BMATH — STRUCTURES MATHÉMATIQUES

Bruno Teheux[*]

Université du Luxembourg

Ces notes de cours sont destinées aux étudiant·e·s du premier semestre du Bachelor en mathématiques de l'Université du Luxembourg pour l'année 2023 - 2024. Elles sont complétées par une liste d'exercices dont la résolution fait partie intégrale de la formation.

Version du 5 avril 2025

Nous tâchons de corriger les erreurs typographiques régulièrement. Les mises à jour seront déposées en ligne, dans le dossier partagé.

TABLE DES MATIÈRES

[*]bruno.teheux@uni.lu

1 INTRODUCTION

Le cours de structures mathématiques a deux objectifs. Le premier est d'introduire petit à petit un certains nombres d'objets mathématiques « structurés » dont la présence est omniprésente dans le développement des mathématiques contemporaines. Ces structures, vous les utiliserez quotidiennement dans votre vie étudiante, souvent sans vous en rendre compte, ou quand vous serez devenus mathématicien·nes.

Le deuxième objectif est de vous initier à la *structure de la pensée mathématique*. L'objet d'étude des mathématiques est constitué d'idées. Mais contrairement aux autres disciplines qui ont des idées comme champs d'investigation (comme la philosophie, la métaphysique, l'économie…) les idées mathématiques ont la remarquable propriété d'être universelles : une fois validées, elles les sont pour tous, partout et pour toujours. N'est-il pas remarquable que nous utilisons toujours des théorèmes prouvés par Euclide ou Archimède plusieurs siècles avant note ère ?

Cette universalité n'est pas arrivée par hasard. Elle est le produit de la rigueur de la pensée mathématique. Pourquoi les mathématicien·nes sont iels reconnu·es pour leur rigueur ? En voici la raison : pour que tout le monde s'accorde sur une idée, celle-ci doit être précisément énoncée. Formellement, cela passe par l'utilisation d'un (ou plutôt plusieurs) langage mathématique, avec une grammaire précise qui délimite le pouvoir d'expression de ce langage.

Heureusement, de nombreuses libertés peuvent être prises par rapport à ce langage pour *communiquer* les mathématiques. Pour jouir de ces libertés, il faut en connaître les limites. C'est une apprentissage indispensable durant la première année d'étude en mathématiques. Elle se fait au travers de tous les cours du programme - souvent de manière vicariante (*i.e.*, par observation du comportement des professeur·e·s et assistant·e· s). Dans ce cours, nous nous attacherons particulièrement à la formalisation (ou plutôt la *formulation*, au sens de la mise en mots) de cet apprentissage. Bref, nous espérons que ce cours aura un effet *structurant* sur votre pensée mathématique !

1.1 *Transition lycée -université*

Vous êtes étudiant·e à l'université ! Que signifie ce nouveau statut ? On peut le résumer de la manière suivante : *vous êtes totalement responsable de votre apprentissage*. Dans ce cadre, le rôle de vos enseignant·e·s et encadrant·e·s est de vous fournir différents outils pour apprendre (cours en présentiel, notes de cours, bibliographie, listes d'exercices, Math Forge…) À vous de sélectionner et d'utiliser ceux qui vous conviennent le mieux.

Du point de vue de la quantité de travail, on peut grossièrement estimer que *quelque soit la quantité de travail que vous déployiez au lycée, elle sera double à l'université*. Ne vous laissez pas dépasser par la quantité de matière !

Du point de vue du contenu mathématique, vous allez découvrir un nouvel univers. Petit à petit, les exercices qui vous seront proposés seront de moins en

moins routiniers et demanderont de plus en plus de créativité mathématiques.

Mais ne paniquez pas ! Tout est mis en place pour adoucir cette transition et tou·te·s les étudiants qui ont été diplômés sont passés par là avant vous !

1.2 *Comment lire ces notes ?*

Ces notes servent de référence pour le cours de Structure Mathématiques. Elles font foi [1] en ce qui concerne les définitions, énoncés de théorèmes… Elles doivent être consultées régulièrement, après chaque cours. Elles sont écrites dans une optique d'apprentissage : elles ne sont pas succinctes (surtout au début) afin de mettre en évidence les pièges connus dans les premiers pas d'un apprenti mathématicien·ne. Parfois, elles ouvrent des perspectives sur la matière couverte.

Elles constituent un complément à la participation au cours théorique, auquel elles ne pourraient se substituer, et servent de base à la participation *active* aux séances d'exercices.

1.3 *Théorème, lemme, conjecture...*

La terminologie mathématique (plus noblement appelé *métalangue*) regorge de mots pour qualifier le statuts des énoncés mathématiques : on parle de théorème, corollaire, lemme, proposition, conjecture (mais aussi d'hypothèse, de contre exemple, axiome, scolie, prolégomènes, preuves…) Nous donnons ci-dessous un bref panorama des éléments les plus importants de ce bestiaire destiné à classifier (de manière arbitraire) les énoncés selon leur importance, leur utilisation ou leur statut logique (sont-ils démontrés ou pas ?)

— *Proposition (n. f.)* : Une proposition (mathématique) est un énoncé mathématique qui a été démontré comme vrai. Dans la construction d'une théorie mathématique, une proposition est un énoncé intéressant mais dont la portée n'est pas suffisante pour qu'elle soit considérée comme un jalon ou un résultat essentiel du domaine.

— *Théorème (n. m.)* : Un théorème est une proposition dont l'importance en fait un résultat fondamental du domaine mathématique dans lequel il est énoncé. Cette importance peut tenir à la portée du résultat, la difficulté de la preuve (à relativiser par rapport à l'époque à laquelle le théorème a été prouvé), aux nombres d'années qu'il a été nécessaire pour en obtenir une preuve ou pour son rôle de jalon dans un domaine mathématique. Certains théorèmes sont à ce point centraux dans une théorie mathématique qu'on leur a attribué le qualificatif de *fondamental* (on parle de Théorème fondamental de l'algèbre, ou de Théorème fondamental de l'arithmétique par exemple).

— *Corollaire (n.m.)* : Un corollaire est un énoncé dont la preuve découle facilement d'un autre énoncé déjà prouvé (théorème ou proposition). Du point de vue du contenu mathématique, il n'apporte pas grand chose de

1. Il s'agit de la première édition, et elles contiennent sans doute encore de nombreuses erreurs et fautes de frappe.

neuf mais la manière dont il est formulé le rend parfois plus accessible que le théorème ou la proposition dont il est issu (parfois, un corollaire énonce un cas particulier).

— *Lemme (n. m.)* : Le Lemme est un résultat technique qui est utilisé dans la preuve d'un résultat dont l'importance est plus universelle (proposition ou théorème). Un lemme énonce donc un résultat qui n'est pas très intéressant en soi, mais qui est un outil dans la construction d'un domaine mathématique. Parfois, certaines parties de preuves de théorèmes sont isolées dans des lemmes, soit pour simplifier la structure de la preuve du théorème (et la rendre plus lisible), soit parce qu'elles constituent un outil qui sera utilisé plusieurs fois à l'avenir. Certains lemmes sont si souvent utiles qu'on leur donne un nom (on parle du Lemme de la pompe en théorie des langages réguliers, du Lemme des poignées de mains en théorie des graphes, du Lemme de la vérité en logique mathématique…)
— *Conjecture (n. m.)* : Une conjecture est un énoncé mathématique qui n'a pas encore été prouvé mais dont (une partie au moins) de la communauté mathématique pense qu'il est vrai. Seuls les énoncés importants sont dignes d'être qualifié de conjecture, le cas échéant.
— *Axiome (n. m.)* : Dans un un système de déduction, un axiome (ou *postulat*) est un énoncé considéré comme vrai par convention. L'axiome le plus célèbre est peut-être le *cinquième postulat* d'Euclide, ou *axiome des parallèles* qui stipule que (en géométrie euclicienne) par un point il ne passe qu'une et une seule droite parallèle à une droite donnée [2].
— *Contre-exemple (n. m.)* : Un contre exemple est un modèle (objet mathématique) qui illustre qu'une assertion est fausse. Par exemple, si l'assertion a la forme

  Si φ alors ψ,

  un contre-exemple de cette assertion est un objet mathématique qui satisfait φ mais pas ψ.

2 LOGIQUE PROPOSITIONNELLE CLASSIQUE

Un·e mathématicien·e, ça raisonne énormément. Et ça raisonne bien. Mais qu'est-ce qu'un raisonnement ? Est-ce qu'on peut identifier les raisonnements valides des raisonnements fallacieux ? Mieux, est-ce qu'on peut considérer les raisonnements comme des objets mathématiques ? C'est-à-dire, les imaginer comme un objet d'étude des mathématiques, alors même que la pratique de celles-ci reposent précisément sur les raisonnements ?

Oui, on le peut et c'est l'objet d'une discipline appelée *logique mathématique*. Dans cette section, nous allons considérer les éléments les plus rudimentaires de la logique, matérialisés dans la *logique propositionnelle classique* - abrégée par LPC. Celle-ci ne s'occupe que du Vrai et du Faux, et des liens logiques entre ceux-ci. Il s'agit donc du rouage fondamental du raisonnement mathématique,

2. Il s'agit ici d'un énoncé équivalent à l'énoncé original

et plus généralement de toute discipline scientifique, ou de tout discours basé sur la notion de déduction et de raisonnement valide.

2.1 *Assertions et connecteurs*

Commençons par définir l'objet d'étude de LPC.

1 DÉFINITION. Une *assertion* est un énoncé (mathématique ou en langage naturel) qui est soit vrai soit faux, et cela de manière absolue.

2 EXEMPLE. ¸

1. L'énoncé $1 < 4$ est une assertion vraie. L'énoncé $4 < 1$ est une assertion fausse.
2. L'énoncé « En 2023, les élections communales se sont déroulées le 11 juin au Luxembourg » est une assertion vraie. L'assertion « Xavier Bettel est plus jeune que Taina Bofferding » est une assertion fausse (Xavier Bettel est né en 1973 et Taina Bofferding est née en 1982).
3. L'énoncé « Aujourd'hui, il pleut » n'est pas une assertion. En effet, elle n'est ni absolument vraie ni absolument fausse. Sa véracité dépend de l'endroit où elle est énoncée, et il se peut qu'il n'y ait eu qu'une averse sur la journée.
4. L'énoncé « Je suis plus intelligent que Keanu Reeves » n'est pas une assertion. Sa véracité dépend de nombreux facteurs (interlocuteur, type d'intelligence), elle n'est pas constante dans le temps et est relative.
5. L'énoncé « Le 14 juillet 2023, il faisait froid à Belval » n'est pas une assertion. En effet, la notion « faire froid » est une notion floue, dont l'interprétation dépend d'ailleurs de l'interlocuteur.

LPC s'occupe donc des énoncés dont la véracité ne laisse aucune place à l'arbitraire. C'est en cela qu'elle est la logique de base des raisonnements mathématiques (et informatique, scientifique, politique...)

3 NOTATION. Nous allons génériquement noter les assertions par des lettres grecques φ, ψ, $\rho\ldots$ Chaque assertion a *une valeur de vérité*. Par convention, on dit qu'une assertion ψ a la valeur de vérité 1 si elle est vraie, et la valeur de vérité 0 si elle est fausse.

Voilà. Nous savons ce qu'est une assertion. Mais nous sommes dans la position d'un charpentier qui n'aurait pas d'outils : devant son tas de bois, il n'est pas bien avancé. Il nous faudrait un moyen de donner un peu de structure aux assertions. Ou plus précisément, il serait utile de pouvoir construire de nouvelles assertions à partir d'assertions existantes. Un peu comme on assemble des briques de Lego®. C'est ci qu'interviennent les connecteurs logique.

4 DÉFINITION. Soient φ et ψ des assertions.

(1) L'assertion $\varphi \vee \psi$ (lire « φ *ou* ψ ») est l'assertion qui est vraie si au moins une des assertions φ, ψ est vraie. On appelle $\varphi \vee \psi$ la *disjonction de* φ *et* ψ.

φ	ψ	$\varphi \vee \psi$	$\varphi \wedge \psi$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

ψ	$\neg\psi$
0	1
1	0

FIGURE 1 – Tables de vérités des connecteurs $\vee$, $\wedge$ et $\neg$.

(2) L'assertion $\varphi \wedge \psi$ (lire « φ *et* ψ ») est l'assertion qui est vraie si les deux assertions φ, ψ sont vraies. On appelle $\varphi \wedge \psi$ la *conjonction de* φ *et* ψ.

(3) L'assertion $\neg\psi$ (lire « *non* ψ ») est l'assertion qui est vraie si ψ est faux[3]. On appelle $\neg\psi$ la *négation de* ψ.

Remarquez que pour définir les nouvelles assertions ci-dessus, il nous a suffit de préciser sous quelles conditions elles sont vraies ou fausses. Ces définitions sont synthétisées dans la Fig. 1.

Les symboles $\vee$, $\wedge$ et $\neg$ sont appelés *connecteurs* (ou *opérateurs*) logiques. Les connecteurs $\vee$ et $\wedge$ sont *binaires* (car ils ont deux arguments, c'est-à-dire qu'ils connectent deux assertions pour en former une autre) tandis que le connecteur $\neg$ et *unaire*. On peut imaginer des tas d'autres connecteurs (et on en introduira de nouveaux pas la suite). Vous pouvez vous amuser à introduire votre propre connecteur logique !

5 REMARQUE. Le connecteur $\vee$ est une version *inclusive* du « ou ». Il faut le distinguer du « ou » *exclusif*, noté $\oplus$, qui est défini de la sorte que l'assertion $\varphi \oplus \psi$ est vraie si exactement une des assertions φ, ψ est vraie. C'est la version exclusive du « ou » que l'on trouve par exemple dans les menus de restaurant, où on peut lire « Fromage ou dessert » (le client est invité à prendre le fromage ou le dessert, mais pas les deux).

Nous allons distinguer les assertions qui sont obtenues en « connectant » des assertions existantes des autres assertions. C'est l'objet de la définition suivante.

6 DÉFINITION. On appelle *assertion composée* une assertion qui est obtenue à partir d'une (ou plusieurs) autre·s assertions à l'aide d'un connecteur. On appelle *variable propositionnelle* ou *assertion atomique* une assertion qui n'est pas composée.

On introduit l'assertion atomique $\top$ (qui peut aussi être vu comme un connecteur 0-aire) comme l'assertion dont la valeur de vérité est 1 et sa negation $\bot$ qui

3. On voit apparaître ici une convention d'écriture en mathématiques : les symboles mathématiques sont masculins. On écrit ainsi « ψ est faux » et non pas « ψ est fausse » . Bien sûr, on continue d'écrire « L'assertion ψ est fausse. »

est l'assertion dont la valeur de vérité est 0.

7 EXEMPLE. L'assertion $(5 < 4) \wedge (3 + 3 = 9)$ est une assertion composée qui est fausse, tandis que $3 + 3 = 6$ est assertion atomique qui est vraie.

Ainsi, les assertions atomiques se comportent un peu comme les atomes en chimie : ce sont des entités insécables qui permettent de créer de nouvelles assertions par assemblage via les connecteurs logiques.

8 NOTATION. (1) Si on veut insister sur le caractère atomique de certaines assertions, on utilisera les symboles $p, q, r, \ldots, p_1, p_2 \ldots$ au lieu des lettres grecques $\varphi, \psi \ldots$ Si φ est une assertion composée, on utilisera la notation $\varphi(p_1, \ldots, p_n)$ pour indiquer que les assertions atomiques qui la composent se trouvent parmi $p_1, \ldots p_n$.

(2) Dans l'algèbre des nombres réels, l'opération $\times$ a priorité sur le $+$. Ainsi, on écrit $3 \times 4 + 9$ pour $(3 \times 4) + 9$. De manière similaire, en logique, l'opérateur $\neg$ a priorité sur les autres. On écrit $\neg p \vee q$ au lieu de $(\neg p) \vee q$.

9 EXEMPLE. Les assertions $(p \vee q) \wedge \neg r$ et $(\neg p \vee r) \vee q$ sont des assertions composées à partir des assertions atomiques p, q et r.

Ainsi, la valeur de vérité d'une assertion composée s'obtient à partir des valeurs de vérité des assertion atomiques qui la composent. On peut emboîter un nombre indéterminé d'assertions à l'aide des connecteurs, et construire des assertions composées extrêmement complexes, avec un nombre arbitraire d'assertions atomiques. Mais comment déterminer la valeur de vérité d'une telle assertion ? On procède de proche en proche [4] en commençant par la valeur de vérité des assertions atomiques. On construit ainsi la table de vérité de l'assertion composée.

10 DÉFINITION. Soit $\psi(p_1, \ldots, p_n)$ une assertion composée. La *table de vérité de* ψ est un tableau qui donne la valeur de vérité de ψ en fonction des 2^n valeurs possibles du tuple $(p_1, \ldots, p_n)$.

On a coutume de synthétiser la définition de ces connecteurs logiques en en donnant leur *table de vérité*, c'est-à-dire un tableau donnant la valeur de vérité de l'assertion composée en fonction des valeurs de vérités des connecteurs qui la compose.

11 EXEMPLE. On construit la table de vérité de $(p \vee q) \wedge \neg r$, on commençant par construite la table de $p \vee q$, puis celle de $\neg r$, puis en connectant les deux à l'aide de la table de $\wedge$. Voir Fig. 2

De manière similaire, on construit la table de vérité de $(\neg p \vee r) \vee q$, on commençant par construiee la table de $\neg p \vee q$, en la connectant avec celle de r grâce à la table du connecteur $\vee$. Voir Fig. 3

4. par *induction* sur le nombre de connecteurs de l'assertion

p	q	r	$(p \vee q)$	$\neg r$	$(p \vee q) \wedge \neg r$
0	0	0	0	1	0
0	0	1	0	0	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	0	0

FIGURE 2 – Table de vérité de $(p \vee q) \wedge \neg r$

p	q	r	$\neg p \vee r$	$(\neg p \vee r) \vee q$
0	0	0	1	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	0	1
1	1	1	1	1

FIGURE 3 – Table de vérité de $(\neg p \vee r) \vee q$

12 DÉFINITION. On appelle *tautologie* une assertion composée ψ qui est vrai quelles que soient les valeurs de vérité des assertions atomiques qui la composent. On appelle contradiction une assertion ψ telle que $\neg\psi$ est une tautologie.

Une formule composée ψ pour laquelle il possible d'assigner les valeurs de vérité de ses assertions atomiques de telle sorte que ψ soit vrai est dite *satisfaisable*.

13 EXEMPLE. On vérifie facilement que $p \vee \neg p$ est une tautologie tandis que $p \wedge \neg p$ est une contradiction. L'assertion $p \vee q$ est satisfaisable sans être une tautologie.

Ainsi, une tautologie est une assertion qui est tout le temps vrai *de part sa construction*. Une contradiction est une assertion dont la négation est une tautologie.

SAT - Problème de satisfaisabilité booléenne

Dans une assertion atomique $\psi(p_1, \ldots, p_n)$ à $n \geq 1$ variables propositionnelles, chaque variable propositionnelle peut prendre 2 valeurs de vérité (vrai ou faux). Ainsi, la table de vérité de ψ contiendra 2^n lignes. Cette taille grandit exponentiellement avec n, ce qui rend très vite ingérable la manipulation d'une telle table, même pour un ordinateur.
Par exemple, pour stocker la table d'une formule à 40 variables il faudrait une mémoire à $2^{40} \simeq 10^{12}$ bits, c'est à dire 1 térabit. Et pour les applications industrielles, représenter un problème de contraintes en une assertion à 40 variables est un problème de petite dimension…
Le problème *SAT* (*Boolean SATisfcation Problem*) est défini de la manière suivante :

> Étant donné une assertion composée, trouver une affectation de ses variables propositionnelles qui rend la formule vraie.

Du point de vue algorithmique, c'est un problème en général très difficile. On ne connaît pas d'algorithme en temps polynomial pour le résoudre. Mieux, il s'agit d'un problème NP-complet. Informellement, cela signifie que

- on peut vérifier facilement (*i.e.*, en temps polynomial) qu'une solution proposée et effectivement une solution ; un tel problème fait partie de la classe NP ;
- tout problème de la classe NP peut être réduit en un temps polynomial au problème SAT.

Ainsi, un problème NP est un problème dont il est facile de vérifier les solutions, mais dont les solutions sont peut-être difficiles à trouver. Il y a un grand problème en mathématiques et en informatiques (dont la résolution procurerait à son auteur·e la coquette somme de $\$10^6$ offert par l'Institut Clay) qui consiste à déterminer si P=NP, c'est-à-dire si les

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

FIGURE 4 – Les assertions $p \vee (q \wedge r)$ et $(p \vee q) \wedge (p \vee r)$ sont sémantiquement équivalentes

problèmes qu'on peut résoudre en un temps polynomial sont exactement ceux dont on peut vérifier la solution en un temps polynomial (la plupart des mathématiciens espèrent que ce n'est pas le cas).

2.2 *Équivalence sémantique et algèbre de Boole des assertions*

En logique mathématique, on distingue deux aspects :
— les aspects *syntaxiques* qui concernent la manière dont sont *écrites* les formules (ou les assertions dans notre cas),
— les aspects *sémantiques* qui concernent la manière dont sont *interprétées* les formules (*via* les tables de vérités dans notre cas).

Pour faire simple, on pourrait dire que la syntaxe s'occupe de *la forme* alors que la sémantique s'occupe du *sens*. Bien sûr, les deux aspects ne sont pas indépendants, puisque la syntaxe (la manière dont s'écrit une assertion dans notre cas) influe sur la sémantique (sous quelles conditions l'assertion est vraie).

Ainsi, le contenu informatif logique se trouve du côté de la sémantique, ce qui justifie la définition suivante.

14 DÉFINITION. Deux assertions composées $\varphi(p_1, \ldots, p_n)$ et $\psi(p_1, \ldots, p_n)$ sont *sémantiquement équivalentes*, ce qu'on l'on note $\varphi \equiv \psi$, si elle ont la même table de vérité. On dit que $\varphi \equiv \psi$ est *une identité propositionnelle*.

Autrement dit, les assertions $\varphi(p_1, \ldots, p_n)$ et $\psi(p_1, \ldots, p_n)$ sont sémantiquement équivalente si pour toute affection des variables $p_1, \ldots, p_n$ à des valeurs de vérité, la valeur de vérité de φ et ψ coïncident. Ainsi, si $\varphi \equiv \psi$ alors φ et ψ sont indiscernables du point de vue logique (au sens sémantique), même si elles ont une écriture (syntaxe) différente.

15 EXEMPLE. Les assertions $p \vee (q \wedge r)$ et $(p \vee q) \wedge (p \vee r)$ sont sémantiquement équivalentes. En effet, leur table de vérité (donnée dans la Fig. 7) coïncident.

L'important, c'est que si $\varphi \equiv \psi$ alors on peut remplacer toute occurrence de

Identité	**Nom**
$p \wedge q \equiv q \wedge p$	Commutativité de $\wedge$
$p \vee q \equiv q \vee p$	Commutativité de $\vee$
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associativité de $\wedge$
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associativité de $\vee$
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distribution de $\wedge$ sur $\vee$
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distribution de $\vee$ sur $\wedge$
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	Loi de De Morgan pour $\vee$
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	Loi de De Morgan pour $\wedge$
$p \wedge (p \vee q) \equiv p$	Loi d'Absorption
$p \vee (p \wedge q) \equiv p$	Loi d'Absorption
$p \vee \neg p \equiv \top$	Principe du tiers exclu
$p \wedge \neg p \equiv \bot$	Principe de contradiction
$\neg(\neg p) \equiv p$	Double négation
$p \vee \bot \equiv p$	$\bot$ est neutre pour $\vee$
$p \wedge \top \equiv p$	$\top$ est neutre pour $\wedge$

FIGURE 5 – Identités propositionnelles

φ par une occurrence de ψ tout en gardant un contenu logique équivalent. On peut par exemple remplacer une assertion par une assertion sémantiquement équivalente mais plus courte (en terme de nombre de connecteurs), donc plus facile à manipuler.

16 DÉFINITION. L'*algèbre de Boole des assertions* est l'ensemble des formules considérées à l'identification des formules sémantiquement équivalentes près.

C'est une définition un peu abstraite qui fait en réalité apparaître la notion de relation d'équivalence et de quotient que nous verrons plus tard. À ce stade, on va se contenter de lister les identités propositionnelles les plus utiles (on peut même montrer qu'elles permettent de générer toutes les autres).

17 PROPOSITION. *La Fig. 5 liste des identités propositionnelles.*

Démonstration. Pour chaque identité, la preuve consiste à montrer que les deux membres de l'identité ont même table de vérité et est laissée aux lecteur·rice·s à titre d'exercice. □

2.3 *Implication et équivalence syntaxique*

Pour le moment, nous avons à notre disposition des assertions atomiques (ou variables propositionnelles) et des connecteurs $\wedge$, $\vee$ et $\neg$ pour les assembler en des assertions composées.

Ne nous manque-t-il pas quelque chose pour mettre en musique les aspects élémentaires du raisonnement mathématique ? Si bien sûr ! Il nous manque la possibilité de formuler des assertions du type « Si $[\cdots]$ alors $[\cdots]$ » qui sont au

φ	ψ	$\varphi \Rightarrow \psi$
0	0	1
0	1	1
1	0	0
1	1	1.

FIGURE 6 – Table de vérité de $\varphi \Rightarrow \psi$.

coeur de la majorité des énoncés des théorèmes mathématiques, ou des tests dans les langages de programmation. Pour y remédier, nous alons introduire un nouveau connecteur binaire $\Rightarrow$, appelé *implication* et qui servira à capturer le « Si $[\cdots]$ alors $[\cdots]$ » mathématique. Pour le définir, nous savons qu'il suffit d'en donner sa table de vérité. Nous allons essayer d'en inférer sa forme (qui est une convention) à partir d'un exemple concret.

18 EXEMPLE. Partons de l'observation que l'assertion

Si $x \geq 5$ alors $x \geq 3$.

est vraie, que que soit la valeur de x. En admettant que le connecteur $\Rightarrow$ a pour but de traduire le « Si $[\cdots]$ alors $[\cdots]$ » mathématique, nous avons donc les contraintes suivantes sur la table de vérité de $\Rightarrow$

x	$x \geq 5$	$x \geq 3$	$(x \geq 5) \Rightarrow (x \geq 3)$
1	0	0	1
4	0	1	1
6	1	1	1

Trois des quatre lignes de la table de vérité de $\Rightarrow$ sont donc fixés par cet exemple. La table complète est donnée dans la définition suivante.

19 DÉFINITION. Si φ et ψ sont des assertions, l'assertion $\varphi \Rightarrow \psi$ (lire *Si* φ, *alors* ψ ou φ *implique* ψ) est l'assertion dont la table de vérité est donnée dans la figure Fig. 6.

Dans $\varphi \Rightarrow \psi$, on dit que φ est une *condition suffisante* à ψ et que ψ est une condition nécessaire à φ.

Lorsqu'on la rencontre pour la première fois, la table de vérité de l'implication peut sembler contre-intuitive. L'exemple 18 montre pourtant qu'il s'agit de la table qui modélise le « Si $[\cdots]$ alors $[\cdots]$ » mathématique. Voici un moyen mnémotechnique de retenir cette table :

La seule situation pour que l'assertion $\varphi \Rightarrow \psi$ soit fausse est que φ soit vrai et ψ soit faux.

20 EXEMPLE. Donnons un exemple en langage naturel pour mieux appréhender l'implication. Considérons l'assertion ρ donnée par

S'il pleut, alors je prends mon parapluie.

La condition *il pleut* est suffisante à *je prends mon parapluie*. La condition *je prends mon parapluie* est nécessaire (*i.e.*, *s'ensuit nécessairement à*) *il pleut*.

La seule manière pour cette assertion ρ d'être fausse est qu'il pleuve *et que je n'ai pas mon parapluie*. Dans toute autre situation, l'assertion ρ est vraie.

La proposition suivante illustre que l'implication est une abréviation pour une formule composée à partir des connecteurs $\vee$ et $\neg$

21 PROPOSITION. *Les assertions $\varphi \Rightarrow \psi$ et $\psi \vee \neg\varphi$ sont sémantiquement équivalentes.*

Démonstration. Il suffit de montrer que les tables de vérité de $\varphi \Rightarrow \psi$ et celle de $\psi \vee \neg\varphi$ sont identiques, ce qui est laissé à titre d'exercice. □

Nous en déduisons un corollaire évident, mais très important dans les techniques de preuve.

22 COROLLAIRE. *Si φ est une assertion fausse, alors $\varphi \Rightarrow \psi$ est une assertion vraie, quelque soit la valeur de vérité de ψ.*

23 EXEMPLE. L'assertion

> Si 3 est un nombre pair, alors moi je suis le Pape.

est vraie. Il s'agit d'une application du corollaire précédent avec φ défini comme *3 est un nombre pair* et ψ définit comme *moi je suis le Pape*.

Le résultat suivant montre qu'on peut en fait définir le connecteur $\neg$ en utilisant uniquement les connecteurs $\Rightarrow$ et $\bot$. Il nous sera utile lorsque nous apprendrons les différentes techniques de preuve.

24 PROPOSITION. *Pour toute assertion ψ, on a*

$$\neg\psi \quad \equiv \quad \psi \Rightarrow \bot.$$

Démonstration. Il suffit de montrer que la table de vérité de $\psi \Rightarrow \bot$ est égale à celle de $\neg\psi$. Une autre preuve consiste à utiliser une suite d'équivalence syntaxique. On a successivement

$$\psi \Rightarrow \bot \quad \equiv \quad \bot \vee \neg\psi \quad \equiv \quad \neg\psi,$$

ce qui conclut la preuve. □

On associe à l'implication $\varphi \Rightarrow \psi$ deux autres assertions définies ci-dessous.

25 DÉFINITION. Soient φ et ψ deux assertions. La *réciproque* de $\varphi \Rightarrow \psi$ est l'assertion $\psi \Rightarrow \varphi$. La *contraposée* de $\varphi \Rightarrow \psi$ est l'assertion $\neg\psi \Rightarrow \neg\varphi$.

26 EXEMPLE. Considérons l'assertion ρ suivante :

> Si tu finis le projet, alors tu as une prime.

