Axiomes et nombres

Gijs M. Tuynman

Table des matières

Préface 5

Introduction 7

Chapitre 1. Des axiomes 11
1. Les 5 premiers axiomes 11
2. Le produit Cartésien 19
3. Relations et relations d'ordre 23
4. Applications 28
5. Quelques résultats classiques 32
6. Ensembles infinis et la construction de **N** 35
7. Dedekind, Peano et Landau 39

Chapitre 2. Des nombres 45
8. Les opérations sur **N** 45
9. Relations d'équivalences 52
10. Construction des nombres rationnels positifs 61
11. Construction de **Z** 66
12. Multiples et puissances avec un entier naturel 81
13. Multiples et puissances avec un entier relatif 86
14. Construction de **Q** 93
15. Construction de **R** par coupures de Dedekind 102
16. Le symbole $\sum$ 111
17. Le développement décimal d'un réel 115

Chapitre 3. Des choix 119
18. L'axiome du choix 119
19. La trinité du choix 125
20. Ne fait qu'une 134

Chapitre 4. Comparer la taille d'ensembles 137
21. Introduction 137
22. Applications injectives et surjectives 140
23. Définition de la comparaison 142
24. L'exponentielle d'ensembles 146
25. Ensembles finis 150
26. Ensembles dénombrables 152
27. Arithmétique d'ensembles infinis 154

Chapitre 5. Ordinaux et cardinaux 157
28. Ordinaux 157
29. L'axiome de remplacement 163
30. Ensembles bien ordonnés et ordinaux 168
31. Cardinaux 171

32. L'axiome de fondation 177

Chapitre 6. Les preuves 179

La liste des axiomes 297

Bibliographie 299

Préface

AVERTISSEMENT : ce texte est très loin d'être achevé. Il comporte certainement des erreurs d'une gravité variable. De certaines je suis au courant mais je n'ai pas encore eu le temps de les corriger ; d'autres me sont (encore) inconnues. Mais je pense qu'il est suffisamment avancé que des étudiants peuvent en tirer du profit. Je remercie d'avance tout lecteur qui aura la gentillesse de me faire parvenir ses remarques, critiques et corrections.

Ce texte est destiné à des lecteurs avec une certaine expérience en mathématique et en particulier aux étudiants en troisième année d'étude de mathématique à l'université. Mais il ne faut pas confondre expérience avec connaissances, car les prérequis en termes de connaissances sont minimales. À part une familiarité avec les notation ensemblistes, la logique élémentaire et les connaissances de bases acquis à l'école maternelle et au collège, aucune connaissance précise est nécessaire (bien qu'on utilisera de temps en temps des mathématiques un peu plus avancées dans les exemples). Par contre, l'expérience d'au moins une année d'étude en mathématiques à l'université est souhaitable pour pouvoir apprécier ce texte.

Le but est de combler une lacune dans l'enseignement des mathématiques aujourd'hui : la *construction* des nombres et la *connaissance* des axiomes de bases de la théorie des ensembles. Trop souvent on prend l'existence des entiers naturels comme acquis, aussi bien que l'existence des nombres réels. Pour le dernier on se contente d'énoncer la propriété de l'existence d'une borne supérieur (pour tout ensemble de réels majoré). On parle de temps en temps de l'axiome du choix, on prononce l'acronyme ZFC, mais on ne rentre (presque) jamais dans plus de détail. Pourtant, l'axiomatique de Zermelo et Fraenkel (le Z et le F dans ZFC) est à la base de toutes les mathématiques "modernes." En conséquence, pour un lecteur avec une certaine expérience en mathématique, les chapitres sont (presque) indépendants dans le sens que les *résultats* qu'on démontre dans chaque chapitre sont (fort probablement) connus par un tel lecteur. Mais les preuves sont peut-être inconnues ; on les fournira en tout détail. L'état d'esprit de ce texte est (donc) le même que celui du livre **[Lan51]** de Landau. Ce dernier traite aussi, et en autant de détail, la construction des nombres usuels. Ici on est plus modeste dans le sens qu'on n'exhorte pas l'étudiant fraîchement arrivé du lycée d'oublier tout ce qu'il sait sur les nombres. Mais on est plus ambitieux dans les sens qu'on parle aussi de la théorie axiomatique des ensembles ainsi que des (nombres) ordinaux et cardinaux.

Au niveau des notations et des symboles, on se sert des symboles $\Rightarrow$, $\Leftrightarrow$ et $\Leftarrow$ pour indiquer l'implication directe, l'équivalence logique et l'implication inverse respectivement. Les opérateur logique "et" et "ou" seront toujours écrites en toutes lettres. Par contre, l'opérateur de négation sera notée $\neg$: si p est une formule logique, alors $\neg\, p$ est sa négation. Par exemple pour un nombre réel x la négation de $x > 1$ est notée $\neg(x > 1)$; c'est équivalent à $x \leq 1$. Si la formule logique est formée par une opération binaire entre deux objets comme ci-dessus $x > 1$, alors la négation sera aussi écrit en mettant une barre dans le symbole de l'opération binaire. Dans

l'exemple de $x > 1$ on écrit donc sans distinction $\neg(x > 1)$, $x \leq 1$ et $x \not> 1$. Les symboles $\exists$ et $\forall$ désignent les quantificateurs existentiel et universel respectivement. On ne les utilise pas seulement sous la forme "libre" comme $\forall A$ ou $\exists x$, mais aussi sous la forme "restreinte" comme $\forall x \in A$ ou $\exists y > 1$. Si $p(x)$ est une formule logique avec une variable libre x, alors

$$\forall x \in A : p(x) \quad \text{est une abréviation pour} \quad \forall x : x \in A \Rightarrow p(x)$$

et

$$\exists y > 1 : p(y) \quad \text{est une abréviation pour} \quad \exists y : y > 1 \text{ et } p(y) \ .$$

Gijs M. Tuynman

Lille, 27 juin 2019

Introduction

Tout mathématicien connaît les entiers naturels $\mathbf{N}$, les entiers relatifs $\mathbf{Z}$, les nombres rationnels $\mathbf{Q}$, les nombres réels $\mathbf{R}$ et les nombres complexes $\mathbf{C}$. Mais si on se pose la question ce que sont exactement ces nombres, souvent on est obligé d'avouer qu'on ne sait pas trop. C'est exactement la question que s'est posé Dedekind. En 1872 il publia un article [**Ded72**] sur la construction des nombres réels à partir des nombres rationnels. Et en 1887 il publia un article [**Ded87**] sur la construction des entiers naturels. Quant à la construction des entiers relatifs $\mathbf{Z}$ à partir de $\mathbf{N}$ et la construction des nombres rationnels $\mathbf{Q}$ à partir de $\mathbf{Z}$, elles sont "simples" et n'ont jamais été l'objet d'une publication spéciale.

La construction de Dedekind des réels à l'aide de coupures n'est plus tellement enseigné aujourd'hui, on préfère la construction de $\mathbf{R}$ à l'aide des suites de Cauchy. Cette préférence pour les suites de Cauchy s'explique par le fait que cette méthode se généralise très facilement à la complétion d'un espace métrique quelconque. Mais conceptuellement la construction de Dedekind est plus simple et plus facile à utiliser dans les preuves des propriétés de $\mathbf{R}$. En plus elle peut être copié sans problèmes dans le language moderne ; on le fera au §15.

En ce qui concerne la construction des entiers naturels, ce n'est que très rarement qu'on en parle dans un cursus mathématique universitaire d'aujourd'hui. En plus, la construction de $\mathbf{N}$ par Dedekind a une petite zone d'ombre due à l'utilisation d'arguments concernants l'existence de certains ensembles, arguments qui ne sont plus acceptables aujourd'hui. À part ce détail de l'existence d'un ensemble, la construction de Dedekind se traduit facilement dans le language moderne. Dans §6 et §7 on présentera cette construction dans une version qui tient compte des axiomes qui lèvent la zone d'ombre.

À l'époque où Dedekind écrivit son traité sur la construction des nombres, on commençait à se poser des questions sur la nature des ensembles. Intuitivement un ensemble est une collection d'objets et on peut voir un ensemble comme un objet en soi. Cette idée imprécise d'un ensemble conduit rapidement à des contradictions comme le paradoxe de Russell que voici. On considère la collection U de toutes les collections. Par définition on doit donc avoir $U \in U$. Dans cet univers U on regarde la sous-collection $P \subset U$ de toutes les collections C qui ont la propriété $C \notin C$, ce qu'on écrit comme

$$P = \{\, C \in U \mid C \notin C \,\} \ .$$

P étant une collection, on a $P \in U$ et on peut se poser la question si on a $P \in P$ ou $P \notin P$. Dans le premier cas, selon la définition de P, on doit avoir $P \notin P$, ce qui est en contradiction avec le fait qu'on a supposé $P \in P$. Mais dans le deuxième cas, de nouveau par la définition de P, la collection P doit être membre de P, ce qui contredit l'hypothèse $P \notin P$. Ce paradoxe est l'équivalent mathématique du paradoxe du barbier qui ne rase que les gens qui ne se rasent pas eux-mêmes ; est-ce-que le barbier se rase lui-même ?

La solution adoptée par les mathématiciens n'est pas de dire qu'il faut abandonner le concept d'ensemble, mais qu'il faut restreindre le domaine d'application, c'est-à-dire qu'il faut accepter qu'il y a des collections qui n'ont pas le droit d'être appelées ensemble. Plus précisément, on garde la notion intuitive de collection, mais on accorde le label "ensemble" à certaines collections. En gros, il y a une sorte de garantie que les collections qui comportent ce label ne nous conduisent pas à des contradictions, contrairement aux collections sans ce label, dont on ne sait jamais si on ne tombe dans des pièges. Ainsi l'univers U et la sous-collection P n'ont pas le droit d'être appelée "ensemble." Et même plus précis, la collection de tous les ensembles (qui est donc plus petite que la collection de toutes les collections) n'a pas le droit d'être appelée un ensemble, car on aura le même paradoxe. La grande question devient alors : quelles seront les collections qui auront le label "ensemble" ? Posée comme telle, cette question est ambitieuse, car elle demande un critère qui nous dit quand une collection aura ce label. Une question moins ambitieuse est : quelles sont les procédures/constructions qui nous permettent de construire de nouveaux ensembles à partir de collections qui ont déjà le label "ensemble" ?

