \to r) \wedge (q \to r)\end{aligned}$$

Déterminez par vous-même quelles règles ont été employées !

Exercice 21 : Non, ceci est impossible. Un chevalier ne peut pas dire cela car ce serait un mensonge, et un coquin non plus car l'énoncé serait vrai dans ce cas.

Exercice 22 : Premièrement, le locuteur ne peut pas être un chevalier, car il mentirait dans ce cas. Donc, le locuteur est un coquin et l'énoncé est faux. La seule façon selon laquelle cet énoncé peut être faux est si l'autre personne est un chevalier.

Exercice 24 : Si la première personne est un chevalier, alors son énoncé est vrai, puis les deux sont des chevaliers. Mais alors, le deuxième énoncé serait un mensonge. Contradiction. Ainsi, la première personne est un coquin, et son énoncé est faux, i.e. les deux personnes sont de types différents. Ainsi, la deuxième personne doit être un chevalier. (Et donc, la deuxième personne émet un énoncé vrai en disant que le premier énoncé est faux.)

Exercice 27 : Rappelons-nous qu'une implication est toujours vraie lorsque le conséquent est vrai. Ainsi, les énoncés de A et de C sont vrais, et donc, ils doivent avoir été prononcés par des chevaliers.

En ce qui concerne B, notons qu'il ne peut pas être un chevalier. Sinon, dans ce cas, l'implication aurait un antécédent vrai et une conclusion fausse, et ceci voudrait dire que l'implication en soi serait un mensonge. B peut-il être un coquin ? Si oui, alors l'implication serait fausse, et ceci est possible seulement lorsque l'antécédent est vrai, ce qui n'est pas le cas. Conclusion : B ne peut pas avoir dit une telle chose.

Finalement, considérons le cas de D. L'énoncé peut être exprimé par un chevalier (et dans ce cas, l'antécédent et le conséquent seraient tous les deux faux, puis l'implication en soi serait vraie). Toutefois, il peut également être exprimé par un coquin : dans ce cas, l'antécédent est vrai et la conclusion est fausse, donc l'implication est fausse. Nous ne pouvons rien déduire sur la nature de D et de son énoncé ici.

Exercice 28 : Supposons que A est un chevalier. Alors, son énoncé est vrai, ce qui veut dire que B est un coquin. Puis, l'énoncé de B est faux, et il s'ensuit que A et C sont de types opposés. Donc, C est un coquin. Maintenant, supposons que A est un coquin. Dans ce cas, son énoncé est faux, et B est un chevalier. Puis, l'énoncé de B est vrai, ce qui veut dire que A et C sont de même type. Donc, C est un coquin.

Dans les deux cas, C est un coquin.

Leçon III

Exercice 32 : Pour la liste suivante, nous employons $P(x)$ pour « x est premier », $E(x)$ pour « x est pair », et $O(x)$ pour « x est impair ».

(a) $\exists x \in \mathbb{N}.E(x) \wedge \exists x.P(x)$.

(b) $\neg\forall x.(O(x) \to P(x))$.

(c) $\exists x.(E(x) \wedge P(x))$.

(d) $\neg\forall x.(P(x) \to O(x))$.

(e) $\forall x.[P(x) \wedge x \neq 2 \to O(x)]$

(f) $\exists x.[\neg P(x) \wedge \neg E(x)]$

(g) $\forall x.[\neg P(x) \to (\neg O(x) \vee x \neq 2)]$.

Exercice 33 :

(a) Ceci est faux. Un contre-exemple : $x = 2, y = 0$.

(b) Également faux : avec $x = 1, y = 1$.

(c) Vrai.

(d) Vrai : étant donné $x \in \mathbb{N}$ avec $x > 0$, nous pouvons prendre $y = \frac{1}{n}$.

(e) Faux : par exemple, lorsque $x = \pi$, le seul nombre y avec $xy = 1$ est $y = \frac{1}{\pi}$. Mais ce nombre n'est pas dans $\mathbb{N}$.

(f) Vrai : Par exemple, prenons $x = \frac{1}{2}$. Puis, si y est un nombre réel quelconque, il y a deux cas possibles : soit $y \leq 0$, et nous avons terminé dans ce cas ; soit $y > 0$, et nous avons $\frac{1}{2}y < y$ dans ce cas.

(g) Vrai. (Cet énoncé exprime qu'il existe un unique élément x pour lequel $xy = y$ pour tout y. Bien entendu, il s'agit de $x = 1$.)

(h) Vrai : prenons $x = 2$. Alors, étant donné y, z, il y a deux cas possibles. Cas 1 : $y < z$. Ceci donne $y < 2z$, et donc $zx > y$. Cas 2 : $z \leq y$. Ceci donne $z > 2y$, et nous obtenons $xy > z$.

Exercice 34 : Cet énoncé dit que dans chaque rangée de la matrice, il y a une entrée qui est ≤ -5 ou bien qui est le carré d'un nombre positif naturel. Dans la matrice A, ceci échoue pour la deuxième rangée (et la troisième). Dans la matrice B, nous retrouvons un 1 dans chaque rangée, lequel est le carré d'un nombre positif naturel (lui-même). Donc l'énoncé est vrai pour B. Il est vrai pour C également : les rangées 1 et 3 admettent des entrées plus petites que -5, et la rangée 2 admet un carré, notamment $(3+1)^2 = 16$. Dans la matrice D, toutes les rangées ont un 1, donc l'énoncé est vrai. Pour E l'énoncé est également vrai. Et pour F, il est faux, car la rangée 3 n'admet pas d'entrée plus petite que -5, ni même d'entrée de la forme $(n+1)^2$.

Exercice 35 : C'est Daniel qui est hors de son élément ici. Quoiqu'il ait raison lorsqu'il dit que, pour $x = 1$, l'énoncé qui suit est incorrect, tout ce qu'il nous faut est un exemple de x pour lequel l'énoncé est vrai. Comme Guillaume l'indique, l'énoncé est vrai pour $x = -1$ car dans ce cas, pour tout y, l'antécédent de l'implication est faux, et ceci rend l'implication vraie. Un autre exemple témoin est $x = \frac{1}{2}$, car pour $0 < y \leq \frac{1}{2}$ nous avons $y^2 < y$.

Exercice 36 : Nous avons

$$\begin{aligned}
\neg\exists x \in \mathbb{R}\forall y \in \mathbb{R}.((0 < y \wedge y \leq x) \rightarrow y^2 < y) &\equiv \forall x \in \mathbb{R}\neg\forall y \in \mathbb{R}.((0 < y \wedge y \leq x) \rightarrow y^2 < y) \\
&\equiv \forall x \in \mathbb{R}\exists y \in \mathbb{R}.\neg((0 < y \wedge y \leq x) \rightarrow y^2 < y) \\
&\equiv \forall x \in \mathbb{R}\exists y. \in \mathbb{R}.((0 < y \wedge y \leq x) \wedge \neg(y^2 < y)) \\
&\equiv \forall x \in \mathbb{R}\exists y \in \mathbb{R}.((0 < y \wedge y \leq x) \wedge y \leq y^2)
\end{aligned}$$

Exercice 38 : Nous employons le lexique suivant :

$D(x)$ – x est un chien

$C(x)$ – x est un chat

$B(x)$ – x est gros

$S(x)$ – x est petit

$R(x, y)$ – x chasse y

(a) $\forall x\forall y.(D(x) \wedge C(y) \rightarrow R(x, y))$

(b) $\exists x.(D(x) \wedge \neg\exists y.(C(y) \wedge R(x, y)))$

(c) « Certains chiens chassent certains chats » se traduirait par $\exists x\exists y.(D(x)\wedge C(y)\wedge R(x, y))$. Toutefois, le « seulement » suggère qu'ils ne chassent pas *tous* les chats. Si c'est là votre interprétation, vous devriez traduire l'énoncé par : $\exists x\exists y.(D(x) \wedge C(y) \wedge R(x, y) \wedge \neg\forall z.(C(z) \rightarrow R(x, z)))$.