φ	ψ	$\varphi \Rightarrow \psi$	$\psi \Rightarrow \varphi$	$(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$	$\varphi \Rightarrow \psi$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	1	0	0
1	1	1	1	1	1

FIGURE 7 – Table de vérité de $\varphi \Leftrightarrow \psi$

On peut l'écrire en langage symbolique par $\varphi \Rightarrow \psi$ si φ est l'assertion *tu as fini le projet* et ψ est l'assertion *tu as une prime*.

La réciproque de ρ est

> Si tu as une prime, alors tu as fini le projet

et la contraposée est

> Si tu n'as pas de prime, alors tu n'as pas fini le projet.

Le grand intérêt de la contraposée d'une implication est qu'elle contient exactement le même contenu logique que l'implication de départ, comme exprimé dans le résultat suivant.

27 PROPOSITION. *Pour toutes assertions φ, ψ on a*

$$\varphi \Rightarrow \psi \quad \equiv \quad \neg\psi \Rightarrow \neg\varphi.$$

Démonstration. Il suffit de vérifier que la table de vérité de $\neg\psi \Rightarrow \neg\varphi$ est égale à celle de $\varphi \Rightarrow \psi$, ce qui est laissé à titre d'exercice. □

Nous verrons plus tard dans le cours à quel point cette simple observation peut être utile : pour démontrer une implication $\varphi \Rightarrow \psi$ il est parfois plus simple de démontrer sa contraposée $\neg\psi \Rightarrow \neg\varphi$ (qui lui est sémantiquement équivalente).

Dans la panoplie des connecteurs logiques, il nous manque encore le plus célèbre. J'ai nommé la *bi-implication* (ou *équivalence syntaxique*) $\Leftrightarrow$.

28 DÉFINITION. Soient φ, ψ deux assertions. L'assertion $\varphi \Leftrightarrow \psi$ (lire φ *si et seulement si* ψ ou φ *équivalent à* ψ) est définie comme une abréviation de $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$.

Cette définition signifie qu'on définit $\varphi \Leftrightarrow \psi$ comme l'assertion dont la table de vérité est celle de $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$. Elle est indiquée dans la Fig. 7. Ainsi, l'assertion $\varphi \Leftrightarrow \psi$ signifie que φ est *une condition nécessaire et suffisante* à ψ, et aussi que φ est *une condition nécessaire et suffisante* à ψ.

On observe que l'assertion $\varphi \Leftrightarrow \psi$ est vrai exactement sous la condition que φ et ψ ont la même valeur de vérité.

29 EXEMPLE. Soit φ l'assertion *tu finis le projet* et ψ l'assertion *tu as une prime*. L'assertion $\varphi \equiv \psi$ signifie que *tu as une prime* exactement dans les situations ou

tu as une prime.

La proposition suivante établit une relation ente l'*équivalence sémantique* et *l'équivalence syntaxique*.

30 PROPOSITION. *Soient $\varphi(p_1, \ldots, p_n)$ et $\psi(p_1, \ldots, p_n)$ deux assertions. Les conditions suivantes sont équivalentes.*

(i) $\varphi \Leftrightarrow \psi$ *est une tautologie.*

(ii) $\varphi \equiv \psi$.

Démonstration. L'énoncé signifie précisément que $(i) \Leftrightarrow (ii)$ est une tautologie, ou encore que $(i) \Rightarrow (ii)$ et $(ii) \Rightarrow (i)$.

Démontrons que $(i) \Rightarrow (ii)$. Si $\varphi \Leftrightarrow \psi$ est une tautologie, alors dans toutes les situations où φ est vrai, l'assertion ψ l'est aussi, et inversement. Autrement dit, les tables de vérité de φ et ψ coïncident.

Démontrons que $(ii) \Rightarrow (i)$. Si $\varphi \equiv \psi$, alors φ et ψ ont même table de vérité. En particulier, dans toute situation où φ est vrai, il en est de même pour ψ. Ceci prouve que $\varphi \Rightarrow \psi$ est une tautologie. Un raisonnement similaire indique que $\psi \Rightarrow \varphi$ est également une tautologie. Au final $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$, c'est-à-dire $\varphi \Leftrightarrow \psi$, est une tautologie. □

La proposition précédente nous permet d'identifier l'*équivalence sémantique* et l'*équivalence syntaxique*. Dès lors, on écrira $\phi \Leftrightarrow \psi$ au lieu de $\phi \equiv \psi$ si on le souhaite.

2.4 *Fonctions et polynômes Booléens*

Dans cette section, nous allons comprendre pourquoi on a basé la construction des ordinateurs sur l'assemblage de portes logiques (c'est-à-dire la réalisation physique de connecteurs logiques).

31 DÉFINITION. Une *fonction booléenne f à $n \geq 1$ variables booléennes* est une loi [5] qui à tout n-uplet [6] $(p_1, \ldots, p_n)$ constitués d'éléments de $\{0, 1\}$ associe un et un seul élément de $\{0, 1\}$, appelé la *valeur* de f en $(p_1, \ldots, p_n)$ et noté $f(p_1, \ldots, p_n)$.

Par exemple, toute assertion composée $\psi(p_1, \ldots, p_n)$ définit une fonction booléenne à n variables booléenne. Pour connaître la valeur de la fonction en un n-uplet $(p_1, \ldots, p_n)$, il suffit de regarder la valeur correspondante dans la table de vérité.

32 EXEMPLE. Considérons l'assertion ψ définie comme $(p_1 \Rightarrow \neg p_2) \wedge (\neg p_2 \Rightarrow p_3)$. Cette assertion ψ définit une fonction f_ψ à trois variables booléennes. On a par

5. Nous définirons formellement la notion de fonction ultérieurement.
6. Un *n-uplet* est une suite ordonnée de n éléments.

exemple

$$f_\psi(0,0,0) = (0 \Rightarrow 1) \wedge (1 \Rightarrow 0) = 1 \wedge 0 = 0,$$

$$f_\psi(0,1,0) = (0 \Rightarrow 0) \wedge (0 \Rightarrow 0) = 1 \wedge 1 = 1,$$

$$f_\psi(1,1,1) = (1 \Rightarrow 0) \wedge (0 \Rightarrow 1) = 0 \wedge 1 = 0.$$

Nous allons considérer le problème réciproque, à savoir

> Étant donné une fonction booléenne à n-variables booléennes f, existe-t-il un assertion composée $\psi(p_1, \ldots, p_n)$ telle que $f(p_1, \ldots, p_n) = \psi(p_1, \ldots, p_n)$ pour tous $p_1, \ldots, p_n \in \{0,1\}$?

La réponse à cette question est positive. Avant d'en donner la preuve en toute généralité, introduisons la technique sur un exemple illustratif.

33 EXEMPLE. Considérons la fonction booléenne f à trois variables booléennes définie par la table suivante.

#	p	q	r	$f(p,q,r)$
0	0	0	0	0
1	0	0	1	0
2	0	1	0	1
3	0	1	1	1
4	1	0	0	0
5	1	0	1	1
6	1	1	0	0
7	1	1	1	0

où on a indiqué les numéros de ligne par simplicité. La fonction $f(p,q,r)$ est vraie si et seulement si (p,q,r) prend des valeurs qui correspondent à la ligne 2, 3 ou 5, c'est dire si et seulement si

$$(p = 0 \wedge q = 1 \wedge r = 0) \vee (p = 0 \wedge q = 1 \wedge r = 1) \vee (p = 1 \wedge q = 0 \wedge r = 1).$$

De manière équivalente, on a que $f(p,q,r) = 1$ si et seulement si[7]

$$\psi(p,q,r) := (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg^q \wedge r)$$

est vraie. Cela signifie que $\psi(p,q,r) = f(p,q,r)$ pour tous $p,q,r \in \{0,1\}$.

Cet exemple se généralise sous la forme du résultat suivante.

34 THÉORÈME. *Soit f une fonction booléenne à $n \geq 1$ variables booléennes. Il existe une assertion composée $\psi_f(p_1, \ldots, p_n)$ telle que $f(q_1, \ldots, q_n) = \psi_f(q_1, \ldots, q_n)$ pour*

7. Le symbole := signifie que le membre de gauche est défini comme égal au membre de droite. Autrement dit, l'expression à gauche de := est un raccourci d'écriture pour l'expression qui se trouve à droite. L'asymétrie visuel du symbol := est là pour indiquer qu'il s'agit d'une *identité par définition*. Il rappelle les symboles d'affectation de variables dans certains langages de programmation.

tous $q_1, \ldots, q_n \in \{0, 1\}$.

Démonstration. Désignons par $\mathcal{I}_f$ la collection des n-uplets $(p_1, \ldots, p_n)$ d'éléments de $\{0, 1\}$ tels que $f(p_1, \ldots, p_n) = 1$. Pour tout élément $(p_1, \ldots, p_n)$ de $\mathcal{I}_f$, définissons l'assertion $\psi_{(p_1,\ldots,p_n)}$ par

$$q_1^{\epsilon_1} \wedge \cdots \wedge q_n^{\epsilon_n},$$

où pour tout $i \leq n$, on pose $q_i^{\epsilon_i} := q_i$ si $p_i = 1$ et $q_i^{\epsilon_i} := \neg q_i$ si $q_i = 0$. Finalement, définissons ψ_f comme la disjonction des $\psi_{(p_1,\ldots,p_n)}$ pour $(p_1, \ldots, p_n)$ dans $\mathcal{I}$, ce qui s'écrit

$$\psi_f := \bigvee_{(p_1,\ldots,p_n)\in\mathcal{I}} \psi_{(p_1,\ldots,p_n)}.$$

L'assertion ψ_f satisfait aux conditions de l'énoncé. □

On appelle *forme normale disjonctive* de f l'assertion ψ_f définie dans l'énoncé précédent.

35 EXERCICE. Procédez de manière analogue pour définir la forme normale conjonctive (qui est une disjonction de conjonction de variables propositionnelles ou de leur négation).

L'ordinateur : une grosse machine logique

Les ordinateurs ont été conçus comme de grosses machines implémentant LPC. Essayons de préciser un peu cette assertion. D'un point du vue rudimentaire et abstrait, un ordinateur peut à tout instant être caractérisé par l'état de sa mémoire. Celle ci est constituée d'un certains nombres de bits (de l'ordre de 10^9 bits par exemple), chacun desquels pouvant prendre deux états (0 ou 1). Un programme qui tourne sur l'ordinateur peut donc être vu comme une fonction qui fait passer un état de la mémoire à un autre (plusieurs millions de fois par seconde). Il peut donc être vu comme une fonction booléenne à 10^9 variables booléennes.

Ce que dit le Théorème 34 de ce point de vue, c'est que si on est capable de réaliser physiquement, au sein d'un ordinateur (typiquement le CPU) un grand nombre de connecteurs logiques, alors on est capable d'implémenter toutes les fonctions booléennes à 10^9 variables booléennes possibles, c'est-à-dire tous les programmes imaginables.

En résumé, les connecteurs logiques sont suffisamment riches pour permettre de réaliser tous les programmes !

3 THÉORIE NAÏVE DES ENSEMBLES

La notion d'ensemble peut-être vue comme le concept de base de la totalité des mathématiques. La théorie des ensembles est donc un fondement des mathématiques contemporaine [8].

La théorie des ensembles est une discipline axiomatique. Tout comme la géométrie ne définit pas la notion de *point*, mais spécifie un ensemble de règles pour les utiliser, la théorie des ensembles ne définit pas la notion d'ensemble, mais donne un ensemble de règles spécifiant comment les utiliser.

La théorie des ensembles est une théorie mathématique à part entière qui dépasse largement le cadre de ce cours. La grande majorité des mathématicien·ne·s ne sont pas experts en théorie des ensembles, mais tous et toutes, sans exception, sont capables de manipuler les ensembles dans le cadre d'une utilisation *en bon·ne père/mère de famille*. Les ensembles sont essentiels à leur travail quotidien. On qualifie de *naïve* le fragment de la théorie des ensembles qui fait partie de la connaissance commune des mathématicien·ne·s. Nous en esquissons ici les rudiments.

3.1 *Ensemble et appartenance*

On a naturellement envie de définir la notion d'ensemble comme une collection d'objets. Mais cette définition est bien trop naïve donne rapidement lieu à des paradoxes, comme illustré dans l'exemple suivant.

36 EXEMPLE (Paradoxe de Russel). Considérons l'ensemble E des ensembles qui ne se contiennent pas comme élément. Est-ce que E est un élément de E ? On constate facilement que E ne peut pas appartenir à E mais aussi qu'il ne se peut pas que E n'appartienne pas à E. Paradoxal !

Ce genre de paradoxes ont fait trembler les mathématiciens et les philosophes à la fin du XIXe siècle et au début du XXe siècle. Si la théorie des ensembles sert de fondement aux mathématiques, elle ne peut pas souffrir de tels paradoxes ! C'est ce qu'on a appelé *la crise des fondements*.

Heureusement, des solutions ont été trouvées pour renforcer les fondations. Sans entrer dans les détails, le paradoxe de Russell est par exemple évité en considérant qu'uniquement certaines collections sont *dignes* d'être des ensembles. C'est *grosso modo* le paradigme que nous allons utiliser dans ces notes, en ne développant notre théorie naïve des ensembles que pour des ensembles usuels en mathématiques.

Ainsi, nous ne considérons que les ensembles suivants :

(1) l'ensemble vide,

(2) les ensembles de nombres,

8. Les mathématiques peuvent être développée à partir d'autres fondements, comme la théorie des types. Les mathématiques obtenues sont essentiellement identiques, ce qui rend arbitraire la question du choix des fondements.

(3) les ensembles définis par extension,

(4) les ensembles définis par compréhension,

(5) les ensembles définis par union, intersection, complémentaire et les ensembles de parties.

Ces termes paraissent bien mystérieux pour le moment. Nous les explicitons dans la première partie de cette section.

D'abord, nous introduisons le *principe d'extensionnalité*, fondamental en théorie (naïve) des ensembles. Il indique que c'est la relation d'appartenance qui définit complètement un ensemble.

37 NOTATION. Soit A un ensemble. On note $x \in A$ pour indiquer que *x est un élément de* A.

Il n'y a pas de raison particulière pour indiquer les éléments par des lettres minuscules $x, \ldots$ et les ensembles par des lettres majuscules $A, \ldots$ En fait, les éléments d'un ensemble peuvent être de nature arbitraire : nombres, fonctions, chaînes de caractères... voir des ensembles eux-même [9] (c'est-à-dire qu'on peut considérer des ensembles d'ensemble [10] !

38 DÉFINITION (Principe d'extensionnalité). Deux ensembles A et B sont égaux si et seulement ils ont les mêmes éléments.

Ainsi, les ensembles A et B sont égaux si et seulement si pour tout $x \in A$ on a $x \in B$, et inversement [11] (c'est-à-dire, pour tout $x \in B$ on a $x \in A$). On peut aussi écrire le principe d'extensionnalité de la manière suivante :

$$A = B \text{ si et seulement si pour tout } x, \text{ on a } x \in A \iff x \in B.$$

Parfois, on applique le principe d'extensionnalité de la manière suivante :

> Pour montrer que $A = B$, il suffit de montrer que tout élément de A est un élément de B, et qu'il n'existe aucun élément de B qui n'est pas un élément de A.

Nous devons ensuite faire œuvre de foi et admettre, sans preuve (il s'agit d'un axiome [12] de la théorie des ensembles) l'existence de l'ensemble vide.

39 DÉFINITION. Il existe un ensemble qui ne contient aucun élément. On l'appelle l'*ensemble vide* et on le note $\varnothing$.

40 PROPOSITION. *L'ensemble vide $\varnothing$ est l'unique ensemble qui ne contient aucun élément.*

9. Un des principes fondamentaux de la théorie axiomatique des ensemble est justement de considéré que tout objet mathématique est un ensemble.

10. L'objet d'étude de base de la *topologie générale* (cours du 3e semestre) est la notion de *topologie* qui est un ensembles d'ensembles qui vérifie certaines propriétés

11. *Inversement* est ici un synonyme de réciproquement. La phrase *Si φ alors ψ, et* inversement signifie en fait $\varphi \Leftrightarrow \psi$.

12. Un axiome est une assertion acceptée comme vrai sans preuve.

Démonstration. Soit B un ensemble qui n'a aucun élément. On a donc, pour tout x

$$x \in \mathrm{B} \iff x \in \varnothing.$$

Il s'ensuit que $\mathrm{B} = \varnothing$ par le principe d'extensionnalité. □

41 DÉFINITION. On dit qu'un ensemble A est *inclus dans* (ou est *une partie de*) un ensemble B, et on écrit $\mathrm{A} \subseteq \mathrm{B}$, si tous les éléments de A sont aussi des éléments de B.

Il est crucial de bien distinguer les relation $\subseteq$ et $\in$ qui ne sont pas équivalentes. Par exemple, on a $1 \in \{1, 2\}$ alors que $\{1\} \subseteq \{1, 2\}$.

42 PROPOSITION. *(1) Si* B *est un ensemble, alors* $\varnothing \subseteq \mathrm{B}$.

(2) Soient A *et* B *deux ensembles. On a* $\mathrm{A} = \mathrm{B}$ *si et seulement si* $\mathrm{A} \subseteq \mathrm{B}$ *et* $\mathrm{B} \subseteq \mathrm{A}$.

(3) Si A *est un ensemble, on a* $\mathrm{A} \subseteq \mathrm{A}$.

Démonstration. 1. Pour tout x on doit montrer que

$$x \in \varnothing \implies x \in \mathrm{B}.$$

Comme $x \in \varnothing$ est toujours faux, l'implication précédente est toujours vraie.

2. C'est une reformulation du principe d'extensionnalité. □

Même s'il s'agit d'une reformulation élémentaire du principe d'extensionnalité, la Proposition 42 2 indique une stratégie à suivre pour montrer que deux ensembles A et B sont égaux : il suffit de montrer que $\mathrm{A} \subseteq \mathrm{B}$ et $\mathrm{B} \subseteq \mathrm{A}$.

3.2 *Ensembles de nombres*

Les premières collections non vides que nous allons considérer comme ensembles sont les ensembles de nombres. Des nombres, il y en a de différents types (nombres entiers, rationnels, réels…), et ils forment donc différents ensembles. Chaque type de nombre a une définition mathématique bien précise. Les constructions successives par « enrichissement » de ces différents types de nombres est passionnante, mais sort largement du cadre introductif de ce cours. Nous nous contenterons de définitions informelles et non rigoureuses des différents ensembles de nombres, ainsi que d'une connaissance « de travail » les concernant et qui a été acquise au fil des ans, par une utilisation régulière à l'école. Ces définitions sont suffisantes pour travailler avec les nombres sans arriver à des paradoxes.

43 DÉFINITION. On désigne par $\mathbb{N}$ l'ensemble des *nombres entiers naturels* (ou *entiers positifs*) $0, 1, 2, 3, \ldots$

On désigne par $\mathbb{Z}$ l'ensemble des *nombres entiers relatifs* $0, 1, -1, 2, -2, \ldots$

On désigne par $\mathbb{Q}$ l'ensemble des *nombre rationnels*, qui s'obtiennent à partir des entiers relatifs en ajoutant les fractions $\frac{m}{n}$ où $m, n \in \mathbb{Z}$ et $n \neq 0$. Ce sont les

nombres qui ont une écriture décimale finie ou périodique à partir d'un certain rang.

On désigne par $\mathbb{R}$ l'ensemble des nombres réels, qui ont une écriture décimale quelconque (éventuellement infinie).

On a donc

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Bien sûr, il existe d'autres ensembles de nombres, comme les nombres complexes, les nombres irrationnels (*i.e.*, les nombres réels qui ne sont pas rationnels) ou les nombres transcendants (*i.e.*, les nombres réels qui ne peuvent pas être obtenus comme racine d'un polynôme non nul à coefficients entiers).

3.3 *Ensembles définis par extension*

La manière la plus simple de définir un ensemble est d'en donner précisément ses éléments.

44 DÉFINITION. Un ensemble A est défini *par extension* si A est défini en donnant ses éléments. On écrit $\{a_1, \ldots, a_n\}$ l'ensemble constitué des éléments $a_1, \ldots, a_n$.

N'oubliez pas les symboles { et } lorsque vous définissez un ensemble par extension. Ils sont là pour indiquer que vous définissez un objet mathématique de type ensemble. Sans eux, il est impossible de distinguer un ensemble de la liste des éléments.

45 NOTATION. Un ensemble ne peut pas contenir plusieurs fois un élément donné. Par convention, on considère donc que $\{2, 2\}$ et $\{2\}$ sont les mêmes ensembles.

Des exemples d'ensembles définis par extension sont donnés par

$$\{1, 2\}, \quad \{\text{“Pierre”}, \text{“Papier”}, \text{“Ciseau”}\}, \quad \{\varnothing, \{\varnothing\}\}.$$

Le premier est un ensemble de nombres, le deuxième un ensemble de chaînes de caractères et le troisième est un ensemble d'ensembles.

Il y a une limitation majeure dans la technique de définition d'ensembles par extension : elle ne permet que de définir des ensembles qui ne contiennent qu'un nombre fini d'éléments [13].

Pour remédier à ce problème, nous allons introduire la technique de définition d'ensembles par *compréhension*. Pour cela, nous devons introduire le concept de *prédicat*.

3.4 *Logique des prédicats*

Nous allons introduire la notion de prédicat de manière informelle.

13. Définir un ensemble infini par extension prendrait beaucoup trop de temps car, comme le disait Woody Allen, l'infini c'est long, surtout vers la fin.

46 DÉFINITION. Un *prédicat à une variable x sur un ensemble* A est une assertion $P(x)$ dont la valeur de vérité dépend de l'interprétation de x par un éléments de A.

En quelque sorte, un prédicat sur A est une propriété qui peut être satisfaite par certains éléments de A mais pas d'autres.

47 EXEMPLE. Examinons quelques exemples de nature variée.

(1) L'assertion $P_0(x)$ définie sur $\mathbb{R}$ par

$$x \geq 2$$

est un prédicat sur $\mathbb{R}$. On a P(3) est vrai alors que P(1) est faux.

(2) L'assertion $P_1(x)$ définie sur $A := \{\{1\}, \{2, 1\}, \{3\}\}$ par

$$\{1\} \subseteq x$$

est un prédicat sur A. On a $P_1(\{1\})$ est vrai tandis que $P(\{3\})$ est faux.

(3) L'assertion $P_3(x)$ définie par

$$x \text{ est une ville de Luxembourg}$$

est un prédicat sur {Wiltz, Schifflange, Arlon}. On a que P_3 est vrai en Schifflange et Wiltz, mais est faux en Arlon.

La définition de prédicat s'étend naturellement à plusieurs variables. Par exemple

$$x \geq y$$

est un prédicat à deux variables x, y sur $\mathbb{R}$. De plus, elle va de pair avec la notion de *quantificateur* que nous introduisons maintenant.

48 DÉFINITION. Soit $P(x)$ un prédicat sur un ensemble A.

(1) L'assertion $\forall x P(x)$ (le symbole $\forall$ se lit *pour tout* est est appelé *quantificateur universel*) est définie comme l'assertion qui est vraie si et seulement si $P(a)$ est vraie pour tous les choix de a pour interpréter $P(x)$ dans A.

(2) L'assertion $\exists x P(x)$ (le symbole $\exists$ se lit *il existe* et est appelé *quantificateur universel*) est définie comme l'assertion qui est vraie si et seulement si il existe une interprétation a de x dans A telle que $P(a)$ est vraie.

L'occurrence de la variable x qui apparaît dans $\exists x P(x)$ ou dans $\forall x P(x)$ est qualifiée de *liée* (par le quantificateur). Dans une assertion avec quantificateur, une variable qui a au moins une occurrence non liée est qualifiée de *libre*.

49 EXEMPLE. (1) L'assertion $\exists x\ x \geq 2$ est vraie sur $\mathbb{R}$ mais l'assertion $\forall x\ x \geq 2$ ne l'est pas. En revanche l'assertion $\forall x\ x \geq 2$ est vrai sur $[2, +\infty[$.

(2) L'assertion $\exists n \exists k\ n = 2k$ est vraie sur $\mathbb{N}$, tout comme l'assertion $\exists n \forall k\ n = kn$ (pourquoi ?) Mais l'assertion $\exists n\ \forall kn = 2k$ est fausse sur $\mathbb{N}$.

(3) La variable y est libre dans $\forall x\ x \geq y$, tandis que x ne l'est pas. Ainsi, l'assertion $Q(y) := \forall x\ x \geq y$ devient elle même un prédicat (sa valeur de vérité va dépendre de la manière dont on interprète y).

50 NOTATION. Dans une assertion avec quantificateur, on s'autorise parfois à spécifier dans quel ensemble sont interprétées les variables qui apparaissent quantifiés. On écrit par exemple

$$\forall x \in \mathbb{Z}\ x^2 \geq 0$$

Cette notation n'est pas strictement conforme au langage de la logique des prédicats, mais on s'autorise cette petite liberté car on ne se sert pas du langage des prédicats comme d'un langage formel pur, mais comme un élément de la méta-langue qui nous permet de parler des mathématiques.

Étant donné un prédicat $P(x)$, on dispose de deux nouvelles assertions, à savoir $\exists x P(x)$ et $\forall x P(x)$. Quelles sont les négations de ces deux assertions ? Avant de donner la règle générale qui permet de les obtenir, considérons les deux exemples suivants.

(1) La négation de « À Belval, tous les chats sont gris » est « À Belval, il existe un chat qui n'est pas gris ». En effet, je veux vous prouver que la phrase « À Belval, tous les chats sont gris » est *fausse*, il faut et il suffit que je vous montre à Belval un chat qui n'est pas gris.

(2) La négation de la phrase « À l'uni.lu, tous les étudiants sont majeurs » est « À l'uni.lu, il existe un étudiant mineur ». En effet, si je veux vous prouver que la phrase « À l'uni.lu, tous les étudiants sont majeurs » esy fausse, il faut et il suffit que je trouve à l'uni.lu un étudiant mineur.

51 DÉFINITION. Soit $P(x)$ un prédicat sur un ensemble A.

(1) La négation de $\forall x P(x)$ est $\exists x \neg P(x)$.

(2) La négation de $\exists x P(x)$ est $\forall x \neg P(x)$.

52 EXEMPLE. La négation de

$$\forall x \left(x^2 \neq 0 \implies \exists y (y < 0 \wedge y^2 = x^2)\right)$$

est

$$\exists x \left(x^2 \neq 0 \wedge \forall y (y \geq 0 \vee y^2 \neq x^2)\right)$$

3.5 *Ensembles définis par compréhension*

En gros, définir un ensemble par compréhension consiste à constituer cet ensemble en sélectionnant des éléments dans un autre ensemble en suivant un critère spécifique donné. Définir B par compréhension [14], c'est donner un règle

14. La *compréhension* désigne en français la capacité de comprendre. Définir un ensemble par compréhension, c'est donc comprendre la manière dont sont sélectionnés les éléments de cet ensemble.

qui détermine quels sont les éléments qui « ont le droit et l'obligation » d'être dans B. Par exemple, vous pourriez créer un ensemble de nombres entiers en ne sélectionnant que les nombres pairs.

Sous quelle forme donner cette règle de sélection ? Sous la forme d'un prédicat ! Formalisons cette approche.

53 DÉFINITION (Définition d'un ensemble par compréhension). Soit A un ensemble et $P(x)$ un prédicat sur A. On désigne par

$$\{x \mid P(x)\}$$

et on lit *l'ensemble des x tels que* $P(x)$, l'ensemble constitué des éléments a de A tels que $P(a)$ es vrai.

54 EXEMPLE. (1) Considérons le prédicat $x \geq 2$ sur $\mathbb{R}$. Alors $\{x \mid x \geq 2\}$ est égal à l'interval $[2, +\infty[$.

(2) Considérons le prédicat binaire $n = 2k$ sur $\mathbb{N}$. Alors $\exists k\ n = 2k$ est une prédicat unaire sur $\mathbb{N}$ et $\{n \mid n = 2k\}$ est l'ensemble des nombres pairs.

(3) Considérons le prédicat $P(x)$ définit par *x est une ville du Luxembourg* sur l'ensemble {Wiltz, Luxembourg, Arlon}. Alors, l'ensemble $\{x \mid P(x)\}$ est égal à {Wiltz, Luxebourg}.

Un des grands avantages de la définition par compréhension est qu'on peut maintenant définir des ensembles infinis !

55 NOTATION. Si $P(x)$ est un prédicat sur un ensemble A, on écrit parfois $\{x \in A \mid P(x)\}$ au lieu de $\{x \mid P(x)\}$.

3.6 *Opérateurs ensemblistes*

Tout comme nous avons définis des opérateurs logiques pour connecter des assertions pour en créer de nouvelles, nous définissons des connecteurs ensemblistes pour créer de nouveaux ensembles en connectant des ensembles existants.

56 DÉFINITION. Soient A et B deux ensembles.

(1) L'*intersection de* A *et* B, notée $A \cap B$, est l'ensemble des éléments qui appartiennent à la fois à A et à B. Formellement,

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

(2) *L'union* de A et B, notée $A \cup B$, est l'ensemble des éléments qui appartiennent à l'un des ensembles A ou B (voire aux deux puisque nous n'utilisons pas le *ou* exclusif). Formellement,

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

Loi	**Nom**
$A \cap B = B \cap A$	Commutativité de l'intersection
$A \cup B = B \cup A$	Commutativité de l'union
$(A \cup B) \cup C = A \cup (B \cup C)$	Associativité de l'union
$(A \cap B) \cap C = A \cap (B \cap C)$	Associativité de l'intersection
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distribution de l'intersection sur l'union
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distribution de l'union sur l'intersection
$A \cup (A \cap B) = A$	Loi d'absorption
$A \cap (A \cup B) = A$	Loi d'absorption
$A \cup \varnothing = A$	$\varnothing$ est neutre pour $\cup$
$A \cap \varnothing = \varnothing$	$\varnothing$ est absorbant pour $\cap$

Si en plus $A \subseteq C$ et $B \subseteq C$,

Loi	**Nom**
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	Loi de De Morgan pour l'union
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	Loi de De Morgan pour l'intersection
$A = \overline{\overline{A}}$	Double négation)

FIGURE 8 – Identités de l'algèbre de Boole d'ensembles

(3) Si $A \subseteq B$, le *complémentaire de* A *dans* B, noté $B \setminus A$ ou $\overline{A}$, est l'ensemble des éléments de B qui ne sont pas dans A. Formellement,

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

57 EXEMPLE. Considérons les ensembles $A = \{1, 2, 3\}$, $B = \{3, 5, 7\}$ et $C = \{n \in \mathbb{N} \mid \exists k\ n = 2k + 1\}$. On a

$$A \cap B = \{3\} \quad \text{et} \quad A \cup B = \{1, 2, 3, 5, 7\}.$$

Par ailleurs, il vient

$$C \setminus B = \{n \in \mathbb{N} \mid \exists k(k \notin \{1, 2, 3\} \wedge n = 2k + 1)\}.$$

D'après la définition 56, l'intersection est une forme ensembliste du $\wedge$, l'union une forme du $\vee$ et le complémentaire une forme de négation. Grâce à cette correspondance, on montre facilement que chaque identité propositionnelle de la Fig. 5 a un équivalent au niveau des ensembles (on parle d'ailleurs d'*algèbres de Boole d'ensembles*).