Un système d'axiomes pour la théorie des ensembles est une réponse à cette question moins exigeante, car, grosso modo, chaque axiome nous donne une procédure pour créer un nouvel ensemble à partir d'autres ensembles. Zermelo a été le premier, en 1908, à fournir un système d'axiomes pour la théorie des ensembles. Aujourd'hui il existe plusieurs systèmes d'axiomes différentes pour la théorie des ensembles, mais les différences sont plus de nature philosophique que pratique. Plus précisément, les différences n'ont pas d'incidence sur la pratique des mathématiciens "ordinaires." Par contre, pour les spécialistes de la théorie des ensembles, les logiciens et les philosophes, les différences ont toute leur importance. Dans ce texte on présentera le système le mieux connu, appelé le système ZF ou ZFC. C'est le système élaboré par Zermelo en 1908 et complété en 1922 par Fraenkel. La différence entre ZF et ZFC est que le dernier inclut l'axiome du choix, qu'on exclut quand on parle du système ZF. Le système ZF comporte 9 axiomes, mais on montrera que dans la pratique d'un mathématicien "ordinaire" on n'utilise que 7 parmi ces 9 axiomes. Et notamment on n'utilise pas l'axiome ajouté en 1922 par Fraenkel. Quant à l'utilisation de l'axiome du choix, les opinions sont divisées. Comme on peut lire dans le livre [**Her06**], il y a des bonnes raisons pour accepter cet axiome, il y a des bonnes raisons pour ne pas l'accepter et il y a des bonnes raisons pour accepter un axiome presque opposé.

Pour mieux comprendre le rôle des axiomes, on pourrait penser à une analogie avec le "jeux" de construction d'enfants avec les briques LEGO et/ou DUPLO. Avec une quantité assez limité de type de briques, on peut construire (presque) tout ce qu'on peut s'imaginer. Avec des briques de tailles 2×2 et 2×4 on peut se fabriquer des maisons simples avec portes et fenêtres. Si on rajoute la taille 2×3 on peut même faire des murs intérieurs pour diviser la maison en chambres. Par contre, si on n'a pas assez de formes, on est sérieusement limité dans les possibilités. Comme par exemple dans les distributions de briques DUPLO pour petits enfants qui ne comportent (quasiment) que des briques de taille 2×2. Avec ces briques, on peut construire des tours et des pyramides en 2 ou 3 dimensions. Mais l'absence des tailles 2×3 et 2×4 fait qu'on ne peut plus construire des maisons simples. Par contre, avec les trois tailles 2×2, 2×3 et 2×4 on peut même construire des charnières de portes ! Il est vrai que le résultat n'est pas aussi beau qu'avec des briques spéciales prévus pour cette utilisation, mais c'est possible. Ce phénomène se traduit pour les axiomes dans le fait que parfois on rajoute un axiome pour simplifier l'exposition

des résultats, mais qu'on pourrait faire sans. Si on le fait sans, on a moins d'axiomes, mais l'exposition sera moins jolie.

Le but de ce texte, outre l'aspect "culturel," est double : d'une part d'expliquer le sens des axiomes et de donner toutes les détails des constructions des nombres à partir des axiomes, que ce soit $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ ou $\mathbf{R}$ (et on passera même aux nombres cardinaux et ordinaux), et d'autre part de montrer qu'il est possible d'interpréter tous les objets mathématiques comme des ensembles, que ce soit des ensembles (bien évidemment), des applications, des relations, des nombres ou autres. Par contre, aucune discussion de nature philosophique sera donnée pour la simple raison que je n'en suis pas capable ni compétent. Le lecteur intéressé pourrait consulter pour cela le livre [**Pot04**] et les références qu'il trouve là-dedans.

Chapitre 1

Des axiomes

1. Les 5 premiers axiomes

Dans ce premier chapitre on introduit les premiers axiomes de base (nos briques de construction) et on regarde ce qu'on peut construire avec (pas grand chose). Ce qu'il faut savoir c'est que dans le système axiomatique de Zermelo on se sert, outre les symboles logiques standards, de variables qui désignent des ensembles et d'un symbole $\in$ qui désigne la notion d'appartenance. Les axiomes ne précisent pas ce que ces notions (ensemble et appartenance) veulent dire, ils disent seulement comment on peut les utiliser. Avec ces cinq premiers axiomes on définit (on pourrait dire qu'on justifie) les ingrédients de base de la théorie des ensembles : les notions d'inclusions $\subset$ et d'intersection et union $\cap$ et $\cup$. Mais aussi les notations pour différentes sortes d'ensembles : $\emptyset$, $\{a\}$, $\{a, b, c\}$ ou encore $\{a \in A \mid p(a)\}$. Car, bien que tout le monde connaît tout cela, il faut montrer que ces objets ont un sens. Prenons $\emptyset$, qui désigne l'ensemble vide. Mais qui justifie que c'est bien un ensemble ? Ou $\{a, b, c\}$, qui désigne un ensemble qui n'a que trois éléments : a, b et c. Plus précisément :

$$x \in \{a, b, c\} \qquad \Longleftrightarrow \qquad x = a \text{ ou } x = b \text{ ou } x = c \ .$$

Mais encore faut il justifier que c'est bien un ensemble, même si on sait déjà que a, b et c sont des ensembles. On pourrait même dire que c'est exactement que font ces premières axiomes : justifier que ces notations ont bien un sens. Plus précisément, on pourrait dire que l'axiome de la paire (Z3) (en combinaison avec l'axiome de la réunion (Z4)) justifie la notation $\{a, b, c\}$ et que l'axiome de séparation justifie la notation $\{a \in A \mid p(a)\}$. Je n'ai aucune idée si ces notations étaient oui on non utilisées avant l'introduction de ces axiomes, mais logiquement elles devraient venir après.

Nota Bene. Le domaine d'application des quantificateurs universelles et existentielles $\forall$ et $\exists$ est constitué des *ensembles*. La formule $\forall A$ se lit donc comme "pour tout ensemble A" et la formule $\exists A$ comme "il existe un ensemble A."

(Z1) Axiome d'extensionnalité. $\forall A, B \ : \ \big[\ \forall C \ : \ C \in A \Longleftrightarrow C \in B \ \big] \implies \big[\ A = B \ \big] \ .$

Ce premier axiome (qu'on pourrait appeler l'axiome d'égalité) nous dit que si deux ensembles ont les mêmes éléments, alors ils sont égaux. Vu que l'autre implication est évidente, cet axiome nous dit donc que deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments. Avec l'écriture habituelle d'ensembles, cet axiome dit que la façon dont on décrit un ensemble n'a pas d'importance. Par exemple, les ensembles

$$\{a,b,c\} \quad , \quad \{c,b,a\} \quad et \quad \{a,b,a,a,b,b,c\}$$

sont tous les trois égaux, car ils contiennent tous les trois les éléments a, b et c. Une première application de cet axiome est le principe bien connu de l'égalité par double inclusion.

1.1 Définition. Si A et B sont deux ensembles, alors on écrit $A \subset B$ pour la formule

$$\forall C \ : \ C \in A \ \Rightarrow \ C \in B$$

et on dit que l'ensemble A est *inclu* dans l'ensemble B, ou bien que A est un *sous-ensemble* de B.

Ⓟ **1.2 Lemme.** *Si A et B sont deux ensembles tels qu'on a $A \subset B$ et $B \subset A$, alors on a l'égalité $A = B$.*

Ⓟ **1.3 Lemme.** *Soit A, B et C trois ensembles. Si on a les inclusions $A \subset B$ et $B \subset C$, alors on a aussi l'inclusion $A \subset C$.*

Les résultats [1.2] et [1.3] disent tous les deux quelque chose sur la relation d'inclusion $\subset$. Mais on ne peut pas montrer le premier sans l'axiome d'extensionnalité, tandis que le deuxième est une simple transcription de la transitivité de l'implication logique : la formule logique en trois variables p, q et r donnée par

$$(\, p \Rightarrow q \ \textit{et} \ q \Rightarrow r \,) \ \Rightarrow \ (\, p \Rightarrow r \,)$$

est une tautologie. Et c'est cette tautologie qu'on a utilisé dans la preuve de [1.3].

La notation des négations. Il est d'usage de simplifier l'écriture d'une négation concernant les symboles d'appartenance $\in$ et d'inclusion $\subset$ en mettant une barre oblique dans ces symboles. On a donc les "abréviations" suivantes :

$$\neg(a \in A) \quad \overset{\text{déf}}{\Longleftrightarrow} \quad a \notin A \qquad \text{et} \qquad \neg(a \subset A) \quad \overset{\text{déf}}{\Longleftrightarrow} \quad a \not\subset A \ .$$

(Z2) Axiome de l'ensemble vide. $\exists A \, \forall B \ : \ B \notin A$.

En mots, l'axiome de l'ensemble vide dit qu'il existe un ensemble qui a la propriété que tout autre ensemble ne lui appartient pas. Autrement dit, il existe un

ensemble qui ne contient aucun ensemble : c'est ce qu'on appelle un ensemble vide. L'axiome de l'ensemble vide est un des deux axiomes (l'autre est l'axiome de l'infini) qui se prononce sur l'existence *d'un ensemble. Les autres axiomes présupposent l'existence d'un ou deux ensembles pour en construire un nouvel ensemble.*

Une fois qu'on a un axiome qui donne l'existence d'un ensemble vide, on peut se poser la question de l'unicité, ce qui est réglé par l'axiome d'extensionnalité.

Ⓟ **1.4 Lemme/Définition.** *Il n'existe qu'un seul ensemble vide qu'on note* $\emptyset$.