(d) $\forall x.(D(x) \wedge B(x) \rightarrow \forall y.(C(y) \wedge S(y) \rightarrow \neg R(x, y)))$.

(e) $\forall x\forall y((C(y) \wedge B(y) \wedge R(x, y)) \rightarrow (D(x) \wedge B(x)))$.

(f) $\exists x.(C(x) \wedge B(x) \wedge \neg\exists y.(D(y) \wedge R(x, y)))$.

(g) $\neg\forall x.((D(x) \wedge S(x)) \rightarrow \forall y.((C(y) \wedge B(y)) \rightarrow R(x, y)))$.

(h) $\forall x\forall y.((C(x) \wedge D(y) \wedge R(x, y)) \rightarrow (B(x) \wedge S(y)))$.

Exercice 40 : Ceci n'est pas une tautologie. Considérons le domaine {Jean, Marie}, et posons $L(x, y)$ pour dire que « x aime y ». Alors, l'énoncé dit que pour chaque personne, soit cette personne aime quelqu'un, soit elle est aimée par tout le monde. Lorsque Jean n'aime personne, cet énoncé est faux.

Exercice 42 :

(a) $\forall x\forall y.\neg P(x, y)$

(b) $\forall x \forall y.(\neg P(x,y) \wedge \neg Q(x,y))$

(c) $\forall x \forall y.(\neg P(x,y) \vee \neg Q(x,y))$

(d) $\exists x \exists y.\neg P(x,y)$

(e) $\exists x \exists y.(P(x,y) \wedge \neg Q(x,y))$

(f) $\forall x \exists y.\neg P(x,y)$

(g) $\forall x \exists y.(P(x,y) \wedge \neg Q(x,y))$

(h) $\exists x \forall y.\neg P(x,y)$

(i) $\exists x.(\forall y.\neg P(x,y) \wedge \forall z.\neg Q(x,z))$

(j) $\exists x.(P(x) \wedge \exists y.\neg P(y))$

(k) $\exists x.(\exists y.P(x,y) \wedge \exists z.\neg Q(x,y))$

Exercice 45 : Avec le lexique habituel, nous obtenons

$$\frac{\begin{array}{c}\forall x.[L(J,x) \leftrightarrow x \neq J] \\ \forall x.[L(J,x) \rightarrow L(M,x)]\end{array}}{L(J,M) \wedge L(M,J)}$$

Cette argument est invalide : $L(J,M)$ découle de la première prémisse, mais $L(M,J)$ peut être faux et les prémisses toutes vraies.

Exercice 48 : Tout d'abord, notons que B ne peut pas être un chevalier. Étant donné que la première partie de la conjonction qu'il énonce est vraie, la deuxième partie doit être fausse. Donc, B est sobre. Ceci, en revanche, est un contre-exemple au premier énoncé de A. Il s'ensuit que A est un coquin aussi, et donc il a menti lorsqu'il a déclaré sa sobriété.

Leçon V

Exercice 49 : Voici un indice : demandez si le barbier se rase lui-même.

Exercice 50 : Si nous avons $X \in X$, alors nous obtenons une *régression infinie*

$$\cdots X \in X \in X \in X \in X.$$

En termes plus précis, ceci veut dire que la relation d'appartenance ne serait pas bien fondée, au sens qu'elle admettrait des chaînes descendantes infinies. Dans la théorie standard des ensembles, cette situation ne peut pas se produire, mais il y a des versions de la théorie des ensembles (appelées *théories non bien fondées*) où ce genre de chaîne est admis.

Exercice 51 : Nous obtiendrions $U \in U$. Voir l'exercice 50.

Leçon VI

Exercice 56 : $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Exercice 58 : Lorsque X a n éléments (où $n \in \mathbb{N}$), l'ensemble $\mathcal{P}(X)$ a 2^n éléments. Une preuve rigoureuse requiert une preuve par induction sur n.

Exercice 64 : Vrai. Notons tout d'abord que $A \subseteq C$ comme antécédemment. Pour montrer que $A \neq C$, prenons $x \in B$ avec $x \notin A$. Mais alors, $x \in C$. Ceci montre que $A \neq C$.

Exercice 67 : Non. $A \subset B$ implique $A \subseteq B$. Similairement, $B \subset A$ implique $B \subseteq A$. Ensemble, ils donnent $A = B$. Mais $A \subset B$ implique $A \neq B$. Contradiction.

Exercice 69 : Prenons $A = \emptyset, B = \{\emptyset\}, C = \{\emptyset, \{\emptyset\}\}$. Généralement, $A \in B$ et $B \in C$ n'implique pas $A \in C$ tout simplement, comme le démontre l'exemple suivant :

$$A = \emptyset, B = \{\emptyset\}, C = \{\{\emptyset\}\}$$

Leçon VII

Exercice 74 :

(a) $\emptyset \in \mathcal{P}(A)$ est vrai pour tout ensemble A, car $\emptyset \subseteq A$.

(b) $\emptyset \subseteq A$ pour tout ensemble A ; donc, en particulier, pour $A = \mathcal{P}(\emptyset)$.

(c) $A \in \mathcal{P}(A)$ pour tout ensemble A ; donc, en particulier, pour $A = \mathcal{P}(\emptyset)$.

(d) Vrai : nous avons $\emptyset \in \mathcal{P}\mathcal{P}(\emptyset)$, de telle sorte que $\{\emptyset\} \in \mathcal{P}^3(\emptyset)$.

(e) Nous avons $\emptyset \in \mathcal{P}\mathcal{P}(\emptyset)$, et donc $\{\emptyset\} \in \mathcal{P}\mathcal{P}\mathcal{P}(\emptyset)$. Aussi $\emptyset \in \mathcal{P}\mathcal{P}\mathcal{P}(\emptyset)$. Donc, les deux éléments de $\mathcal{P}(\emptyset)$ sont également des éléments de $\mathcal{P}\mathcal{P}\mathcal{P}(\emptyset)$.

(f) Faux. Car $\{X\} \in \mathcal{P}(X)$ veut dire que $\{X\} \subseteq X$, et ceci donne $X \in X$. Contradiction.

(g) Vrai, car $X \in \mathcal{P}(X)$.

(h) Vrai, car $A \in \mathcal{P}(A)$ pour tout A ; en particulier, pour $A = \{X\}$.

(i) Faux. Prenons par exemple $X = \{\emptyset\}$. Alors, $\mathcal{P}(\{\{\emptyset\}\}) = \{\emptyset, \{\{\emptyset\}\}\}$. Puis, $X \notin \mathcal{P}(\{X\})$.

Exercice 75 : Supposons que $A = B$. Alors, $A \subseteq B$ et $B \subseteq A$. Par la proposition VII.3.1, ceci donne $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ et $\mathcal{P}(B) \subseteq \mathcal{P}(A)$, donc $\mathcal{P}(A) = \mathcal{P}(B)$.

La réciproque est également vraie. Si $\mathcal{P}(A) = \mathcal{P}(B)$, alors $A \in \mathcal{P}(A)$, et aussi $A \in \mathcal{P}(B)$. Ceci veut dire que $A \subseteq B$. Par symétrie, $B \subseteq A$ s'ensuit également. Donc $A = B$.