58 PROPOSITION. *Les identités de la Fig. 8 sont vraies pour tous ensembles* A, B *et* C.

3.7 *Ensembles des parties*

On peut créer un nouvel ensemble en collectant les parties d'un ensemble donné.

59 DÉFINITION. Si A est un ensemble, on appelle *ensemble des parties de* A, et on note 2^A (ou $\mathcal{P}(A)$ l'ensemble des parties de A. C'est-à-dire

$$2^A := \{B \mid B \subseteq A\}.$$

60 PROPOSITION. *Pour tout ensemble* A, *on a* $A \in 2^A$ *et* $\varnothing \in 2^A$.

Démonstration. Simple application de la Proposition 42. □

61 EXEMPLE. . On a

$$2^{\varnothing} = \{\varnothing\}, \quad 2^{\{1\}} = \{\varnothing, \{1\}\}, \quad 2^{\{1,2\}} = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}.$$

Lorsque nous aborderons la notion de cardinalité, nous comprendrons pourquoi nous avons adopté la notation 2^A pour désigner l'ensemble des parties de A.

3.8 *Produits cartésiens d'ensembles*

62 DÉFINITION. Soient A et B deux ensembles. Le *produit cartésien* (ou simplement *produit*) de A et B, noté $A \times B$, est l'ensembles des couples (c'est-à-dire des listes ordonnées de deux éléments) (a, b) où $a \in A$ et $b \in B$. Autrement dit, on a

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

On généralise aisément la notion de produit cartésien à un nombre fini $n \geq 1$ d'ensembles en recourant à la notion de n-uplet, c'est-à-dire de liste ordonnée $(u_1, \dots u_n)$ de la manière suivante : si $A_1, \dots, A_n$ sont des ensembles, on définit

$$A_1 \times \cdots \times A_n := \{(a_1, \dots, a_n) \mid \forall i \leq n \; a_i \in A_i\}.$$

63 EXEMPLE. (1) Soient $A = \{1, 2\}$ et $B = \{a, b, c\}$. On a

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\},$$

$$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}.$$

En particulier le produit cartésien n'est pas commutatif (on a ici $A \times B \neq B \times A$).

(2) On a $\varnothing \times \mathbb{N} = \mathbb{N} \times \varnothing = \varnothing$.

(3) En géométrie, vous avez identifié le plan à $\mathbb{R} \times \mathbb{R}$

64 NOTATION. On écrit A^n pour $A \times A \times \cdots \times A$, où le facteur A apparaît n fois.

Notons que la notion de produit cartésien se généralise à un nombre infini

de facteurs en recourant à la notion de fonction. Cette généralisation sort du cadre de ce cours, mais sera considérée au semestre 2 au au semestre 3.

3.9 *Relations et applications*

Bien qu'elles ont l'air innocentes, les relations sont l'un des objets les plus présents en mathématiques.

65 DÉFINITION. Soient A et B deux ensembles. Une *relation de* A *dans* B est une partie du produit cartésien $A \times B$.

Autrement dit une relation de A dans B est un ensemble de couples $R \subseteq A \times B$. On parle aussi de *relation binaire*.

La notion de relation se généralise facilement à un nombre fini d'ensembles : une relation entre les ensembles $A_1, \ldots, A_n$ (où $n \geq 1$) est une partie de $A_1 \times \cdots \times A_n$. On parle de *relation n-aire sur* A (où $n \geq 1$) pour désigner une relation $R \subseteq A^n$.

66 EXEMPLE. (1) Désignons par A l'ensemble $\{1, 2, 3\}$ alors $\varnothing$, $\{(1, 1)\}$, $\{(1, 2), (2, 3)\}$ et A sont des exemples de relations binaires sur A.

(2) Si A est un ensemble quelconque, l'ensemble $\{(x, x) \mid x \in A\}$ est une relation binaire sur A, mieux connue sous le nom de *relation égalité* et sous le symbole $=$.

(3) La relation $\leq$ usuelle sur $\mathbb{N}$ est une relation binaire. On pourrait la définir par

$$\leq = \{(n, m) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N}\ m = n + k\}.$$

Bien sûr, on écrit $a \leq b$ plutôt que $(a, b) \in \leq$.

(4) Si $A := \{\text{Wiltz, Bous, Arlon, Paris}\}$ et $B := \{\text{FR, LU, BE, NL}\}$, on peut définir une relation R par

$$R := \{(x, y) \in A \times B \mid a \text{ est une ville de } b\}.$$

On peut donc décrire R en extension par

$$R = \{(\text{Wiltz, LU}), (\text{Bous, LU}), (\text{Arlon, BE})\}.$$

67 DÉFINITION. Soit $R \subseteq A \times B$ une relation de A dans B. On définit *le domaine* $\mathrm{dom}(R)$ *de* R par

$$\mathrm{dom}(R) := \{a \in A \mid \exists b \in B\ (a, b) \in R\}.$$

et *l'image* $\mathrm{im}(R)$ *de* R par

$$\mathrm{im}(R) := \{b \in B \mid \exists a \in A\ (a, b) \in R\}.$$

68 EXEMPLE. Si R désigne la relation définie dans l'Exemple 66 (4), alors on a

$$\mathrm{dom}(R) = \{\text{Wiltz, Arlon, Bous}\} \quad \text{et} \quad \mathrm{im}(R) = \{\text{LU, BE}\}.$$

Un des types de relations les plus importants est celui d'*application*.

69 DÉFINITION. Soient A et B deux ensembles. Une *application* (ou *fonction*) *de* A *dans* B est une relation f de A dans B telle que pour tout $a \in \mathrm{A}$, il existe exactement un $b \in \mathrm{B}$ tel que $(a, b) \in f$. Cet unique élément b est appelé *image de* a *par* f et est noté $f(a)$, et on écrit $b = f(a)$ au lieu de $(a, b) \in f$. On dit aussi que a *est l'antécédent de* b *par* f.

On écrit $f : \mathrm{A} \to \mathrm{B}$ pour indiquer que f est une fonction de A dans B.

Qu'a-t-on fait ? On a donné un sens mathématique rigoureux à l'idée intuitive de la notion de fonction de A dans B vue comme « *une loi qui à tout d'élément de* A *associe exactement un élément de* B ». Pour s'en convaincre, vous êtes invités à résoudre l'exercice suivant.

70 EXERCICE. Écrire la définition de *être une fonction de* A *dans* B en utilisant uniquement le langage de logique des prédicats.

Pour définir une fonction de A dans B, il suffit donc de spécifier une règle pour associer un et un seul élément de B à tout élément de A. Examinons quelques exemples.

71 EXEMPLE.

1. La relation f de $\mathbb{N}$ dans $\mathbb{N}$ définie par $(n, m) \in \mathbb{N} \iff m = n^2$ est une fonction de $\mathbb{N}$ dans $\mathbb{N}$. Pour tout $n \in \mathbb{N}$ on a $f(n) = n^2$. À l'avenir, pour définir cette fonction, on écrira
$$\text{Soit } f : \mathbb{N} \to \mathbb{N} \text{ la fonction définie par } f(n) = n^2.$$
2. La relation R définie dans l'Exemple 68 est en fait une fonction. On a par exemple
$$\mathrm{R}(\text{Wiltz}) = \mathrm{R}(\text{Bous}) = \text{LU} \quad \text{et} \quad \mathrm{R}(\text{Arlon}) = \text{BE}.$$
3. Pour tout ensemble A on définit la *fonction identité* id_A *sur* A par $\mathrm{id}_\mathrm{A}(a) = a$.

72 DÉFINITION. Soit $f : \mathrm{A} \to \mathrm{B}$. Si $\mathrm{C} \subseteq \mathrm{A}$, on définit l'*image de* C *(par* f*)* comme[15] le sous-ensemble de B
$$f(\mathrm{C}) := \{f(c) \mid c \in \mathrm{C}\}.$$

Si $\mathrm{D} \subseteq \mathrm{B}$ on définit la *pré-image* $f^{-1}(\mathrm{D})$ *(par* f*)* comme le sous-ensemble de A
$$f^{-1}(\mathrm{D}) := \{a \in \mathrm{A} \mid f(a) \in \mathrm{D}\}.$$

73 EXEMPLE. Soit $f : \mathbb{Z} \to \mathbb{Z}$ définie par $f(z) = z^2$. Si $\mathrm{C} := \{-2, 0, 2\}$ et $\mathrm{D} := \{-3, 0, 1, 4, 5\}$, on a $f(\mathrm{C}) = \{0, 2\}$ et $f^{-1}(\mathrm{D}) = \{0, 1, -1, 2, -2\}$.

74 PROPOSITION. *Soit* $f : \mathrm{A} \to \mathrm{B}$.

1. *Si* $\mathrm{C}, \mathrm{D} \subseteq \mathrm{A}$, *on a* $f(\mathrm{C} \cap \mathrm{D}) \subseteq f(\mathrm{C}) \cap f(\mathrm{D})$, *mais l'inclusion réciproque peut ne pas être vraie.*
2. *Si* $\mathrm{C}, \mathrm{D} \subseteq \mathrm{A}$, *on a* $f(\mathrm{C} \cup \mathrm{D}) = f(\mathrm{C}) \cup f(\mathrm{D})$.

15. On *surcharge* donc la terminologie « image », ce qui ne peut pas prêter à confusion.

3. *Si* C, D ⊆ B, *on a* $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$ *et* $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

Démonstration. Les preuves sont laissées à titre d'exercices, à réaliser durant les séances d'exercices. □

Remarquez que si $f : A \to B$ alors $\mathrm{dom}(f) = A$. Par contre il se peut que $\mathrm{im}(f) \neq B$ (mais on a toujours $\mathrm{im}(f) \subseteq B$), comme l'illustre l'Exemple 71 puisque $NL \notin \mathrm{im}(R)$. Les fonctions $f : A \to B$ telles que $\mathrm{im}(f) = B$ ont droit à leur propre qualificatif !

75 DÉFINITION. Soit $f : A \to B$. On dit que f est *surjective* si $\mathrm{im}(f) = B$, c'est-à-dire si

$$\forall b \in B \; \exists a \in A \; f(a) = b.$$

76 EXEMPLE. La fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$ n'est pas surjective car -2 est un élément de $\mathbb{R}$ qui n'a pas d'antécédent par f (c'est-à-dire que $-2 \in \mathbb{R} \setminus \mathrm{im}(f)$). Par contre la fonction $f' : \mathbb{R} \to [0, +\infty[$ définie[16] par $f'(x) = x^2$ est surjective car pour tout $y \in [0, +\infty[$, on a $f(\sqrt{y}) = y$.

Les fonctions $f : A \to B$ pour lesquelles ils n'existent pas d'éléments $a \neq a'$ de A tels que $f(a) = f(a')$ ont également droit à leur petit nom.

77 DÉFINITION. Une fonction $f : A \to B$ est *injective* si pour tous $a, a' \in A$, on a

$$a \neq a' \implies f(a) \neq f(a'). \tag{1}$$

On prenant la contraposée de (1), on obtient qu'une fonction $f : A \to B$ est injective si pour tous $a, a' \in A$, on a

$$f(a) = f(a') \implies a = a'.$$

Un moyen mnémotechnique pour retenir cette définition est

> *Une fonction est injective si des éléments distincts ont des images distinctes.*

78 DÉFINITION. Une fonction $f : A \to B$ est *bijective* si elle est injective et surjective.

Ainsi, si $f : A \to B$ est une fonction bijective, pour tout élément b de B il existe (par surjectivité) un unique (par injectivité) antécédent de b par f, c'est-à-dire un élément $a \in A$ tel que $f(a) = b$. La règle qui sélectionne pour tout $b \in B$ son unique antécédent peut servir à définir une fonction de B dans A.

79 DÉFINITION. Soit $f : A \to B$ une application bijective. On définit la *fonction*

16. Notez que les fonctions f et f' sont différentes car elles ne sont pas définies à partir des mêmes ensembles.

inverse (ou *réciproque*) de f comme la $f^{-1}\colon \mathrm{B} \to \mathrm{A}$ définie par

$$f^{-1}(b) = a \iff b = f(a).$$

80 REMARQUE. Attention ! Nous avons (comme il est d'usage) surchargé la notation f^{-1}. Cette notation peut désigner la réciproque d'une fonction bijective, ou être utilisée comme $f^{-1}(\mathrm{D})$ pour calculer la pré-image d'un ensemble. Cette surcharge ne peut et ne doit pas mener à confusion.

81 EXEMPLE. La fonction $f\colon [0,+\infty[\to [0,+\infty[$ définie par $f(x) = x^2$ est bijective. Sa fonction réciproque $f^{-1}\colon [0,+\infty[\to [0,+\infty[$ est définie par la règle

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

On a donc $f^{-1}(y) = \sqrt{y}$ pour tout $y \in [0,+\infty[$.

On peut définir de nouvelles fonctions à partir de fonctions existantes en utilisant l'opérateur de composition, défini ci-dessous.

82 DÉFINITION. Soient $f\colon \mathrm{A} \to \mathrm{B}$ et $g\colon \mathrm{B} \to \mathrm{C}$. On définit la *fonction composée* $g \circ f\colon \mathrm{A} \to \mathrm{C}$ par $(g \circ f)(a) := g(f(a))$ pour tout $a \in \mathrm{A}$.

83 EXEMPLE. On considère la fonction $f\colon \mathbb{R} \to [0,+\infty[$ définie par $f(x) = x^2$ et $g\colon [0,+\infty[\to [0,+\infty[$ définie par $g(y) = y + 1$. La fonction $g \circ f\colon \mathbb{R} \to]0,+\infty[$ est définie par $(g \circ f)(x) = x^2 + 1$.

84 PROPOSITION. *Soient $f\colon \mathrm{A} \to \mathrm{B}$, $g\colon \mathrm{B} \to \mathrm{C}$ et $h\colon \mathrm{C} \to \mathrm{D}$.*

1. *On a $h \circ (g \circ f) = (h \circ g) \circ f$ (*i.e., *la composition de fonction est associative)*
2. *On a $f \circ \mathrm{id}_\mathrm{A} = f$ et $\mathrm{id}_\mathrm{B} \circ f = f$.*
3. *Pour tout $\mathrm{E} \subseteq \mathrm{C}$, on a $(g \circ f)^{-1}(\mathrm{E}) = f^{-1}(g^{-1}(\mathrm{E}))$.*
4. *Si f est une bijection, alors f^{-1} l'est aussi.*
5. *Si f est une bijection, alors $f \circ f^{-1} = \mathrm{id}_\mathrm{B}$ et $f^{-1} \circ f = \mathrm{id}_\mathrm{A}$.*
6. *Si f et g sont injectives, alors $g \circ f$ l'est aussi.*
7. *Si f et g sont surjectives, alors $g \circ f$ l'est aussi.*

Démonstration. Les démonstrations sont laissées à titre d'exercices, à réaliser aux séance d'exercices. □

3.10 *Cardinaux*

La notion de *cardinal* a été inventée pour capturer la notion de « *taille* » d'un ensemble (en sens du nombre d'éléments dans le cas fini). Tout comme nous pouvons facilement calculer avec la taille (*i.e.*, le nombre d'éléments) des ensembles finis (comme faire des additions, de multiplications ...), il est possible de définir une arithmétique des cardinaux infinis. Nous n'introduirons pas cette arithmétique dans ce cours, et nous contenterons d'une définition pragmatique de la notion de cardinal (ou plus précisément de *dominance* entre ensembles).

85 DÉFINITION. On dit qu'un ensemble A *domine* un ensemble B ou que *le cardinal de* A *est plus grand que le cardinal de* B, et on nota $\#A \leq \#B$ s'il existe une application injective $f : A \to B$. On dit que A et B sont *équivalents* ou *ont même cardinal*, et on note $A \simeq B$, s'il existe une bijection $f : A \to B$. On écrit $\#A < \#B$ si $\#A \leq \#B$ et si $A \not\simeq B$.

Puisque la fonction réciproque d'une fonction bijective est aussi bijective, la relation $\simeq$ définie ci-dessus est symétrique (*i.e.*, on a $A \simeq B$ si $B \simeq A$). de plus, a par définition que si $A \simeq B$ alors $\#A \leq \#B$ et $\#B \leq \#A$. Par ailleurs, comme la composition de fonction injective est injective, on a que la relation de dominance est *transitive*, c'est-à-dire que si $\#A \leq \#B$ et $\#B \leq \#C$ alors $\#A \leq \#C$.

Le but de la notion de cardinal est de pouvoir comparer des ensembles du point de vue de leur taille, sans pour autant qu'ils soient inclus l'un dans l'autre. Il s'agit de généraliser la notion de *nombre d'éléments* à des ensembles qui n'ont pas nécessairement un nombre fini d'éléments.

86 EXEMPLE.
1. On $\varnothing \leq A$ pour tout ensemble A. En effet, la fonction $f = \varnothing$ est une fonction injective de $\varnothing$ dans A.
2. Si $n \leq m$ sont deux entiers naturels, alors $\#\{0, \dots, n\} \leq \#\{0, \dots, m\}$.
3. Si n est un entier naturel, on a
$$\#\{0, \dots, m\} \leq \#\mathbb{N} \leq \#\mathbb{Q} \leq \#\mathbb{R}.$$
4. On a $\#(\mathbb{N} \setminus \{0\}) \leq \#\mathbb{N}$ et $\#\mathbb{N} \leq \#(\mathbb{N} \setminus \{0\})$.
5. Si $2\mathbb{N} := \{2n \mid n \in \mathbb{N}\}$ alors $\#2\mathbb{N} \leq \#\mathbb{N}$ et $\mathbb{N} \leq \#2\mathbb{N}$.

Le résultat suivant est le premier théorème du cours.

87 THÉORÈME (Schröder - Bernstein). *Si* $\#A \leq \#B$ *et* $\#B \leq \#A$ *alors* $A \simeq B$.

Démonstration. Sans perte de généralité, supposons que A et B sont disjoints (sinon, on remplace par exemple A par un ensemble qui lui est équivalent mais disjoint de B). Soit $f : A \to B$ et $g : B \to A$ deux applications injectives, et construisons une bijection $h : A \to B$. Convenons de la terminologie suivante : pour tout $a \in A$ on dit que a est le parent de $f(a)$. De même, pour tout $b \in B$ on dit que b est le parent de $g(b)$. On dit que $z \in A \cup B$ est un *ancêtre* de $z' \in A \cup B$ si $z = z'$, ou si z est le parent d'un ancêtre de z'.

Pour tout élément z de $A \cup B$, nous avons trois cas mutuellement disjoints :

(1) il existe dans A un ancêtre de z sans parent,

(2) il existe dans B un ancêtre de z sans parent,

(3) tout ancêtre de z a un parent.

On décompose A en l'union $A_1 \cup A_2 \cup A_3$ de trois sous-ensembles deux à deux

disjoints correspondants au trois cas précédents :

$$A_A := \{a \in A \mid a \text{ a un ancêtre } a' \in A \text{ sans parent}\},$$

$$A_B := \{a \in A \mid a \text{ a un ancêtre } b' \in B \text{ sans parent}\},$$

$$A_\infty := \{a \in A \mid \text{ tous les ancêtres de } a \text{ ont un parent}\}.$$

On décompose B de la même manière en l'union de trois sous-ensembles B_A, B_B, B_∞ disjoints. On a alors

(1) La restriction f' de f à A_A est une bijection de A_A dans B_A. En effet, si $a \in A_A$ on a que a a un ancêtre $a' \in A$ sans parent. Donc $f'(a)$ a le même ancêtre $a' \in A$ sans parent. Donc $f' : A_A \to B_A$ est injective. Par ailleurs, si $b \in B_A$ alors il existe un ancêtre $a' \in A$ de b sans parent, c'est-à-dire que $b = f(a'')$ pour un $a'' \in A_A$.

(2) De la même manière, la restriction g' de g à B_B est une bijection de B_B dans A_B. Donc sa réciproque g'^{-1} est une bijection de A_B dans B_B.

(3) La restriction f'' de f à A_∞ est une bijection de A_∞ dans B_∞. En effet, on sait déjà que f'' est une injection. Par ailleurs, si $b \in B_\infty$, alors b a un parent $a \in A$ dont tous les ancêtres ont un parent, c'est-à-dire $b = f(a)$ pour un certain $a \in A_\infty$.

Au total la fonction h definie pas $h = f' \cup g'^{-1} \cup f''$, c'est-à-dire par

$$h(a) = \begin{cases} f'(a) & \text{si } a \in A_A \\ g'^{-1}(a) & \text{si } a \in A_B \\ f''(a) & \text{si } a \in A_\infty \end{cases}, \qquad a \in A,$$

est une bijection de A dans B. □

On peut paraphraser le Théorème de Schröder - Bernstein en disant

> Si le cardinal de A est plus grand que le cardinal de B et si le cardinal de B est plus grand que le cardinal de A, alors A et B ont même cardinal.

88 EXEMPLE. En appliquant le théorème de Schröder - Bernstein à l'Exemple 86, on obtient que $\mathbb{N} \simeq 2\mathbb{N} \simeq \mathbb{N} \setminus \{0\}$.

De plus nous allons démontrer l'assertion suivante.

> *Il y a autant de nombres entiers relatifs que de nombre entiers naturels.*

Cet énoncé informel se formalise de la manière suivante : $\mathbb{Z}$ *et* $\mathbb{N}$ *ont même cardinal.* Pour le prouver, nous pouvons appliquer le Théorème de Schröder - Bernstein. En effet, il est clair que la fonction inclusions $\iota : \mathbb{N} \to \mathbb{Z}$ définie par $\iota(n) = n$ est une injection. De la même manière, la fonction $f : \mathbb{Z} \to \mathbb{N}$ définie par

$$f(z) := \begin{cases} 2z & \text{if } z \geq 0 \\ 2|z| + 1 & \text{if } z < 0 \end{cases}$$

est une injection. On en déduit que $\mathbb{Z} \simeq \mathbb{N}$ par le Théorème de Schröder - Bernstein [17].

89 EXERCICE. Prouver que *si* $\#A \leq \#B$, $\#B \leq \#C$ *et qu'au moins un de ces relations de dominance est stricte, alors* $\#A < \#C$.

Solution. Il suffit que prouver que $\#C \not\leq \#A$. Supposons que $\#C \leq \#A$. Alors par transitivité de la relation de dominance, on a $\#C \leq \#B$. On total, on a $C \simeq B$ et $C \simeq A$, donc $A \simeq B$ et $B \simeq C$, ce qui contredit notre hypothèse. Nous avons prouver que $\#A < \#C$. □

90 DÉFINITION. (Axiome de l'infini) On dit qu'un ensemble A est *infini* si est seulement si $\mathbb{N} \leq \#A$. Un ensemble A est *dénombrable* [18] si $\#A \leq \#\mathbb{N}$. Il est *infini dénombrable* si $\#A = \#\mathbb{N}$. Un ensemble A qui n'est pas infini est qualifié de *fini*. Si A est un ensemble fini, on note (par abus de notation) #A le *nombre d'éléments de* A, c'est-à-dire l'unique nombre $n \in \mathbb{N}$ tel que $A \simeq \{1, \ldots, n\}$.

91 EXERCICE. *Prouver qu'un ensemble* A *est fini si et seulement si* $\#A < \#\mathbb{N}$. Tout d'abord, supposons que $A \neq \varnothing$ est un ensemble fini (c'est-à-dire non infini, *i.e.*, il n'existe pas d'application injective de $\mathbb{N}$ dans A). Alors, toute énumération de ses éléments $a_1, a_2, \ldots$ telle que $a_1 \in A$ et $a_{i+1} \in A'_i := A \setminus \{a_1, \ldots, a_i\}$ pour tout $i \geq 1$ s'arrête à une valeur n (qui est en fait le nombre d'éléments de A) tel que $A_n = \varnothing$, sinon cette énumération définirait une injection de $\mathbb{N}$ dans A (et A serait infini). L'énumération en question définit une injection (mais pas une surjection) de A dans $\mathbb{N}$, donc $\#A \leq \#\mathbb{N}$. On conclut que $\#A < \#\mathbb{N}$, sinon $A \simeq \mathbb{N}$ par le Théorème de Schröder - Bernstein, ce qui contredit la finitude de A.

Inversement, supposons que $\#A < \#N$. On a clairement que A n'est pas infini, sinon $\#N \leq \#A$ et par le théorème de Schröder - Bernstein on obtient $\#A \simeq \#N$, une contradiction.

Selon l'axiome de l'infini [19], l'ensemble $\mathbb{N}$ réalise le « plus petit infini. » On peut légitimement se demander s'il existe d'autres types d'infini, c'est-à-dire des ensembles infinis qui dominent strictement l'ensemble des entiers naturels. Nous allons donner réponse à cette question. La première étape est de prouver que l'ensemble des parties d'un ensemble domine strictement cet ensemble.

92 THÉORÈME. *Si* A *est un ensemble, alors* $\#A < \#\mathcal{P}(A)$.

Démonstration. La fonction $f : A \to \mathcal{P}(A)$ définie par $f(x) = \{x\}$ est une injection, ce qui prouve que $\#A \leq \#\mathcal{P}(A)$. Pour prouver que $\#A < \#\mathcal{P}(A)$ il suffit donc de prouver que $A \not\simeq \mathcal{P}(A)$, c'est-à-dire que $(A \simeq \mathcal{P}(A)) \implies \bot$. Nous tâchons donc de déduire une contradiction à partir de l'assertion $A \simeq \mathcal{P}(A)$. Supposons ainsi

17. On aurait aussi pu montrer que f est une bijection

18. En anglais, un ensemble est *denumerable* s'il est en bijection avec $\mathbb{N}$. Il est *countable* s'il est fini ou en bijection avec $\mathbb{N}$.

19. La version de l'axiome de l'infini présenté ici n'est pas la version originale, mais elle permet quelques raccourcis de raisonnement qui sont acceptés par la communauté mathématique qui ne s'intéressent pas aux détails des rouages de la théorie des ensemble.

qu'il existe une bijection $f : \mathrm{A} \to \mathcal{P}(\mathrm{A})$, et désignons par X l'ensembles

$$\mathrm{X} := \{a \in \mathrm{A} \mid a \notin f(a)\}.$$

Comme f est surjective et que $\mathrm{X} \in \mathcal{P}(\mathrm{A})$, il existe un $x \in \mathrm{A}$ tel que $\mathrm{X} = f(x)$. Deux cas sont possibles :

— soit $x \in \mathrm{X}$, c'est-à-dire $x \notin f(x) = \mathrm{X}$, ce qui est une contradiction $\bot$;
— soit $x \notin \mathrm{X} = f(x)$, c'est-à-dire $x \in \mathrm{X}$ par définition de X, ce qui est une contradiction $\bot$.

Dans les deux cas, on a déduit $\bot$ à partir de $\mathrm{A} \simeq \mathcal{P}(\mathrm{A})$, ce qui prouve $\mathrm{A} \not\simeq \mathcal{P}(\mathrm{A})$. □

En combinant le théorème précédent avec l'axiome de l'infini, on obtient donc qu'il y a au moins deux types d'infini (on dit que deux ensembles infinis ont le *même type* s'ils ont même cardinal) : l'infini de $\mathcal{P}(\mathbb{N})$ est différent de celui de $\mathbb{N}$. Mieux, on poursuivant la construction, on obtient une suite $\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}\big(\mathcal{P}(\mathbb{N})\big), \ldots$ d'ensembles infinis tous de type différent ! Quel vertige ! Auriez-vous cru qu'après seulement quelques cours, vous auriez accès à tour infinie d'infinis ?

La question se pose maintenant de comparer l'infini des nombres réels, avec celui des naturels. La théorème suivant, lui aussi dû à Cantor, affirme que $\mathbb{R}$ n'est pas dénombrable.

93 THÉORÈME. *On a $\#\mathbb{N} < \#\mathbb{R}$, c'est-à-dire que $\mathbb{R}$ est non-dénombrable.*

Démonstration. D'abord, la fonction $\imath : \mathbb{N} \to \mathbb{R}$ définie par $\imath(n) = n$ est une injection, ce qui prouve $\#\mathbb{N} \leq \#\mathbb{R}$. Démontrons que $\#\mathbb{N} < \#\mathbb{R}$ en prouvant que $\#\mathbb{R} \not\leq \#\mathbb{N}$. Supposons que $\#\mathrm{R} \leq \#\mathrm{N}$, en particulier que $\#[0,1[\leq \#\mathbb{N}$ donc que $[0,1[\simeq \mathbb{N}$. Considérons une énumération $r_1, r_2, \ldots$ de tous les éléments de $[0,1[$ (cela correspond à donner une bijection de $\mathbb{N}$ dans $[0,1[$) et pour tout $i \in \mathbb{N}$, désignons par

$$0, r_{i1} r_{i2} r_{i3} \ldots$$

une écriture décimale infinie de r_i (quitte à répéter une infinité de 0 à fin de l'écriture pour les nombres décimaux.)

On construit un nombre a de $[0,1[$ en en spécifiant une écriture décimale :

la i^e décimale d'une écriture de a est 8 si la i^e décimale r_{ii} de r_i est 9, et est 9 sinon.

Ainsi, a est un nombre de $[0,1[$ qui n'est pas dans $\{r_i \mid i \in \mathbb{N}_0\}$. En effet, a ne peut pas être égal à r_1 car a et r_1 n'ont pas la même première décimale [20], a ne peut pas être égal à r_2 car a et r_2 n'ont pas la même deuxième décimale...Nous avons construit un nombre de $[0,1[$ qui n'apparaît pas dans l'énumération r_1, r_2 des nombres de $[0,1[$ que nous avons choisie, une contradiction. On conclut que $\#[0,1[\not\leq \#\mathbb{N}$, donc que $\#\mathbb{R} \not\leq \#\mathbb{N}$. □

20. La non unicité de l'écriture décimale d'un nombre pourrait poser un problème dans cet argument. Cela n'est pas le cas, car a n'est pas un nombre décimal et possède donc une écriture décimale unique.