Si on n'avait que ces deux axiomes, on ne pouvait pas faire grand chose. Les axiomes suivants nous disent comment on peut construire des nouveaux ensembles à partir d'ensembles existants. Et c'est grace à l'axiome d'extensionnalité qu'on peut utiliser le mot "construire," car il nous permet de montrer l'unicité de l'ensemble dont l'existence est garanti par nos axiomes. Plus précisément, la plupart des axiomes est de la forme : si on dispose d'un ou deux ensembles, alors il existe un ensemble X tel qu'un ensemble Y appartient à X si et seulement si Y a une propriété particulière (qui dépendra des ensembles donnés préalablement). Autrement dit, il existe un ensemble X dont les éléments sont exactement les ensembles qui vérifient la propriété donnée. Et par l'axiome d'extensionnalité, l'ensemble X est unique. C'est donc tout-à-fait justifié d'appeler une tel axiome un axiome de construction : le nouvel ensemble est "construit" (dans le sens "défini d'une façon unique") à partir d'un ou deux ensembles donnés préalablement.

(Z3) Axiome de la paire.

$$\forall A, B\ \exists C\ \forall D\ :\ D \in C \iff \left[\ D = A \text{ ou } D = B\ \right]\ .$$

Par l'axiome d'extensionnalité l'ensemble C est unique et complètement déterminé par les ensembles A et B. On le note comme

$$C \overset{\text{not}}{=} \{A, B\}\ .$$

L'axiome de la paire nous dit que si A et B sont deux ensembles, alors il existe un ensemble qui a exactement A et B comme éléments. Avec la notation $\{A, B\}$ pour cet ensemble, on peut donc reformuler cet axiome comme

si A et B sont deux ensembles, alors $\{A, B\}$ est un ensemble.

Si on prend $A = B$, l'axiome de la paire dit qu'il existe un ensemble C avec la propriété

$$D \in C \qquad \iff \qquad D = A \text{ ou } D = A \qquad \iff \qquad D = A\ .$$

L'unicité de cet ensemble est (comme toujours) assuré par l'axiome d'extensionnalité et ne dépend que de l'ensemble A. C'est un ensemble qui contient seulement l'ensemble A. Avec la notation de la collection à un élément $\{A\}$ on peut donc dire qu'on a

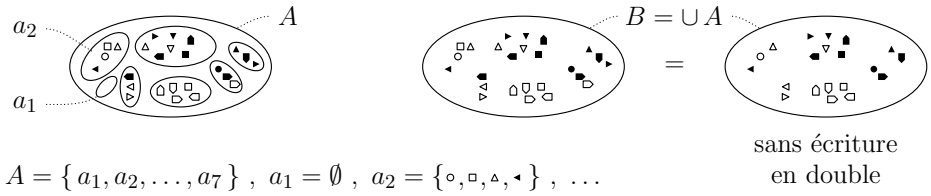
si A est un ensemble, alors $\{A\}$ est un ensemble.

Et l'axiome d'extensionnalité nous garantit que l'ensemble $\{A, A\}$ est le même que l'ensemble $\{A\}$. Sachant que $\emptyset$ est un ensemble, on peut construire les ensembles

$$\{\emptyset\} \quad , \quad \{\emptyset, \{\emptyset\}\} \quad , \quad \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \quad , \quad \{\{\emptyset\}\} \quad , \quad \{\emptyset, \{\{\emptyset\}\}\}$$

et cœtera. Mais chacun de ces ensembles a au plus deux éléments.

Pour construire des ensembles avec plus d'éléments on voudrait bien avoir le droit de faire des réunions, ce qui est autorisé par l'axiome de la réunion. L'idée de cet axiome est parfaitement illustrée par l'analogie avec le boulanger qui fait ces courses pour fabriquer un gateau. Pour faire le gateau on prend un sac de farine, un paquet de beurre, un œuf, un sac de sucre et un sachet de sel. Ensuite on réunit les contenus de chaque paquet/sachet/sac dans une casserole. Cette opération correspond à merveille avec l'idée qu'on a intuitivement d'une réunion : on a plusieurs ensembles, on prend les éléments dans chaque ensemble et on les réunit dans un nouvel ensemble. Mais avant de pouvoir faire son gateau, le boulanger doit faire des courses pour acheter ces ingrédients qu'il va réunir. En revenant du supermarché il a donc un sac qui contient ses courses : un sac qui contient un sac de farine, un sac de sucre, un œuf, un paquet de beurre et un sachet de sel. Autrement dit, il a un ensemble d'ensembles. Et pour faire le gateau il prend les éléments de son sac de courses et il réunit les contenus des ces "éléments." L'axiome de la réunion exprime cette opération qui part du sac contenant les courses et en fabrique la casserole avec les ingrédients.



(Z4) Axiome de la réunion.

$$\forall A \; \exists B \; \forall C \; : \; C \in B \iff \big[\; \exists D \; : \; D \in A \text{ et } C \in D) \; \big] \; .$$

Par l'axiome d'extentionnalité l'ensemble B est unique et complètement déterminé par l'ensemble A. Il y a deux notations "standards" pour cette ensemble : une compacte et surtout utilisée par les logiciens et les mathématiciens qui travaillent dans la théorie des ensembles mais peu connue par la plupart des mathématiciens ; et une moins compacte mais beaucoup plus connue. La notation compacte est

$$B \overset{\text{not}}{=} \cup A \tag{1.5}$$

et la notation plus connue est

$$B \overset{\text{not}}{=} \bigcup_{D \in A} D \; . \tag{1.6}$$

L'axiome de la réunion dit que pour tout ensemble A il existe un autre ensemble B qui a la propriété que ses éléments (les éléments de B) sont exactement les ensembles qui appartiennent aux éléments de A. Autrement dit, l'axiome de la réunion affirme que la réunion d'un ensemble d'ensembles est un ensemble. Regardons quelques cas

particuliers, en commençant par le cas très particulier $A = \emptyset$. Pour l'ensemble vide, l'axiome de la réunion dit qu'il existe un ensemble B tel que

$$\forall C \ : \ [\ C \in B \Leftrightarrow (\exists D \ : \ D \in \emptyset \ et \ C \in D)\ ] \ ,$$

c'est-à-dire que les éléments C de B sont caractérisés par la condition

$$\exists D \ : \ D \in \emptyset \ et \ C \in D \ .$$

Mais cette condition ne peut jamais être satisfaite car $\emptyset$ ne contient pas d'éléments. Il n'y a donc pas d'ensembles C vérifiant cette condition et B est donc l'ensemble vide. Ceci se résume dans la formule

$$\cup \emptyset = \emptyset \ .$$

Un autre cas un peu moins particulier est le cas d'un singleton : $A = \{X\}$ pour un certain ensemble X (A est bien un ensemble par l'axiome de la paire). Dans ce cas, l'axiome de la réunion dit qu'il existe un ensemble B tel que

$$\forall C \ : \ [\ C \in B \Leftrightarrow (\exists D \ : \ D \in \{X\} \ et \ C \in D)\ ] \ .$$

Mais l'ensemble $\{X\}$ ne contient qu'un seul élément, donc $D \in \{X\}$ implique automatiquement $D = X$ et cette condition se simplifie en

$$\forall C \ : \ [\ C \in B \Leftrightarrow C \in X\ ] \ ,$$

ce qui veut exactement dire (avec l'axiome d'extensionnalité) qu'on a $B = X$. On a donc la formule

$$\cup \{X\} = X \ .$$

Regardons maintenant le cas particulier où $A = \{X, Y\}$ est un ensemble à deux éléments (ce qui existe grace à l'axiome de la paire). Selon l'axiome de la réunion il existe un ensemble B avec la propriété

$$\forall C \ : \ C \in B \Leftrightarrow [\, \exists D \in \{X, Y\} \ : \ C \in D\,] \ ,$$

ce qui est équivalent à la propriété

$$\forall C \ : \ C \in B \Leftrightarrow [\, C \in X \ ou \ C \in Y\,] \ . \tag{1.7}$$

Ici on reconnait la définition usuelle de la réunion de deux ensembles.

Définition. Si X et Y sont deux ensembles, on définit la *réunion* de X et Y, notée $X \cup Y$, par

$$X \cup Y \ \stackrel{\text{déf}}{=} \ \cup \{X, Y\} \ . \tag{1.8}$$

Une propriété souvent utilisée avec les réunions est le fait que si un ensemble X figure dans la liste des ensembles à réunir, alors X est un sous-ensemble de la réunion. L'axiome de la réunion permet bien de montrer ce résultat.

Ⓟ **1.9 Lemme.** $\forall A, X \ : \ X \in A \ \Rightarrow \ X \subset \underset{D \in A}{\cup} D \equiv \cup A.$

Revenons maintenant sur la question de former des ensembles de plus que deux éléments. Si A, B et C sont trois ensembles, alors par l'axiome de la paire on a les existences suivantes :

$$\exists X \ : \ \forall D : D \in X \Leftrightarrow X = A \qquad et$$
$$\exists X \ : \ \forall D : D \in X \Leftrightarrow (X = B \ ou \ X = C) \ ,$$

ce qui exprime que $\{A\}$ et $\{B, C\}$ sont des ensembles. Mais on ne sait pas (encore) l'existence

$$\exists X \ : \ \forall D : D \in X \Leftrightarrow (X = A \ ou \ X = B \ ou \ X = C) \ ,$$

ce qui dira que $\{A, B, C\}$ est un ensemble. Mais l'application répétée de l'axiome de la paire nous donne que $\{A\}$, $\{B, C\}$ et $\{\{A\}, \{B, C\}\}$ sont des ensembles. Par l'axiome de la réunion on en déduit que

$$\cup\{\{A\}, \{B, C\}\} \equiv \{A\} \cup \{B, C\}$$

est un ensemble. Selon (1.7) on a donc

$$\begin{aligned} D \in \{A\} \cup \{B, C\} \quad &\Longleftrightarrow \quad D \in \{A\} \ ou \ D \in \{B, C\} \\ &\Longleftrightarrow \quad D = A \ ou \ \big[\, D = B \ ou \ D = C \, \big] \\ &\Longleftrightarrow \quad D = A \ ou \ D = B \ ou \ D = C \ . \end{aligned}$$

Et ceci est la définition de la collection notée $\{A, B, C\}$ qui contient exactement A, B et C comme (trois) éléments. On a donc montré que c'est un ensemble :

$$\{A, B, C\} = \cup\{\{A\}, \{B, C\}\} \quad \textit{est un ensemble.}$$

L'axiome de la réunion nous permet donc de former des ensembles à plusieurs éléments, mais ces ensembles restent des ensembles finis (bien que cette notion n'est pas encore définie ; on le prend donc dans le sens intuitif). Mais dans le contexte d'ensembles finis *il n'est pas difficile de se convaincre que la simple réunion de deux ensembles suffit pour accomplir le même résultat. L'axiome*

$$\forall A, B \ \exists C \ \forall D \ : \ [\ D \in C \ \Leftrightarrow \ (D \in A \ ou \ D \in B) \ ]$$

qui dit que la réunion de deux ensembles A et B est un ensemble C aurait suffit. L'axiome de la réunion tel qu'il est donné ne se prononce pas sur le nombre d'éléments dans A. La force de cette façon de le formuler est que plus tard on aura le droit de l'appliquer à des ensembles infini (dont on ignore pour le moment l'existence). Et cela ne serait pas possible avec l'axiome plus simple qui n'autorise que la réunion de deux ensembles.