Exercice 77 : Non. S'il existe un tel X, étant donné que $X \in \mathcal{P}(X)$, nous aurions $X \in X$.

Exercice 78 : Considérons un ensemble arbitraire X. Puis, posons

$$\emptyset = \{x \in X | x \neq x\}.$$

Ceci définit l'ensemble vide. Notons que ceci fonctionne seulement dans la mesure où nous avons montré l'existence d'au moins un ensemble X à priori.

Leçon VIII

Exercice 81 :

(a) $A \cap B = \{2\}$

(b) $A \cup B = \{0, 1, 2, 3, 4, 5\}$

(c) $A \cap B \cap C = \emptyset$

(d) $A - B = \{0, 1\}$

(e) $A^c - B^c = \{3, 4, 5\}$

(f) $(A - B)^c = \{x \in \mathbb{N} | x > 1\}$

(g) $(A^c \cap C^c)^c = \{0, 1, 2, 3, 5\}$

Exercice 82 :

(a) $\{x \in \mathbb{R} | x \notin \mathbb{Q} \text{ et } x \leq 0\}$ (i.e. l'ensemble de tous les nombres négatifs irrationnels).

(b) $\{x \in \mathbb{R} | x \geq 0 \text{ et } x \in \mathbb{Q} \to x \geq 1\}$. (Tous les nombres réels ≥ 1 et les nombres irrationnels entre 0 et 1.)

(c) $\{1\}$.

Exercice 84 : Premièrement, supposons que $A \subseteq B$. Nous avons toujours $A \cap B \subseteq A$. Ainsi, nous devons montrer que $A \subseteq A \cap B$. Pour arriver à cette fin, il suffit de démontrer que chaque élément de A est également un élément de $A \cap B$ (i.e. qu'il est dans A et dans B). Le premier est trivial, et le second découle de $A \subseteq B$.

Réciproquement, supposons que $A \cap B = A$. Nous avons, en particulier, $A \subseteq A \cap B$, ce qui veut dire que chaque élément de A est également un élément de B. Donc, $A \subseteq B$.

Exercice 89 : Soit $x \in (A - B) \cap (B - A)$. Alors, $x \in A - B$ et $x \in B - A$. Le premier veut dire que $x \in A$, mais que $x \notin B$. Le second veut dire que $x \in B$ et $x \notin A$. Contradiction. Nous concluons qu'il n'y a pas d'éléments dans $(A - B) \cap (B - A)$.

Exercice 91 : Nous avons

$$\begin{aligned} u \in \mathcal{P}(A \cap B) &\Leftrightarrow u \subseteq A \cap B \\ &\Leftrightarrow u \subseteq A \text{ et } u \subseteq B \\ &\Leftrightarrow u \in \mathcal{P}(A) \text{ et } u \in \mathcal{P}(B) \\ &\Leftrightarrow u \in \mathcal{P}(A) \cap \mathcal{P}(B). \end{aligned}$$

Leçon IX

Exercice 94 : $\{\emptyset\} \times \{\emptyset\} = \{(\emptyset, \emptyset)\}$. (En employant la définition de paire ordonnée, ce dernier est égal à $\{\emptyset, \{\emptyset\}\}$.)

Exercice 95 : Oui, c'est un produit de $\{\emptyset, \{\emptyset\}\}$ avec $\{\emptyset\}$.

Exercice 97 : Nous démontrons que $A \times B \neq B \times A$. Prenons $A = \{\emptyset\}$ et $B = \{\{\emptyset\}\}$. Alors, $A \times B = \{(\emptyset, \{\emptyset\})\}$, tandis que $B \times A = \{(\{\emptyset\}, \emptyset)\}$. Puisque $\emptyset \neq \{\emptyset\}$, ces deux ensembles sont distincts. Toutefois, pour le cas où $A = \emptyset$ ou $B = \emptyset$, l'égalité est vraie.

Exercice 101 : Supposons que $A \subseteq A', B \subseteq B'$. Prenons $(x, y) \in A \times B$. Alors, $x \in A, y \in B$. Puis, nous avons aussi $x \in A', y \in B'$. Ceci veut dire $(x, y) \in A' \times B'$, ce qui démontre $A \times B \subseteq A' \times B'$.

Exercice 103(a) : Pour commencer, considérons un élément $(x, y) \in A \times (B \cup C)$. Nous obtenons $x \in A$ et $y \in B \cup C$.

Cas 1 : $y \in B$. Donc, $(x, y) \in A \times B$, et il s'ensuit que $(x, y) \in (A \times B) \cup (A \times C)$ également.

Cas 2 : $y \in C$. Donc, $(x, y) \in A \times C$, et il s'ensuit que $(x, y) \in (A \times B) \cup (A \times C)$ également.

D'une façon ou d'une autre, nous avons $(x, y) \in (A \times B) \cup (A \times C)$, de telle sorte que $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Pour la réciproque, supposons que $(x, y) \in (A \times B) \cup (A \times C)$.

Cas 1 : $(x, y) \in A \times B$. Donc $x \in A, y \in B$, puis $y \in B \cup C$. Ainsi, $(x, y) \in A \times (B \cup C)$.

Cas 2 : $(x, y) \in A \times C$. Donc $x \in A, y \in C$, puis $y \in B \cup C$. Ainsi, $(x, y) \in A \times (B \cup C)$.

Dans les deux cas, le résultat est vrai, et nous concluons que $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.

Leçon X

Exercice 108 :

(a) $R^\circ = \{(b, a), (d, c), (d, a)\}$

(b) $R \circ R = \emptyset$

(c) $R \circ R^\circ = \{(b, b), (b, d), (d, b), (d, d)\}$

(d) $R^\circ \circ R = \{(a, a), (a, c), (c, c), (c, a)\}$

(e) $S \circ R = \{(a, p), (a, r), (c, p), (c, r)\}$

(f) $S \circ R^\circ = \{(b, p), (b, q), (d, p), (d, q)\}$

Exercice 109 : Les relations suivantes sont celles qui satisfont $R = R^\circ$:

$R_1 = \emptyset$ $\quad$ $R_2 = \{(0, 0)\}$
$R_3 = \{(1, 1)\}$ $\quad$ $R_4 = \{(0, 0), (1, 1)\}$
$R_5 = \{(0, 1), (1, 0)\}$ $\quad$ $R_6 = \{(0, 0), (0, 1), (1, 0)\}$
$R_7 = \{(1, 1), (0, 1), (1, 0)\}$ $\quad$ $R_8 = \{(0, 0), (1, 1), (0, 1), (1, 0)\}$

Exercice 112 : Oui : Prenons $A = \{a, b\}$ et $R = S = \{(a, b)\}$. Nous obtenons alors $R \circ S = \emptyset$.

Exercice 115 : Nous avons $(x, y) \in (< \circ <)$ si et seulement s'il existe z tel que $x < y$ et $y < z$. Ceci, en revanche, revient à dire que $x < y + 1$. Ainsi, $< \circ <$ est la relation $\{(x, y) | x < y + 1\}$.

Ensuite, $(x, y) \in (< \circ\circ <)$ si et seulement s'il existe z tel que $x < z$ et $y < z$. Mais pour n'importe quels x, y, nous pouvons toujours trouver z avec $x < z$ et $y < z$ (prenons $z = x + y + 1$ par exemple). Ainsi, la relation $<^\circ \circ <$) est la relation maximale.