94 REMARQUE. L'argument qui nous as permis de construire l'élément a dans la preuve précédente est mondialement et historiquement connu sous le nom d'*argument diagonal de Cantor*. Le nom se réfère au fait qu'on a construit a en modifiant la i^e décimale de r_i, c'est à dire à partir de la diagonale du tableau suivant.

$$\begin{aligned} r_1 &= 0, \mathbf{r_{11}} r_{12} r_{13} r_{14} r_{15} \dots \\ r_2 &= 0, r_{21} \mathbf{r_{22}} r_{23} r_{24} r_{25} \dots \\ r_3 &= 0, r_{31} r_{32} \mathbf{r_{33}} r_{34} r_{35} \dots \\ \dots &= \dots \end{aligned}$$

À ce stade, une question naturelle se pose. Nous savons que $\mathcal{P}(\mathbb{N})$ domine strictement $\mathbb{N}$ et que $\mathbb{R}$ domine strictement $\mathbb{N}$. Est-ce que $\mathbb{R} \simeq \mathcal{P}(\mathbb{N})$, ou existe-t-il un type d'infini strictement entre les deux ? Il est en fait possible de démontrer (dans l'axiomatique de ZF de la théorie des ensembles avec l'axiome du bon ordre) que $\mathcal{P}(\mathbb{N}) \simeq \mathbb{R}$.

Une autre question se pose alors : existe-il un type d'infini strictement compris entre celui de $\mathbb{N}$ (l'infini dénombrable) et celui de $\mathbb{R}$ (qu'on a appelé l'*infini du continu*), c'est-à-dire un ensemble #A tel que $\#\mathrm{N} < \#\mathrm{A}\# < \mathbb{R}$? Cantor a énoncé cette assertion au XIXe siècle comme une conjecture, appelée *conjecture du continu* : il n'y a pas de cardinal strictement compris entre celui de $\mathbb{N}$ et celui de $\mathbb{R}$.

Ce n'est que bien des années plus tard, en 1963, que Paul Cohen démontra le résultat suivant :

> La conjecture du continu ne peut pas se démontrer dans l'axiomatique ZFC+AF (Zormelo - Fraenkel avec l'axiome du choix et l'axiome de fondation) de la théorie des ensembles.

Comme Kurt Gödel avait démontré en 1938 que la négation de cette conjecture n'est pas non plus démontrable dans ZFC, la conjecture du continu s'est révélée être un énoncé mathématique *indécidable* (ou *indépendant*) de la théorie axiomatique ZFC+AF : ZFC+AF ne peut pas prouver ni la conjecture du continu, ni sa négation. La conjecture du continu constitue donc une hypothèse supplémentaire qu'on peut faire le choix d'ajouter à l'axiomatique ZFC+AF, ou (c'est un ou exclusif ici) on peut faire le choix d'ajouter le négation. Un des résultat de Paul Cohen est de montrer qu'aucun de ces choix ne va créer de contraction dans la théorie des ensembles (sous la condition que celle-ci ne contient pas elle-même de contradiction).

Le dernier résultat de cette section concerne les ensembles dénombrables, qui jouent un rôle particulier dans la formation d'un·e mathématicien·ne. Nous généralisons d'abord la notion d'union et à un « nombe infini » d'ensembles.

95 DÉFINITION. Soit X et I deux ensembles. Une *famille* $\{\mathrm{A}_i \mid i \in \mathrm{I}\}$ *de sous-ensembles de* X (également notée $(\mathrm{A}_i)_{i\in\mathrm{I}}$, ou $\{\mathrm{A}_i\}_{i\in\mathrm{I}}$ ou $\{\mathrm{A}_i\}$ si l'ensemble I est clair par le contexte) est une fonction $f : \mathrm{I} \to \mathcal{P}(\mathrm{X})$ telle que $f(i) = \mathrm{A}_i$ pour tout $i \in \mathrm{I}$.

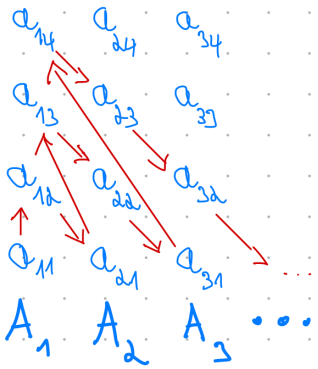


FIGURE 9 – Argument Zig - Zag

Définir une famille de sous-ensembles A_i de X est juste une manière de se donner un ensemble de parties de X qui peut avoir une cardinalité arbitraire. Si X est clair par le contexte, on parlera de familles d'ensembles $\{A_i\}$.

96 DÉFINITION. Soit $\{A_i \mid i \in I\}$ une famille de sous-ensembles de X. L'*intersection de* $\{A_i \mid i \in I\}$, noté $\bigcap\{A_i \mid i \in I\}$ ou $\bigcap_{i\in I} A_i$, est le sous-ensemble de X défini par

$$\bigcap\nolimits_{i\in I} A_i := \{x \in X \mid \forall i \in I \; x \in A_i\}.$$

L'*union de* $\{A_i \mid i \in I\}$, noté $\bigcup\{A_i \mid i \in I\}$ ou $\bigcup_{i\in I} A_i$, est le sous-ensemble de X défini par

$$\bigcup\nolimits_{i\in I} A_i := \{x \in X \mid \exists i \in I \; x \in A_i\}.$$

97 EXERCICE. *Montrer que si* $\{A_i \mid i \in I\}$ *est une famille de sous-ensembles d'un ensemble dénombrable* X *alors* $\bigcap_{i\in I} A_i$ *est dénombrable.*

98 THÉORÈME (AC). *Si* $\{A_i \mid i \in \mathbb{N}\}$ *est une famille dénombrables de sous-ensembles dénombrables* A_i *d'un ensemble* X *alors* $\bigcup_{i\in I} A_i$ *est dénombrable.*

Démonstration. Pour tout $i \in \mathbb{N}$, on considère une énumération $a_{i1}, a_{i2}, \ldots$ des éléments de A_i. Alors, le liste suivante est une énumération des éléments de $\bigcup_{i\in I} A_i$ (voir aussi la Fig. 9) :

$$a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, a_{14}, a_{23}, a_{32}, a_{41} \ldots.$$

La fonction qui à chaque élément a de $\bigcup_{i\in I} A_i$ associe sa position dans l'énumération précédente est une injection de $\bigcup_{i\in I} A_i$ dans $\mathbb{N}$ □

L'énoncé de ce théorème peut se retenir de la manière suivante :

Toute union dénombrable d'ensembles dénombrables est dénombrable.

Nous avons mentionné (AC) en préalable à l'énoncé du Théorème 98. Cela signifie que pour se théorème, nous devons supposer un axiome appelé l'*axiome du choix*. Tout comme l'hypothèse du continu, il s'agit d'un indécidable de la théorie des ensembles : il n'es pas prouvable dans la théorie des ensembles

et sa négation non plus. On peut donc soit supposer l'axiome du choix, soit sa négation (mais pas les deux) sans introduire de contradiction. La grande majorité des mathématiciens et mathématiciennes travaille en supposant l'axiome du choix. De nombreux théorèmes importants (comme l'existence d'une base dans les espaces vectoriels de dimension finie) sont en fait équivalent à l'axiome du choix, ou à une de ses formes faibles. Une formulation de l'axiome du choix est la suivante :

Si $\{A_i \mid i \in I\}$ est une famille d'ensembles, alors il existe une fonction f définie sur I telle que $f(i) \in A_i$ pour tout $i \in I$.

4 TECHNIQUES DE DÉMONSTRATION

Qu'est-ce qu'une preuve ? Il en existe de nombreux types qui dépendent du contexte dans lequel elles sont utilisées : preuve formelle en mathématiques, preuve d'identité en informatique, preuve judiciaire, preuve à divulgation nulle de connaissance… Dans tous les cas, *prouver* c'est convaincre. Il s'agit en effet de convaincre son interlocuteur de l'exactitude d'une information, ou de sa véracité.

Évidement, nous allons uniquement nous concentrer sur les preuves en mathématiques. Là encore, il en existe de nombreux types. On distingue d'abord les preuves formelles dans des systèmes de déduction axiomatique (comme celui de la théorie des ensembles, mais il en existe aussi pour LPC, pour la logique du premier ordre ou pour d'autres systèmes de fondation comme la théorie des types qui revient sur le devant de la scène ces dernières années).

Ces preuves formelles sont très importantes car elle peuvent être vérifiées par un ordinateur. Mais nous sommes loin des preuves qui constituent l'activité journalière du/de la mathématicien·ne type, et qui sont au cœur de cette section.

Si on se réfère à Wikipedia [21],

> une *preuve* ou *démonstration* est un ensemble structuré d'étapes correctes de raisonnement.

Cette définition informelle (et elle ne peut que rester informelle dès lors qu'on sort du cadre de la notion de preuve dans des systèmes axiomatiques) cache bien des réalités. Il y a de nombreuses techniques de preuves (nous en verrons les plus courantes), mais même en appliquant la même technique pour prouver la même assertion, des auteur·rice·s différent·e·s arriveront bien souvent à des expositions de preuves différentes, en fonction de leur expérience et de leur public cible. On ne présente pas une preuve de la même manière à un·e mathémticien·ne aguerri·e et à un·e élève de lycée.

Dans tous les cas, *prouver* est la compétence majeure du/de la mathématicien·ne. Une telle compétence, cela se travaille ! Lorsque vous rédigerez une preuve, vous n'y arriverez pas du premier coup. Il faudra d'abord tâtonner, écrire des bouts de raisonnement, tout effacer, restructurer et finalement exposer votre preuve dans votre meilleure prose mathématique. Le démonstration est l'écrin de la solution à l'énigme mathématiques que vous résolvez, et constitue un des meilleurs arguments de vente dans la communauté mathématique.

Qu'est-ce qui distingue une *bonne preuve* d'une *mauvaise preuve* [22] ? Il y a sans doute autant de réponses à cette question qu'il n'y a de mathématicien·ne·s. Néanmoins, tous et toutes s'accordent à dire qu'une bonne preuve est

- rigoureuse (le raisonnement est valide et complet ; si l'auteur applique un théorème dans la preuve, il en vérifie les hypothèses),
- bien structurée (elle met en avant les étapes importantes de la démonstration ; identifie les hypothèses et les thèses, et les techniques utilisées),
- claire (elle ne laisse pas de place à l'interprétation ou au doute),

21. https ://fr.wikipedia.org/wiki/Démonstration_(logique_et_mathématiques) consulté le 25 juillet 2023 à 22 :00 UTC+2.

22. https ://youtu.be/QuGcoOJKXT8 ?t=180

— détaillée (elle ne laisse pas au lecteur un trop grand travail de vérification des assertions prouvées sans démonstration ; le niveau de détails dépend évidement du public visé),
— concise (elle ne présente pas d'arguments inutiles, hors sujets ou redondants),
— et bien-sûr… correcte !

La critère de concision semble être en opposition avec celui du détail ! C'est vrai, et une bonne preuve réalise un équilibre entre les deux. Pour simplifier, un·e mathématicien·ne essaye d'économiser les mots, sans sacrifier à la clarté et à la rigueur.

4.1 *Preuve directe*

Bien souvent, nous avons à démontrer une assertion du type *Si* A *alors* B, c'est à dire $A \Rightarrow B$ où A et B sont des assertions quelconques. La technique la plus élémentaire, c'est de montrer que cette implication est vrai en recourant à la table de connecteur de $\Rightarrow$.

Pour une *preuve directe*,

> *sous l'hypothèse que* A *est une assertion vraie, on prouve que l'assertion* B *est aussi vraie.*

Donnons un exemple de preuve directe.

99 EXEMPLE. *Si n est un entier pair alors n^2 est pair.*

Démonstration. Prouvons cette assertion par preuve directe. Supposons que n est un entier pair. Alors, il existe par définition un entier k tel que $n = 2k$. On a donc successivement

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2),$$

où la deuxième égalité est vraie pour commutativité de la multiplication dans $\mathbb{Z}$ et la dernière égalité s'obtient par associativité de la multiplication. □

100 REMARQUE. Dans cette preuve, nous avons justifié les égalités par des propriétés élémentaires de la multiplication. Quand bien même nous n'aurions pas écrit ces justifications, vous auriez accepté la démonstration comme valide, car vous manipulez ces propriétés avec aisance. Par contre, un jeune élève de l'enseignement secondaire aurait peut-être bien eu besoin des justifications pour suivre le raisonnement. L'exemple illustre bien que la manière d'*exposer* une preuve dépend du public cible auquel elle va être présentée, même si sa validité mathématique en est indépendante.

4.2 *Preuve par contraposition*

Nous avons vu qu'une implication $A \Rightarrow B$ est équivalente à sa contraposée $\neg B \Rightarrow \neg A$. Pour prouver un énoncé du type

> Si A alors B,

il est donc équivalent de prouver

> Si ¬B alors ¬A.

On dit qu'on procède par *contraposition*, ou bien que l'on prouve *la contraposée*. Cela peut paraître étonnant, mais parfois prouver la contraposée s'avère plus facile que prouver l'énoncé original. Donnons un exemple.

101 EXEMPLE. *Soit q un nombre réel positif. Si q est irrationnel alors $\sqrt{q}$ est irrationnel.*

Démonstration. Procédons par contraposition et supposons que q est un nombre réel positif tel que $\sqrt{q}$ est rationnel. Nous devons en déduire que q est rationnel. Par hypothèse, il existe $m, n \in \mathbb{Z}$ tels que $n \neq 0$ et $\sqrt{q} = m/n$. En élevant cette identité au carré, on en déduit que $q = m^2/n^2$. Nous avons écrit q comme le quotient de deux nombres entiers, ce qui prouve que q est rationnel. On conclut la preuve par le principe de contraposition. □

102 REMARQUE. Dans la preuve précédente, nous avons écrit

> Il existe $m, n \in \mathbb{Z}$ tels que $n \neq 0$ et $\sqrt{q} = m/n$. En élevant cette identité au carré, on en déduit que $q = m^2/n^2$

Cette assertion signifie en langage symbolique

$$\exists m, n \in \mathbb{Z}\Big((n \neq 0 \wedge \sqrt{q} = m/n) \Rightarrow q = m^2/n^2\Big).$$

C'est-à-dire que « on en déduit » se traduit par une implication $\Rightarrow$ et pas par une équivalence $\Leftrightarrow$. C'est une remarque importante car l'équivalence est fausse dans notre cas [23]. *La terminologie utilisée pour structurer la preuve est donc d'une importance capitale, puisqu'une erreur peut invalider la démonstration.*

4.3 *Preuve d'une équivalence*

Pour prouver une équivalence entre deux assertions, rien de plus simple (en tout cas du point de vue de la structure de la preuve). En effet, rappelons que l'assertion $\varphi \Leftrightarrow \psi$ est en fait une abréviation de $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$. Prouver $\varphi \Leftrightarrow \psi$ est donc équivalent à prouver les deux assertions $(\varphi \Rightarrow \psi)$, $(\psi \Rightarrow \varphi)$.

103 EXEMPLE. *Pour tout entier $z \in \mathbb{Z}$, on a z est impair si et seulement si z^2 est impair*

Démonstration. (Nécessité) Supposons que z est impair et déduisons-en que z^2 est impair. Nous savons qu'il existe $k \in \mathbb{Z}$ tel que $z = 2k + 1$. En élevant au carré et en développant, on obtient

$$z^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k + 2) + 1.$$

Ainsi, $z^2 - 1 = 2(2k + 2)$ est un multiple de 2, c'est-à-dire que z^2 est impair.

23. Pourquoi ? Et comment aurait-on pu reformuler l'assertion pour avoir une équivalence ?

(Suffisance) Supposons que z^2 est impair et déduisons-en que z est impair. Il suffit de prouver la contraposée, à savoir que si z est un entier pair alors z^2 est une entier pair. Cette preuve a été faite dans l'Exemple 99. □

104 REMARQUE. L'assertion à démontrer dans l'exemple précédent prenait la forme $\varphi \Leftrightarrow \psi$ où φ est l'assertion *z est impair* et ψ l'assertion z^2 *est impair*. Dans la première partie de la preuve intitulée « Nécessité », nous avons démontrer que l'assertion $\varphi \Rightarrow \psi$ est vraie, et dans la deuxième partie de la preuve intitulée « Suffisance », nous avons démontrer que l'assertion $\psi \Rightarrow \varphi$ est vraie. Bien que d'un point de vue logique l'expression $\varphi \Leftrightarrow \psi$ est symétrique, lorsque nous structurons une preuve de cette équivalence, nous considérons donc une asymétrie (parfaitement justifiée par le fait que la *syntaxe* $\varphi \Leftrightarrow \psi$, elle, n'est pas symétrique). En effet, φ est considérée comme assertion « de référence » par rapport à laquelle on compare ψ : dans la première partie ψ est qualifiée de condition *nécessaire* (sous-entendu *à* φ) et dans la deuxième, de condition *suffisante* (sous-entendu à φ).

Au lieu du terme « Néssecité », on peut utiliser une terminologie alternative, comme l'une des suivantes

($\Longrightarrow$)

Prouvons l'implication de gauche à droite [...]

Prouvons que φ *implique* ψ *[...]*

Similairement, au lieu du terme « suffisance », on peut utiliser une terminologie alternative, comme l'une des suivantes

($\Longleftarrow$)

Prouvons l'implication de droite à gauche [...]

Prouvons que ψ *implique* φ *[...] Prouvons la réciproque [...]*

Parfois, il est aussi simple de démontrer l'équivalence $\varphi \iff \psi$ en prouvant les deux implications $\varphi \Rightarrow \psi$ et $\psi \Rightarrow \psi$ *en même temps*, c'est-à-dire par une suite d'équivalence [24]. Donnons un exemple.

105 EXEMPLE. Soit $x \in \mathbb{R}$. On a $\sqrt{(x-1)^2 + (y-3)^2} = 0$ si et seulement si ($x = 1$ et $y = 3$).

24. On utilise implicitement pour cela la transitivité de l'implication, à savoir le fait que l'assertion $(\varphi \Rightarrow \psi) \Rightarrow ((\psi \Rightarrow \rho) \Rightarrow (\varphi \Rightarrow \rho))$ est une tautologie (bien connue des enfants au travers de la chanson *Biquette* .)

Démonstration. On obtient les équivalences successives suivantes.

$$\sqrt{(x-1)^2+(y-3)^2}=0 \iff (x-1)^2+(y-3)^2=0 \tag{2}$$

$$\iff (x-1)^2=0 \wedge (y-3)^2=0 \tag{3}$$

$$\iff (x-1)=0 \wedge (y-3)=0 \tag{4}$$

$$\iff x=1 \wedge y=3, \tag{5}$$

où (2) et (4) sont obtenus parce qu'un nombre réel est nul si et seulement si son carré est nul, et (3) parce que la somme de deux nombres positifs est nul si et seulement si ils sont tous les deux nuls. □

Parfois, on est amené à prouver que plusieurs assertions sont mutuellement équivalentes, comme dans l'exemple suivant. Dans ce cas, on peut à nouveau se servir de la transitivité de l'implication et se compter de prouver un cycle d'implication qui contient toutes les assertions.

106 EXEMPLE. *Pour tout nombre réel x, les conditions suivants sont équivalentes.*

(i) $\sqrt{x^2}=x$.

(ii) $|x|=x$.

(iii) $x\geq 0$.

Démonstration. (i) $\Longrightarrow$ (iii) Par définition, pour un nombre positif y, le nombre $\sqrt{y}$ est l'unique nombre positif donc le carré vaut y. Ainsi, si $\sqrt{x^2}=x$ alors x est positif.

(iii) $\Longrightarrow$ (ii) Par définition, on a

$$|x|=\begin{cases} x & \text{si } x\geq 0 \\ -x & \text{si } x<0. \end{cases}$$

En particulier, si $x\geq 0$ alors $|x|=x$.

(ii) $\Longrightarrow$ (i) On a toujours $\sqrt{y^2}=|y|$. Donc si $|x|=x$, on a $\sqrt{x^2}=|x|=x$.

Au total on a prouvé (i) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i), donc toutes ces conditions sont équivalentes. □

4.4 *Preuves par cas*

Parfois, la preuve directe d'une implication $\varphi \Longrightarrow \psi$ ne se fait pas en une seule suite d'implications, mais on sépare la preuve en différents cas mutuellement exclusifs, comme dans l'exemple ci-dessous.

107 EXEMPLE. *Si $n\in\mathbb{N}$ alors $1+(-1)^n(2n-1)$ est un multiple de 4.*

Démonstration. Si $n\in\mathbb{N}$ alors soit n est pair, soit n est impair, mais pas les deux.

Cas 1. *Supposons que n est pair*. Il existe $k \in \mathbb{Z}$ tel que $n = 2k$. Il vient successivement

$$1 + (-1)^n(2n-1) = 1 + (-1)^{2k}(4k) - 1 = 1 + 4k - 1 = 4k,$$

qui est un multiple de 4.
Cas 2. *Supposons que n est impair*. Il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. Il vient successivement

$$1 + (-1)^n(2n-1) = 1 + (-1)^{2k+1}(2(2k+1) - 1) = 1 - (4k + 2 - 1) = -4k,$$

qui est un multiple de 4.

Les deux cas prouvent que $1 + (-1)^n(2n-1)$ est toujours un multiple de 4. □

108 REMARQUE. Dans une preuve par cas, il faut bien faire attention à couvrir tous les cas possibles, sous peine de produire une preuve invalide. Les cas ne doivent pas nécessairement être exclusifs, mais leur disjonction doit couvrir la situation la plus générale.

4.5 *Preuve de la négation*

Nous avons déjà remarqué que la négation $\neg$A d'une assertion A est équivalente à $A \Rightarrow \bot$. Pour prouver que $\neg$A esr vrai, il est donc équivalent de prouver

Si A est vrai alors on en déduit une contradiction.

Donnons un exemple célèbre, connu depuis l'antiquité.

109 EXEMPLE. $\sqrt{2}$ n'est pas rationnel.

Démonstration. Prouvons que $(\sqrt{2} \in \mathbb{Q}) \Rightarrow \bot$. Supposons que $\sqrt{2} \in \mathbb{Q}$, c'est-à-dire qu'il existe deux entiers positifs m et n qui n'ont pas de diviseur commun, tels que $n \neq 0$ et $\sqrt{2} = m/n$. On obtient successivement

$$\sqrt{2} = m/n \Leftrightarrow 2 = m^2/n^2 \tag{6}$$

$$\Leftrightarrow 2n^2 = m^2 \tag{7}$$

$$\Rightarrow m^2 \text{ est pair} \tag{8}$$

$$\Rightarrow m \text{ est pair .} \tag{9}$$

Il existe donc $k \in \mathbb{N}$ tel que $m = 2k$. L'identité (7) est donc équivalence à $2n^2 = 4k^2$, c'est-à-dire à $n^2 = 2k^2$. On en déduit que n^2 est pair, donc n l'est aussi. On a obtenu que m et n sont des multiples de deux, ce qui contredit le fait que m et n n'ont pas de diviseur commun. Nous avons prouvé que $\sqrt{2} \notin \mathbb{Q}$. □

110 REMARQUE.
1. Pour obtenir (8), nous avons à nouveau élever l'identité $\sqrt{2} = m/n$ au carré. Nous obtenons cette fois une équivalence (par opposition à une implication dans la preuve précédente) car nous avons supposé que m et n étaient positifs.

2. La relation (8) n'est qu'une implication, et nous l'avons identifié comme tel (la réciproque est fausse).
3. En revanche, on peut montrer (exercice) que la réciproque de ((9)) est vraie. Comme la réciproque ne nous sert pas à la preuve, nous ne l'avons pas indiqué comme tel, ce qui nous permet d'en économiser la preuve.

4.6 *Preuve par contradiction*

Le principe de *preuve pas contradiction* (ou de *preuve par l'absurde*) s'énonce comme ceci :

> Si φ n'est pas faux, alors φ est vrai.

Sa validité est ancrée dans le principe du tiers-exclu $\varphi \vee \neg\varphi$. Formellement, il s'énonce donc comme

$$\neg\neg\phi \Rightarrow \phi,$$

ou encore

$$(\neg\phi \Rightarrow \bot) \implies \phi,$$

qui est équivalent au tiers-exclu $\phi \vee \neg\phi$. Pour l'utiliser pour démontrer une assertion ϕ, on procède donc en deux étapes.

(1) On suppose $\neg\phi$ et on en déduit une contradiction $\bot$. C'est-à-dire qu'on a démontré $\neg\phi \Rightarrow \bot$, à savoir $\neg\neg\phi$

(2) Par le principe de contradiction $\neg\neg\phi \Rightarrow \phi$, on en déduit ϕ.

Donnons un exemple archétypal, connu depuis l'antiquité grecque (depuis Euclide, pour être plus précis). Rappelons qu'un entier naturel $n > 1$ est qualifié de *nombre premier* s'il n'est divisible que par 1 et par n. Pour le moment, nous acceptons sans preuve le résultat suivant (nous le prouverons plus tard, dans la section relative aux relations d'ordre)

111 LEMME. *Tout entier naturel $n > 1$ qui n'est pas premier est divisible par un nombre premier*[25].

C'est sous la forme de sa contraposée *si $n > 1$ est un naturel qui n'est divisble par aucun nombre premier p différent de n alors n est premier* que nous allons utiliser le lemme précédent.

112 THÉORÈME. *Il existe une infinité de nombres premiers.*

Démonstration. Procédons par contradiction. Supposons que l'ensemble A des nombres premiers soient fini, et que $p_1, p_2, \ldots, p_\ell$ soit une liste de tous les éléments de A (on a donc $\ell \geq 2$). Définissons le nombre $p \in \mathbb{N}$ comme

$$p := p_1 p_2 \cdots p_\ell + 1.$$

25. C'est-à-die que pour tout naturel $n > 1$ qui n'est pas premier, il existe un nombre premier $p \neq n$ qui divise n.

Comme $\ell \geq 2$, on sait que $p > \max\{p_i \mid i \leq \ell\} > 1$. De plus, on sait que $p - 1$ est un multiple de p_i pour tout $i \leq \ell$, donc p n'est pas un multiple de p_i. Ainsi, $p > 1$ qui n'est pas premier (puisqu'il est différent de $p_1, \ldots, p_\ell$) mais qui n'est pas divisible par un nombre premier. C'est en contradiction avec le Lemme 111. Par le principe de contradition, on conclut que l'ensemble des nombres premiers A est infini. □

Preuve de la négation et principe de contradiction

En y regardant bien, une preuve de $\neg\varphi$ qui consiste en ceci :

Supposons φ *et déduisons une contradiction* $\bot$

ressemble fort au début d'un preuve par contradiction de φ :

Supposons $\neg\varphi$ *et déduisons une contradiction* $\bot$.

Évidement, ce n'est qu'une ressemblance : d'un côté on veut prouver $\neg\varphi$ et de l'autre on veut prouver φ. Mais la différence est beaucoup plus profonde. En effet, en procédant à la preuve de $\neg\varphi$, on procède par une preuve directe de $\neg\phi$ *qui est indépendant de la règle du tiers-exclus* $\psi \vee \neg\psi$. Tandis que le principe de contradiction est *équivalent au tiers-exclus.*

Or, la règle du tiers-exclu est d'un statut particulier : elle permet d'affirmer que φ est vrai simplement parce que $\neg\varphi$ n'est pas vrai, donc sans avoir *obtenu une preuve directe de* φ. Les résultats mathématiques qu'on peut obtenir *sans utiliser le tiers-exclus* (donc sans le principe de contradiction qui lui est équivalent) sont appelés *constructifs*, et on parle de *mathématiques constructives*.

Il y a des résultats mathématiques fondamentaux qu'il est *impossible d'obtenir de manière constructive*, comme l'existence d'une base dans les espaces vectoriels de dimension infinie. Plus généralement, tous les résultats qui dépendent de l'*Axiome du choix* sont non constructifs (l'axiome du choix est en fait *équivalent* au tiers-exclus). Dans votre *cursus*, vous découvrirez le *Prime Ideal Theorem*, le Théorème de Tychonoff (tout produit d'espaces compacts est compacts), le Théorème de Hahn - Banach qui dépendent tous de l'Axiome du choix.

Pourquoi faire une telle distinction entre *mathématiques constructives* et *mathématiques non-constructives*? Acceptons d'utiliser le tiers-exclus (c'est ce qu'on va faire) et oublions tout cela. C'est vrai, mais gardons dans le coin de notre tête que le tiers-exclus, via son équivalent l'axiome du choix, permet aussi d'énoncer des résultats contre-intuitifs comme le « pardoxe » de Banach - Tarski : *il est possible de découper une boule de l'espace usuel* $\mathbb{R}^3$ *en un nombre fini de morceaux et de réassembler ces morceaux pour former deux boules identiques à la première, à un déplacement près.*[a] La clé pour déjouer le paradoxe apparent est que les morceaux en questions sont *non mesurables*.

a. Source : `https://fr.wikipedia.org/wiki/Paradoxe_de_Banach-Tarski` consultée le 31 juillet 2023 à 15 :15 UTC+2.

4.7 *Preuves par induction*

Supposons avoir une suite d'assertions $\varphi_0, \varphi_1, \ldots \varphi_n, \ldots$ de nature « similaires », comme par exemple la suite $(\varphi_n)_{n\in\mathbb{N}}$ dont le n^e terme est l'assertion

$$\sum_{i=0}^{n} i = n(n+1)/2.$$

La technique de *preuve par induction* ou *par récurrence* consiste en ceci :

> Pour prouver que toutes les assertions $\varphi_0, \varphi_1, \ldots$ sont vraies, il suffit
>
> (1) De prouver que φ_0 est vrai.
>
> (2) De prouver que si pour un n donné l'assertion φ_n est vraie, alors l'assertion φ_{n+1} est vraie.

En effet, par (1) on sait que ϕ_0 est vrai. Par (2) appliqué avec $n = 0$, on sait que S_1 est vrai. Par (2) appliqué avec $n = 1$, on sait que S_2 est vrai...Ainsi, le principe d'induction (qui peut être formellement défini en théorie des ensembles) permet d'obtenir une infinité (dénombrable) de résultats en en prouvant un nombre fini.