Il est important de remarquer qu'on utilise le symbole $\cup$ dans trois sens différents. Le premier sens est celui d'un opérateur unaire qui opère sur un ensemble. C'est dans ce sens qu'on l'a défini dans (1.5). Le deuxième sens est celui d'un opérateur binaire qu'on écrit entre deux ensembles. C'est l'utilisation la plus connue et qui est utilisée dans (1.8). Le troisième sens est quand on y attache un indexe comme dans (1.6). À ce moment ce n'est plus un opérateur sur un seul ensemble, mais sur une famille d'ensembles (bien qu'on ne sait pas encore trop ce que cela veut dire). C'est une autre façon d'écrire l'opérateur unaire d'une façon plus proche de l'opérateur binaire. Il est généralement évident du contexte quelle interprétation il faut choisir. Par exemple, la formule

$$A \cup \cup \underset{D \in B}{\cup} D$$

a un sens : le premier symbole $\cup$ est l'opérateur binaire, le deuxième l'opérateur unaire et le troisième l'opérateur avec indexe. C'est le même ensemble que donné par la formule $A \cup \cup \cup B$.

Quand on sait que la réunion d'ensembles reste un ensemble, on se pose tout de suite la question si l'intersection d'ensembles reste aussi un ensemble. Cette question est réglée par l'axiome de séparation, qui est probablement l'axiome le plus utilisé par les mathématiciens, car cela concerne la possibilité de définir des sous-ensembles par une propriété. Pour cela on part d'une propriété qu'un ensemble x peut avoir, ce qui est exprimé par une formule $p(x)$ qui ne prend que les valeurs "vrai" ou "faux" en fonction de l'ensemble x. Ensuite on prend un ensemble A et on sélectionne dans A les éléments (ensembles) pour lesquels la formule $p(x)$ est "vrai." L'axiome de séparation dit que le résultat est encore un ensemble. Et strictement parlant, ce n'est pas un seul axiome, mais un schéma d'axiomes : il y a un axiome pour chaque formule p.

(Z5) Axiome de séparation.

$$\forall A\ \exists B\ \forall C\ :\ C \in B \iff \big[\ C \in A \text{ et } p(C)\ \big]\ ,$$

où $p(x)$ est une formule logique dépendant d'une variable x qui exprime une propriété d'un ensemble x. Par l'axiome d'extensionnalité l'ensemble B est unique et complètement déterminé par l'ensemble A et la propriété p. On le note comme

$$B \overset{\text{not}}{=} \{C \in A \mid p(C)\}\ .$$

Avant d'énoncer l'existence de l'intersection, regardons d'abord un peu de ce qu'on attend. Par analogie avec la notation pour la réunion, on utilise les deux notations suivantes (une compacte et une courante) pour l'intersection d'un ensemble :

$$\cap A \qquad \text{et} \qquad \bigcap_{D \in A} D\ . \tag{1.10}$$

La définition usuelle de cela est

$$C \in \cap A \equiv \bigcap_{D \in A} D \iff \forall D \in A\ :\ C \in D\ . \tag{1.11}$$

Le but est donc de montrer que cela définit bien un ensemble. Si on épluche un peu la description (1.11), on voit qu'il y a un problème quand A est l'ensemble vide : la condition $D \in \emptyset$ n'est jamais vraie, donc l'implication est toujours vraie. Par l'équivalence on doit donc conclure que $\cap\emptyset$ contient tous les ensembles : $\cap\emptyset$ est l'ensemble de tous les ensembles, ce qui nous conduit directement aux paradoxes. Ce qui explique pourquoi on a la clause $A \neq \emptyset$ dans [1.12].

Ⓟ **1.12 Existence et unicité de l'intersection.**

$$\forall A\ :\ A \neq \emptyset\ \Rightarrow\ \big[\ \exists B\ \forall C\ :\ C \in B\ \Leftrightarrow\ [\forall D\ :\ D \in A\ \Rightarrow\ C \in D]\ \big]\ .$$

Par l'axiome d'extensionnalité l'ensemble B est unique et complètement déterminé par l'ensemble A. On est donc justifié de le noter comme dans (1.10).

Avec [1.12] on a donc justifié, quand A n'est pas vide, l'existence de l'intersection $\cap A$ (1.10), (1.11). Comme pour le symbole d'une réunion $\cup$, on utilise le symbole de l'intersection $\cap$ dans trois sens différents. D'abord comme un opérateur unaire, après comme un opérateur avec un indexe opérant sur une famille d'ensembles. Ces deux sens sont utilisés dans (1.10). Et finalement comme opérateur binaire en tant qu'abréviation pour l'opérateur unaire agissant sur un ensemble à deux éléments.

Définition. Si X et Y sont deux ensembles, on définit *l'intersection* de X et Y, notée $X \cap Y$, par

$$A \cap B \stackrel{\text{déf}}{=} \cap \{A, B\} \ . \tag{1.13}$$

2. Le produit Cartésien

Avec les axiomes qu'on a vu jusqu'à présent on peut faire des réunions, des intersections, on peut définir des sous-ensembles par une propriété et on peut faire des ensembles à deux éléments à partir de deux ensembles. Mais comment définir le produit cartésien (aussi appelé le produit direct) ? L'idée qui vient directement à l'esprit est de dire que le produit cartésien est l'ensemble de tous les couples ordonnés (a, b) avec $a \in A$ et $b \in B$. Cette approche pose deux problèmes : comment définir un couple ordonné et comment montrer que la collection de tous ces couples est un ensemble. Une solution possible pour le premier problème est de dire qu'il faut rajouter la notion de couple ordonné à notre théorie comme un symbole "primitif" supplémentaire à côté du symbole d'appartenance "$\in$" et de dire, par le biais d'axiomes, comment il faut l'utiliser. Une autre façon d'approcher le premier problème est d'essayer d'interpréter un couple ordonné comme un ensemble. Il se trouve que c'est effectivement possible avec les axiomes déjà donnés et la solution proposée par Kuratowski est la suivante.

Définition. Si a et b sont deux ensembles, alors le couple ordonné (a, b) est une abréviation pour l'ensemble

$$(a, b) \stackrel{\text{déf}}{=} \{\, \{a\}, \{a, b\} \,\} \ .$$

Si a et b sont deux ensembles, alors l'axiome de la paire (appliqué trois fois !) garantit que (a, b) défini ainsi est un ensemble.

Ⓟ **2.1 Lemme.** *Si x, y et z sont trois ensembles, on a l'implication*

$$\{x, y\} = \{x, z\} \quad \Longrightarrow \quad y = z \ .$$

Ⓟ **2.2 Lemme.** *Si a, b, c et d sont quatre ensembles, alors on a l'équivalence*

$$(a, b) = (c, d) \qquad \Longleftrightarrow \qquad a = c \text{ et } b = d \ .$$

Si on ne veut pas définir un couple ordonné comme un ensemble, mais qu'on opte pour l'approche avec un symbole primitif, c'est la propriété [2.2] qu'il faut coder par un axiome supplémentaire, car c'est cette propriété qui est caractéristique pour un couple ordonné.

Contrairement au premier problème, le deuxième concernant la collection de tous les couples ordonnés ne peut pas être résolu sans axiome supplémentaire. Plusieurs approches sont possibles et on choisit ici celui qui utilise l'axiome de l'ensemble des parties. Cet axiome dit que la collection de tous les sous-ensembles d'un ensemble A est de nouveau un ensemble, qu'on note $\mathcal{P}(A)$, la lettre $\mathcal{P}$ étant une indication qu'il s'agit des parties de A :

$$C \in \mathcal{P}(A) \qquad \Leftrightarrow \qquad C \subset A \ .$$

Si A est un ensemble fini, on n'a pas vraiment besoin de cet axiome pour conclure que $\mathcal{P}(A)$ est un ensemble. Il suffit d'appliquer l'axiome de la paire et l'axiome de la réunion pour le faire. Par exemple, si a et b sont des ensembles, $A = \{a, b\}$ est un ensemble. Par l'axiome de la paire on sait que $\{a\}$ et $\{b\}$ sont aussi des ensembles. De nouveau par l'axiome de la paire (et l'axiome de l'ensemble vide) on en déduit que

$$\big\{\{a,b\}\big\} \quad , \quad \big\{\{a\}\big\} \quad , \quad \big\{\{b\}\big\} \quad \text{et} \quad \big\{\emptyset\big\}$$

sont des ensembles. À l'aide de l'axiome de la réunion il s'ensuit que

$$\big\{\{a,b\}\big\} \cup \big\{\{a\}\big\} \cup \big\{\{b\}\big\} \cup \big\{\emptyset\big\} = \big\{\ \{a,b\}\ ,\ \{a\}\ ,\ \{b\}\ ,\ \emptyset\ \big\} = \mathcal{P}(A)$$

est un ensemble. Un même raisonnement reste valable si A est un ensemble fini quelconque (bien qu'officiellement on ne sait toujours pas (encore) ce que c'est un ensemble fini). Par contre, dès que l'ensemble n'est plus fini, cet argument ne suffit plus pour montrer que la collection de tous *les sous-ensembles d'un ensemble donné est de nouveau un ensemble. D'où la nécessité de l'axiome.*

(Z6) Axiome de l'ensemble des parties.

$$\forall A\ \exists B\ \forall C\ :\ C \in B \iff C \subset A\ .$$

Par l'axiome d'extensionnalité l'ensemble B est unique et complètement déterminé par l'ensemble A. On le note comme $B \overset{\text{not}}{=} \mathcal{P}(A)$.