Finalement, $(x, y) \in (< \circ <^\circ)$ si et seulement s'il existe z tel que $z < x$ et $z < y$. Un tel z existe précisément lorsque x et y sont tous les deux non égal à zéro. Ainsi, nous pouvons constater que $< \circ <^\circ$ est la relation $\{(x, y) | x \neq 0, y \neq 0\}$.

Leçon XI

Exercice 118 : Un contre-exemple aux trois problèmes est donné par $A = \{0, 1\}$, $R = \{(0, 1), (1, 1)\}$. Ce R est une relation fonctionnelle de A vers lui-même, mais la réciproque n'est ni totale, ni univaluée.

Exercice 120 : Cette relation est le graphe de $f(x) = x^3$, donc elle est fonctionnelle. En général, la réciproque d'un graphe n'est pas fonctionnelle (voir l'exercice 118), mais c'est vrai pour ce cas : pour tout $y \in \mathbb{R}$, il existe x avec $y = x^3$, de telle sorte que la relation est totale. De plus, un tel x est nécessairement unique, donc la relation est univaluée.

Exercice 122 : Toute relation $R \subseteq A \times \emptyset$ est nécessairement vide. Donc, à fortiori, c'est le cas de toute fonction vers l'ensemble vide aussi. Mais les fonctions sont totales, donc A doit être vide. (Sinon, étant donné un $a \in A$, nous aurions un $b \in \emptyset$ avec $f(a) = b$.)

Exercice 125 : Il s'agit d'une fonction bijective : elle a un inverse $f^{-1}(x) = \sqrt[3]{x}$.

Exercice 127 : Une fonction affine est bijective ssi elle est injective ssi elle est surjective ssi elle a une pente non nulle ; la valeur de b est sans importance.

Exercice 129 : Supposons que $(g \circ f)(x) = (g \circ f)(y)$, c'est-à-dire que $g(f(x)) = g(f(y))$. Puis, étant donné que g est injective, nous obtenons $f(x) = f(y)$. Ensuite, étant donné que f est injective, nous obtenons $x = y$. Donc $g \circ f$ est injective.

Exercice 132 : Il suffit de démontrer que f^{-1} a un inverse. Mais son inverse est simplement f, car nous avons $f \circ f^{-1} = 1$ et $f^{-1} \circ f = 1$. (Donc, l'énoncé que f^{-1} est l'inverse de f est essentiellement le même que l'énoncé que f est l'inverse de f^{-1}.)

Exercice 135 :

$$\begin{array}{ll} a \mapsto a, b \mapsto b, c \mapsto c & a \mapsto a, b \mapsto c, c \mapsto b \\ a \mapsto b, b \mapsto a, c \mapsto c & a \mapsto c, b \mapsto b, c \mapsto a \\ a \mapsto b, b \mapsto c, c \mapsto a & a \mapsto c, b \mapsto a, c \mapsto b \end{array}$$

Exercice 140 : Oui, la fonction $f(x) = x + 1$ est injective lorsqu'interprétée comme une fonction de $\mathbb{N}$ vers $\mathbb{N}$. La fonction de valeur absolue sur $\mathbb{Z}$ (ou sur $\mathbb{Q}$ ou $\mathbb{R}$) est surjective, mais pas injective.

Leçon XII

Exercice 148 : (cf. exercice 135)

$$\begin{array}{ll} a \mapsto 0, b \mapsto 1, c \mapsto 2 & a \mapsto 0, b \mapsto 2, c \mapsto 1 \\ a \mapsto 1, b \mapsto 0, c \mapsto 2 & a \mapsto 2, b \mapsto 1, c \mapsto 0 \\ a \mapsto 1, b \mapsto 2, c \mapsto 0 & a \mapsto 2, b \mapsto 0, c \mapsto 1 \end{array}$$

Exercice 152 : $\chi_P : \mathbb{N} \to \{0,1\}$ est donné par

$$\chi_P(x) = \begin{cases} 1 & \text{si } x \text{ est premier} \\ 0 & \text{sinon.} \end{cases}$$

Exercice 153 : Nous devons trouver des éléments de $\{0,1\} \times \{0,1\}$ qui sont envoyés par la fonction max sur 1. Nous avons $\max(\mathrm{x}, \mathrm{y}) = 1$ ssi $x = 1$ ou $y = 1$ (ou les deux). Ainsi, le sous-ensemble avec fonction caractéristique max est $\{(0,1),(1,0),(1,1)\}$.

Exercice 154 : Calculons :

$$\begin{aligned} \chi_{U\cap V}(x) = 1 &\Leftrightarrow x \in U \cap V \\ &\Leftrightarrow x \in U \text{ et } x \in V \\ &\Leftrightarrow \chi_U(x) = 1 \text{ et } \chi_V(x) = 1 \\ &\Leftrightarrow \chi_U(x)\chi_V(x) = 1 \end{aligned}$$

Exercice 157 : Étant donné $a \in A$, nous avons $r(a) \neq \emptyset$, car il existe $b \in B$ tel que $R(a,b)$, i.e. $b \in r(a)$. Ainsi, l'ensemble vide n'est pas de la forme $r(a)$, peu importe le $a \in A$.

Exercice 160 : Nous devons définir $\phi : A \times (B+C) \to (A \times B) + (A \times C)$. Un élément de $A \times (B+C)$ est une paire (x,y) où $x \in A$ et $y \in B + C$. Donc y est lui-même une paire de la forme $y = (z,0)$ avec $z \in B$, ou $y = (z,1)$ avec $z \in C$. Or, un élément de $(A \times B) + (A \times C)$ est de la forme $((x,z),0)$ avec $(x,z) \in A \times B$, ou $((x,z),1)$ avec $(x,z) \in A \times C$. Nous définissons alors :

$$\phi(x,(z,i)) =_{\text{déf}} ((x,z),i) \qquad \text{pour } i = 0,1.$$

Un inverse de ϕ est donné par

$$\psi((x,z),i) =_{\text{déf}} (x,(z,i)) \qquad \text{pour } i = 0,1.$$

Il reste seulement à vérifier que ϕ et ψ sont des inverses l'un de l'autre, et ceci est plutôt direct.

Exercice 161 (d) : Définissons $\phi : (A \times B)^C \to A^C \times B^C$ par $\phi(f) = (\pi_A \circ f, \pi_B \circ f)$, où $\pi_A : A \times B \to A$ est la première projection et $\pi_B : A \times B \to B$ est la deuxième. Définissons un inverse par $\psi(h,k)(c) = (h(c),k(c))$. Alors,

$$\psi\phi(f)(c) = \psi(\pi_A f, \pi_B f)(c) = (\pi_A f(c), \pi_B f(c)) = f(c)$$

et

$$\phi\psi(h,k) = (\pi_A \psi(h,k), \pi_B \psi(h,k)),$$

puis $\pi_A\psi(h,k)(c) = \pi_A(h(c),k(c)) = h(c)$. Et similairement, $\pi_B\psi(h,k)(c) = k(c)$.

Exercice 164 : Nous avons

$$\mathsf{Rel}(A \times B, C) =_{\text{déf}} \mathcal{P}((A \times B) \times C) \cong \mathcal{P}(A \times (B \times C)) =_{\text{déf}} \mathsf{Rel}(A, B \times C).$$

L'isomorphisme au milieu est une conséquence du fait que $(A \times B) \times C \cong A \times (B \times C)$, combiné avec le fait que $X \cong Y$, implique $\mathcal{P}(X) \cong \mathcal{P}(Y)$.

Leçon XIII

Exercice 169 :

(a) $\Delta_A \subseteq R$ veut dire que, pour tout $x \in A$, nous avons $(x,x) \in R$. Ceci exprime précisément que R est réflexive.