Dans une preuve par récurrence, on appelle l'étape (1) le *cas de base* et l'étape (2) *l'étape de récurrence*. Dans cette étape, l'hypothèse φ_n sous laquelle on travaille s'appelle *hypothèse de récurrence*, que nous noterons (HR).

Donnons en tout de suite un exemple.

113 PROPOSITION. *Pour tout entier naturel n on a*

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Démonstration. Pour tout $n \geq 0$ désignons par φ_n l'assertion $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. Prouvons par récurrence que pour tout $n \geq 0$ l'assertion φ_n est vraie.

Prouvons le cas de base φ_0. D'une part on a $\sum_{i=0}^{0} i = 0$, d'autre par $0(0+1)/2 = 0$, ce qui prouve φ_0.

Démontrons maintenant l'étape de récurrence, et supposons (HR) que $n \geq 0$ est un naturel pour lequel φ_n est vrai, à savoir

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \tag{HR}$$

Prouvons que φ_{n+1} est vrai, à savoir

$$\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}.$$

Il vient successivement

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) \tag{10}$$

$$= \frac{n(n+1)}{2} + (n+1) \tag{11}$$

$$= \frac{(n+1)(n+2)}{2}, \tag{12}$$

où (11) est obtenu en appliquant l'hypothèse d'induction (HR), et (11) par mise en évidence de $(n+1)$ et addition des fractions. Nous avons bien obtenu (HR). On conclut la preuve par le principe d'induction. □

114 REMARQUE.
1. Dans une preuve par récurrence, prouver le cas de base est *indispensable*. Il sert de socle au raisonnement. Il est possible d'énoncer des suites $\varphi_0, \varphi_1 \ldots$ d'assertions pour lesquelles on peut prouver l'étape de récurrence *mais pas le cas de base*. Pour ces assertions, le principe d'induction ne s'applique pas.
2. Si vous arrivez à prouver l'étape d'induction *sans faire appel à l'hypothèse d'induction*, c'est que vous avez fait une erreur. Arrêtez-vous et éliminez la.
3. Parfois, la suite d'assertions que l'on souhaite prouver commence à $n = 1$ et est tu type $\varphi_1, \varphi_2 \ldots$. Dans ce cas, le cas de base est φ_1, et l'étape de récurrence consiste à supposer que φ_n est vrai pour un certain $n \geq 1$ et à en déduire φ_{n+1}. De même, cette suite commence parfois à $n = 2$ ou ...
4. Il existe une version plus forte du principe de récurrence, qui consiste à prouver l'étape de récurrence de la manière suivante :

   Supposons que pour un $n \geq 0$, les assertions $\varphi_0, \varphi_1 \ldots, \varphi_n$ sont vraies et déduisons-en φ_{n+1}.

Donnons encore un très intéressant exemple d'application du principe d'induction : les tours de Hanoï.

115 EXEMPLE (Tours de Hanoï). Considérons le célèbre casse-tête des *Tours de Hanoï*, inventé par le mathématicien Édouard Lucas à la fin du XIXe siècle. Un nombre $n \geq 1$ de disques de taille strictement décroissante (du haut vers le bas) sont placés sur une tour. Vous devez déplacez ces disques pour former une nouvelle tour finale, en utilisant une tour auxiliaire et en respectant les règles suivantes (voir aussi la Fig. 10) :

1. vous ne pouvez déplacer qu'un disque à la fois ;
2. vous ne pouvez pas placer un disque sur un disque plus petit que lui.

Quel est le nombre minimum de déplacements de disques à effectuer pour déplacer la tour ?

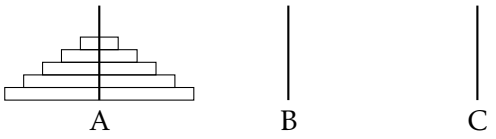


FIGURE 10 – Tours de Hanoï

n	H_n
0	0
1	1
2	3
3	7
4	15
...	...

FIGURE 11 – Valeurs des premiers termes de $(H_n)_{n\in\mathbb{N}}$

Solution. Définissons un algorithme récursif[26] Han(n, A, C, B) pour déplacer la tour de $n \geq 0$ disques de l'emplacement A à l'emplacement C (dans la Fig. 10) en utilisant l'emplacement auxiliaire B :

Si $n = 0$, ne rien faire ; sinon

1. déplacer les $n-1$ premiers disques de l'emplacement A à l'emplacement B en utilisant l'algorithme Han($n-1$, A, B, C) ;
2. déplacer le disque de taille n de la tour A à la tour C ;
3. déplacer les $n-1$ disques de l'emplacement B à l'emplacement C en utilisant l'algorithme Han($n-1$, B, C, A).

Désignons par $(H_n)_{n\in\mathbb{N}}$ la suite dont le n^e terme est le nombre de déplacements de disques effectués par Han(n, A, C, B). Nous allons en fait prouver l'assertion suivante :

> *Pour tout $n \geq 0$ on a $H_n = 2^n - 1$ mouvements. De plus, l'algorithme* Han(n, A, C, B) *est optimal, dans le sens où il n'existe pas d'autres algorithme qui déplacerait les n disques en m mouvements avec $m < n$.*

Tout d'abord, prouvons l'identité

$$H_n = 2^n - 1, \qquad n \geq 0, \tag{13}$$

par récurrence sur n. Nous avons déjà démontré le cas de base, à savoir que $H_0 = 0$. Passons à l'étape de récurrence et supposons (HR) que $H_n = 2^n - 1$ pour un $n \geq 0$ donné. Prouvons sous l'hypothèse (HR) que

$$H_{n+1} = 2^{n+1} - 1. \tag{14}$$

26. Un *algorithme récursif* est un algorithme qui résout un problème en calculant des solutions d'instances plus petites du même problème. Source : https://fr.wikipedia.org/wiki/Algorithme_r%C3%A9cursif consulté le 1 août 2023 à 10 :32

En appliquant la définition de l'algorithme, on constate que

$$H_{n+1} = H_n + 1 + H_n$$

car il faut H_n mouvements pour réaliser l'étape 1 de l'algorithme, de même pour l'étape 3 et un seul mouvement pour l'étape 2. On appliquant l'hypothèse de récurrence (HR) on a donc

$$H_{n+1} = 2H_n + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 1,$$

et on obtenu l'identité (14). On conclut que l'assertion (13) tient par le principe d'induction.

Prouvons maintenant que l'algorithme Han(n, A, C, B) est optimal, en procédant pas récurrence sur n. Le cas de base $n = 0$ est trivial : l'algorithme Han(n, A, C, B) déplace 0 disque en 0 mouvement, c'est optimal.

Supposons maintenant (HR) que l'algorithme déplace de manière optimale une tour de n disques pour une valeur de n fixée, et prouvons que Han($n+1$, A, C, B) déplace $n+1$ disques de manière optimale, c'est-à-dire que tout autre algorithme déplacerait les disques en H_{n+1} mouvements *au moins*. En effet, cet autre algorithme doit d'abord déplacer les n premiers disques de A à B, ce qui utiliser au moins H_n mouvements (on utilise ici l'hypothèse de récurrence). Ensuite il doit déplacer le plus grand disque en 1 mouvement, puis à nouveau les n disques de la tour B à la tour C en au moins H_n mouvements (par HR,à nouveau). Au total, cet autre algorithme effectue au moins $2H_n + 1 = H_{n+1}$ mouvements.

On conclut que l'algorithme Han(n, A, C, B) est optimal pour tout $n \geq 0$ par le principe d'induction. □

L'exemple suivant illustre qu'un brin d'étourderie peut être désastreux dans une preuve par récurrence (comme dans toute preuve, d'ailleurs).

116 EXEMPLE. Voici une tentative de preuve de l'assertion *Dans ton groupe de n personnes (pour $n \geq 1$), tous les individues ont la même couleur d'yeux.*

Pour conclure cette section, notons qu'il est également d'usage courant en mathématiques de *définir* une suite (A_n) d'objets mathématiques (ensembles, nombres, espaces, structures…) par récurrence. L'idée est de définir le premier terme A_0 de la suite, et de donner une règle de construction du $(n+1)^e$ terme à partir du *ne* terme (ou des termes A_0 à A_n). L'avantage est de pouvoir utiliser cette définition par récurrence pour prouver, par récurrence, des assertions à propos de cette suite.

117 EXEMPLE. Définissons une suite d'ensembles $(A_n)_{n\in\mathbb{N}}$ par récurrence par

$$A_n = \begin{cases} \varnothing & \text{si } n = 0, \\ \mathcal{P}(A_{n-1}) & \text{si } n \geq 1. \end{cases}$$

Démontrer par récurrence (exercice) que pour tout $n \geq 0$ on a $\#A^n = 2^n$

118 EXERCICE (Factorielle). On définit la fonction *factorielle* $\cdot!\colon \mathbb{N} \to \mathbb{N}$ par induction en suivant les règle suivantes :

$$n! := \begin{cases} 1 & \text{si } n = 0 \\ n \times (n-1)! & \text{si } n \geq 1. \end{cases}$$

Prouver par récurrence sur $n \geq 0$ que $n!$ est égal au produit de n premiers entiers naturels.

4.8 *Contre-exemple et preuve de la négation*

Quand ils sont exprimés dans le langage naturel (en anglais, français…) les énoncés mathématiques prennent souvent la forme

Si $\varphi(x_1, \ldots, x_\ell)$ alors $\psi(x_1, \ldots, x_\ell)$,

où $\varphi(x_1, \ldots, x_\ell)$ et $\psi(x_1, \ldots, x_\ell)$ sont des assertions à plusieurs variables (qui peuvent être de type différent : nombres, fonctions…). Une telle assertion est en fait une traduction en langage naturel de l'assertion

$$\forall x_1, \ldots, x_\ell \ (\varphi(x_1, \ldots, x_\ell) \Rightarrow \psi(x_1, \ldots, x_\ell)).$$

Cela signifie que si nous souhaitons montrer que l'assertion est fausse, nous devons prouver

$$\exists x_1, \ldots, x_\ell \ \varphi(x_1, \ldots, x_\ell) \wedge \neg\psi(x_1, \ldots, x_\ell).$$

Il s'agit donc de trouver un *contre-exemple* (ou *contre-modèle*, c'est-à-dire une interprétation des variables $x_1, \ldots, x_\ell$ telle que $\varphi(x_1, \ldots, x_\ell)$ est vrai mais $\psi(x_1, \ldots, x_\ell)$ est faux.

119 EXEMPLE. Démontrez que l'assertion

Si A_1 *et* A_2 *sont des ensembles alors* $\#(A_1 \cup A_2) = \#A_1 \cup \#A_2$.

est fausse.

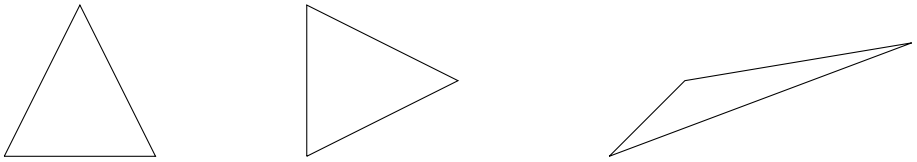
Solution. Nous en donnons un contre-exemple. Si A_1 désigne l'ensemble $\{1, 2\}$ et A_2 désigne l'ensemble $\{2, 3\}$ alors $\#(A_1 \cup A_2) = 3$ alors que $\#A_1 \cup \#A_2 = 4$. □

Pour s'entraîner

Produire des preuves est le cœur de métier du mathématicien et de la mathématicienne. Pour s'entraîner ou en découvrir d'avantage, les lecteur·rice·s peuvent se référer à [3]

5 ÉQUIVALENCE

Imaginons que vous étudiez la géométrie dans le plan, et que vous vous intéressiez aux triangles. Voici trois triangles dans le plan



Il s'agit là de trois triangles différents (en tant qu'ensemble de points du plan). Néanmoins, face à ces triangles, un enfant vous dira que les deux premiers sont identiques, mais que le troisième est différent des autres. On peut en effet superposer les deux premiers triangles parfaitement, mais pas avec le troisième.

Pour capturer cette notion de triangles « identiques », les mathématicien·ne·s ont introduit la notion d'isométrie, que vous avez découverte dans l'enseignement secondaire. Les deux premiers triangles sont isométriques, mais ne sont pas égaux. Dans le géométrie du triangle, ce n'est pas la notion d'égalité qui est pertinente pour comparer les triangles, mais le notion d'isométrie. Nous ne sommes pas intéressés à distinguer des triangles qui sont isométriques car ils ont les mêmes propriétés géométriques : ils sont équivalents du point de vue de la géométrie.

Une telle identification est monnaie courante en mathématique. On pourrait même grossièrement résumer l'activité mathématique à la classification des « motifs » à une forme d'équivalence prêt.

Dans cette section, nous donnons un sens mathématique à la notion d'équivalence, et à celle de quotient qui va de pair.

120 DÉFINITION. Une relation binaire R sur un ensemble X est une *équivalence* (ou une *relation d'équivalence*) si

- elle est *réflexive*, c'est-à-dire $x\mathrm{R}x$ pour tout $x \in \mathrm{X}$;
- elle est *symétrique*, c'est-à-dire pour tous $x, y \in \mathrm{X}$ si $x\mathrm{R}y$ alors $y\mathrm{R}x$;
- elle est *transitive*, c'est-à-dire pour tous $x, y, z \in \mathrm{X}$, si $x\mathrm{R}y$ et $y\mathrm{R}z$ alors $x\mathrm{R}z$.

121 EXEMPLE.

1. Les relations $\Delta := \{(x, x) \mid x \in \mathrm{X}\}$ (à savoir la relation égalité) et $\nabla := \mathrm{X} \times \mathrm{X}$ sont des équivalences sur l'ensemble X. Si R est une équivalence sur X alors on a $\Delta \subseteq \mathrm{R} \subseteq \nabla$.
2. La relation d'isométrie sur les triangles du plan est une relation d'équivalence.
3. Si $n \geq 2$ est un entier, la relation $\cdot \equiv \cdot \bmod n$ définie par $x \equiv y \bmod n$ si $(x - y)$ est un multiple de n est une équivalence sur $\mathbb{Z}$. On l'appelle *équivalence modulo n* et elle fera l'objet d'une section ultérieure.
4. La relation « être le même animal »est une relation d'équivalence sur l'ensemble

   $$\mathrm{X} := \{\text{Pluto, Petit Papa Noël, Snoopy, Bill, Garfield, Félix, Tom, Jerry, Mickey}\}.$$

5. Soit $f : \mathrm{X} \to \mathrm{Y}$ une application. La relation $\ker(f)$, définie par

   $$(x, y) \in \ker(f) \qquad \Longleftrightarrow \qquad f(x) = f(y)$$

est une équivalence sur X, appelée *noyau de* f. La vérification est laissée à titre d'exercices.

122 EXERCICE. Est-ce que les assertions suivantes sont vraies ou fausses ? Justifier

1. Si R_1 et R_2 sont deux équivalences sur un ensemble X, alors $R_1 \cap R_2$ l'est aussi.
2. Si R_1 et R_2 sont deux équivalences sur un ensemble X, alors $R_1 \cup R_2$ l'est aussi.

Une relation d'équivalence sert à classer les objets : on crée des classes d'objets équivalents. Cette construction est détaillée dans le définition suivante.

123 DÉFINITION. Si R est une équivalence sur X et si $x \in X$, la *classe de* x (*pour* R), notée x/R (ou $[x]_R$) est le sous-ensemble de X défini par

$$x/R := \{y \in X \mid xRy\}.$$

On dit que x est un *représentant* de x/R.

Le *quotient de* X *par* R est l'ensemble X/R des classes des éléments de X, à savoir

$$X/R := \{x/R \mid x \in X\}$$

124 EXEMPLE. Pour tout élément x d'un ensemble X, on a

$$x/\Delta = \{x\} \qquad \text{et} \qquad x/\nabla = X.$$

La classe de 2 pour l'équivalence modulo 2 est l'ensemble des nombres x tels que $x \equiv 2 \mod 2$, à savoir $\{0, 2, -2, 4, -4, \ldots\}$, c'est-à-dire les nombres pairs. Similairement, la classe de 3 pour cette équivalence est l'ensemble des nombre impairs.

La classe de Pluto pour l'équivalence definie dans l'Exemple 121 (4) est [27]

$$\{\text{Pluto, Petit Papa Noël, Snoopy, Bill}\}.$$

La preuve du résultat suivant est laissée à titre d'exercice.

125 LEMME. *Soit* R *une équivalence sur* X.

1. *Pour tous* $x, y \in X$ *on a* xRy *si et seulement si* $x/R = y/R$.
2. *Pour tous* $x, y \in X$ *on a* $x/R \cap y/R \neq \varnothing \implies x/R = y/R$.
3. *On a* $X = \bigcup_{x \in X} x/R$.

L'assertion (2) du Lemme précédent indique que pour une équivalence donnée, deux classes d'équivalences différentes (en tant qu'ensembles) sont disjointes. L'assertion (3) indique que X est l'union des classes d'équivalence. La combinaison de ces deux propriétés donne lieu à la notion de *partition*.

27. Rappelons que Petit Papa Noël est les chien dans la série animée *Les Simpsons*.

126 DÉFINITION. Une famille $(A_i)_{i\in I}$ de sous-ensembles de X est une *partition* de X si

1. pour tous $i \neq j$ dans I on a $A_i \cap A_j = \varnothing$,
2. on a $\bigcup\{A_i \mid i \in I\} = X$.

Le Lemme 125 indique en particulier que le quotient X/R d'un ensemble X par une équivalence R est une partition de X. Mais est-ce que toute partition de X peut s'obtenir comme le quotient de X par une relation d'équivalence ? Le résultat suivant donne une réponse positive.

127 PROPOSITION. *Soit* $\mathcal{A} := \{X_i \mid i \in I\}$ *une partition d'un ensemble* X. *La relation* $R_{\mathcal{A}}$ *définie sur* X *par*

$$x R_{\mathcal{A}} y \qquad ssi \qquad \exists i \in I\ \{x, y\} \subseteq A_i$$

est une équivalence sur X.

Démonstration. Prouvons d'abord que $R_{\mathcal{A}}$ est réflexif. Soit $x \in X$. Par la condition 2 de la Définition 126, il existe $i \in I$ tel que $x \in A_i$. Donc $\{x\} \subseteq A_i$ et $x R_{\mathcal{A}} x$.

Ensuite, comme la condition $\{x, y\} \subseteq A_i$ est symétrique en x et y, la relation $R_{\mathcal{A}}$ est clairement symétrique.

Prouvons enfin qu'elle est transitive. Soient $x, y, z \in X$ tels que $y R_{\mathcal{A}} y$ et $y R_{\mathcal{A}} z$. Alors, il existe $i, j \in I$ tels que

$$\{x, y\} \in A_i \qquad \wedge \qquad \{y, z\} \in A_j.$$

En particulier $A_i \cap A_j \neq \varnothing$, donc $i = j$ par la condition 1 de la Définition 126. Au final $\{x, z\} \subseteq A_i$, ce qui prouve que $x R_{\mathcal{A}} y$. □

Le résultat suivant indique qu'il n'y a pas de différence entre une équivalence R et l'équivalence $R_{X/R}$ associée à son quotient définie dans la Proposition 123. Inversement, il n'y a pas de différence entre une partition $\mathcal{A}$ et le quotient $X/R_{\mathcal{A}}$.

128 PROPOSITION. *Soit* X *un ensemble.*

1. *Si* R *est une équivalence sur* X *alors* $R = R_{X/R}$.
2. *Si* $\mathcal{A}$ *est une partition de* X *alors* $\mathcal{A} = X/R_{\mathcal{A}}$.

Démonstration. 1. Pour tous $x, y \in R$ on a les équivalences suivantes

$$x R y \iff x/R = y/R \iff x R_{X/R} y,$$

ce qui prouve que $R = R_{X/R}$.

2. Prouvons d'abord que $\mathcal{A} \subseteq X/R_{\mathcal{A}}$. Soit $A \in \mathcal{A}$, et $a \in A$. On a $A = a/R_{\mathcal{A}}$. Prouvons ensuite l'inclusion réciproque $X/R_{\mathcal{A}} \subseteq \mathcal{A}$. Considérons un élément $x/R_{\mathcal{A}}$ de $X/R_{\mathcal{A}}$. Par définition d'une partition, il existe $A \in \mathcal{A}$ tel que $x \in A$. On a alors $x/R_{\mathcal{A}} = A$ par définition de $R_{\mathcal{A}}$. □

129 DÉFINITION. Soit R une équivalence sur un ensemble X. L'application $\pi_R : X \to X/R$ définie par

$$\pi_R(x) = x/R$$

est appelée *application de passage au quotient*.

130 NOTATION. Si aucune confusion n'est possible, nous noterons par π l'application π_R.

131 EXERCICE. Soit R une équivalence sur un ensemble X. Démontrer les assertions suivantes.

1. L'application π_R est surjective.
2. L'application π_R est injective si et seulement si $\pi_R = \Delta$.
3. On a $R = \ker(\pi_R)$.

6 RELATIONS D'ORDRE

Après les relations d'équivalence, nous introduisons les relations d'ordre, qui sont un autre type de relation qu'on rencontre fréquemment en mathématiques.

132 DÉFINITION. Une relation binaire $\leq$ sur un ensemble X est un *ordre* (ou une *relation d'ordre*) si

— elle est *réflexive*, c'est-à-dire $x \leq x$ pour tout $x \in X$;
— elle est *antisymétrique*, c'est-à-dire pour tous $x, y \in X$ si $x \leq y$ et $y \leq x$ alors $x = y$;
— elle est *transitive*, c'est-à-dire pour tous $x, y, z \in X$, si $x \leq y$ et $y \leq z$ alors $x \leq z$.

On dit que (X, R) est un *ensemble ordonné* (ou un *ensemble partiellement ordonné*).

133 NOTATION. Si cela ne prête pas à confusion, on a l'habitude de noter $\leq$ n'importe quelle relation d'ordre, quelle que soit sa définition ou l'ensemble sur lequel elle est définie.

134 EXEMPLE.

1. La relation d'ordre usuelle sur $\mathbb{N}$ (ou celle sur $\mathbb{Z}$ ou sur $\mathbb{R}$) est une relation d'ordre au sens de la définition précédente.
2. Si X est un ensemble, alors la relation d'inclusion $\subseteq$ est une relation d'ordre sur $\mathcal{P}(X)$.
3. La relation | définie sur l'ensemble des diviseurs positifs de 12 par $a|b$ si b est un multiple de a est une relation d'ordre. Cet exemple se généralise facilement à l'ensemble des diviseurs d'un entier non nul, voir à l'ensemble des naturels.
4. La relation $\leq$ définie sur l'ensemble des assertions composées à trois variables par $\varphi(x_1, x_2, x_3) \leq \psi(x_1, x_2, x_3)$ si $\varphi \Rightarrow \psi$ est une tautologie est une relation d'ordre.

135 DÉFINITION. Deux éléments x, y d'un ensemble ordonnée $(X, \leq)$ sont *incomparables*, et on note $x \parallel y$, si $x \not\leq y$ et $y \not\leq x$. On dit que $\leq$ est *total* ou que $(X, \leq)$ est un *ensemble totalement ordonnée* si aucune paire d'éléments de X est incomparable.

136 EXEMPLE. 1. $(\mathbb{N}, \leq)$ est totalement ordonné.

2. Dans $\mathcal{P}(\{0, 1\})$, on a $\{0\} \parallel \{1\}$.

137 EXERCICE. Donner une condition nécessaire et suffisante sur $n \in \mathbb{N}$ pour que l'ensemble des diviseurs positifs de n ordonné par la relation | définie dans l'Exemple 134 (3) soit totalement ordonné.

6.1 *Diagramme de Hasse*

Il est commode de représenter les ensembles ordonnés par un diagramme.

138 DÉFINITION. Un *diagramme de Hasse* d'un ensemble ordonné (X, R) est construit dans le plan (orienté) en respectant les règles suivantes.

1. Si $x \leq y$ alors x est représenté par un point sous y,
2. Si $x \leq y$ alors on relie le point qui représente x au point qui représente y par un segment de droite, sauf si l'inégalité $x \leq y$ peut être déduite par transitivité à partir d'autres inégalités (c'est-à-dire, s'il existe $z \in X$ tel que $x < z < y$.

139 EXEMPLE. Donner des diagrammes de Hass des ensembles ordonnés définis dans l'Exemple 134.

6.2 *Minorant, majorant, bornes et treillis*

140 DÉFINITION. Soit $Y \subseteq X$ une partie d'un ensemble ordonné (X, R). Un élément z de X est un *majorant* de Y si $z \geq y$ pour tout y de Y. Si z est un majorant de Y et si $z \leq z'$ pour tout majorant z' de Y, alors z est *une borne supérieure de* Y.

De même, un élément z de X est un *minorant* de Y si $z \leq y$ pour tout y de Y. Si z est un minorant de Y et si $z \geq z'$ pour tout minorant z' de Y, alors z est une *borne inférieure de* Y.

141 PROPOSITION. *Soient* (X, R) *un ensemble ordonné et* Y *une partie de* X.

1. *Si* Y *admet une borne supérieure, alors elle est unique.*
2. *Si* Y *admet une borne inférieure, alors elle est unique.*

Démonstration. 1. Si z et z' sont deux bornes supérieures de Y, alors $z \leq z'$ car z est une borne supérieur de Y et z' est un majorant de Y. De même, on a $z' \leq z$ car z' est une borne supérieur de Y et z est un majorant de Y. Donc $z = z'$.

2. La preuve est similaire et laissée à titre d'exercice. □

142 NOTATION. L'unicité de la borne supérieure et de la borne inférieure d'une partie Y de $(X, \leq)$ (si ces bornes existent) nous permet d'introduire une notation

pour les désigner. On désigne par sup Y ou $\bigvee$ Y la borne supérieure de Y. On désigne par inf Y ou $\bigwedge$ Y la borne inférieure de Y.

143 EXERCICE. Dans chacun des cas suivants, donner un exemple d'ensemble ordonné (par exemple en donnant son diagramme de Hasse) qui satisfait à la condition indiquée.

1. Un ensemble ordonné dans lequel toute partie admet une borne supérieur et une borne inférieure.
2. Un ensemble ordonné dans lequel il existe une partie qui admet une borne supérieure mais pas de borne inférieure.
3. Un ensemble ordonné dans lequel il existe une partie qui admet une borne inférieure mais pas de borne supérieure.
4. Un ensemble ordonné dans lequel il existe une partie qui n'admet ni un borne inférieure, ni une borne supérieur.

En complément de la notion de borne supérieure et de borne inférieure, on trouve la notion de *maximum* et *minimum*.

144 DÉFINITION. Un élément M d'une partie X d'un ensemble ordonné $(Y, \leq)$ est qualifié de *maximum* de X, et on note $M = \max X$ si pour tout z dans X on a $x \geq z$.

De même, un élément m de X est qualifié de *minimum* de X, et on note $m = \min X$ si pour tout z dans X on a $z \geq x$.

Le maximum de X, si il existe, est donc égal au plus grand élément de X.

145 PROPOSITION. *Soit* X *une partie d'un ensemble ordonné* $(Y, \leq)$.

1. *Si* X *admet un maximum* M *alors* $M = \sup X$.
2. *Si* X *admet un minimum* m *alors* $m = \inf X$.
3. *S'il existe, le maximum de* X *est unique. S'il existe, le minimum de* X *est unique.*

Démonstration. 1. Nous avons par définition

$$M \in X \wedge \forall x \in X \; x \leq M.$$

On sait donc déjà que M est un majorant de X. Considérons un majorant M′ de X. On a donc $x \leq M'$ pour tout $x \in X$. Comme $M \in X$ on a donc $M \leq M'$. Nous avons prouvé que M est le plus petit des majorants de X, à savoir $M = \sup X$.

2. se prouve similairement.

3. Découle de 1. et 2. et de la Proposition 141. □

146 LEMME. *Soit* Y *une partie d'un ensemble ordonné* $(X, \leq)$ *qui admet une borne supérieure. Pour tout* $x \in X$, *on a* x *est un majorant de* Y *si et seulement si* $x \geq \bigvee Y$.

147 DÉFINITION. Un ensemble ordonné $(X, \leq)$ tel que X admet une borne supérieure et une borne inférieure est qualifié de *borné*.

Un *treillis* est un ensemble ordonnée $(X, \leq)$ dans lequel toute paire $\{a, b\}$ d'éléments admet une borne supérieure et une borne inférieure (forcément uniques). On écrit $a \vee b$ au lieu de $\sup\{a, b\}$, et $a \wedge b$ au lieu de $\inf\{a, b\}$.

Un *treillis complet* est un treillis dans lequel toute partie Y admet une borne supérieure $\bigvee Y$ et une borne inférieur $\bigwedge Y$.

Voici une caractérisation alternative des treillis complets.

148 PROPOSITION. *Soit* $(X, \leq)$ *un ensemble ordonné. Les conditions suivantes sont équivalentes.*

(i) $(X, \leq)$ *est un treillis complet.*

(ii) Tout sous-ensemble Y *de* X *a une borne supérieure* $\bigvee Y$

Démonstration. (i) $\implies$ (ii) est trivial par définition de la notion de treillis complet.

(ii) $\implies$ (i) Soit Y une partie de X. On désigne par A l'ensemble des minorants de Y (cet ensemble peut être vide, mais $\bigvee A$ existe par (ii)). Nous prouvons

(a) $\bigvee A$ est un minorant de Y.

(b) Si x est un minorant de Y alors $x \leq \bigvee A$.

Pour (a), on obtient par définition de A que

$$\forall z \in A \; \forall y \in Y \; z \leq y$$

c'est-à-dire

$$\forall y \in Y \; \forall z \in A \; z \leq y$$

ou encore, tout élément de Y est un majorant de A. Donc

$$\forall y \in Y \; y \geq \bigvee A,$$

c'est-à-dire que $\bigvee A$ est un minorant de Y.

On obtient (b) en notant que si x est un minorant de Y alors $x \in A$, donc $x \leq A$. □

149 REMARQUE.

1. Si $(X, \leq)$ est un treillis complet, alors X admet un élément maximum, souvent noté 1. On a $1 = \bigwedge \varnothing$ (exercice). On obtient duallement que $(X, \leq)$ a un élément minimum, souvent noté 0 et que $0 = \bigvee \varnothing$.
2. On peut aussi démontrer qu'un ensemble ordonné $(X, \leq)$ est un treillis complet si et seulement si il admet un élément maximum et toute partie non vide admet une borne inférieure (exercice).