Comme annoncé, c'est avec l'axiome de l'ensemble des parties qu'on va montrer que le produit cartésien de deux ensembles est un ensemble. Pour préparer l'énoncé exacte, regardons d'abord l'idée intuitive du produit cartésien $A \times B$ de deux ensembles A et B. C'est la collection qui contient tous les couples ordonnés (a, b) avec $a \in A$ et $b \in B$. Un ensemble C est donc un élément de $A \times B$ si et seulement si c'est un tel couple. Autrement dit :

$$C \in A \times B \qquad \Leftrightarrow \qquad \exists a \in A\ \exists b \in B : C = (a,b) \overset{\text{déf}}{=} \{\,\{a\}, \{a,b\}\,\}\ .$$

Vu qu'on précise les éléments de cet ensemble, l'axiome d'extensionnalité dit que c'est unique dès que cela existe. Vu que cet ensemble ne dépend que des ensembles A et B, on peut le noter comme on le fait (par $A \times B$).

Ⓟ **2.3 Existence et unicité du produit cartésien.** *Le produit cartésien $P = A \times B$ de deux ensembles A et B est un ensemble :*

$$\forall A, B\ \exists P\ \forall C\ :\ \big(\ C \in P\ \Leftrightarrow\ [\ \exists a \in A\ \exists b \in B : C = (a,b)\ ]\ \big)\ .$$

Par l'axiome d'extensionnalité l'ensemble P est unique et complètement déterminé par les ensembles A et B. On le note comme $P = A \times B$.

2.4 Nota Bene/Simplification de notation. Si on regarde bien la définition du produit cartésien $P = A \times B$ telle qu'elle est donnée dans la preuve de [2.3], on a l'impression qu'on pourrait simplifier l'écriture. La condition qu'on utilise pour appliquer l'axiome de séparation donne une formule explicite pour C, ce qui suggère

d'écrire partout cette formule explicite et de supprimer l'invocation de l'ensemble C. Avec cette idée, on réécrira la définition

$$P = \{\, C \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big) \mid \exists a \in A\ \exists b \in B : C = (a,b) \,\} \tag{2.5}$$

comme

$$P = \{\, (a,b) \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big) \mid a \in A \text{ et } b \in B \,\} \ .$$

L'omission des quantificateurs existentielles devant les expressions $a \in A$ et $b \in B$ se justifie par la remarque qu'il y a une quantificateur universel pour l'ensemble C : tout ensemble C vérifiant les conditions appartient à P. La condition étant qu'il existe des éléments de A et de B, il faut donc parcourir les éléments de A et de B pour obtenir tous les ensembles C autorisés. Il faut donc lire, dans la deuxième façon d'écrire l'ensemble P, les conditions $a \in A$ et $b \in B$ comme "où a parcourt l'ensemble A et b parcourt l'ensemble B."

Une fois qu'on l'a réécrit de cette façon, on peut remarquer que l'élément (a,b) appartient évidemment à $\mathcal{P}\big(\mathcal{P}(A \cup B)\big)$, donc que ce n'est pas vraiment la peine de l'écrire. Ce qui donne l'écriture

$$P = \{\, (a,b) \mid a \in A \text{ et } b \in B \,\} \ , \tag{2.6}$$

ce qu'on lit comme "l'ensemble des couples (a,b) où a parcourt A et b parcourt B." Mais quand on écrit la définition du produit cartésien de cette façon, il n'est plus évident que cela définit bien un *ensemble*. Pour s'en convaincre, il faut remonter les simplifications. Par contre, il est devenu coutume d'utiliser cette simplification d'écriture, et pas seulement parce que c'est plus court, donc plus facile à comprendre. Une autre raison est que cette écriture sera autorisée par un autre axiome qu'on rencontrera que beaucoup plus tard dans ce texte : l'axiome de remplacement. En gros cet axiome dit directement que (2.6) définit un ensemble, sans avoir à remonter l'écriture à (2.5). En plus, l'axiome de séparation est une conséquence de cet axiome de remplacement. D'où la question légitime : pourquoi introduire d'abord l'axiome de séparation quand on introduira plus tard un autre axiome qui est plus fort. Il y a plusieurs raisons, dont voici deux. La liste d'axiomes donnés par Zermelo ne contenait pas l'axiome de remplacement ; cet axiome a été rajouté plus tard par Fraenkel pour des raisons précises qu'on discutera dans §29. Et on n'a jamais pris l'effort de supprimer l'axiome de séparation de la liste d'axiomes. Mais peut-être plus important est le fait que dans la pratique de tous les jours d'un mathématicien, on n'a pas besoin de l'axiome de remplacement, mais seulement de l'axiome de séparation. Comme on a vu ci-dessus, on n'a pas besoin de l'axiome de remplacement pour vérifier que P est bien un ensemble, il suffit de l'écrire d'une "bonne" manière.

Dans la suite on utilisera la notation "simplifiée" souvent, comme il est coutume. Mais on indiquera (surtout au début) comment on devrait l'écrire à l'aide de l'axiome de séparation pour se convaincre que c'est bien un ensemble qu'on décrit.

Ⓟ **2.7 Une équivalence en logique.** *Soit $p(x)$ une formule logique dépendant d'une variable x qui exprime une propriété d'un ensemble x. Si A et B sont deux ensembles, alors on a l'équivalence logique*

$$\Big(\ \forall C \in A \times B : p(C)\ \Big) \qquad \Longleftrightarrow \qquad \Big(\ \forall a \in A\ \forall b \in B : p\big((a,b)\big)\ \Big) \ .$$

Ⓟ **2.8 Lemme.** *Si A est un ensemble, alors $\emptyset \times A = A \times \emptyset = \emptyset$.*

Ⓟ **2.9 Lemme.** *Soit A, A', B, B' quatre ensembles. Si on a les inclusions $A \subset A'$ et $B \subset B'$, alors on a l'inclusion $A \times B \subset A' \times B'$.*

3. Relations et relations d'ordre

Une fois qu'on sait que le produit cartésien de deux ensembles est un ensemble, on est prêt pour définir la notion d'une relation entre deux ensembles A et B, ainsi que les cas particuliers d'une relation d'ordre et d'une application qu'on représente par son graphe ; les relations d'équivalence seront discutées plus tard. Un exemple typique d'une relation est la relation entre voitures et personnes donnée par "a été conduit par." Avec cette définition, une voiture peut être en relation avec plusieurs personnes (tous les personnes qui ont conduit la voiture) et plusieurs voitures peuvent être en relation avec une personne (on ne roule pas toujours dans la même voiture). Mais il y a aussi des voitures qui ne sont en relation avec personne (les voitures neuves) et il y a des personnes qui ne sont en relation avec aucune voiture (ceux qui ne conduisent pas).

3.1 Définition d'une relation. • Soit A, B et R trois ensembles. On dit que R est une *relation entre A et B* (dans cette ordre !) si on a l'inclusion $R \subset A \times B$. On dit que l'élément $a \in A$ est lié par R à l'élément $b \in B$ si le couple (a, b) appartient à R. Une autre notation pour l'appartenance d'un couple (a, b) à une relation R est aRb :

$$aRb \quad \overset{\text{déf}}{\Longleftrightarrow} \quad (a, b) \in R \ , \tag{3.2}$$

ce qu'on lit comme "l'élément $a \in A$ est en relation R avec l'élément $b \in B$," ou plus court comme "a est en relation R avec b."

• Si R est une relation entre A et B, alors la *relation inverse*, notée R^{-1}, est la relation entre B et A obtenue en échangeant les rôles de A et B et définie comme

$$R^{-1} \overset{\text{déf}}{=} \{\, (b, a) \in B \times A \mid (a, b) \in R \,\} \ .$$

Si R est une relation entre l'ensemble A et l'ensemble B et si on a les inclusions $A \subset A'$ et $B \subset B'$, alors on a, par définition d'une relation et par [2.9], les inclusions

$$R \subset A \times B \subset A' \times B' \ .$$

L'ensemble R est donc aussi une relation entre A' et B'. D'où la question si oui ou non R, vu comme relation entre A et B, est une autre relation que R, vu comme relation entre A' et B'. D'une part, c'est le même ensemble R, donc cela devrait être la même relation. D'autre part, on ne regarde pas d'un même œil une relation entre hommes et chiens et une relation entre mammifères et animaux. Dans la pratique mathématique, on précise (presque) toujours les ensembles A et B quand on parle d'une relation R, bien qu'on est conscient qu'on peut varier A et B sans que R en tant qu'ensemble change.