(b) $\Delta_A \cap R = \emptyset$ veut dire que $(x,x) \notin R$ pour tout $x \in A$. Ceci exprime donc que R est irréflexive.

(c) $R^\circ \subseteq R$ veut dire que pour tous $x, y \in A$, si yRx, alors xRy. Ceci exprime que R est symétrique. En général, nous avons que $R \subseteq S$ implique $R^\circ \subseteq S^\circ$. En combinant cela avec $R^{\circ\circ} = R$, nous obtenons l'équivalence avec les autres conditions.

(d) $R \cap R^\circ \subseteq \Delta_A$ veut dire que $(x,y) \in R$ et $(y,x) \in R$ implique $(x,y) \in \Delta_A$, i.e. que $x = y$. Ceci veut dire que R est antisymétrique.

(e) $R \circ R \subseteq R$ veut dire que, pour tous $x, z \in A$, s'il existe un certain y avec xRy et yRz, alors xRz. Ceci revient à dire que R est symétrique.

Exercice 174 : Définissons $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ par $f(x,y) = x + y$. Alors, la relation est de la forme $(x,y) \sim (u,v) \Leftrightarrow f(x,y) = f(u,v)$, et nous avons prouvé que c'est une relation d'équivalence. La classe d'équivalence d'un point (a,b) est la droite (l'ensemble des points sur cette droite) $y = -x + (a+b)$ qui passe par (a,b) et dont la pente est -1.

Exercice 176 : La classe d'équivalence de 0 est $\{0\}$, la classe d'équivalence de 1 est l'ensemble de tous les nombres positifs, et la classe d'équivalence de -1 est l'ensemble de tous les nombres négatifs. Ainsi, il y a trois classes d'équivalence, et le quotient $\mathbb{Z}/\sim$ est en correspondance bijective avec $\{-1, 0, 1\}$.

Exercice 177 (a) : $R \cap S$ est réflexive : étant donné $x \in A$, nous avons xRx et xSx car R et S sont réflexives. Conséquemment, $(x,x) \in (R \cap S)$. $R \cap S$ est symétrique : étant donné $(x,y) \in (R \cap S)$, nous avons xRy et xSy. Puisque R et S sont symétriques, nous obtenons yRx et ySx. Donc, $(y,x) \in (R \cap S)$. Finalement, $R \cap S$ est transitive : étant donné $(x,y) \in (R \cap S)$ et $(y,z) \in (R \cap S)$, nous avons xRy, yRz, xSy, ySz. Par la transitivité de R et de S, nous obtenons xRz et xSz. Donc, $(x,z) \in (R \cap S)$ comme requis.

Nous pouvons faire une preuve différente en faisant appel au calcul des relations et à l'exercice 169. La réflexivité est établie comme suit : $\Delta_A \subseteq R, \Delta_A \subseteq S$, donc $\Delta_A \subseteq R \cap S$. La symétrie est prouvée par $(R \cap S)^\circ = R^\circ \cap S^\circ = R \cap S$. Finalement, la transitivité découle de

$$(R \cap S) \circ (R \cap S) \subseteq (R \circ R) \cap (R \circ S) \cap (S \circ R) \cap (S \circ S) = R \cap (R \circ S) \cap (S \circ R) \cap S \subseteq R \cap S.$$

(La première inclusion découle d'un énoncé à propos de l'interaction entre la composition et l'intersection, que vous voudriez peut-être formuler et vérifier séparément.)

Exercice 178 : Définissons la fonction ϕ par $\phi[x]_R = [x]_S$. Nous devons montrer qu'elle est bien définie. Considérons y tel que yRx. Alors, $\phi[y]_R = [y]_S$, donc nous devons montrer que $[y]_S = [x]_S$. Mais $R \subseteq S$, donc yRx implique ySx, d'où $[y]_S = [x]_S$.

Leçon XIV

Exercice 182 : Tout d'abord, chaque ensemble de la forme $[n, n+1)$ est non vide (il contient le point $n + 1/2$ par exemple). Ensuite, étant donné deux ensembles de la forme $[n, n+1)$ et $[m, m+1)$, nous avons soit $n = m$, et les deux ensembles sont égaux dans ce cas ; soit $n \neq m$, et les deux ensembles sont disjoints dans ce cas. Finalement, pour tout $x \in \mathbb{R}$, posons n comme étant le plus grand entier tel que $n \leq x$. Nous obtenons $x \in [n, n+1)$.

Exercice 183 : Non, car ces ensembles ne sont pas disjoints deux à deux ; par exemple $(-1, 1) \cap (-2, 2) = (-1, 1) \neq \emptyset$.

Exercise 185 : Chaque $[x]$ correspond à l'ensemble de points sur le graphe de f, lesquels s'étendent également le long de la droite horizontale $y = f(x)$.

Exercice 187 : Il y a exactement une partition de $\emptyset$, notamment la famille vide de sous-ensembles de $\emptyset$.

Exercice 188 :

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

(b) Que s est une permutation de t dans ce cas veut simplement dire que s et t ont le même nombre de 0. Clairement, « avoir le même nombre de 0 » est une relation d'équivalence.

(c) Il y a cinq classes d'équivalence, notamment

$$\{0000\},$$
$$\{0001, 0010, 0100, 1000\},$$
$$\{0011, 0101, 0110, 1001, 1010, 1100\},$$
$$\{0111, 1011, 1101, 1110\},$$
$$\{1111\}$$

Leçon XV

Exercice 191 : L'union est $\mathbb{R}$, car pour chaque $x \in \mathbb{R}$, il y a un $n \in \mathbb{N}$ avec $-n < x < n$, i.e. avec $x \in (-n, n)$. L'intersection est vide car, pour $a = 0$, l'ensemble $(-a, a)$ est vide.

Exercice 192 : L'union est $\mathbb{R} - \mathbb{Z}$: chaque $x \in \mathbb{R}$ est dans un des intervalles $(a, a+1)$, à l'exception des entiers. L'intersection est vide.

Exercice 193 : L'union est $(-1, 1)$. (Lorsque $n = 0$ nous obtenons cet intervalle, et les intervalles subséquents sont plus petits.) L'intersection est $\{0\}$, car 0 est le seul élément que les intervalles de la forme donnée ont en commun.

Exercice 194 : Notez tout d'abord que, si $n = 1$, alors $\log_2 n = 0$, puis $[0, \log_2 0) = \emptyset$. Donc, l'intersection est vide. Dans la mesure où $n \to \infty$, nous avons $\log_2 n \to \infty$, ce qui démontre que l'union est $[0, \infty)$.

Exercice 196 : C'est la relation $x \sim y \Leftrightarrow x - y$ divise 2012. C'est une relation d'équivalence qui contient R de toute évidence. Maintenant, considérons n'importe quelle relation d'équivalence S qui contient R. Nous voulons démontrer que S contient $\sim$. Donc, supposons que $x \sim y$. Alors, $x - y = k(2012)$ pour un entier quelconque k. Considérons le cas de $k \geq 0$. Nous pouvons alors prouver par induction sur k que xSy : si $k = 0$, le résultat découle de la réflexivité de S. Si nous avons prouvé l'énoncé pour k, alors l'H.I. (hypothèse inductive) nous donne $(x, k(2012) \cdot x) \in S$. Puisque $R \subseteq S$, nous avons aussi $(k(2012) \cdot x, (k+1)(2012) \cdot x) \in S$. La transitivité nous donne ensuite le résultat cherché. Finalement, pour le cas de $k < 0$, il suffit d'employer la symétrie de S.