6.3 *Les nombres réels comme ensemble ordonné*

Les nombres réels jouissent d'un statut particulier dans votre formation car ils sont à la base de vos cours d'analyse. Nous donnons quelques propriétés de $\mathbb{R}$ vu comme ensemble ordonné.

La première propriété est une caractérisation alternative du la borne supérieure. Elle vous sera très utile dans vos cours d'analyse et de topologie.

150 PROPOSITION. *Soient* $A \subseteq \mathbb{R}$ *et* $\ell \in \mathbb{R}$. *Le nombre* ℓ *est une borne supérieure de* A *si et seulement si*

$$\ell \text{ est un majorant de } A \quad \wedge \quad \forall \epsilon > 0 \;]\ell - \epsilon, \ell] \cap A \neq \varnothing. \tag{15}$$

Démonstration. Supposons d'abord que $\ell = \sup A$. On sait déjà que ℓ est un majorant de A. Prouvons que pour tout $\epsilon > 0$ alors $]\ell - \epsilon, L] \cap A \neq \varnothing$. On prouve la contraposée, c'est-à-dire que si il existe $\epsilon > 0$ tel que $]\ell - \epsilon, L] \cap A = \varnothing$ alors $\ell \neq \sup A$. En effet, on a donc

$$\ell - \epsilon < \ell \quad \wedge \quad \forall a \in A (a \leq \ell - \epsilon \; \vee \; a > \ell).$$

Comme ℓ est un majorant de A l'assertion précédente est équivalente à

$$\ell - \epsilon < \ell \quad \wedge \quad \forall a \in A \; a \leq \ell - \epsilon.$$

On a donc obtenu un majorant $\ell - \epsilon$ strictement plus petit que ℓ. Donc $\ell \neq \sup A$.

Réciproquement, supposons que la condition 15 soit satisfaite, et prouvons que $\ell = \sup A$. On sait déjà que ℓ est un majorant de A, il nous suffit de prouver qu'il en est le plus petit A. On prouve la contraposée, c'est-à-dire que si L n'est pas le plus petit majorant de A alors la condition (16)n'est pas satisfaite. Si ℓ n'est pas le plus petits des majorants, il existe $z \in \mathbb{R}$ tel que

$$z < \ell \; \wedge \; \forall a \in A \; z \geq a.$$

Définissons ϵ par $\epsilon := L - z$. On a $\epsilon > 0$ et

$$]\ell - \epsilon, \ell] \cap A \; =]z, \ell] \cap A \; = \; \varnothing,$$

ce qui prouve que (16) ne tient pas. □

Cette proposition a son équivalent pour la borne inférieure.

151 PROPOSITION. *Soient* $A \subseteq \mathbb{R}$ *et* $\ell \in \mathbb{R}$. *Le nombre* ℓ *est une borne inférieure de* A *si et seulement si*

$$\ell \text{ est un minorant de } A \quad \wedge \quad \forall \epsilon > 0 \; [\ell, \ell + \epsilon[\cap A \neq \varnothing. \tag{16}$$

Les nombres réels ont une propriété particulière relative à l'ordre, que l'on appelle souvent *la propriété de la borne supérieure* et que nous allons accepter sans démonstration (vous en verrez peut-être la preuve au cours d'Analyse I).

152 THÉORÈME. *Si* A *est une partie de* $\mathbb{R}$ *qui admet un majorant, alors* A *a une borne supérieure. De même, si* A *admet un minorant, alors* A *admet une borne inférieure.*

6.4 *Ordre produit et ordre lexicographique.*

Si $(X, \leq)$ et $(Y, \leq)$ sont deux ensembles ordonnés. Est-il possible de définir une relation d'ordre sur $X \times Y$ en utilisant les ordres connus sur X et Y ? Nous pouvons procéder d'au moins deux manières différentes, que nous détaillons dans cette section.

153 DÉFINITION. Soient $(X, \leq)$ et $(Y, \leq)$ deux ensembles ordonnés. L'*ordre produit* sur $X \times Y$ est définit par

$$(x, y) \leq (x', y') \quad \Longleftrightarrow \quad x \leq x' \text{ et } y \leq y'.$$

154 LEMME. *Si* $(X, \leq)$ *et* $(Y, \leq)$ *sont deux ensembles ordonnés alors l'ordre produit sur* $X \times Y$ *est une relation d'ordre.*

Autrement dit, pour calculer l'ordre produit, on procède composante à composante.

155 EXEMPLE. Donner le diagramme de Hasse de l'ordre produit sur $\{0, 1\} \times \{0, 1\}$ si $\{0, 1\}$ est muni de l'ordre naturel $\leq$ défini par $0 \leq 1$.

Comme le montre l'exemple précédent, l'ordre produit de deux ensembles totalement ordonné n'est pas forcément un ensemble totalement ordonné. Si l'on désire avoir cette propriété, on peut faire appel à l'ordre lexicographique, ainsi nommé car il est inspiré de l'ordre du dictionnaire.

156 DÉFINITION. Soient $(X, \leq)$ et $(Y, \leq)$ deux ensembles ordonnés. L'*ordre lexicographique* sur $X \times Y$ est définit par

$$(x, y) \leq (x', y') \quad \Longleftrightarrow \quad x < x' \vee (x = x' \text{ et } y \leq y').$$

157 LEMME. *Si* $(X, \leq)$ *et* $(Y, \leq)$ *sont deux ensembles ordonnés alors l'odre produit sur* $X \times Y$ *est une relation d'ordre.*

158 EXEMPLE. Donner le diagramme de Hasse de l'ordre lexicographique sur $\{0, 1\} \times \{0, 1\}$ si $\{0, 1\}$ est muni de l'ordre naturel $\leq$ défini par $0 \leq 1$.

L'exemple précédent se généralise de la manière suivante.

159 PROPOSITION. *Si* $(X, \leq)$ *et* $(Y, \leq)$ *sont deux ensembles totallement ordonnés, alors l'ordre lexicographique sur* $X \times Y$ *est totalement ordonné.*

Démonstration. La preuve est un exercice formateur. □

Pour aller plus profond

La théorie de l'ordre est une des théories fondamentales en mathématique et en informatique. Les ordres sont partout. Les lecteur·rice·s qui souhaitent approfondir le sujet peuvent se référer à [2].

7 ARITHMÉTIQUE MODULAIRE

Dans cette section, nous allons définir une arithmétique sur un ensemble fini de nombres (en fait *des* arithmétiques). Cette construction se base sur la notion de congruence modulo n que nous introduisons maintenant. En informatique, il est bien pratique de pouvoirs disposer d'une arithmétique finie (tous les nombres rentrent en mémoire en même temps, au besoin) et de nombreuses applications (comme la cryptographie ou les codes correcteurs d'erreurs) trouvent leur origine dans ce type d'arithmétique.

7.1 *Arithmétique : les fondements*

Commençons par réviser quelques propriétés de bases de l'arithmétique des nombres entiers. Nous avons déjà utilisé le notion de *nombre premier*, c'est-à-dire d'un entier $p > 1$ uniquement divisible par 1 et p. Ils ont en quelques sorte un caractère atomique puisqu'ils ne peuvent pas être décomposés en produit de nombres propres différents de 1.

Lorsqu'un nombre a n'est pas premier, on peut s'intéresser à ses diviseurs : on écrit $c|a$ si a est un multiple de c, c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $a = kc$. De manière plus général, on peut s'intéresser aux diviseurs communs de $(a, b) \neq (0, 0)$. Parmi ceux-ci, on repère le plus grand, ce qui donne lieu à la définition suivante.

160 NOTATION. Soit $n \geq 2$ et $z \in \mathbb{Z}$. On note $z\%n$ le reste de la division euclidienne de z par n. En particulier, on a $z\%n \in \{0, \ldots, n-1\}$. Cette notation est compatible avec la notation utilisée dans une vaste majorité de langages de programmation.

161 DÉFINITION. Soit $a, b \in \mathbb{Z}$ tel que $(a, b) \neq (0, 0)$. Le *plus grand commun diviseur* $\gcd(a, b)$ de a et b est défini comme le maximum de l'ensemble des entiers positifs qui divisent à la fois a et b. Si $\gcd(a, b) = 1$, on dit que a et b sont *premiers entre eux*.

Par exemple, on a $\gcd(2, -4) = 2$ et $\gcd(15, 6) = 3$. On démontre facilement les propriétés suivantes à partir de la définition.

162 PROPOSITION. *Soient $a, b \in \mathbb{N}$ tels que $(a, b) \neq (0, 0)$.*

1. $\gcd(a, b) = \gcd(b, a)$.
2. *Si $a \neq 0$, on a* $\gcd(a, 0) = a$.
3. *Pour tout $q \in \mathbb{Z}$, on a* $\gcd(a, b) = \gcd(a, b + qa)$.
4. *On a* $\gcd(a, b) = \gcd(b, a\%b)$.

Démonstration. Prouvons la troisième assertion. Soit $q \in \mathbb{Z}$. On prouve que

$$\{c \in \mathbb{N} \mid c|a \ \wedge \ c|b\} = \{c \in \mathbb{N} \mid c|a \ \wedge \ c|(b + qa)\}$$

Prouvons l'inclusion $\subseteq$ et désignons par c un diviseur commun de a et b. Il existe donc $c_0, c_1 \in \mathbb{Z}$ tels que $a = c_0 c$ et $b = c_1 c$. Il s'ensuit que $b + qa = c_1 c + q c_0 c =$

$(c_0 + qc_1)c$ est un multiple de c.

Prouvons l'inclusion réciproque $\supseteq$ et designons par c un diviseur commun de a et de $b + qa$. Il existe donc $c_0, c_1 \in \mathbb{Z}$ tels que $a = c_0 c$ et $b + qa = c_1 c$. Il s'ensuit que $b = c_1 c - qa = c_1 c - qc_0 c = (c_1 c - qc_0)c$ est un multiple de c. Donc c est un multiple commun de a et b.

Pour la dernière assertion, on effectue la division euclidienne de a par b : il existe $q \in \mathbb{Z}$ tel que $a = qb + a\%b$, donc $a\%b = a - qb$, et la quatrième assertion découle donc de la troisième. □

163 REMARQUE. Pourquoi ne définit-on pas la notion de $\gcd(a, b)$ lorsque $a = b = 0$?

Une question naturelle se pose : comment calculer *efficacement* le $\gcd(a, b)$? Vous avez sans doute appris à calculer les gcd en utilisant la décomposition en facteurs premiers. Mais cette technique n'est pas efficace pour des grands nombres [28] car on ne dispose simplement pas d'algorithme efficace (*i.e.*, en temps polynomial) de factorisation en nombres premiers.

Heureusement, Euclide (3e siècle avant JC) nous a légué une solution [29], qui utilise la division euclidienne. Il s'agit de l'*algorithme d'Euclide*, dont un pseudocode est donné dans l'Algorithm 1, où on désigne par $a\%b$ le reste de la division euclidienne de a par b.

Algorithm 1 Euclidean Algorithm

```
1: function EUCLIDE(a, b)                    ▷ Input (a, b) ≠ (0, 0)
2:     while b ≠ 0 do
3:         r ← b
4:         b ← a%b
5:         a ← r
6:     end while
7:     return a
8: end function
```

164 PROPOSITION. *Si* $(a, b) \neq (0, 0)$ *alors l'algorithme d'Euclide retourne le* $\gcd(a, b)$.

Avant de démonter cette assertion, donnons un exemple de déroulement de cet algorithme.

165 EXEMPLE. Appliquons l'algorithme d'Euclide pour calculer $\gcd(59, 31)$ (on sait déjà que $\gcd(59, 31) = 1$ car 59 et 31 sont premiers, mais le but est ici

28. La notion de *grand nombre* est ici informelle. Elle désigne des nombres dont la taille rend la décomposition en facteurs premiers très difficiles. Cela dépend bien sûr de la puissance de calcul à disposition. En 2023, on considère qu'un nombre de 4096 bits est un grand nombre.

29. Dans le livre VII des *Éléments*.

d'illustrer l'algorithme. On obtient successivement

$$59 = 1 \times 31 + 28 \tag{17}$$
$$31 = 1 \times 28 + 3 \tag{18}$$
$$28 = 9 \times 3 + 1 \tag{19}$$
$$3 = 3 \times 1 + 0 \tag{20}$$

L'algorithme d'Euclide retourne le dernier reste non nul dans cette suite de division euclidienne, à savoir 1. Il s'agit bien du gcd(59, 31).

166 REMARQUE. Il est facile de retenir l'algorithme d'Euclide par le moyen mnémotechnique suivant : dans la suite de divisions euclidienne, *le diviseur devient le divisé, et le reste le diviseur*.

Démonstration de la proposition . Considérons $(a, b) \neq (0, 0)$ et supposons sans perte de généralité que $b \neq 0$. Désignons par $r_1, r_2, \ldots$ la suite de restes obtenus dans l'exécution de l'algorithme d'Euclide avec a, b en entrée :

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ \cdots &= \cdots \\ r_{i-2} &= q_i r_{i-1} + r_i \\ \cdots &= \cdots \end{aligned}$$

Pour toute étape i on a $r_i \in \{0, \ldots, r_{i-1} - 1\}$, ce qui prouve que la suite $r_1, r_2, \ldots$ est strictement décroissante et se termine par $r_n = 0$ pour une valeur de $n \geq 0$. En appliquant successivement la dernière assertion de la Proposition 162, on obtient

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_i, r_{i+1}) = \cdots \gcd(r_{n-1}, 0) = r_{n-1}.$$

On a donc prouvé que $\gcd(a, b)$ est le dernier reste non nul obenu dans la suite de divisions euclidiennes de l'algorithme d'Euclide. □

L'algorithme d'Euclide existe en version « étendue » qui permet de prouver le résultat suivant.

167 THÉORÈME (Bezout). *Soient $a, b \in \mathbb{Z}$ tels que $(a, b) \neq (0, 0)$. Il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a + \beta b = \gcd(a, b)$.*

Plutôt que de prouver formellement ce résultat (la preuve n'est pas difficile), illustrons comment l'algorithme d'Euclide permet de calculer effectivement la valeur de α et β en reprenant l'Exemple 165.

168 EXEMPLE. Déterminons des $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha 31 + \beta 59 = 1$ (car $\gcd(31, 59) =$

1). On obtient successivement

$$\begin{aligned} 1 &= 28 - 9 \times 3 && \text{par (19)} \\ &= 28 - 9 \times (31 - 1 \times 28) && \text{par (18)} \\ &= 10 \times 28 - 9 \times 31 \\ &= 10 \times (59 - 1 \times 31) - 9 \times 31 && \text{par (17)} \\ &= 10 \times 59 - 19 \times 31. \end{aligned}$$

On obtient donc $\alpha = -19$ et $\beta = 10$.

Le Théorème de Bezout permet de prouver aisément le Lemme de Gauss, qui est une des pierres angulaires du théorème de décomposition en facteurs premiers.

169 LEMME (Lemme de Gauss). *Soient $a, b, c \in \mathbb{Z}$ des entiers non nuls. Si a divise bc et $\gcd(a, b) = 1$ alors a divise c.*

Démonstration. Dans les conditions du théorème, il existe $\alpha, \beta \in \mathbb{Z}$ tels que

$$\alpha a + \beta b = 1.$$

En multipliant par c on obtient

$$\alpha ac + \beta bc = c.$$

Par hypothèse, on sait que a divise bc. Comme a divise ac, on a que a divise $\alpha ac + \beta bc = c$. □

Terminons cette courte section consacrée aux rudiments d'arithmétiques par énoncer le théorème de décomposition en facteurs premiers, également appelés *théorème fondamentale de l'arithmétique*. Sa preuve est accessible mais sort du cadre de ce cours.

170 THÉORÈME. *Pour tout $n > 1$ dans $\mathbb{N}$ il existe des nombres premiers $p_1, \dots, p_\ell$ distincts et des entiers $n_1, \dots, n_\ell > 1$ tels que*

$$n = p_1^{n_1} \times \cdots \times p_\ell^{n_\ell}.$$

De plus cette décomposition est unique, à l'ordre des facteurs près.

7.2 *Introduction aux entiers modulaires : le jeux de Nim*

Le jeux de Nim est un jeux à deux joueurs. Dans sa formule la plus simple, au début du jeux les joueurs disposent 21 allumettes devant un. Chacun à leur tour, les joueurs doivent retirer 1, 2 ou trois allumettes du tas. Le joueur qui perd la partie est le joueur qui est forcé de retirer la dernière allumette. Le problème considéré est le suivant :

Est-ce que le deuxième joueur possède une stratégie gagnante ?

> C'est-à-dire, lui est-il toujours possible, à chaque étape du jeux, de choisir un nombre d'allumettes à retirer du tas de telle sorte qu'il assure sa victoire, quelles que soient les choix du premier joueur ?

Une analyse de l'ensemble des déroulements possibles du jeux montrer que pour assurer sa victoire il faut et il suffit que le deuxième joueur laisse dans les tas après chaque manche un nombre d'allumettes égal à 5, 9, 13 ou 17, c'est-à-dire un nombre dont le reste de la division par 4 vaut 1.

L'information importante pour gagner le jeux n'est donc pas le nombre d'allumettes laissées à son adversaire, mais son reste pour la division par 4. En généralisant cette exemple, nous allons construire l'arithmétique modulaire.

7.3 *Entiers modulo n*

Dans l'optique de définir des arithmétiques sur des ensembles finis de nombres, nous allons commencer par définir ces ensembles de nombres.

171 DÉFINITION. Soit $n \geq 2$. Deux entiers $a, b \in \mathbb{Z}$ sont *congrus modulo* n, et on note $a \equiv b \bmod n$, si $a\%n = b\%n$.

172 LEMME. *Soit $n \geq 2$.*

(1) Pour tous $a, b \in \mathbb{Z}$ on a $a \equiv b \bmod n$ si et seulement si $a - b$ est un multiple de n.

(2) La relation congruence modulo n *est une équivalence sur $\mathbb{Z}$.*

Démonstration. (1) Supposons d'abord que $a \equiv b \bmod n$. Donc, il existe $q, q' \in \mathbb{Z}$ et $r, r' \in \{0, \ldots, n-1\}$ tels que $a = qn + r$ et $b = q'n + r$. Ainsi $a - b = (q - q')n$ est un multiple de n.

Réciproquement, si $a - b$ est un multiple de n, alors il existe $q \in \mathbb{Z}$ tel que $a - b = qn$, donc $a = b + qn$. Il s'ensuit que $a\%n = b\%n$ donc $a \equiv b \bmod n$.

(2) La relation congruence modulo n est clairement réflexive et symétrique. Prouvons qu'elle est transitive. Supposons que $a \equiv b \bmod n$ et $b \equiv c \bmod n$, c'est-à-dire qu'il existe $q, q' \in \mathbb{Z}$ tels que $a - b = qn$ et $b - c = q'n$. Donc $a - c = a - b + b - c = (q + q')n$ est un multiple de n, ce qui signifie que $a \equiv c \bmod n$. □

173 NOTATION. On note par $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$ le quotient de $\mathbb{Z}$ par la relation de congruence modulo n. Par abus de notation, on note par $\overline{z}$ la classe de z pour la relation de congruence modulo n. Les éléments de $\mathbb{Z}_n$ sont appelés *entiers modulo n*. Formellement, un entier modulo n est donc un sous-ensemble infini de $\mathbb{Z}$, puisque c'est une classe d'équivalence sur $\mathbb{Z}$.

174 EXEMPLE. En choisissant $n = 2$ on obtient $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ où

$$\overline{0} = \{2k \mid k \in \mathbb{Z}\} \qquad \text{et} \qquad \overline{1} = \{2k + 1 \mid k \in \mathbb{Z}\},$$

sont les deux classes d'équivalence pour la relation de congruence modulo 2.

175 LEMME. *Soit $n \geq 2$ et $z \in \mathbb{Z}$. Alors $\overline{z}$ contient un unique élément r (appelé* représentant standard de $\overline{z}$*) tel que $0 \leq r < n$. De plus, on a $r = z\%n$.*

Démonstration. D'abord, on a clairement que $z\%n \in \overline{z}$ et $0 \leq z\%n < n-1$ par définition de la division euclidienne. Ensuite, si $r, r' \in \overline{z}$ sont tels que $r, r' \in \{0, \ldots, n-1\}$ et $r \geq r'$ alors $r-r'$ est un multiple de n tel que $0 \leq r-r' < n-1$. On en conclut que $r = r'$. □

176 NOTATION. Chaque classe d'équivalence $\overline{z} \in \mathbb{Z}_n$ a donc un représentant standard r entre 0 et $n-1$. Il est commode et coutumier *d'identifier* $\overline{z}$ avec son représentant standard r. Ainsi, on écrira parfois $\mathbb{Z}_n = \{1, \ldots, n-1\}$ au lieu de $\mathbb{Z}_n = \{\overline{1}, \ldots, \overline{n-1}\}$. Il s'agit d'un abus de notation consacré par l'usage.

7.4 *Opérations modulo n*

Nous voilà équipés avec une nouvelle classe de « nombres », à savoir les entiers modulo n. Mais à quoi bon avoir des nombres, sans opération entre ces nombres ? Nous avons besoin d'une forme d'addition et de multiplication sur les entiers modulo n. Comment définir ces opérations ? Nous sommes naturellement tentés de définir, par exemple, une opération + sur $\mathbb{Z}_n$ par

$$\overline{x} + \overline{y} := \overline{x+y}.$$

Bonne idée ! Mais pour que cette définition ait le moindre sens, il faut que le résultat $\overline{x+y}$ ne dépende pas des entiers x et y choisis pour représenter les *classes* $\overline{x}$ et $\overline{y}$, respectivement. Nous nous en assurons dans le lemme suivant.

177 LEMME. *Soient $n \geq 2$ et $x, x', y \in \mathbb{Z}$ tels que $x \equiv x' \bmod n$.*

(1) On a $x + y \equiv x' + y \bmod n$.

(2) On a $xy \equiv x'y \bmod n$.

Démonstration. Nous savons que $(x - x')$ est un multiple de n.
(1) Il vient $(x + y) - (x' + y) = (x - x')$ est un multiple de n.
(2) Il vient $xy - x'y = (x - x')y$ est un multiple de n. □

En particulier, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ alors $\overline{x+y} = \overline{x'+y'}$ et $\overline{xy} = \overline{x'y'}$, ce qui donne un sens à la définition suivante.

178 DÉFINITION. Soit $n \geq 2$. On définit les opérations $+ \colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ et $\times \colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ par

$$\overline{x} + \overline{y} := \overline{x+y}$$

$$\overline{x} \times \overline{y} := \overline{x \times y}$$

pour tous $\overline{x}, \overline{y} \in \mathbb{Z}_n$.

179 EXEMPLE. Par exemple, dans $\mathbb{Z}_{10}$ on a $\overline{7} + \overline{8} = \overline{15} = \overline{5}$, et $\overline{7} \times \overline{8} = \overline{56} = \overline{6}$.

180 NOTATION. 1. Pour faciliter la lecture, en choisit de présenter une classe *via* son représentant standard. Par exemple, dans $\mathbb{Z}_{10}$ on écrira $\overline{7} \times \overline{8} = \overline{6}$, et rarement $\overline{7} \times \overline{8} = \overline{56}$.

Identité	Nom
$(a+b)+c \equiv a+(b+c) \bmod n$	Associativité de +
$(a\times b)\times c \equiv a\times(b\times c) \bmod n$	Associativité de ×
$a+b \equiv b+a \bmod n$	Commutativité de +
$a\times b \equiv b\times a \bmod n$	Commutativité de ×
$a\times(b+c) \equiv ab+ac \bmod n$	Distribution de × sur +
$a+0 \equiv a \bmod n$	0 est neutre pour ×
$a-a \equiv 0 \bmod n$	$-a$ est l'inverse de a pour +
$a\times 1 \equiv a \bmod n$	1 est neutre pour ×
$a\times 0 \equiv 0 \bmod n$	0 est absorbant pour ×

FIGURE 12 – Propriété des opérations modulo n

2. Ce choix canonique du représentant standard nous permet d'alléger les notations - lorsque cela ne prête pas à confusion - en laissant tomber les $\overline{\ }$ pour représenter les classes (entiers modulo n). Par exemple, on écrira

$$5\times 2 = 2 \text{ dans } \mathbb{Z}_8,$$

à la place de

$$\overline{5}\times\overline{2} = \overline{2} \text{ dans } \mathbb{Z}_8.$$

3. On pourra aussi rappeler que les identités ont lieu modulo n en utilisant la relation de congruence modulo n. Par exemple, on peut écrire

$$5+3 \equiv 1 \bmod 7.$$

4. Comme de coutume, nous écrirons xy au lieu de $x\times y$ lorsqu'aucune confusion n'est possible.

Les opérations sur les entiers modulo n héritent de certaines propriétés des opérations correspondantes sur $\mathbb{Z}$ à partir des quelles elle sont définies.

181 PROPOSITION. *Pour tout $n \geq 2$ les opérations + et × sur $\mathbb{Z}_n$ jouissent des propriétés listées dans la Fig. 12.*

182 DÉFINITION. Pour tout $n \geq 2$, l'ensemble $\mathbb{Z}_n$ équipé des opérations + et × et des constantes $\overline{0}$ et $\overline{1}$ est appelé *anneau des entiers modulo n*.

7.5 *Inverse et diviseur de zero*

L'arithmétique que nous avons définie sur $\mathbb{Z}_n$ a beaucoup de propriétés analogues à celles des entiers. Mais où s'arrête cette analogie ? Nous allons donner deux exemples, à savoir l'existence de diviseurs de zero et l'existence d'inverse.

183 EXEMPLE. Dans $\mathbb{Z}$, l'équation $3x = 0$ n'a pas de solution non nulle. La même

équation considérée dans $\mathbb{Z}_6$ a en revanche 2 comme solution non nulle car $3 \times 2 \equiv 0 \bmod 6$.

184 DÉFINITION. Des éléments $a, b \in \{1, \ldots, n-1\}$ tels que $ab = 0$ dans $\mathbb{Z}_n$ sont appelés *diviseurs de zéro (modulo n)*.

185 EXERCICE. Prouver que $0 < a \leq n-1$ est un diviseur de zero dans $\mathbb{Z}_n$ si et seulement si a divise n.

186 EXEMPLE. Dans $\mathbb{Z}$, les seuls éléments a inversibles, c'est-à-dire pour lesquels il existe un élément a^{-1} tels que $aa^{-1} = 1$ sont 1 et -1. Dans $\mathbb{Z}_n$, il peut y avoir plus d'éléments inversibles. Par exemple, dans $\mathbb{Z}_7$ tous les éléments non nuls sont inversibles car

$$1 \times 1 = 1, \quad 2 \times 4 = 1, \quad 3 \times 5 = 1, \quad 6 \times 6 = 1 \quad \text{dans } \mathbb{Z}_7.$$

187 DÉFINITION. Soit $n \geq 2$. Un élément a de $\mathbb{Z}_n$ est *inversible* s'il existe un élément a^{-1}, appelé *inverse de a modulo n* tel que $aa^{-1} \equiv 1 \bmod n$.

188 EXERCICE. Montrer que si un élément est inversible dans $\mathbb{Z}_n$ alors son inverse est unique.

Sans le savoir, nous avons déjà à notre disposition les outils pour caractériser les éléments inversibles de $\mathbb{Z}_n$ et calculer les inverses, comme le montre la proposition suivante.

189 PROPOSITION. *Soit $n \geq 2$ et $a \in \mathbb{Z}$. Les conditions suivantes sont équivalentes.*

(i) $\gcd(a, n) = 1$.

(ii) $\overline{a}$ *est inversible dans* $\mathbb{Z}_n$.

Démonstration. (i) $\Rightarrow$ (ii) Nous savons par le théorème de Bezout qu'il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a + \beta n = 1$, donc $\alpha a - 1 = \beta n$ est un multiple de n. Nous avons prouvé que $\alpha a \equiv 1 \bmod n$, donc que $\overline{a}$ admet $\overline{\alpha}$ comme inverse dans $\mathbb{Z}_n$.

(ii) $\Rightarrow$ (i) Supposons qu'il existe $\overline{b} \in \mathbb{Z}_n$ tel que $\overline{a} \times \overline{b} = 1$ dans $\mathbb{Z}_n$. Alors il existe un $k \in \mathbb{Z}$ tel que $ab - 1 = kn$. Donc, si c est un diviseur commun de a et n, on a c divise $ab - kn = 1$, donc $c = 1$. □

La preuve du résultat précédant nous montre même le chemin à suivre pour calculer les inverses dans $\mathbb{Z}_n$. En effet, si $\gcd(a, n) = 1$, alors par le théorème de Bezout il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a + \beta n = 1$. Donc $\alpha a - 1$ est multiple de n, c'est-à-dire $\alpha a \equiv 1 \bmod n$. Ainsi $(\overline{a})^{-1} = \overline{\alpha}$.

190 EXEMPLE. Calculons l'inverse de 39 dans $\mathbb{Z}_{51}$. Nous avons prouver dans l'Exemple 168 que $10 \times 59 - 19 \times 31 = 1$. Donc

$$31^{-1} \equiv -19 \equiv 40 \bmod 59.$$

On vérifie facilement que $31 \times 40 \equiv 1 \mod 59$ car $31 \times 40 - 1 = 1239 = 21 \times 59$.

Le cas de $\mathbb{Z}_p$ où p est premier est un corollaire intéressant de la Proposition 189.

191 COROLLAIRE. *Si p est premier alors tous les éléments non nuls de $\mathbb{Z}_p$ sont inversibles.*

192 NOTATION. On note $\mathbb{Z}_p^*$ l'ensemble des inversibles de $\mathbb{Z}_p$, c'est-à-dire

$$\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}.$$

Notez que $\mathbb{Z}_p^*$ est fermé par multiplication, c'est-à-dire que si $\overline{a}, \overline{c} \in \mathbb{Z}_p^*$ alors $\overline{a} \times \overline{c} \in \mathbb{Z}_p^*$.