On pourrait croire que ce problème est seulement philosophique, mais cela devient très concret quand on veut définir le domaine et l'image (on parle aussi de source et but) d'une relation R. Si R est une relation entre deux ensembles A et B, c'est-à-dire qu'on a $R \subset A \times B$, alors il est naturel de définir l'image de R, notée $\mathrm{Im}(R)$, *comme*

$$\mathrm{Im}(R) = \{y \in B \mid \exists x : (x, y) \in R \,\} \ ,$$

l'ensemble des éléments de B qui apparaissent dans les couples dans R. Mais si C et D sont deux autre ensembles tels qu'on peut voir R comme une relation entre C et D (ce qui veut dire qu'on a aussi $R \subset C \times D$), alors on devrait écrire pour la définition de l'image de R la formule

$$\mathrm{Im}(R) = \{ y \in D \mid \exists x : (x,y) \in R \} \ .$$

Et si on pense aux écritures

$$\{ z \in \mathbf{R} \mid z^2 = -1 \} \qquad et \qquad \{ z \in \mathbf{C} \mid z^2 = -1 \} \ ,$$

on s'aperçoit que ce n'est pas automatique que ces deux définitions de $\mathrm{Im}(R)$ *décrivent le même ensemble.*

Ⓟ **3.3 Lemme.** *Soit A, B, C, D et R des ensembles vérifiant $R \subset A \times B$ et $R \subset C \times D$. Alors on a l'égalité*

$$\{ y \in B \mid \exists x : (x,y) \in R \} = \{ y \in D \mid \exists x : (x,y) \in R \} \ .$$

3.4 Définition. Soit R une relation entre deux ensembles A et B, alors on définit *l'image de* R, notée $\mathrm{Im}(R)$ et *le domaine de* R, notée $\mathrm{Dom}(R)$ comme

$$\mathrm{Im}(R) \stackrel{\text{déf}}{=} \{ y \in B \mid \exists x : (x,y) \in R \}$$

et

$$\begin{aligned} \mathrm{Dom}(R) \stackrel{\text{déf}}{=} \mathrm{Im}(R^{-1}) &\equiv \{ x \in A \mid \exists y : (y,x) \in R^{-1} \} \\ &\equiv \{ x \in A \mid \exists y : (x,y) \in R \} \ . \end{aligned}$$

Le fait qu'on ne rajoute pas le symbole B respectivement A aux définitions de $\mathrm{Im}(R)$ respectivement $\mathrm{Dom}(R)$ est justifié par [3.3]. Vu qu'il est évident de la définition qu'on a l'égalité $(R^{-1})^{-1} = R$, on obtient l'égalité (duale)

$$\mathrm{Im}(R) = \mathrm{Dom}(R^{-1}) \ .$$

Quand on sait que la définition de l'image d'une relation R entre A et B ne dépend pas de l'ensemble B et que dans cette définition l'ensemble A ne figure pas, alors on peut se poser la question s'il est vraiment nécessaire de préciser qu'une relation est entre deux ensembles. L'indépendance de B suggère qu'on écrive

$$\mathrm{Im}(R) = \{ y \mid \exists x : (x,y) \in R \} \ , \tag{3.5}$$

ce qui est une façon d'écrire qui ressemble fortement à l'écriture simplifié discutée en [2.4]. Le problème avec cette écriture ici est qu'on ne peut pas affirmer (sans axiome supplémentaire, voir §29) que cela définit bien un ensemble. On a besoin de l'ensemble B pour pouvoir invoquer l'axiome de séparation (Z5) pour garantir que c'est bien un ensemble.

Ⓟ **3.6 Lemme.** *Soit A, B et R trois ensembles tels que R est une relation entre deux ensembles non-précisés. Alors R est une relation entre A et B si et seulement si* $\mathrm{Dom}(R) \subset A$ *et* $\mathrm{Im}(R) \subset B$.

Définition. • Soit R est une relation entre A et B et soit X un ensemble (on se restreint souvent à des sous-ensembles de A, mais cela n'est pas une obligation), alors *l'image (direct) de X par la relation R*, noté $R[X]$ est défini comme

$$R[X] \stackrel{\text{déf}}{=} \{\, b \in \mathrm{Im}(R) \mid \exists a \in X : (a,b) \in R \,\} \ .$$

Ce sont les éléments de l'image de R qui sont en relation avec (au moins) un élément de X.

• Si R est une relation entre A et B, alors R^{-1} est une relation entre B et A. Si Y est un ensemble (et comme pour l'image directe on se restreint souvent à des sous-ensembles de B), alors l'image (directe) $R^{-1}[Y]$ de Y par la relation R^{-1} est appelée *l'image réciproque de Y par la relation R*. Cet ensemble est donc défini comme

$$\begin{aligned} R^{-1}[Y] &= \{\, a \in \mathrm{Im}(R^{-1}) \mid \exists b \in Y : (b,a) \in R^{-1} \,\} \\ &= \{\, a \in \mathrm{Dom}(R) \mid \exists b \in Y : (a,b) \in R \,\} \ . \end{aligned}$$

Si on reprend l'exemple de la relation entre voitures et personnes "a été conduit par," notons la R, alors la relation inverse R^{-1} est donnée par l'expression "a été conducteur de." Si V est une collection de voitures, alors $R[V]$, l'image de V par la relation R, est l'ensembles des personnes qui ont conduit une des voitures de la collection V. Et si P est un ensemble de personnes, alors l'ensemble des voitures qui ont été conduit par une de ces personnes est $R^{-1}[P]$, l'image réciproque de P par la relation R. En particulier, si v est une voiture, alors $R[\,\{v\}\,]$ est l'ensemble des conducteurs de cette voiture. Et si p est une personne, alors $R^{-1}[\,\{p\}\,]$ désigne l'ensemble des voitures qu'elle a conduit.

3.7 Proposition. *Soit A, B, R, X et Y cinq ensembles tels que R est une relation entre A et B. Alors on a les propriétés*

(i) $R[X] = \{\, b \in B \mid \exists x \in X : (x,b) \in R \,\}$,

(ii) $R^{-1}[Y] = \{\, a \in A \mid \exists y \in Y : (a,y) \in R \,\}$,

(iii) $\mathrm{Im}(R) = R[A]$ *et* $\mathrm{Dom}(R) = R^{-1}[B]$.

Une incohérence de notation. Soit $R \subset A \times B$ une relation entre A et B. La notation aRb pour l'appartenance $(a,b) \in R$ n'est pas cohérente avec la notation $R[X]$ de l'image d'un sous-ensemble X de A dans le sens que dans aRb l'élément de A est mis à gauche du symbole R et que dans $R[X]$ le sous-ensemble de A est mis à droite. L'origine de cette incohérence se trouve dans le fait que historiquement on décrit le graphe d'une fonction f comme l'ensemble des couples $\big(x, f(x)\big)$, où l'élément x de l'ensemble source est écrit en premier (donc à gauche) mais aussi après le symbole de la relation f (donc à droite).

À part le vocabulaire (les mots relation (inverse), image direct et réciproque), il n'y a pas de nouveauté dans ces notions : ce sont des simples sous-ensembles. Les choses deviennent intéressantes quand on considère des relations d'un type particulier. La première qu'on va étudier est la relation d'ordre.

3.8 Définition d'une relation d'ordre. Soit A un ensemble. Alors une *relation d'ordre (partiel) sur* A est un sous-ensemble $R \subset A \times A$ vérifiant les conditions (i), (ii) et (iii) ci-dessous. Mais avant d'énoncer ces trois propriétés, il faut remarquer qu'il est d'usage de noter une relation d'ordre, non pas par une lettre mais par un symbole comme $\leq$ ou un symbole qui ressemble à cela (comme par exemple $\leqq$, $\preccurlyeq$ ou $\geqslant$). Et, comme en (3.2), au lieu de noter $(a, b) \in \leq$ on écrit $a \leq b$:

$$a \leq b \qquad \overset{\text{déf}}{\iff} \qquad (a, b) \in \leq \quad .$$

Avec cette notation, les trois conditions s'écrivent comme

(i) $\forall a \in A : a \leq a$ (*réflexivité*),

(ii) $\forall a, b \in A : a \leq b$ et $b \leq a \;\Rightarrow\; a = b$ (*antisymétrie*) et

(iii) $\forall a, b, c \in A : a \leq b$ et $b \leq c \;\Rightarrow\; a \leq c$ (*transitivité*).

On dit qu'une relation d'ordre est *totale* si elle vérifie en plus

(iv) $\forall a, b \in A : a \leq b$ ou $b \leq a$.

Si $\leq$ est une relation d'ordre (partiel ou total) sur un ensemble A, on dit aussi que (le couple) $(A, \leq)$ est un ensemble (partiellement ou totalement) ordonné.

Si $\leq$ est une relation d'ordre sur un ensemble A, on lui associe trois autre relations sur A qu'on peut décrire en mots comme "la relation d'ordre stricte associée", "la relation inverse" et "l'inverse de la relation d'ordre stricte." La façon de noter ces trois relations dépend fortement du symbole utilisé pour la relation d'ordre ; dans le cas du symbole $\leq$ ces trois relations associées sont notées comme $<$, $\geq$ et $>$. Et comme pour la relation d'ordre d'origine, il est d'usage d'utiliser la notation alternative (3.2) et d'écrire ces symboles entre les deux "arguments." Avec cette notation, la définition officielle de ces trois relations est donnée par :

$$\begin{aligned} a < b \quad &\overset{\text{déf}}{\iff} \quad a \leq b \text{ et } a \neq b \\ a \geq b \quad &\overset{\text{déf}}{\iff} \quad b \leq a \\ a > b \quad &\overset{\text{déf}}{\iff} \quad b < a \quad \iff \quad b \leq a \text{ et } b \neq a \quad . \end{aligned}$$

3.9 Lemme. *Soit $\leq$ une relation d'ordre sur un ensemble A et soit $<$ la relation d'ordre stricte associée. Alors pour tout $a, b \in A$ on a les équivalences*

$$a \leq b \quad \iff \quad a < b \text{ ou } a = b \qquad \text{et} \qquad a \geq b \quad \iff \quad a > b \text{ ou } a = b \quad .$$

3.10 Lemme. *Si $\leq$ est une relation d'ordre sur un ensemble A, alors la relation inverse $\geq$ est aussi une relation d'ordre sur A. Et si $\leq$ est une relation d'ordre total, alors $\geq$ l'est aussi.*

La façon dont on lit (à haute voix) une relation d'ordre dépend évidemment du symbole utilisé. Dans le cas du symbole $\leq$ il est d'habitude de lire l'appartenance $a \leq b$ comme "a plus petit ou égalé à b" et dans le cas du symbole $\geq$ on lit "a plus grand ou égalé à b" pour $a \geq b$. Dans le même esprit on lit $a < b$ comme "a strictement plus petit que b" et $a > b$ comme "a strictement plus grand que b."