Exercice 198 : Il s'agit de la relation $xRy \Leftrightarrow |x| = |y|$. La relation $\sim$ est symétrique, mais pas réflexive, ni transitive. Toutefois, en la rendant réflexive, nous la rendons transitive également. Puisque R est obtenue en ajountant la diagonale à $\sim$, ceci démontre que R est la plus petite relation d'équivalence contenant $\sim$.

Leçon XVI

Exercice 202 :

$$\begin{array}{ll} f[U_0] = \emptyset & f^{-1}[V_0] = \emptyset \\ f[U_1] = \{7\} & f^{-1}[V_1] = \emptyset \\ f[U_2] = \{6,7\} & f^{-1}[V_2] = \{1,4\} \\ f[U_3] = \{6,7,8\} & f^{-1}[V_3] = \{0,1,4\} \\ f[U_4] = \{6\} & f^{-1}[V_4] = \{0,2,3\} \\ f[U_5] = \{6,7,8\} & f^{-1}[V_5] = \{0,1,2,3,4\} \end{array}$$

Exercice 204 : Supposons que $U \subseteq U'$. Pour démontrer $f[U] \subseteq f[U']$, considérons un élément $y \in f[U]$. Par la définition d'une image directe, ceci veut dire $y = f(x)$ pour un certain $x \in U$. Puisque $U \subseteq U'$, ceci implique que $x \in U'$. Conséquemment, $f(x) \in f[U']$, par la définition d'une image directe encore une fois. Nous avons démontré que $x \in f[U]$ implique $x \in f[U']$, et l'assertion est prouvée ainsi.

Exercice 206 : Une solution élégante est $f(x) = x \sin x$. (Dessiner le graphe pour voir pourquoi, pour toute valeur y, il y a une infinité de valeurs x telles que $f(x) = y$.)

Exercice 209 : L'énoncé est faux : le plus petit contre-exemple est $f : \emptyset \to \{*\}$, la fonction vide (quoique la même idée fonctionne pour n'importe quelle fonction non surjective). Nous avons, pour $U = \emptyset$, $f[U]^c = \emptyset^c = \{*\}$, tandis que $f[U^c] = f[\emptyset] = \emptyset$.

Exercice 211 : Pour une variante, nous donnons une preuve en utilisant les lois de la logique des prédicats :

$$\begin{array}{rcl} y \in f[U \cup U'] & \equiv & \exists x.[y = f(x) \wedge x \in U \cup U'] \\ & \equiv & \exists x.[y = f(x) \wedge (x \in U \vee x \in U')] \\ & \equiv & \exists x.[(y = f(x) \wedge x \in U) \vee (y = f(x) \wedge x \in U')] \\ & \equiv & \exists x.[y = f(x) \wedge x \in U] \vee \exists x.[y = f(x) \wedge x \in U'] \\ & \equiv & y \in f[U] \vee y \in f[U'] \\ & \equiv & y \in f[U] \cup f[U'] \end{array}$$

Exercice 215 : Il y a deux fibres, notamment $f^{-1}(p) = \{a, b\}$ et $f^{-1}(q) = \{c\}$. La partition est $\{\{a, b\}, \{c\}\}$.

Exercise 216 : Les fibres sont précisément les sous-ensembles singleton de A. En fait, ceci est non seulement vrai pour l'identité, mais pour n'importe quelle fonction bijective de domaine A.

Exercice 217 : Notons tout d'abord que pour $a \in A$, nous pouvons décrire la fibre en a comme suit

$$\pi_A^{-1}(a) = \{(x,y)|\pi_A(x,y) = a\} = \{(a,b)|b \in B\}.$$

Cet ensemble est en correspondance bijective avec B, à travers la bijection qui envoie (a,b) sur b.

Exercice 218 : Nous obtenons $A = \{(a,1),(b,1),(b,2),(c,2),(d,2),(c,3)\}$. La fonction f est définie par

$$f(a,1) = f(b,1) = 1, f(b,2) = f(c,2) = f(d,2) = 2, f(c,3) = 3.$$

Il y a trois fibres (parce que I a trois éléments) : $\{(a,1),(b,1)\}$, $\{(b,2),(c,2),(d,2)\}$ et $\{(c,3)\}$.

Exercice 219 : Le domaine est l'ensemble

$$A = \{(n-1,n)|n \in \mathbb{Z}\} \cup \{(n,n)|n \in \mathbb{Z}\} \cup \{(n+1,n)|n \in \mathbb{Z}\}.$$

La fonction $A \to \mathbb{Z}$ envoie (x,y) sur y. La fibre en $n \in \mathbb{Z}$ est l'ensemble

$$\{(n-1,n),(n,n),(n+1,n)\}.$$

Exercice 221 : Il y a trois fibres, parce que le codomaine $\mathbb{Z}/3$ a trois éléments. La fibre en $[0]$ est l'ensemble $\{3k|k \in \mathbb{Z}\}$, la fibre en $[1]$ est $\{3k+1|k \in \mathbb{Z}\}$ et la fibre en $[2]$ est $\{3k+2|k \in \mathbb{Z}\}$.

Leçon XVII

Exercice 224 :

- $s(1) = a, s(2) = b, s(3) = c$
- $s(1) = a, s(2) = c, s(3) = c$
- $s(1) = a, s(2) = d, s(3) = c$
- $s(1) = b, s(2) = b, s(3) = c$
- $s(1) = b, s(2) = c, s(3) = c$
- $s(1) = b, s(2) = d, s(3) = c$

Exercice 227 : Nous avons $\mathcal{P}_+\{0,1\} = \{\{0\},\{1\},\{0,1\}\}$. Les fonctions de choix sont uniquement déterminées sur les singletons, donc nous obtenons $s\{0\} = 0, s\{1\} = 1$. Nous devons simplement spécifier les valeurs possibles de s sur $\{0,1\}$, et donc il y a deux possibilités :

- $s\{0\} = 0, s\{1\} = 1, s\{0,1\} = 0$
- $s\{0\} = 0, s\{1\} = 1, s\{0,1\} = 1$

Exercice 228 :

(a) L'ensemble vide n'a pas de sous-ensemble non vide, donc $\mathcal{P}_+(\emptyset) = \emptyset$. Donc, il y a une seule fonction de choix, notamment l'unique fonction $\mathcal{P}_+(\emptyset) \to \emptyset$.

(b) Un singleton admet une unique fonction de choix $\mathcal{P}\{\emptyset\} \to \{\emptyset\}$.

(c) Ceci est la même chose pour n'importe quel ensemble singleton.

(d) Une possibilité pour une fonction de choix est donnée par $s(U) =$ le plus petit élément de U.

(e) Pour un sous-ensemble U de nombres premiers, nous pouvons choisir celui qui est le plus proche de 0. (Si cette approche ne détermine pas un élément unique, prenez en un positif.)

(f) Étant donné un sous-ensemble U, écrivez tous les éléments de U sous la forme $\frac{m}{n}$ où $n > 0$ et n, m relativement premiers. Ensuite, considérons tout d'abord les éléments pour lesquels n est minimal ; puis, parmi ces éléments, prenez celui avec le plus grand m.

Exercice 230 :

- $s(p) = e, s(q) = a, s(r) = b$
- $s(p) = e, s(q) = a, s(r) = d$
- $s(p) = e, s(q) = c, s(r) = b$
- $s(p) = e, s(q) = c, s(r) = d$

Exercice 231 : Une bijection a précisément une section, notamment son inverse. Clairement, l'inverse est une section car $ff^{-1} = 1_B$. Toutefois, pour toute section s de f, nous avons $s = 1_A s = f^{-1} f s = f^{-1} 1_B = f^{-1}$.