7.6 *Arithmétique modulaire*

L'arithmétique sur $\mathbb{Z}_p$ avec p premier se rapproche donc de l'arithmétique de $\mathbb{Q}$ (tous les deux sont d'ailleurs des *corps commutatifs*, mais cela dépasse le cadre de ce cours). En particulier, elle permet de prouver le *petit Théorème de Fermat* [30]. Vous connaissez sans doute Fermat pour son *dernier théorème* [31], qui n'en était pas un jusqu'à la toute fin du XXe siècle, époque à laquelle Andrew Wiles en a donné une démonstration. Nous ne parlons pas ici de cette énorme pièce de résistance mathématique, mais du résultat suivant qui est au coeur d'un des systèmes cryptographiques les plus utilisés au monde (j'ai nommé, le RSA).

193 THÉORÈME (Petit théorème de Fermat). *Si p est un nombre premier et $a \in \mathbb{N}$ n'est pas multiple de p alors $a^{p-1} \equiv 1 \bmod p$.*

Démonstration. Prouvons d'abord que l'application $m_{\overline{a}} \colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ définie par $m_{\overline{a}}(\overline{c}) = \overline{a} \times \overline{c}$ est une bijection. Montrons qu'elle est injective : supposons que $\overline{b}, \overline{c} \in \mathbb{Z}_p^*$ sont tels que $m_{\overline{a}}(\overline{b}) = m_{\overline{a}}(\overline{c})$, c'est-à-dire $\overline{a} \times \overline{b} = \overline{a} \times \overline{c}$. Donc, en multipliant à gauche par $\overline{a}^{-1}$ on obtient $\overline{a}^{-1} \times \overline{a} \times \overline{b} = \overline{a}^{-1} \times \overline{a} \times \overline{c}$, c'est-à-dire $\overline{b} = \overline{c}$.

Montrons ensuite que $m_{\overline{a}}$ est surjective. Soir $\overline{c} \in \mathbb{Z}_p^*$. On a

$$m_{\overline{a}}(\overline{a}^{-1} \times \overline{c}) = \overline{a} \times \overline{a}^{-1} \times \overline{c} = \overline{c},$$

ce qui prouve la surjectivité.

En particulier on a

$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{a} \times \overline{1}, \overline{a} \times \overline{2}, \ldots, \overline{a} \times \overline{p-1}\}.$$

Il s'ensuit que

$$\prod_{\overline{c} \in \mathbb{Z}_p^*} \overline{c} = \prod_{\overline{c} \in \mathbb{Z}_p^*} \overline{a} \times \overline{c} = \overline{a}^{p-1} \times \prod_{\overline{c} \in \mathbb{Z}_p^*} \overline{c}.$$

On en conclut que $\overline{a}^{p-1} = \overline{1}$ en multipliant l'identité précédente par l'inverse de

30. Pierre de Fermat, mathématicien français du 17e siècle.
31. Renseignez-vous à ce sujet !

$\prod_{\overline{c}\in\mathbb{Z}_p^*} \overline{c}$. □

194 COROLLAIRE. *Si p est un nombre premier alors $a^p \equiv a \bmod p$ pour tout $a \in \mathrm{Z}$.*

Le petit théorème de Fermat est notamment utile pour simplifier le calcul de grandes puissances modulo p.

195 EXEMPLE. Calculons $6^{2025} \bmod 17$. On a $2025 = 126 \times 16 + 9$. Donc

$$6^{2025} \equiv (6^{16})^{126} \times 6^9 \equiv 6^9 \equiv 11 \bmod 17$$

où on obtient le deuxième identité par le petit théorème de Fermat.

Comme on dispose d'une arithmétique sur $\mathbb{Z}_n$, on peut se poser la question de la résolution des équations polynomiales. L'exemple ci-dessous illustre que, contrairement aux équations à coefficients dans $\mathbb{Q}$ ou $\mathbb{R}$, le cas d'une équation du premier degré à une inconnue peut donner lieu à une solution unique, un ensemble de plusieurs solutions ou pas de solution.

196 EXEMPLE. Posée dans $\mathbb{Z}_4$, l'équation $\overline{2}x + \overline{2} = \overline{0}$ a $x = \overline{1}$ ou $x = \overline{3}$ comme solution. Posée dans $\mathbb{Z}_6$, l'équation $\overline{3}x + \overline{2} = 0$ n'a pas de solution. Posée dans $\mathbb{Z}_7$, l'équation $\overline{3}x + \overline{2} = 0$ a comme solution unique $x = \overline{4}$.

Le résultat suivant permet de traiter le cas des équations de degré 1 en toute généralité.

197 PROPOSITION. *L'équation $\overline{a}x + \overline{b} = 0$ posée dans $\mathbb{Z}_n$ a au moins une solution si et seulement si $\gcd(a, n)$ divise b. Dans ce cas, l'équation a $\gcd(a, n)$ solutions distinctes.*

Démonstration. ($\Rightarrow$) Soit $\overline{c} \in \mathbb{Z}_n$ tel que $\overline{ac} + \overline{b} = \overline{0}$. Alors, il existe $k \in \mathbb{Z}$ tel que $ac + b = kn$, donc $b = kn - ac$. Ainsi tout diviseur commun de a et de n est aussi un diviseur de b.

($\Leftarrow$) Soit $a_0 \in \mathbb{Z}$ premier avec n tel que $a = a_0 g$ où $g := \gcd(a, n)$. Supposons qu'il existe $b_0 \in \mathbb{Z}$ tel que $b = b_0 \gcd(a, n)$. On a donc

$$ax + b \equiv 0 \bmod n \iff \gcd(a, n)(a_0 x + b_0) \equiv 0 \bmod n.$$

Cette dernière équation est équivalente à

$$a_0 x + b_0 \equiv 0 \bmod n \quad \vee \quad a_0 x + b_0 \equiv n/g \bmod n \quad \vee \quad \cdots \quad \vee\, a_0 x + b_0 \equiv (g-1)n/g \bmod n$$

Comme a_0 est premier avec n, chacune de ces équations admet une solution unique dans $\mathbb{Z}_n$. □

Crytpographie : les RSA

La cryptographie désigne l'ensemble des techniques qui permettent de communiquer des informations entre interlocuteurs, sans que des tierces personnes ne puissent connaître le contenu de messages transmis. Sans aller dans les détails, la cryptographie est au coeur de notre économie moderne, puisqu'elle est garante de la confidence des échanges électroniques. Le calcul du gcd, l'arithmétique modulaire et le petit théorème de Fermat sont au coeur d'un des cryptosystèmes à *clé publique* les plus répandu, à savoir le RSA. Vous avez toutes les clés en main pour comprendre le fonctionnement de ce cryptosystème que le manque de temps nous ne permettra pas de voir en cours. Il existe néanmoins de nombreuses videos explicatives à ce sujet sur les plateformes grand public.

8 PERMUTATIONS

198 DÉFINITION. Une *permutation* d'un ensemble E est une bijection $f : E \to E$. On note S_E l'ensemble des permutations de E.

Rappelons les propriétés suivantes.

199 PROPOSITION. *Soit* E *un ensemble.*

(1) Si $f, g \in S_E$ *alors* $f \circ g \in S_E$.

(2) La loi de composition est associative sur S_E *: pour tous* $f, g, h \in S_E$ *on a* $(f \circ g) \circ h = f \circ (g \circ h)$.

(3) La fonction id_E *est neutre pour la composition sur* S_E *: pour tout* $f \in S_E$ *on a* $\mathrm{id}_E \circ f = f \circ \mathrm{id}_E = f$. *De plus* id_E *est l'unique neutre pour la composition.*

(4) Chaque permutation f *admet une unique* permutation inverse, *c'est-à-dire un élément* f^{-1} *de* S_E *tel que* $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_E$.

Démonstration. (1) La composition de deux bijections est une bijection (exercice).

(2) Simple vérification.

(3) Seule l'unicité de id_E comme neutre de la composition mérite une preuve. Soit $\nu \in S_E$ tel que pour tout $f \in S_E$ on a $\nu \circ f = f \circ \nu = f$. En particulier

$$\nu = \nu \circ \mathrm{id}_E = \mathrm{id}_E,$$

où la première identité est obtenue car id_E est neutre pour la composition, et la deuxième car ν est neutre pour la composition. On a donc prouvé que $\nu = \mathrm{id}_E$.

(4) Comme f est une bijection, nous savons qu'elle admet une fonction inverse $f^{-1} : E \to E$ qui satisfait aux identités de l'énoncé. Soit $g \in S_E$ tel que $f \circ g = \mathrm{id}_E$. En composant à gauche par f^{-1}, on obtient

$$f^{-1} \circ (f \circ g) = f^{-1},$$

où on a utilisé (3). Par associativité et (3) on a

$$(f^{-1} \circ f) \circ g = f^{-1},$$

et don $f^{-1} = g$. □

8.1 *Permutations d'un ensemble fini*

Nous allons maintenant nous intéresser à la combinatoire des permutations d'un ensemble fini E. Par convention, nous allons supposer que E contient un nombre $n \geq 1$ d'éléments, et même que $\mathrm{E} = \{1, \ldots, n\}$.

200 NOTATION. Soit f une permutation de $\{1, \ldots, n\}$. Il est coutume de noter f de la manière suivante

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

Si $i \in \{1, \ldots, n\}$ est tel que $f(i) = i$, il est coutume de ne pas écrire la colonne correspondant au couple $(i, f(i))$. Pour favoriser la compacité de l'écriture, nous pouvons aussi utiliser la notation *en ligne*[32] des permutations. Dans ce cas, une permutation f de $\{1, \ldots, n\}$ est notée par $f(1)f(2)\ldots f(n)$, c'est-à-dire la suite finie d'éléments de $\{1, \ldots, n\}$ dont le i^{e} terme est $f(i)$, pour tout i dans $\{1, \ldots, n\}$.

On écrit S_n au lieu de $\mathrm{S}_{\{1,\ldots,n\}}$.

201 EXEMPLE. La permutation f de $\{1, \ldots, 4\}$ définie par

$$f = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix}$$

est telle que $f(1) = 2$, $f(2) = 4$, $f(3) = 3$ et $f(4) = 1$. Sa notation en ligne est 2431.

202 EXERCICE. En utilisant la notation en ligne, déterminer la résultat de la composition

$$13425 \circ 54213.$$

203 EXERCICE. Énumérer les éléments de S_3 (on notation standard et en notation en ligne).

204 EXERCICE. Déterminer toutes les valeurs de n telles que S_n est commutatif.

205 PROPOSITION. *Pour tout $n \geq 1$, on a $\#\mathrm{S}_n = n!$*

La proposition précédente est un corollaire immédiat du Lemme suivant.

206 LEMME. *Pour tout $n \geq 1$ et tous ensembles* E *et* F *a n éléments, il y a $n!$ bijections de* E *dans* F.

32. *In line notation*, en anglais

Démonstration. Nour procédons par induction sur $n \geq 1$. Le cas de base $n = 1$ est trivial, car il y a une seule fonction, qui est une bijection, entre deux singletons fixés.

Supposons ensuite que $n \geq 1$ et que pour tous ensembles E′ et F′ à n éléments, il y a $n!$ bijections de E′ dans F′. Prouvons que si E et F sont des ensembles à $n + 1$ éléments, alors il y a $(n + 1)!$ bijections de E dans F. Pour définir une telle bijection f, nous procédons en deux étapes. Nous choisissons l'image $f(e)$ d'un élément $e \in \mathrm{E}$ fixé arbitrairement, puis une bijection $f' \colon \mathrm{E} \setminus \{e\} \to \mathrm{F} \setminus \{f(e)\}$. Nous avons $n + 1$ possibilités pour le premier choix, et $n!$ possibilités pour le deuxième, par hypothèse d'induction. Au total il y a bien $(n + 1) \times n! = (n + 1)!$ bijections de E dans F. La conclusion s'ensuit par le principe d'induction. □

207 REMARQUE. Comme l'unique bijection sur l'ensemble vide est la fonction $\varnothing$, on a aussi $\mathrm{S}_0 = 0! = 1$.

208 NOTATION. Soit f un élément de S_n et $k \geq 0$. On note f^k la permutation $f \circ \cdots \circ f$, où le facteur f est répété k fois. En particulier, on a $f^0 = \mathrm{id}$.

209 DÉFINITION. Le support $\mathrm{supp}(f)$ d'une permutation $f \in \mathrm{S}_n$ $(n \geq 1)$ est l'ensemble définit par

$$\mathrm{supp}(f) := \{i \in \{1, \ldots, n\} \mid f(i) \neq i\}.$$

Une partie X de $\{1, \ldots, n\}$ est *invariante* par f si $f(\mathrm{X}) = \mathrm{X}$.

210 EXEMPLE. Si f est la permutation 32145, on a $\mathrm{supp}(f) = \{3, 1\}$.

211 LEMME. *Soit $f \in \mathrm{S}_n$ pour un $n \geq 1$.*

(1) Une partie X *de* $\{1, \ldots, n\}$ *est invariante par f si et seulement si $f(\mathrm{X}) \subseteq \mathrm{X}$.*

(2) Le support $\mathrm{supp}(f)$ *de f est invariant par f.*

Démonstration. (1) Comme f est injective, on a que $f(\mathrm{X})$ est une partie de X de même cardinalité finie que X, donc $f(\mathrm{X}) = \mathrm{X}$.

(2) Il suffit par (1) de prouver que $f(\mathrm{supp}(f)) \subseteq \mathrm{supp}(f)$. On procède par contraposition (c'est-à-dire qu'on passe au complémentaire) en prouvant que $\mathrm{X} \setminus \mathrm{supp}(f) \subseteq \mathrm{X} \setminus f(\mathrm{supp}(f))$. Soit $i \in \mathrm{X} \setminus \mathrm{supp}(f)$, c'est-à-dire tel que $f(i) = i$. On a donc $i \in f(\mathrm{X} \setminus \mathrm{supp}(f))$. Comme f est une fonction injective, on a $f(\mathrm{X} \setminus \mathrm{supp}(f)) \subseteq \mathrm{X} \setminus f(\mathrm{supp}(f))$. On a prouvé que $i \in \mathrm{X} \setminus f(\mathrm{supp}(f))$. □

212 PROPOSITION. *Soient $f, g \in \mathrm{S}_n$ pour un $n \geq 1$. Si* $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \varnothing$, *alors* $f \circ g = g \circ f$.

Démonstration. Nous allons montrer que pour tout $i \in \{1, \ldots, n\}$ on a $f(g(i)) = g(f(i))$. On distingue les trois cas suivant.

Si $i \in \mathrm{supp}(f)$, alors $i \notin \mathrm{supp}(g)$ par hypothèse et $f(i) \in \mathrm{supp}(f)$ par le

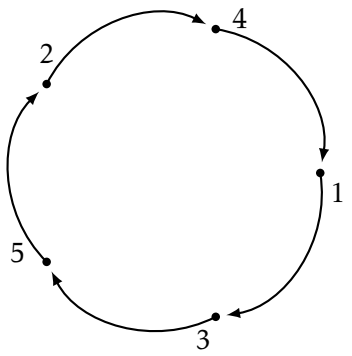


FIGURE 13 – Cycle (13524)

Lemme 211, donc $f(i) \notin \mathrm{supp}(g)$. On a donc

$$f(g(i)) = f(i) = g(f(i))$$

où la première identité est obtenue car $g(i) = i$, et la deuxième car $f(i) \notin \mathrm{supp}(g)$.

Si $i \in \mathrm{supp}(g)$, alors $i \notin \mathrm{supp}(f)$ par hypothèse et au procède comme dans le cas précédent.

Si $i \notin \mathrm{supp}(g) \cup \mathrm{supp}(f)$, alors $f(i) = i = g(i)$ fonc $f(g(i)) = g(f(i))$. Ce qui conclut la preuve. □

8.2 *Cycles et transpositions*

213 DÉFINITION. Soit $n \geq 2$ et $\ell \in \{2, \ldots, n\}$. Un *cycle de longueur* ℓ (ou *ℓ-cycle*) de S_n est une permutation du type

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_\ell \\ a_2 & a_3 & \ldots & a_1 \end{pmatrix} \tag{21}$$

pour certains $a_1, \ldots, a_\ell \in \{1, \ldots, n\}$.

Une *transposition* est un cycle de longueur 2.

214 NOTATION. On note par $(a_1 a_2 \ldots a_\ell)$ le cycle définit en (21). Attention ! Il ne faut pas confondre le cycle $(a_1 a_2 \ldots a_\ell)$ avec la permutation $a_1 a_2 \ldots a_\ell$ écrite en utilisant la notation en ligne. Ces permutations sont différentes.

En représentant l'effet du cycle (13524) sur l'ensemble $\{1, \ldots, 5\}$, la Fig. 13 justifie le choix du terme cycle pour ces permutations : elles peuvent être représentées sous forme de cycle. Remarquez comme la notation d'un cycle n'est pas unique : les cycles (13524), (35241), (52413), (24135), (41352) sont identiques et leur notation en ligne est 34512.

Imaginez avoir les cartes de l'1♢ au K♢ étalées en une rangée sur une tables devant vous, mais dans un ordre mélangé (une permutation de l'ordre initial mentionné ci-avant). Pour récupérez l'ordre initial, il est intuitivement possible

de procéder à une suite d'échanges successifs de deux cartes. Cette expérience fort commune donne lieu au résultat suivant.

215 PROPOSITION. *Toute permutation $f \in \mathrm{S}_n$ (pour un $n \geq 2$) se décompose en un produit d'au plus $n-1$ transpositions.*

Avant d'en donner la preuve, remarquons que même la permutation identité est un produit de transpositions (c'est le produit de 0 transposition).

Démonstration. On procède par récurrence sur $n \geq 2$. Le cas de base $n = 2$ est trivial, car les deux seuls permutations sont l'identité et la transposition (12).

Pour l'étape de récurrence, supposons que tout élément de S_n est un produit d'au plus $n-1$ transpositions pour un $n \geq 2$ et prouvons qu'une permutation quelconque $f \in \mathrm{S}_{n+1}$ est un produit d'au plus n transpositions. On distingue les deux cas suivants.

Si $f(n+1) = n+1$ alors f peut être considéré comme un élément de S_n et est le produit d'au plus $n-1$ transpositions, par hypothèse de récurrence.

Si $f(n+1) \neq n+1$ alors la permutation $f' := (ab) \circ f$, où $a := n+1$ et $b := f(n+1)$ satisfait $f'(n+1) = n+1$. Elle peut donc être considérée comme un élément de S_n et se décompose en un produit $t_1 \circ \cdots \circ t_\ell$ d'au plus $n-1$ transpositions de $1, \ldots, n$ par hypothèse de récurrence. Alors $f = (ab) \circ t_1 \circ \cdots \circ t_\ell$ est bien un produit d'au plus n transpositions. □

216 REMARQUE. Attention ! La décomposition d'une permutation en produit de transposition n'est pas unique (donnez une exemple).

217 EXEMPLE. On vérifie facilement qu'un cycle $(a_1 \cdots a_\ell)$ admet la décomposition suivante :

$$(a_1 \cdots a_\ell) = (a_1 a_2)(a_2 a_3) \cdots (a_{\ell-1} a_\ell).$$

Par exemple, le cycles (12345) se décompose en (12)(23)(34)(45).

La décomposition d'une permutation en un produit de transposition est sympa, mais pas unique. En relaxant la condition sur la longeur des cycles qui apparaissent dans la décomposition, on peut faire mieux : toute permutation se décompose en un produit de cycles de supports disjoints (donc qui commutent entre elles), et ette décomposition est unique (à l'ordre des facteurs près).

218 THÉORÈME (Décomposition en cycles disjoints). *Soit $n \geq 2$ et $f \neq \mathrm{id}$ un élément de S_n.*

1. *Il existe des cycles $s_1, \ldots, s_k$ dont les supports sont deux à deux disjoints tels que $f = s_1 \circ \cdots \circ s_k$.*
2. *Cette décomposition est unique à l'ordre des facteurs près.*

Démonstration. Nous accepterons ce résultat sans démonstration, par manque de temps. □

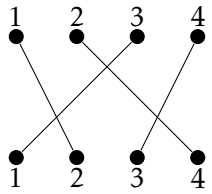


FIGURE 14 – La permutation 2413 a 3 inversions

219 EXEMPLE. La décomposition d'une permutation en cycles de supports disjoints est très facile à obtenir. On commence par choisir un $a \in \{1, \dots, n\}$ et à calculer les $f^k(a)$ jusqu'à obtenir à nouveau a. Ceci nous donne le premier cycle. Les autres cycles s'obtiennent par le même procédé en choisissant comme étape initiales des a qui ne sont pas apparus dans les cycles précédents.

Par exemple la décomposition de

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 5 & 3 & 4 & 2 & 6 & 7 \end{pmatrix}$$

en cycles de supports disjoints est $(2876)(354) = (354)(2876)$.

8.3 *Inversion et signature*

220 DÉFINITION. Une paire $\{i, j\}$ d'éléments de $\{1, \dots, n\}$ est qualifiée d'*inversion* d'une permutation $f \in \mathrm{S}_n$ si $i < j$ et $f(j) < f(i)$. La *signature* $\mathrm{sgn}(f)$ de f est définie par $\mathrm{sgn}(f) = (-1)^{\mathrm{N}}$ où N est le nombre d'inversions de f. On dit que f est *pair* si $\mathrm{sgn}(f) = 1$ et qu'elle est *impaire* sinon.

221 LEMME. *1. L'identité est une permutation paire.*

2. Toute transposition est une permutation impaire.

Démonstration. 1. L'identité n'a aucune inversion. Donc sa signature est $(-1)^0 = 1$.

2. Les inversions de la transposition (ij) où $i < j$ sont les paires $\{i, j\}$ ainsi que les pairs $\{i, k\}$ et $\{k, j\}$ pour $i < k < j$. Il y en a donc un nombre impair. □

222 REMARQUE. On peut représenter graphiquement une permutation $f \in \mathrm{S}_n$ en plaçant deux copies de l'ensemble $\{1, \dots, n\}$ sur deux lignes parallèles, et en reliant chaque élément i de la ligne du haut à son image $f(i)$ sur la ligne du bas par un segment. Le nombre d'inversions de f est alors égal au nombre de croisements entre ces segments (voir Fig. 14 pour un exemple).

En effet, deux éléments $i < j$ forment une inversion si et seulement si $f(i) > f(j)$, ce qui se traduit géométriquement par un croisement des segments reliant i à $f(i)$ et j à $f(j)$. Cette représentation permet donc de compter visuellement le nombre d'inversions d'une permutation.

Une des propriétés les plus intéressantes de la fonction sgn est qu'elle est multiplicative, au sens énoncé dans le résultat suivant.

223 PROPOSITION. *Pour tous $f, g \in \mathrm{S}_n$ (où $n \geq 1$) on a* $\mathrm{sgn}(f \circ g) = \mathrm{sgn}(f) \times \mathrm{sgn}(g)$.

Démonstration. Nous allons évaluer la valeur de $\mathrm{sgn}(f \circ g)$ en comptant le nombre d'inversions de $f \circ g$. Pour toute paire $\{i, j\}$ avec $1 \leq i < j \leq n$, quatre cas sont possibles, résumés dans le tableau suivant :

Cas	$\{i, j\}$	$\{g(i), g(j)\}$
1	inversion pour g	pas inversion pour f
2	inversion pour g	inversion pour f
3	pas inversion pour g	inversion pour f
4	pas inversion pour g	pas inversion pour f

Pour tout $\ell \in \{1, \ldots, 4\}$, désignons par a_ℓ le nombre de pairs $\{i, j\}$ (où $1 \leq i < j \leq n$) qui satisfont au cas ℓ. Le nombre N d'inversions de g est donc égal à $a_1 + a_2$. De plus, comme g est une bijection, l'ensemble $\{\{g(i), g(j)\} \mid 1 \leq i < j \leq n\}$ est égal à l'ensemble des pairs d'éléments de $\{1, \ldots, n\}$. En particulier, le nombre M d'inversions de f est égal à $a_2 + a_3$. Le nombre d'inversion de $f \circ g$ est quand à lui égal à $a_1 + a_3$.

Au total on a donc

$$\mathrm{sgn}(f \circ g) = (-1)^{a_1+a_3} = (-1)^{\mathrm{N}+\mathrm{M}-2a_2} = (-1)^{\mathrm{N}+\mathrm{M}} = \mathrm{sgn}(f) \times \mathrm{sgn}(g),$$

ce qui conclut la preuve. □

Ce résultat a des corollaires intéressants.

224 COROLLAIRE. *Soit $f \in \mathrm{S}_n$.*

1. *Si f est pair, alors toute décomposition de f en produit de transpositions fait apparaître un nombre pair de transpositions.*
2. *Si f est impair, alors toute décomposition de f en produit de transpositions fait apparaître un nombre impair de transpositions.*
3. *Un cycle de longueur pair est une permutation impair.*
4. *Un cycle de longueur impair est une permutation pair.*
5. *On a* $\mathrm{sgn}(f) = \mathrm{sgn}(f^{-1})$.

Démonstration. 1. et 2. Il s'agit d'appliquer la Proposition 223 au produit de transpositions, en se rappelant que toute transposition est une permutation impair.

3. et 4. On a déjà noté qu'un cycle $(a_1 \cdots a_p)$ de longeur p est le produit $(a_1 a_2) \cdots (a_{p-1} a_p)$ de $p - 1$ transpositions.

5. On a $1 = \mathrm{sgn}(\mathrm{id}) = \mathrm{sgn}(f \circ f^{-1}) = \mathrm{sgn}(f) \times \mathrm{sgn}(f^{-1})$, donc f et f^{-1} ont la même parité. □

9 RENCONTRE AVEC LES GROUPES

Le lecteur ou la lectrice attentif·ve aura peut-être observé qu'un motif se répétait souvent dans les structures algébriques (c'est-à-dire les ensembles munis d'opérations) que nous avons introduites, ou qui ont été introduites au cours d'algèbre linéaire. Il s'agit de celui de groupes.

225 DÉFINITION. Un *groupe* $(G, \odot, e)$ est la donnée d'un ensemble G, d'un élément $e \in G$ et d'une opération binaire $\odot\colon G \times G \to G$, qui satisfont aux conditions suivantes.

1. l'opération $\odot$ est *associative*, c'est-à-dire que pour tout $x, y, z \in G$ on a
$$x \odot (y \odot z) = (x \odot y) \odot z,$$
2. l'élément e est un *neutre* pour $\odot$, c'est-à-dire que pour tout $x \in G$ on a
$$x \odot e = e \odot x = x,$$
3. tout élément x de X, admet un *inverse pour* $\odot$, c'est-à-dire un élément noté x^{-1} tel que
$$x \odot x^{-1} = x^{-1} \odot x = e.$$

Si en plus l'opération $\odot$ est commutative, c'est-à-dire si pour tous $x, y \in G$ on a

$$x \odot y = y \odot x,$$

alors on qualifie $(G, \odot, e)$ de *groupe commutatif* ou de *groupe abélien*[33].

On appelle *ordre de* $(G, \odot, e)$ la cardinal #G de G.

Quelle longue définition, et qui semble bien abstraite ! Nous allons décortiquer de nombreux exemples, afin d'illustrer que la la notion de groupe fournit le châssis commun à de nombreuses structures mathématiques que nous connaissons depuis la plus tendre enfance. N'oubliez pas : faire des mathématiques, c'est généraliser !

Pour comprendre où chercher les exemples, il faut réaliser que nous avons utilisé des symboles $\odot$ et e *génériques*, qu'on appelle en fait *symboles fonctionnels*, et que pour créer un groupe sur un ensemble G il faut pouvoir *instancier* ces symboles par une fonction $G \times G \to G$ et un élément de G, respectivement. Donnons des exemples pour éclairer notre lanterne.

226 EXEMPLE ($\mathbb{Z}$, le groupe des entiers relatifs). Vérifions que la structure additive avec laquelle nous calculons sur $\mathbb{Z}$ depuis notre plus tendre enfance définit une structure de groupe sur $\mathbb{Z}$. Pour cela, il nous faut instancier le symbole $\odot$ par une opération binaire associative $\mathbb{Z}$ et e par son neutre. Un choix naturel est de considérer que l'opération $\odot$ est l'addition $+$ de $\mathbb{Z}$ et $e = 0$. L'inverse d'un élément x de $\mathbb{Z}$ est alors donné par $-x$ (on préfère naturellement la notation $-x$

33. Niels Henrik Abel, mathématicien norvégien du début du 19e siècle.

que x^{-1} dans ce cadre, pour éviter toute confusion). Vérifions ainsi que

$$(\mathbb{Z}, +, 0)$$

est un groupe.

1. L'opération + est associative sur $\mathbb{Z}$ car pour tous [34] $x, y, z \in \mathbb{Z}$ on a $x + (y + z) = (x + y) + z$.
2. L'élément 0 est neutre pour + car pour tous $x \in \mathbb{Z}$ on a $x + 0 = 0 + x = 0$.
3. L'opération − fournit l'inverse des éléments de $\mathbb{Z}$ pour +, c'est-à-dire que pour tous $x \in \mathbb{Z}$, on a $x + (-x) = 0$ et $(-x) + x = 0$

Nous avons montré que $(\mathbb{Z}, +, 0)$ est un groupe, appelé *groupe des entiers relatifs* et noté sobrement $\mathbb{Z}$. De plus, il s'agit d'un groupe commutatif car pour tout $x, y \in \mathrm{Z}$, on a $x + y = y + x$.

Bien-sûr, puisqu'aucune confusion n'est possible, on écrit $x - y$ au lieu de $x + (-y)$.

227 REMARQUE. On peut déjà remarquer que la propriété d'associativité de + sur $\mathbb{Z}$ permet de donner sens à l'écriture $x + y + z$ puisqu'elle peut être également lue par $(x + y) + z$ ou par $x + (y + z)$, ce qui donne le même résultat. Cette observation est valable pour toute opération associative et est donc valable dans tout groupe.

228 EXERCICE. Peut-on définir une structure de groupe sur $\mathbb{Z}$ en choisissant la multiplication comme opération binaire $\odot$? Justifier.

229 EXEMPLE. Si $n \geq 2$ alors $(\mathbb{Z}_n, +, \overline{0})$ est un groupe commutatif fini (c'est-à-dire qu'il possède un nombre fini d'éléments). Le fait que + est associatif sur $\mathbb{Z}_n$, que $\overline{0}$ est le neutre pour + et que $-a$ est l'inverse de a est énoncé dans la Proposition 181.

230 EXEMPLE. Soit p un nombre premier et $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$. Alors $(\mathbb{Z}_p^*, \times, 1)$ est un groupe commutatif. En effet, nous avons déjà remarqué dans la Proposition 181 que l'opération $\times$ est associative et commutative sur $\mathbb{Z}_n$. De plus, comme p est premier, on sait que tout élément $a \neq 0$ de $\mathbb{Z}_p$ admet un inverse a^{-1} pour $\times$. On appelle $(\mathbb{Z}_p^*, \times, 1)$ le *groupe des inversibles de* $\mathbb{Z}_p$.