Ⓟ **3.11 Lemme.** *Soit $\leq$ une relation d'ordre sur un ensemble E et soit $<$ la relation d'ordre stricte associée. Alors on a les variantes de la transitivité suivantes :*

$$\forall a,b,c \in E \quad : \quad \big(\ a \leq b \text{ et } b < c\ \big) \text{ ou } \big(\ a < b \text{ et } b \leq c\ \big) \quad \Longrightarrow \quad a < c\ .$$

La notation des négations. Il est d'usage, comme pour le symbole de l'appartenance $\in$, de noter la négation d'une relation d'ordre par une barre oblique dans le symbole de la relation d'ordre concernée. On a donc les "abréviations" suivantes :

$$\begin{array}{lllll} a \not\leq b & \Longleftrightarrow & \neg(a \leq b) & , & a \not\geq b \iff \neg(a \geq b) \\ a \not< b & \Longleftrightarrow & \neg(a < b) & , & a \not> b \iff \neg(a > b)\ . \end{array}$$

Ⓟ **3.12 Lemme.** *Soit $\leq$ une relation d'ordre partiel sur un ensemble A. Alors les quatre propriétés suivantes sont équivalentes :*

(i) *$\leq$ est une relation d'ordre total,*

(ii) *pour tout $a,b \in A$ on a l'équivalence $a \not\leq b \ \Leftrightarrow\ a > b$,*

(iii) *pour tout $a,b \in A$ on a l'équivalence $a \not< b \ \Leftrightarrow\ a \geq b$, et*

(iv) *pour tout $a,b \in A$ il y a une et une seule propriété vraie parmi les trois : $a < b$, $a = b$ et $a > b$.*

Ⓟ **3.13 Lemme.** *Soit A un ensemble. Alors l'inclusion définit une relation d'ordre (partiel) R sur $\mathcal{P}(A)$, l'ensemble des parties de A, par*

$$\forall X, Y \subset A \quad : \quad XRY \quad \overset{déf}{\Longleftrightarrow} \quad X \subset Y\ .$$

Nota Bene. Il est d'usage (et en même temps très naturel) de noter la relation d'ordre sur $\mathcal{P}(A)$ définie en [3.13] par le symbole $\subset$. Mais il ne faut pas oublier que cette utilisation est différente de l'utilisation standard définie dans [1.1]. L'utilisation standard est une abréviation pour une phrase avec quantificateur, tandis qu'en tant que relation d'ordre ce même symbole indique un sous-ensemble du produit cartésien $\mathcal{P}(A) \times \mathcal{P}(A)$. Si on utilise ce symbole en même temps dans les deux sens, on peut obtenir des formules comme

$$\subset\ \subset\ \mathcal{P}(A) \times \mathcal{P}(A) \qquad \text{ou} \qquad \subset\ = \ \{\, (x,y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid x \subset y \,\}\ ,$$

où la première formule est bizarre et la deuxième donne l'impression d'une définition circulaire. Mais en dehors de la définition officielle d'une relation d'ordre comme sous-ensemble du produit cartésien, l'utilisation du symbole $\subset$ pour cette relation d'ordre sur $\mathcal{P}(A)$ ne pose aucun problème.

L'inclusion en tant que relation d'ordre sur $\mathcal{P}(A)$, l'ensemble des parties d'un ensemble A, est une relation d'ordre partiel et en général pas une relation d'ordre total. Dès que l'ensemble A contient deux éléments distincts a et b, alors les deux singletons $\{a\}$ et $\{b\}$ ne sont pas en relation : on n'a ni $\{a\} \subset \{b\}$ ni $\{b\} \subset \{a\}$.

4. Applications

4.1 Définition d'une application. Soit f une relation entre deux ensembles A et B. Alors f est appelée une *application de A dans B*, l'ensemble A est appelé *l'ensemble source de l'application f* et l'ensemble B est appelé *l'ensemble but de l'application f* si le sous-ensemble $f \subset A \times B$ vérifie les deux conditions

(i) $\forall x \in A\ \exists y : (x,y) \in f$ et

(ii) $\forall x,y,z\ :\ \big[\,(x,y) \in f \text{ et } (x,z) \in f\,\big]\ \Rightarrow\ y = z.$

Si $f \subset A \times B$ est une application de A dans B, alors il est d'usage de noter ce fait par $f : A \to B$:

$$f : A \to B \qquad \overset{\text{déf}}{\iff} \qquad f \subset A \times B \text{ vérifie les conditions (i) et (ii) ci-dessus .}$$

Si $f : A \to B$ est une application, alors pour tout $a \in A$ il existe un *unique* élément $b \in B$ tel que $(a,b) \in f$ (c'est cela que disent les deux conditions : (i) dit que cela existe et (ii) dit que c'est unique). Il est d'usage de noter ce $b \in B$ par $b = f(a)$:

$$b = f(a) \qquad \overset{\text{déf}}{\iff} \qquad (a,b) \in f\ .$$

On dit qu'une application $f : A \to B$ est *injective* si $f \subset A \times B$ vérifie la condition

(iii) $\forall x,y,z\ :\ \big[\,(y,x) \in f \text{ et } (z,x) \in f\,\big]\ \Rightarrow\ y = z,$

on dit que f est *surjective* si elle vérifie

(iv) $\forall x \in B\ \exists y : (y,x) \in f$

et on dit que f est *bijective* si elle est injective et surjective. Avec la notation $f(a) = b$ pour $(a,b) \in f$, la condition d'injectivité d'une application s'écrit comme l'implication $f(y) = f(z)\ \Rightarrow\ y = z$.

4.2 Lemme. *Soit f une relation entre deux ensembles A et B. Alors on a les équivalences*

(i) $\qquad \forall x \in A\ \exists y : (x,y) \in f \iff \mathrm{Dom}(f) = A$

(ii) $\forall x,y,z\ :\ \big[\,(x,y) \in f \text{ et } (x,z) \in f\,\big]\ \Rightarrow\ y = z \iff f : \mathrm{Dom}(f) \to B\ .$

Pour certains et/ou dans certains cas, la notion d'application qui n'exige que la condition (ii) est plus naturel que la définition avec les deux conditions (i) et (ii). Selon [4.2.ii], une telle notion correspondrait avec notre définition d'une application définie sur un sous-ensemble de A. C'est surtout dans le contexte de fonctions réelles qu'on utilise cette notion plus faible d'application, et cela dès le lycée. Il suffit de penser à la question :

déterminer le domaine de définition de la fonction réelle $x \mapsto \sqrt{x - x^2}$.

On parle d'une fonction réelle, ce qui veut dire sur $\mathbf{R}$ et à valeurs dans $\mathbf{R}$, mais le domaine de définition est un sous-ensemble de $\mathbf{R}$. La situation est donc légèrement contradictoire, car d'une part on parle d'une fonction sur $\mathbf{R}$ et d'autre part on dit qu'elle est définie sur un sous-ensemble de $\mathbf{R}$. À part cet usage, la notion plus faible (avec seulement la condition (ii)) a beaucoup plus d'inconvénients que d'avantages.

On garde donc la définition donnée avec les deux conditions (i) et (ii). Dans cette optique, la question citée ci-dessus devrait être formulée comme

déterminer le sous-ensemble de $\mathbf{R}$ *sur lequel l'expression* $\sqrt{x-x^2}$ *a un sens.*

Et même cette formulation est ambiguë, car elle dépend dans quel ensemble on autorise la racine carré de prendre ses valeurs. Si c'est dans $\mathbf{R}$*, la réponse est l'intervalle* $0 \leq x \leq 1$*. Mais si c'est dans les nombres complexes* $\mathbf{C}$*, la réponse est* $\mathbf{R}$ *entier.*

Ⓟ **4.3 Lemme.** *Soit* A *et* B *deux ensembles et* $f, g : A \to B$ *deux applications de* A *dans* B*. Alors on a l'égalité* $f = g$ *si et seulement si on a*

$$\forall a \in A : f(a) = g(a) \ .$$

→ **4.4 Lemme/Définition.** *Soit* A *un ensemble. Alors le diagonal* $\Delta \subset A \times A$ *défini comme*

$$\Delta = \{\, C \in A \times A \mid \exists a \in A : C = (a, a) \,\}$$

est une application de A *dans* A*. Si on le considère comme une application (ce qui n'est pas toujours le cas), on le note comme id ou* id_A *et on dit que c'est* l'application identité (sur A).

4.5 Simplification de notation. Avec les mêmes arguments que donnés dans [2.4] pour le produit cartésien, on peut simplifier la notation pour l'ensemble Δ. Cela donne l'écriture

$$\Delta = \{\, (a, a) \mid a \in A \,\} \ .$$

Ici la situation est même meilleure que pour le produit cartésien dans le sens que pour le produit cartésien on pourrait avoir une doute sur l'ensemble dans lequel les éléments se trouvent (à savoir $\mathcal{P}\big(\mathcal{P}(A \cup B)\big)$). Ici, connaissant déjà le produit cartésien de deux ensembles, il est évident qu'il faut prendre l'ensemble $A \times A$, car c'est là dedans que vivent les couples (a, a).

Ⓟ **4.6 Lemme.** *Soit* $f \subset A \times B$ *une application de* A *dans* B*. Alors la relation inverse* $f^{-1} \subset B \times A$ *est une application de* B *dans* A *si et seulement si* f *est bijective.*

En général, si on a deux ensembles A *et* B *et si on veut définir une application* f *de* A *dans* B*, on dispose d'une prescription qui nous dit comment obtenir l'image* $f(a)$ *quand on connaît* $a \in A$*. L'exemple type est l'application* $f : \mathbf{R} \to \mathbf{R}$ *définie par* $f(x) = x^2$*. Connaissant la prescription, on peut poser comme définition de l'application* f *:*

$$\begin{aligned} f &= \{\, c \in \mathbf{R} \times \mathbf{R} \mid \exists x \in \mathbf{R} : c = (x, x^2) \,\} \\ &= \{\, (x, y) \in \mathbf{R} \times \mathbf{R} \mid y = x^2 \,\} = \{\, (x, x^2) \mid x \in \mathbf{R} \,\} \ , \end{aligned} \tag{4.7}$$

ce qui est un ensemble par l'axiome de séparation (la deuxième et troisième écriture utilisent les simplifications de notation décrites dans [2.4]).