Exercice 233 : Nous devons avoir $s(n) \in \{n-1, n, n+1\}$ pour tout $n \in \mathbb{Z}$. Il y a trois choix évidents :

- $s(n) = n - 1$
- $s(n) = n$
- $s(n) = n + 1$.

(Mais, certainement, il y en a bien d'autres.)

Exercice 234 : Pour chaque $i \in I$, nous devons choisir un élément de $A_i = \{i\}$. Mais le seul choix possible est de prendre i. Donc, $c(i) = i$ est l'unique fonction de choix pour cette famille.

Exercice 236 : À travers la correspondance entre les relations de A vers B et les fonctions $A \to \mathcal{P}(B)$, les relations totales R correspondent aux fonctions $r : A \to \mathcal{P}_+(B)$. Ainsi, si nous avions une fonction de choix $c : \mathcal{P}_+(B) \to B$, nous pourrions former $cr : A \to B$, laquelle est contenue dans R.

Exercice 238 : L'option évidente est $s(x) = \arcsin x$. Mais, pour tout entier k, nous pouvons prendre $s(x) = \arcsin x + 2k\pi$, car il s'ensuit que $\sin(\arcsin x + 2k\pi) = \sin \arcsin x = x$ pour tout $x \in [-1.1]$.

Exercice 240 : Le domaine est la somme des ensembles A_i. Ceci donne

$$X = \{(a,1),(b,1),(c,1),(d,1),(p,2),(q,2),(c,3),(p,4),(a,4)\}.$$

La fonction $X \to \bigcup_{i\in I} A_i$ envoie (x,l) sur x.

Une fonction de choix possible est $s(1) = a, s(2) = q, s(3) = c, s(r) = a$. La section correspondante est $m(1) = (a,1), m(2) = (q,2), m(3) = (c,3), m(4) = (a,4)$.

Exercice 241 : Le choix évident est de prendre, étant donné $[x] \in \mathbb{R}/\sim$, le plus petit nombre réel $y \geq 0$ pour lequel $x \sim y$. (Par exemple, nous choisirions de représenter $[14.3322222]$ par 0.3322222, et ainsi de suite.) Or, nous pourrions aussi ajouter n'importe quel entier à cette fonction et nous aurions toujours une fonction de choix.

Leçon XVIII

Exercice 244 : Tout au long, fixons les bijections $\phi_0 : A \to A'$ et $\phi_1 : B \to B'$.

(a) $\phi_0 \times \phi_1 : A \times A' \to B \times B'$ est une bijection.

(b) Soit $\gamma : A + B \to A' + B'$ définie par $\gamma(x,i) = (\phi_i(x), i)$. (Vous voudriez peut-être déballer un peu cette définition pour comprendre pourquoi elle fait l'affaire.) Alors, γ est une bijection.

(c) Soit $\delta : A^B \to A'^{B'}$ définie par $\delta(f) = \phi_0 \circ f \circ \phi_1^{-1}$. Alors, δ est une bijection.

(d) Ceci découle de (c), en prenant $B = B' = \{0,1\}$ et $\phi_1 = 1$.

Exercice 248 : Nous avons $A = B \cup (A - B)$. Supposons que $A - B$ est dénombrable. Alors, étant donné que l'union de deux ensembles dénombrables est dénombrable, ceci implique que A est dénombrable. Contradiction.

Exercice 250 : Clairement, $|\mathbb{R}| \leq |L|$, car pour chaque $r \in \mathbb{R}$, nous avons une fonction constante f_r avec valeur de sortie r, et la fonction $\mathbb{R} \to L$ qui envoie r sur f_r est injective. D'une autre part, la fonction $L \to \mathbb{R} \times \mathbb{R}$ qui envoie $f(x) = ax + b$ sur la paire (a,b) est également injective, donc $|L| \leq |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Exercice 252 : Nous pourrions utiliser le couplage $\mathbb{N}\times\mathbb{N} \to \mathbb{N}$, mais il y a une approche plus élégante ici. Considérons un ensemble fini $A = \{a_1, \ldots, a_k\}$, où nous supposons, sans perte de généralité, que $a_1 < a_2 < \cdots < a_k$. Considérons le nombre

$$\phi(A) = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

où p_i est le i-ème nombre premier. (Donc, par exemple, nous obtenons pour $A = \{0,3,6\}$ que

$$\phi(A) = 2^0 \cdot 3^3 \cdot 5^6,$$

et ainsi de suite.) Si $A = \emptyset$, posons $\phi(A) = 0$. Alors, ϕ est une injection de $\mathcal{P}_{fin}(\mathbb{N}) \to \mathbb{N}$ par l'unicité de la factorisation en nombres premiers.

Exercice 254 : Cet ensemble n'est pas dénombrable ; nous pouvons employer le même argument de la diagonale, puis démontrer que $\mathcal{P}(\mathbb{N})$ est non dénombrable, en remplaçant des séquence arbitraires de 0 et de 1 par des séquences admettant une infinité de 1.

Exercice 255 : S'il y a une surjection $A \to \mathbb{N}$, nous pouvons prendre une section $s : \mathbb{N} \to A$, puis obtenir $|\mathbb{N}| \leq |A|$.

Exercice 257 : Ceci est similaire à l'exercice 250 : identifions un polynôme $f(x) = a_n x^n + \cdots + a_1 x + a_0$ avec l'élément $(a_n, \ldots, a_0) \in \mathbb{R}^{n+1}$ et employons $|\mathbb{R}^{n+1}| = |\mathbb{R}|$.

Exercice 259 : La classe d'équivalence d'un nombre réel a est l'ensemble

$$[a] = \{a + k | k \in \mathbb{Z}\}.$$

La fonction $f : [a] \to \mathbb{Z}$ définie par $f(a + k) = k$ est une bijection, de telle sorte que $|[a]| = |\mathbb{Z}|$.

L'ensemble quotient $\mathbb{R}/\sim$ est en bijection avec l'intervalle semi-ouvert $[0, 1)$ (lequel est non dénombrable, comme nous le savons) : la fonction

$$\phi : [0, 1) \to \mathbb{R}\sim; \qquad \phi(a) = [a]$$

est une bijection. En effet, si $[a] = [b]$ pour tout $a, b \in [0, 1)$, alors nous devons avoir $a = b$ (car $|a - b| < 1$). Ceci veut dire que ϕ est injective. Et pour tout $[x] \in \mathbb{R}/!\sim$, nous pouvons écrire $x = a + k$ avec $a \in [0, 1)$ et $k \in \mathbb{Z}$, ce qui démontre que ϕ est surjective.

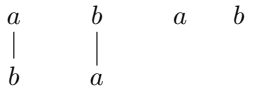
Leçon XIX

Exercice 262 :

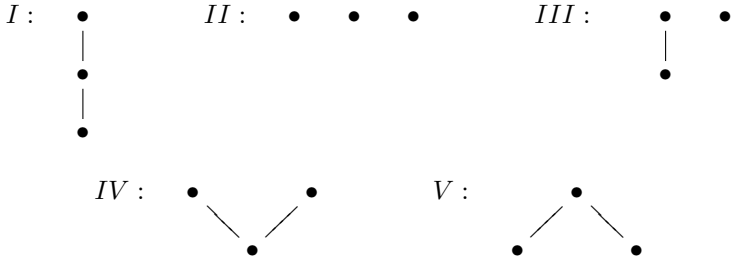
(a) La relation vide est un ordre sur l'ensemble vide.