De la même manière, si on désigne par $\mathbb{R}^*$ l'ensemble des réels non nuls, alors on peut montrer que $(\mathbb{R}^*, \times, 1)$ est un groupe commutatif.

231 EXEMPLE. On peut généraliser l'exemple précédant dans le cas de $\mathbb{Z}_n$ même si n n'est pas premier, mais il faut prendre plus de précautions. Désignons par $\mathbb{Z}_n^*$ l'ensemble $\{\overline{a} \mid \gcd(a, n) = 1\}$. Nous allons montrer que $(\mathbb{Z}_n^*, \times, 1)$ est un groupe, appelé le *groupe des inversibles modulo n*.

Dans un premier temps, nous devons montrer que $\times$ est une opération binaire *interne* à $\mathbb{Z}_n^*$, c'est-à-dire que si $a, b \in \mathbb{Z}_n^*$ alors $a \times b \in \mathbb{Z}_n^*$. Il suffit pour cela de

34. Pour être tout à fait rigoureux, il nous aurait fallu construire la notion de nombre entier relatif à partir de la notion d'ensemble, et définir les opérations + et − à partir de là. C'est l'objet de l'arithmétique de Peano qui dépasse le cadre introductif de ce cours.

prouver que $a \times b$ est inversible dans $\mathbb{Z}_n$. On a

$$(b^{-1} \times a^{-1}) \times (a \times b) = 1 = (a \times b) \times (b^{-1} \times a^{-1}),$$

ce qui prouve que $b^{-1} \times a^{-1}$ est l'inverse de $a \times b$. L'associativité de $\times$, le fait que 1 soit neutre pour $\times$ sont connus. L'existence des inverses est obtenu par construction.

Jusqu'à présent, tous les exemples de groupes que nous avons donnés sont commutatifs. Une question légitimé se pose : est-ce que tous les groupes sont commutatifs ? Non, bien-sûr. Voici un premier exemple de groupe non commutatif.

232 EXEMPLE. Nous allons construire un groupe sur l'ensemble S_3 des permutations de l'ensemble $\{1, 2, 3\}$. Pour cela, il nous faut instancier le symbole $\odot$ de la Définition 225 par une opération binaire associative sur S_3 (qui joue ici le rôle de G). Comme S_3 est constitué de fonctions, on se tourne naturellement vers l'opération de composition $\circ$. Nous avons les propriétés suivantes.

1. L'opération $\circ$ est interne à S_3, c'est-à-dire $\circ : S_3 \times S_3 \to S_3$ par la Proposition 84 (6) et (7).
2. L'opération $\circ$ est associative sur S_3 par la Proposition 84 (1).
3. La fonction identité sur $\{1, 2, 3\}$, que nous notons id, est un neutre pour la composition par la Proposition 84 (2).
4. L'opération $\cdot^{-1}$ de passage à la fonction réciproque est interne à S_3, c'est-à-dire $\cdot^{-1} : S_3 \to S_3$ par la Proposition 84 (4).
5. Pour tout $f \in S_3$, la fonction f^{-1} est l'inverse de f pour la composition par la Proposition (84) 5.

Au total, nous obtenons que $(S_3, \circ, \mathrm{id})$ est un groupe.

Comme S_3 est un petit groupe - il ne contient que 6 éléments - nous pouvons facilement élucider totalement sa structure en construisant sa table de Cayley, comme définie ci-dessous.

233 DÉFINITION. La *table de Cayley* d'un groupe fini $(G, \odot, e)$ est définie comme le tableau à doubles entrées avec les éléments du groupe comme entrées selon les lignes et selon les colonnes, et le résultat de l'opération $a \cdot b$ à l'emplacement correspondant à l'intersection de la ligne correspondant à l'élément a de G et de colonne correspondant à l'élément b de G.

234 EXEMPLE. Désignons par τ la transposition (12) et par σ le cycle (123) vu comme élément de S_3. En effectuant les compositions, on obtient facilement (on omettant le symbole $\circ$ de composition pour alléger les notations) que

$$\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$$

sont 6 éléments distincts de S_3. Comme S_3 contient *exactement* 6 éléments, il

$\circ$	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
id	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	id	$\tau\sigma^2$	τ	$\tau\sigma$
σ^2	σ^2	id	σ	$\tau\sigma$	$\tau\sigma^2$	τ
τ	τ	$\tau\sigma$	$\tau\sigma^2$	id	σ	σ^2
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	τ	σ^2	id	σ
$\tau\sigma^2$	$\tau\sigma^2$	τ	$\tau\sigma$	σ	σ^2	id

TABLE 1 – Cayley table for S_3

s'agit donc de l'ensemble des éléments de S_3. Nous obtenons que

$$\sigma\tau = (13) = \tau\sigma^2.$$

Cette relation, qui illustre que S_3 n'est pas un groupe commutatif, nous permet de produire la table de Cayley de $(S_3, \circ, \mathrm{id})$ dans la Tab. 1.

Remarquez que toute ligne ou toute colonne de cette table est une permutation des éléments de S_3. Cette observation se généralise dans le lemme suivant.

235 LEMME. *Si $(G, \circ, e)$ est un groupe et si $a \in G$ alors l'application $g_a : G \to G$ (resp. $d_a : G \to G$) de multiplication à gauche (resp. à droite) par a définie par $g_a(b) = ab$ (resp. $d_a(b) = ba$) est une bijection.*

En particulier, toute ligne ou colonne d'une table de Cayley d'un groupe fini est une permutation des éléments du groupe[35].

Démonstration. Nous le prouvons pour g_a, le cas de m_a se prouve de manière symétrique.

Par un exercice vu en TD, il suffit de prouver que $g_a \circ g_{a^{-}1} = g_{a^{-}1} \circ g_a = \mathrm{id}$, ce qui est évident.

De manière alternative, nous pouvons montrer que g_a est injective et surjective. Si $b, b' \in G$ sont tels que $g_a(b) = g_a(b')$, on a $ab = ab'$. En multipliant à gauche par a^{-1}, on obtient $b = b'$. On a prouvé l'injectivité de g_a. Par ailleurs, pour tout $b \in G$, on a $g_a(a^{-1}b) = b$, ce qui prouve la surjectivité de g_a. □

236 EXERCICE. Donnez la table de Cayley de $\mathbb{Z}_6$.

237 EXERCICE. Donner la table de Cayley de $\mathbb{Z}_{12}^*$.

238 EXEMPLE. L'Exemple 232 se généralise directement à l'ensemble de permutations d'un ensemble E quelconque. Pour tout ensemble E, on a $(S_E, \circ, \mathrm{id})$ est un groupe. L'élément f^{-1} d'un élément f de E est donné par la fonction réciproque de f.

Donnons un dernier exemple issu de votre cours d'algèbre linéaire.

239 EXEMPLE. Soit $n \geq 1$ et désignons par $GL_n(\mathbb{R})$ l'ensemble des matrices carrés

35. Est-ce que la réciproque est vraie ? Pourquoi ?

inversibles de taille n à coefficients dans $\mathbb{R}$. Montrons que $(\mathrm{GL}_n(\mathbb{R}), \cdot, \mathrm{I})$, où $\cdot$ désigne le produit matriciel et I la matrice identité (de taille n).

1. Le produit matriciel $\cdot$ est associatif (voir cours d'algèbre linéaire, mais vous pouvez faire la démonstration à la main en recourant directement à la définition du produit matriciel).
2. Pour tout $\mathrm{A} \in \mathrm{GL}_n(\mathbb{R})$ on a $\mathrm{A} \cdot \mathrm{I} = \mathrm{I} \cdot \mathrm{A} = \mathrm{A}$, ce qui montre que I est neutre pour $\cdot$
3. Comme $\mathrm{GL}_n(\mathbb{R})$ est constitué des matrices carrées de taille n qui sont inversibles (*i.e.*, de déterminant non nul), l'inverse A^{-1} de toute matrice A de $\mathrm{GL}_n(\mathbb{R})$ existe et appartient à $\mathrm{GL}_n(\mathbb{R})$ (elle peut par exemple être calculée à l'aide des la matrice des cofacteurs). On a $\mathrm{A} \cdot \mathrm{A}^{-1} = \mathrm{A}^{-1} \cdot \mathrm{A} = \mathrm{I}$.

Ainsi $(\mathrm{GL}_n(\mathbb{R}), \cdot, \mathrm{I})$ est un groupe. Il n'est pas commutatif pour $n \geq 2$ car le produit matriciel n'est pas commutatif.

Donnons quelques propriétés élémentaires des groupes.

240 PROPOSITION. *Soit* $(\mathrm{G}, \odot, e)$ *un groupe.*

1. *Le neutre e est unique, c'est-à-dire si e' est un élément de* G *tel que pour tout* $x \in \mathrm{G}$ *on a* $x \cdot e = e \cdot x = x$*, alors* $e' = e$*.*
2. *L'inverse d'un élément x est unique, c'est-à-dire si* $a, b, c \in \mathrm{G}$ *sont tels que* $ab = ba = e$ *et* $ac = ca = e$ *alors* $b = c$*.*
3. *Pour tout* $a \in \mathrm{G}$ *on a* $(a^{-1})^{-1} = a$*.*

Démonstration. 1. Comme e est un neutre on a $e' \odot e = e'$. Comme e' est un neutre on a $e' \odot e = e$.

2. Il vient $ab = e$, donc en multipliant à gauche par c on a $cab = c$, c'est-a-dire b=c.

3. Découle directement de 2. et des identités $a \odot a^{-1} = a^{-1} \odot a = e$. □

241 EXERCICE. Soit T un triangle équilatéral. On appelle *isométrie de* T toute bijection $f : \mathrm{T} \to \mathrm{T}$ qui préserve les mesures d'angle et les longueurs des côtés de T. Prouver que l'ensemble des isométries de T forment un groupe pour la loi de composition $\circ$. Déterminer la table de Cayley de ce groupe.

242 NOTATION. La propriété d'associativité permet de donner sens à la notation suivante. Pour tout élément a d'un groupe $(\mathrm{G}, \odot, e)$ et pour tout $n \geq 0$ on note a^n le produit $a \odot \cdots \odot a$ de n facteurs a. On pose également $a^0 = e$ et $a^{-n} = (a^{-1})^n$.

243 EXERCICE. Pour tous éléments $a_1, \ldots, a_\ell$ d'un groupe $(\mathrm{G}, \odot, e)$, prouvez que

$$(a_1 \odot a_2 \odot \cdots \odot a_\ell)^{-1} = a_\ell^{-1} \odot a_{\ell-1}^{-1} \odot \cdots \odot a_1^{-1}.$$

9.1 *Homomorphisme*

En mathématiques, l'étude des structures s'accompagne généralement d'une considération des transformations qui les affectent. Chaque type de structure

possède une notion naturelle de transformation, souvent incarnée par une famille de fonctions préservant en partie la structure. Dans le domaine de l'algèbre linéaire, on analyse les espaces vectoriels et les transformations linéaires qui les altèrent. De même, la géométrie du triangle explore les triangles et les isométries ainsi que les similitudes qui les caractérisent. En théorie des groupes, la transformation naturelle est désignée sous le nom d'*homomorphisme* (de groupe) et est définie de la manière suivante.

244 DÉFINITION. Soient $(G, \odot, e)$ et $(G', \odot', e')$ deux groupes. Une application $f : G \to G'$ est qualifiée d'*homomorphisme* entre $(G, \odot, e)$ et $(G', \odot', e')$ si pour tous $x, y \in G$ on a $f(x \odot y) = f(x) \odot' f(y)$.

Un *isomorphisme* (de groupes) est un homomorphisme bijectif. S'il existe un isomorphisme entre deux groupes $(G, \circ, e)$ et $(G', \circ', e')$, on dit qu'ils sont isomorphes, et on écrit $(G, \circ, e) \cong (G, \circ, e')$.

Donc, un homomorphisme de groupe est une application qui respecte la structure define par le produit $\odot$. Mais en fait, elle respecte également l'opération de passage à l'inverse et le neutre, comme le montre la proposition suivante.

245 PROPOSITION. *Soient* $(G, \odot, e)$ *et* $(G', \odot', e')$ *deux groupes et* $f : G \to G'$ *un homomorphisme.*

1. *On a* $f(e) = e'$.
2. *Pour tout* $x \in G$, *on a* $f(x^{-1}) = f(x)^{-1}$.

Démonstration. 1. Nous avons $f(e) = f(e \odot e) = f(e) \odot' f(e)$. En multipliant par $f(e)^{-1}$ à gauche on obtient $e' = f(e)$.

2. On a $f(x^{-1}) \odot' f(x) = f(x^{-1} \odot x) = f(e) = e'$ et $f(x) \odot' f(x^{-1}) = f(x \odot x^{-1}) = f(e) = e'$. Donc $f(x^{-1}) = f(x)^{-1}$ par unicité de l'inverse dans $(G', \odot', e')$. □

Donnons quelques exemples.

246 EXEMPLE. L'application $\imath : (\mathbb{Z}, +, 0) \to (\mathbb{R}, +, 0)$ définie par $\imath(x) = x$ est un homomorphisme de groupe. En effet, il vient naturellement

$$\imath(x + y) = x + y = \imath(x) + \imath(y)$$

pour tous $x, y \in \mathbb{Z}$.

L'exemple suivant est plus intéressant et plus fondamental.

247 EXEMPLE. L'application $\pi : \mathbb{Z} \to \mathbb{Z}_3$ définie par $\pi(z) = \overline{z}$ est un homomorphisme de $(\mathbb{Z}, +, 0)$ dans $(\mathbb{Z}_3, +, \overline{0})$. En effet, pour tous $x, y \in Z$ on a successivement

$$\pi(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \pi(x) + \pi(y),$$

où la deuxième égalité découle de la définition de + dans $\mathbb{Z}_3$. Mieux, on peut affirmer que la structure de groupe que nous avons définie sur $\mathbb{Z}_3$ est la seule structure de groupe qui soit telle que $\pi : \mathbb{Z} \to \mathbb{Z}_3$ est un homomorphisme.

Cette exemple se généralise directement au cas de $\pi\colon \mathbb{Z} \to \mathbb{Z}_n$ pour $n \geq 2$.

248 EXEMPLE. L'application $f : \mathbb{Z}_4 \to \mathbb{Z}_4$ définie par

$$f(0) = 0, \quad f(1) = 3, \quad f(2) = 2, \quad f(3) = 1,$$

est un isomorphisme de $(\mathbb{Z}_4, +, 0)$ dans lui même.

249 PROPOSITION. *Soit $f\colon (G, \odot, e) \to (G', \odot', e')$ et $g\colon (G', \odot', e') \to (G'', \odot'', e'')$ deux homomorphismes de groupes.*

1. *Alors $g \circ f : (G, \odot, e) \to (G'', \odot', e')$ est un homomorphisme.*
2. *Si f est un isomorphisme, alors f^{-1} l'est aussi.*

Démonstration. 1. Pour tous $x, y \in X$, il vient successivement

$$\begin{aligned}(g \circ f)(x \odot y) = g(f(x \odot y)) &= g(f(x) \odot' f(y)) \\ &= g(f(x)) \odot'' g(f(y)) = (g \circ f)(x) \odot'' (g \circ f)(y),\end{aligned}$$

où la deuxième égalité est obtenue parce que f est un homomorphisme, et la troisième parce que g est un homomorphisme.

2. Soit $x, y \in G'$ et prouvons que

$$f^{-1}(x \odot' y) = f^{-1}(x) \odot f^{-1}(y),$$

ce qui est équivalent, par définition de la fonction réciproque à

$$f(f^{-1}(x \odot' y)) = f(f^{-1}(x) \odot f^{-1}(y)), \tag{22}$$

D'une part on a $f(f^{-1}(x \odot' y)) = x \odot' y$ puisque $f \circ f^{-1} = \mathrm{id}$. D'autre part on

$$f(f^{-1}(x) \odot f^{-1}(y)) = f(f^{-1}(x)) \odot' f(f^{-1}(x)) = x \odot y',$$

où la deuxième égalité est obtenue parce que f est un homomorphisme. Nous avons prouver l'identité (22). □

250 EXEMPLE. Pour tout $n \geq 2$, l'application $f\colon (S_n, \circ, e) \to (\mathbb{Z}_2, +, \overline{0})$ définie par $f(\sigma) = 0$ si σ est une permutation pair et $f(\sigma) = 1$ si σ est une permutation impair, est un homomorphisme. Nous allons procéder en deux étapes. Notons d'abord que l'application $\mathrm{sgn}\colon (S_n, \circ, \mathrm{id}) \to (\mathbb{Z}_3^*, \times, 1)$ est un homomorphisme. C'est en effet ce qu'affirme la Proposition 223. Par ailleurs, l'application $g\colon (\mathbb{Z}_3^*, \times, 1) \to (\mathbb{Z}_2, +, \overline{0})$ définie par $g(\overline{1}) = \overline{0}$ et $g(\overline{-1}) = \overline{1}$ est un isomorphisme. Au total, l'application $f \circ \mathrm{sgn}$ est un homomorphisme entre $(S_n, \circ, e)$ et $(\mathbb{Z}_2, +, \overline{0})$.

L'isomorphisme permet d'identifier deux groupes dont la structure est essentiellement identique. En fin de compte, deux groupes isomorphes ne se distinguent que par les noms attribués à leurs éléments. La théorie des groupes consiste à étudier les propriétés des groupes à isomorphisme près, c'est-à-dire

les propriétés qui sont préservées par isomorphismes.

251 EXERCICE. Prouver que la relation $\cong$ entre groupes est une relation d'équivalence sur la classe des groupes.

252 EXERCICE. Soit $(G, \odot, e)$ un groupe. On appelle *automorphisme* de $(G, \odot, e)$ tout isomorphisme de $(G, \odot, e)$ dans lui-même. On note $\mathrm{Aut}(G, \odot, e)$ l'ensemble des automorphismes de $(G, \odot, e)$. Prouver que $(\mathrm{Aut}(G, \odot, e), \circ, \mathrm{id})$ est un groupe.

Par exemple, pour prouver que deux groupes ne sont pas isomorphes, il suffit de trouver une propriété préservée par isomorphisme détenue par le premier groupe et absente du second.

253 EXEMPLE. Les groupes $(\mathbb{R}^*, \times, 1)$ et $(\mathrm{GL}_n(\mathbb{R}), \cdot, \mathrm{I})$ ne sont pas isomorphes car le premier est commutatif alors le second ne l'est pas. Or la propriété de commutativité est préservée par isomorphisme, c'est-à-dire que s'il existait un isomorphisme $f : (\mathbb{R}^*, \times, 1) \to (\mathrm{GL}_n(\mathbb{R}), \cdot, \mathrm{I})$ alors $(\mathrm{GL}_n(\mathbb{R}), \cdot, \mathrm{I})$ serait commutatif.

254 EXEMPLE. Soit $K = \{a, b, c, e\}$ et $\odot : K \to K$ qui satisfait les conditions

$$a \odot a = e, \quad b \odot b = e, \quad a \odot b = b \odot a = c, \quad e \text{ est neutre pour } \odot.$$

1. Prouvons qu'il existe un seul groupe $(G, \odot, e)$ qui satisfait aux conditions ci-dessus.
2. Prouvons que $(G, \odot, e)$ n'est pas isomorphe à $\mathbb{Z}_4$.

Pour 1, on note qui si un tel groupe existe, on doit avoir

$$c^2 = a \odot b \odot b \odot a = a \odot e \odot a = e$$

et

$$c \odot a = b \odot a \odot a = b, \quad c \odot b = a \odot b \odot b = a,$$

ainsi que

$$a \odot c = a \odot a \odot b = b, \quad b \odot c = b \odot b \odot a = a.$$

Nous avons calculés toutes les valeurs de $x \odot y$ pour $x, y \in K$ et obtenu que $\odot$ commutatif.

Nous prouvons maintenant que l'opération $\odot$ ainsi obtenue définit une structure de groupe. Sous ces conditions, pour prouver que $\odot$ est associatif, seule l'identité $a \odot (b \odot c) = (a \odot b) \odot c$ n'est pas triviale. Or, il vient

$$a \odot (b \odot c) = a \odot a = e$$

$$(a \odot b) \odot c = c \odot c = e,$$

d'où découle donc l'associativité de $\odot$. Pour prouver que e est neutre pour $\odot$, seule l'identité $c \odot e = c$ n'a pas encore été obtenue. On a $c \odot e = c \odot c \odot c = c$.

Finalement, nous avons par construction

$$x^{-1} = x \qquad \forall x \in \mathrm{K}.$$

Nous avons prouvé qu'il y a un et un seul groupe qui satisfait aux conditions de l'énoncé. On l'appelle le *groupe de Klein* [36].

2. On note simplement que dans $(\mathrm{G}, \odot, e)$ tous les élément satisfaits l'équation $x \odot x = e$, alors que dans $\mathbb{Z}_4$, on $\overline{3} + \overline{3} \neq \overline{0}$.

9.2 *Sous-groupes*

Le sous-espaces vectoriels ont droit à leurs sous-espaces. Similairement les groupes ont droit à leur sous-groupes. Informellement, un sous-groupe d'un groupe $(\mathrm{G}, \odot, e)$ est un sous-ensemble H de G qui devient un groupe s'il est équipé de la restriction à H de la structure de groupe de G. Cette idée se formalise de la manière suivante.

255 DÉFINITION. Soit $(\mathrm{G}, \odot, e)$ un groupe et H une partie non vide de G. On dit que H est un *sous-groupe* de G si pour tous $x, y \in \mathrm{H}$ on a $x^{-1} \in \mathrm{H}$ et $x \odot y \in \mathrm{H}$.

256 PROPOSITION. *Si* $(\mathrm{G}, \odot, e)$ *est un groupe et* H *est un sous-groupe de* G *alors* $(\mathrm{H}, \odot, e)$ *est un groupe.*

Démonstration. Nous devons prouver les assertions suivantes.

1. La fonction $\odot$ est *interne à* H, c'est-à-dire si $x, y \in \mathrm{H}$ alors $x \odot y \in \mathrm{H}$.
2. Le neutre e de G appartient à H.

Nous saurons alors que $\odot \colon \mathrm{H} \times \mathrm{H} \to \mathrm{H}$ est une opération binaire associative (elle l'est sur G qui contient H) de neutre e (qui appartient à H). Nous prouverons également que

3. pour tout $x \in \mathrm{H}$ il existe $x^{-1} \in \mathrm{H}$ tel que $x \odot x^{-1} = x^{-1} \odot x = e$.

Pour 1, on note que cette assertion est vraie par définition de la notion de sous-groupe. Pour 2, on choisit un élément x de H (c'est possible car un sous-groupe est non vide). Comme H est un sous-groupe on a $x^{-1} \in \mathrm{H}$ donc $e = x \odot x^{-1} \in \mathrm{H}$. Pour 3, il suffit de choisir l'inverse x^{-1} de x dans G. Cet élément appartient à H par définition de la notion de sous-groupe. □

Par définition, si $(\mathrm{G}, \odot, e)$ est un groupe, alors G et $\{e\}$ en sont des sous-groupes. Considérons quelques autres exemples.

257 EXEMPLE. On a que $\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +, 0)$.

258 EXEMPLE. On a $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ est un sous-groupe de $\mathbb{Z}_8$.

259 EXEMPLE. Si σ est la permutation (123) alors $\{\mathrm{id}, \sigma, \sigma^2\}$ est un sous-groupe de S_3.

36. Félix Klein, 1849-1925.

260 EXEMPLE. Soit H le sous-ensemble de $\mathrm{GL}_n(\mathbb{R})$ constitué des éléments

$$\mathrm{I} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{A} := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{B} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathrm{C} := \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

1. Montrons que H est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.
2. Montrons que $(\mathrm{H}, \cdot, \mathrm{I})$ est isomorphe au groupe de Klein.

Pour 1, on note d'abord que comme les éléments de H sont des matrices diagonales, elles commutent entre elles. Pour vérifier que $\cdot$ est interne à H il suffit donc de prouver que AB, AC, BC $\in$ H, ce qui est un simple calcul. Enfin, pour tout X $\in$ H on a $\mathrm{X}^{-1} = \mathrm{X}$ est un élément de H.

Pour 2, nous adoptons les notations de l'Exemple 254 pour désigner les éléments du groupe de Klein $(\mathrm{K}, \odot, e)$. Un isomorphisme $f : (\mathrm{K}, \odot, e) \to (\mathrm{H}, \cdot, \mathrm{I})$ est donné par $f(a) = \mathrm{A}$, $f(\mathrm{B}) = b$, $f(\mathrm{C}) = c$ et $f(e) = \mathrm{I}$. Pour le vérifier, comme les opérations $\odot$ et $\cdot$ sont commutatives, il suffit de vérifier que

$$f(a \odot b) = \mathrm{A} \cdot \mathrm{B}, \quad f(a \odot c) = \mathrm{A} \cdot \mathrm{C}, \quad f(b \odot c) = \mathrm{B} \cdot \mathrm{C},$$

ce qui est une simple vérification.

Il y a une façon générique de créer des sous-groupes. Il s'agit de recourir à au noyau et à l'image d'un homomorphisme, comme définis ci-dessous.

261 DÉFINITION. Soit $f : (\mathrm{G}, \odot, e) \to (\mathrm{G}', \odot', e')$ un homomorphisme de groupe. On appelle *noyau* $\ker(f)$ *de* f l'ensemble $f^{-1}(e')$. On appelle *image* $\mathrm{im}(f)$ de f l'ensemble $f(\mathrm{G})$.

262 REMARQUE. Les lecteur·rice·s attentives auront remarqué que nous avons surchargé la notation $\ker(f)$. En effet dans l'Exemple 121 nous avons défini $\ker(f)$ comme une relation d'équivalence définie par $(x, y) \in \ker(f)$ si et seulement si $f(x) = f(y)$. Montrons que cette surcharge de notation est cohérente en montrant que dans le cas d'un homomorphisme de groupes $f : (\mathrm{G}, \odot, e) \to (\mathrm{G}', \odot', e')$, la connaissance de la relation $\ker(f)$ est équivalente à la connaissance de $f^{-1}(e')$ au sens suivant. Pour tout $x, y \in \mathrm{G}$ on a

$$(x, y) \in \ker(f) \iff x \odot y^{-1} \in f^{-1}(e').$$

Il vient successivement

$$\begin{aligned} (x, y) \in \ker(f) &\iff f(x) = f(y) \\ &\iff f(x) \odot' f(y)^{-1} = e' \\ &\iff f(x \odot y^{-1}) = e' \\ &\iff x \odot y^{-1} \in f^{-1}(e'), \end{aligned}$$

ce qui est l'équivalence recherchée.

263 PROPOSITION. *Soit* $f : (G, \odot, e) \to (G', \odot', e')$ *un homomorphisme de groupe.*

1. $\ker(f)$ *est un sous-groupe de* $(G, \odot, e)$.
2. $\mathrm{im}(f)$ *est un sous-groupe de* $(G, \odot', e')$.

Démonstration. 1. Notons que $\ker(f)$ est non vide puisqu'il contient e. Ensuite, si $x, y \in \ker(f)$ alors $f(x) = e' = f(y)$. Donc $f(x \odot y) = f(x) \odot f(y) = e' \odot e' = e'$, ce qui prouve que $x \odot y \in \ker(f)$. Enfin si $x \in \ker(f)$ alors $f(x) = e$ donc $f(x^{-1}) = f(x)^{-1} = e$ et $x^{-1} \in \ker(f)$.

2. On note que $\mathrm{im}(f)$ est non vide car il contient $e' = f(e)$. Ensuite, si $x, y \in \mathrm{im}(f)$ alors il existe $x_0, y_0 \in G$ tels que $x = f(x_0)$ et $y = f(y_0)$. Donc $x \odot' y = f(x_0) \odot' f(y_0) = f(x_0 \odot y_0)$. Donc $x \odot' y \in \mathrm{im}(f)$. De plus $x^{-1} = f(x_0)^{-1} = f(x_0^{-1})$ donc $x^{-1} \in \mathrm{im}(f)$. □

264 EXERCICE. Soit $\pi : (\mathbb{Z}_6, +, \overline{0}) \to (\mathbb{Z}_3, +, \overline{0})$ l'application définie par $\pi(\overline{a}) = \overline{a\%3}$. Prouvez que π est un homomorphisme et calculer $\ker(\pi)$ et $\mathrm{im}(\pi)$.

Un vaste champ à investiguer

Nous avons seulement égratigné la surface de la théorie des groupes. Il s'agit d'une domaine extrêmement vaste qui est étudié pour son intérêt propre, mais aussi parce que les groupes fournissent un outil pour investiguer d'autres structures mathématiques, ou physiques. Les lecteur·rice·s intéressées par pousser plus loin leur apprentissage pour se référer à [4], par exemple.

Letter	Capital Letter	Name
α	A	Alpha
β	B	Beta
γ	Γ	Gamma
δ	Δ	Delta
ϵ	E	Epsilon
ζ	Z	Zeta
η	H	Eta
θ	Θ	Theta
ι	I	Iota
κ	K	Kappa
λ	Λ	Lambda
μ	M	Mu
ν	N	Nu
ξ	Ξ	Xi
o	O	Omicron
π	Π	Pi
ρ	P	Rho
σ	Σ	Sigma
τ	T	Tau
υ	Υ	Upsilon
ϕ	Φ	Phi
χ	X	Chi
ψ	Ψ	Psi
ω	Ω	Omega

Table 2 – Alphabet Grec

10 APPENDICE - ALPHABET GREC

Les mathématicien·ne·s utilisent souvent l'alphabet grec en complément de l'alphabet romain pour rédiger leur résultats. Il est bon de se familiariser d'emblée avec cet alphabet classique, présenté dans la Tab. 2.

RÉFÉRENCES

[1] A. Bauer. Five Stages of Accepting Constructive Mathematics. *Bulletin of the American Mathematical Society*, 54(3) :481 – 498, 2016.

[2] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge University Press, 2002.

[3] R. Hammack. *The Book of Proofs.* Third edition. 2018. Available online at `https://www.people.vcu.edu/~rhammack/BookOfProof/`.

[4] Joseph J. Rotman. *An Introduction to the Theory of Groups.* Fourth edition. Springer, 1995.