(b) Il y a aussi une relation d'ordre unique sur un ensemble singleton, notamment la diagonale.

(c) Pour l'ensemble $\{a, b\}$, il y a trois possibilités :



(d) Sur $\{a, b, c\}$, nous avons des relations d'ordre de la forme suivante :

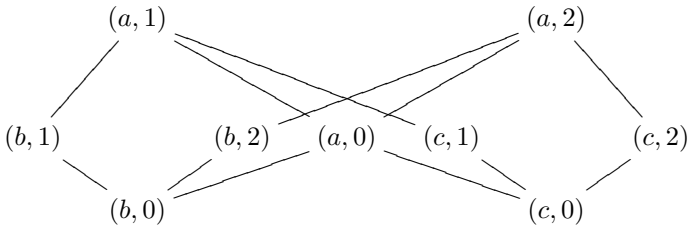


Il y a donc 6 ordres de type I, 1 de type II, 6 de type III, 3 de type IV et 3 de type V. Ceci donne 19 ordres possibles au total.

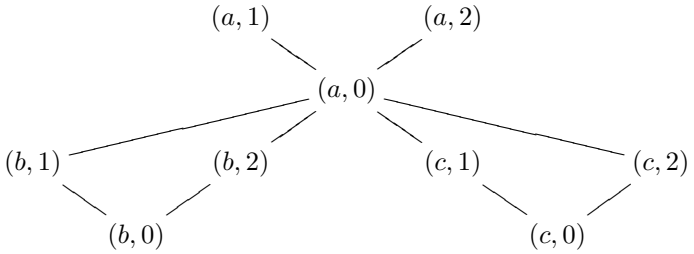
Exercice 264 : Il y a l'ordre de « plus petit ou égal à » habituel ; l'ordre diagonale (identité) $x \leq y$ ssi $x = y$; et il y a $x \leq y$ ssi $x = y$ ou $-x = y \in \mathbb{N}$. (Il y a une tonne d'autres possibilités.)

Exercice 266 : Il s'agit d'un préordre, mais pas d'un ordre partiel, car il est possible d'avoir $\phi \vdash \psi$ et $\psi \vdash \phi$, sans avoir $\phi = \psi$.

Exercice 268 : L'ordre produit est



L'ordre lexicographique sur $A \times B$ est



Exercice 273 : Puisque $f(x) \leq f(x)$ pour tout x, nous obtenons $x \leq x$, donc la relation est réflexive. Et $x \leq y \leq z$ veut dire $f(x) \leq f(y) \leq f(z)$, et ceci implique $f(x) \leq f(z)$, d'où $x \leq z$. Ainsi, la relation est transitive.

Observons que nous ne pouvons pas nécessairement avoir l'antisymétrie : $f(x) = f(y)$ donne $x \leq y$ et $y \leq x$, mais à moins que f soit injective, ceci ne force pas $x = y$.

Leçon XX

Exercice 279 : Si $(A, \leq)$ est linéaire et fini, alors, pour un élément $a \in A$ arbitraire, nous avons que soit a est un plus petit élément (et dans ce cas, nous avons terminé), soit il y a un élément a' strictement plus petit que a (par la linéarité). Répétons cela pour a' ; s'il n'est pas le plus petit élément, nous obtenons un a'' strictement plus petit, et ainsi de suite. Si A n'admettait pas de plus petit élément, nous obtiendrions une suite strictement décroissante d'éléments (infinie par définition), ce qui est impossible car A est fini.

Exercice 281 : Non, les premiers $10^{100}/4$ termes sont en ordre croissant, mais après, la suite décroît.

Exercice 283 : Considérons $\pi = 3.1415\ldots$ Définissons une suite de nombres rationnels par

$$a_0 = 3, a + 1 = 3.1, a_2 = 3.14, a_3 = 3.141, a_4 = 3.1415, \ldots$$

Clairement, cette suite est croissante et converge vers π.

Exercice 285 : Si A, B ont des plus petites éléments respectifs $\bot_A, \bot_B$, alors $(\bot_A, \bot_B)$ est le plus petit élément de $A \times B$, autant pour l'ordre produit que pour l'ordre lexicographique.

Les ordres produits ne sont pas linéaires en général, même si A, B le sont (prenons $\mathbb{N} \times \mathbb{N}$ par exemple), mais l'ordre lexicographique l'est dans ce cas : étant donné deux éléments (x, y) et (u, v),

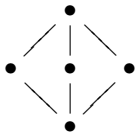
nous avons soit $x < u$ (dans ce cas $(x, y) \leq_l (u, v)$), soit $u < x$ (dans ce cas $(u, v) \leq_l (x, y)$), soit $x = y$. Pour ce dernier cas, nous avons soit $(x, y) \leq_l (u, v)$, soit $(u, v) \leq_l (x, y)$, tout dépendant si $y \leq v$ ou si $v \leq y$.

Exercice 288 : Supposons que $U \subseteq V$. L'élément $\bigvee V$ satisfait $x \leq \bigvee V$ pour tout $x \in V$, et donc $x \leq \bigvee V$ pour tout $x \in U$ en particulier. Mais alors, par définition, nous avons $\bigvee U \leq \bigvee V$.

Exercice 289 : Considérons le sous-ensemble U de $\mathbb{N} \cup \{\infty\}$. Si U est un ensemble fini qui ne contient pas ∞, alors le supremum de U est simplement l'élément maximal dans U. (Et il s'agit de 0 lorsque U est vide.) Dans tous les autres cas, nous avons $\bigvee U = \infty$.

Exercice 290 : Étant donné a, b, la supposition nous donne que $a \wedge b = a$ ou bien que $a \wedge b = b$. Mais $a \wedge b = a$ ssi $a \leq b$ et $a \wedge b = b$ ssi $b \leq a$. Donc, $a \leq b$ ou $b \leq a$, et il s'ensuit que A est linéaire. La réciproque est également vraie ; dans un ordre linéaire, nous pouvons prendre $a \wedge b = min(a, b)$ et $a \vee b = max(a, b)$.

Exercice 291 : Il suffit de prendre



Leçon XXI

Exercice 294 : Il suffit de prendre n'importe quel ensemble avec plus qu'un élément, et de l'ordonner avec l'identité. Ceci fonctionne également pour les ensembles infinis.

Exercice 297 :

(a) Le successeur de n est $n + 1$.

(b) Dans $\mathbb{Q}$, il n'y a *pas* d'élément avec un successeur : si $x < y$, nous pouvons toujours considérer $\frac{y-x}{2}$, et celui-ci est strictement entre x et y.

(c) Si x n'est pas maximal, alors il existe un élément y tel que $x < y$. Un tel y n'a pas besoin d'être un successeur de x, car il pourrait y avoir y' tel que $x < y' < y$. Similairement, un tel y' n'a pas besoin d'être un successeur de x, car il pourrait y avoir y'' tel que $x < y'' < y'$. Mais puisque A est fini, la séquence y, y', y'', ... doit arrêter à un certain point (être finie), et donc x admet un successeur.

(d) $A = \{a, b, c\}$ avec $a \leq b, a \leq c$.

(e) Supposons que x n'est pas maximal, et posons U comme étant l'ensemble de tous les éléments strictement plus grands que x. Alors, U est non vide et, ainsi, il admet un plus petit élément y. Ce y doit être un successeur de x : pour $y \in U$, nous avons $x < y$, et si $x < z$, alors $z \in U$, d'où $z \leq y$.

(f) Dans $\mathbb{N} \cup \{\infty\}$, l'élément ∞ n'est le successeur d'aucun élément.

Index