Dans d'autres circonstances on ne connaît pas une prescription et on est obligé de définir l'application par d'autres moyens. C'est notamment le cas pour les projections canoniques $\pi_A : A \times B \to A$ et $\pi_B : A \times B \to B$ définies comme $\pi_A((a,b)) = a$ et $\pi_B((a,b)) = b$. L'idée naïve est de dire qu'on connaît bien une prescription : $\pi_A((a,b))$ est le premier élément du couple (a,b). Mais cela présuppose qu'on peut extraire la première composante du couple (a,b). Et on aura un cercle vicieux, car c'est exactement cela qu'on veut montrer : dire que la projection canonique π_A existe est équivalent à dire qu'on peut extraire la première composante du couple. Il faut donc employer la méthode directe pour définir la projection canonique π_A.

Ⓟ **4.8 Proposition.** *Soit A et B deux ensembles. Alors les ensembles*

$$\pi_A = \{C \in (A \times B) \times A \mid \exists a \in A\ \exists b \in B : C = \big((a,b),a\big)\ \} \tag{4.9}$$

et

$$\pi_B = \{C \in (A \times B) \times B \mid \exists a \in A\ \exists b \in B : C = \big((a,b),b\big)\ \}$$

sont des applications de $A \times B$ dans A et de $A \times B$ dans B respectivement vérifiant $\pi_A\big((a,b)\big) = a$ et $\pi_B\big((a,b)\big) = b$.

4.10 Simplification de notation. Avec les mêmes arguments que donnés dans [2.4] pour le produit cartésien, on peut ici simplifier la notation pour les deux ensembles π_A et π_B. Cela donne les écritures

$$\pi_A = \{\ \big((a,b),a\big) \mid a \in A \text{ et } b \in B\ \} \quad \text{et} \quad \pi_B = \{\ \big((a,b),b\big) \mid a \in A \text{ et } b \in B\ \}\ .$$

Ici, comme dans le cas de [4.4], la situation est même meilleure que pour le produit cartésien dans le sens qu'il n'y a pas de doute sur l'ensemble dans lequel les éléments se trouvent : pour π_A c'est $(A \times B) \times A$ et pour π_B c'est $(A \times B) \times B$, car c'est là dedans que vivent les éléments $((a,b),a)$ respectivement $((a,b),b)$.

Une fois qu'on dispose d'une définition d'application entre deux ensembles, on peut regarder les cas extrêmes où l'ensemble source ou l'ensemble but est l'ensemble vide. Certains lecteurs vont peut-être être surpris que notre définition d'une application permet d'affirmer qu'il existe une (et une seule) application définie sur l'ensemble vide à valeurs dans n'importe quel autre ensemble. Par contre, le résultat qu'il n'existe pas d'application où l'ensemble but est vide (quand la source ne l'est pas) ne surprendra personne.

Ⓟ **4.11 Proposition.** *Soit A un ensemble. Alors il existe une et une seule application $f : \emptyset \to A$. Cette application est toujours injective ; elle est surjective si et seulement si $A = \emptyset$. Par contre, si A n'est pas vide, alors il n'existe pas d'application de A dans $\emptyset$.*

Maintenant qu'on connaît la notion d'une application, il faut définir la notion de composition de deux applications. Étant donné qu'on a défini la notion d'application

via la notion d'une relation, il est naturel d'élargir la notion de composition aux relations et de montrer que si les deux relations sont des applications, la même chose est vraie pour la composition.

Définition de la composition. Soit A, B et C trois ensembles, soit R une relation entre A et B et soit S une relation entre B et C. Alors on définit la relation $S \circ R \subset A \times C$ par

$$S \circ R = \{\, (a,c) \in A \times C \mid \exists b : (a,b) \in R \text{ et } (b,c) \in S \,\} \ .$$

Ⓟ **4.12 Lemme.** *Soit A, B et C trois ensembles, soit $f : A \to B$ une application de A dans B et soit $g : B \to C$ une application de B dans C. Alors la relation $g \circ f \subset A \times C$ est une application de A dans C.*

5. Quelques résultats classiques

5.1 Lemme. *Soit A un ensemble non-vide.*

(i) *Pour tout $a \in A$ on a les inclusions $\cap A \subset a \subset \cup A$.*

(ii) *Si X est un ensemble tel que tout élément de A est inclus dans X : $\forall a \in A : a \subset X$, alors on a l'inclusion $\cup A \subset X$.*

(iii) *Si Y est un ensemble qui est inclus dans tout élément de A : $\forall a \in A : Y \subset a$, alors on a l'inclusion $Y \subset \cap A$.*

5.2 Corollaire. *Soit A et B deux ensembles, alors on a les inclusions*

$$A \cap B \subset A \subset A \cup B \qquad \text{et} \qquad A \cap B \subset B \subset A \cup B \ .$$

Ⓟ **5.3 Lemme.** *Soit A, B et C trois ensembles. Alors on a les égalités*

(i) *$A \cup B = B \cup A$ (commutativité de l'union) et*

(ii) *$(A \cup B) \cup C = A \cup (B \cup C) = \cup\{A, B, C\}$ (associativité de l'union).*

Ⓟ **5.4 Lemme.** *Soit A, B et C trois ensembles. L'intersection $A \cap B$ est caractérisé par*

$$X \in A \cap B \qquad \Longleftrightarrow \qquad X \in A \text{ et } X \in B \ .$$

On a (donc) les égalités

(i) *$A \cap B = B \cap A$ (commutativité de l'intersection) et*

(ii) *$(A \cap B) \cap C = A \cap (B \cap C) = \cap\{A, B, C\}$ (associativité de l'intersection).*

La différence de deux ensembles. Soit A et B deux ensembles. Alors l'ensemble qui contient tous les éléments de A qui n'appartiennent pas à B, noté par $A \setminus B$ et défini comme

$$A \setminus B \overset{\text{déf}}{=} \{\, a \in A \mid a \notin B \,\} \ ,$$

est bien un ensemble par l'axiome de séparation (Z5). On l'appelle la *différence des ensembles A et B*.

→ **5.5 Lemme.** *Soit A, B, C et D quatre ensembles. Alors on a l'égalité $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.*

Ⓟ **5.6 La restriction d'une relation d'ordre.** *Soit R une relation d'ordre sur un ensemble A et soit $X \subset A$ un sous-ensemble. Alors l'ensemble $R' = R \cap (X \times X)$ est une relation d'ordre sur X. Si on note ces relations d'ordre par les symboles $\leq$ pour R et $\leq'$ pour R', la définition de $\leq'$ s'écrit simplement comme*

$$\forall x, y \in X : x \leq' y \overset{\text{déf}}{\Longleftrightarrow} x \leq y \ .$$

On dit que la relation d'ordre $\leq'$ est la relation d'ordre induite *sur X par la relation d'ordre $\leq$ sur A. Le plus souvent on utilise le* même *symbole pour les deux relations d'ordre.*

5.7 Lemme. *Soit A, B et C trois ensembles et soit $f : A \to B$ et $g : B \to C$ deux applications.*

(i) *Si f et g sont injectives, alors $g \circ f : A \to C$ est injective.*

(ii) *Si $g \circ f$ est injective, alors f est injective.*

(iii) *Si f et g sont surjectives, alors $g \circ f : A \to C$ est surjective.*

(iv) *Si $g \circ f$ est surjective, alors g est surjective.*

Si $f : A \to B$ est une application et $X \subset A$ un sous-ensemble, alors f est en particulier une relation entre A et B, ce qui nous permet de parler de l'image (direct) $f[X]$ de X par f. La définition nous donne la description suivante :

$$\begin{aligned} f[X] &= \{\, b \in B \mid \exists a \in X : (a,b) \in f \,\} = \{\, b \in B \mid \exists a \in X : f(a) = b \,\} \\ &= \{\, f(a) \mid a \in X \,\} \ , \end{aligned} \tag{5.8}$$

où dans la deuxième égalité on a utilisé la notation pour une application et dans la troisième égalité on a utilisé la simplification de notation déjà discutée dans [2.4].

Si f est une relation et si $Y \subset B$ est un sous-ensemble, alors on peut aussi parler de l'image réciproque $f^{-1}[Y]$ de Y par la relation f (mais attention, f^{-1} n'est pas forcément une application, voir [4.6]). Pour cet ensemble on obtient la description

$$\begin{aligned} f^{-1}[Y] &= \{\, a \in A \mid \exists b \in Y : (b,a) \in f^{-1} \,\} = \{\, a \in A \mid \exists b \in Y : (a,b) \in f \,\} \\ &= \{\, a \in A \mid \exists b \in Y : f(a) = b \,\} \\ &= \{\, a \in A \mid f(a) \in Y \,\} \ . \end{aligned}$$

Les descriptions qu'on trouve ici pour $f[X]$ et $f^{-1}[Y]$ sont les descriptions qu'on donne habituellement de l'image et l'image réciproque d'un ensemble par une application.

5.9 Lemme. *Soit $f : A \to B$ une application de A dans B, alors f est une application surjective si et seulement si on a l'égalité $f[A] = B$. Si f est injective, alors f est une application bijective de A dans $f[A]$.*

Ⓟ **5.10 Changer l'ensemble but d'une application.** *Soit $f : A \to B$ une application de A dans B et soit C un ensemble vérifiant $f[A] \subset C$. Alors f est (aussi) une application de A dans C : $f : A \to C$. En particulier pour $C = f[A]$, l'application $f : A \to f[A]$ est surjective.*

5.11 Corollaire. *Soit $f : A \to B$ une application injective. Alors $f : A \to f[A]$ est une application bijective.*

La morale du résultat [5.10] est que l'ensemble but d'une application f est hautement artificiel dans le sens qu'on peut le modifier presque à volonté. Sans changer l'ensemble f, on peut changer l'ensemble but B avec la seule contrainte que le nouvel

ensemble but contient l'image $f[A]$. Une fois arrivé là, il faut se poser la question sur la définition de l'image (directe) d'un sous-ensemble $X \subset A$ par l'application f. Quand on voit f comme une application $f : A \to B$, la définition de $f[X]$ est

$$f[X] = \{\, b \in B \mid \exists a \in X : b = f(a) \,\} \ ,$$

mais si on voit f comme une application $f : A \to C$, cette définition change en

$$f[X] = \{\, c \in C \mid \exists a \in X : c = f(a) \,\} \ .$$

Si on pense aux écritures

$$\{\, z \in \mathbf{R} \mid z^2 = -1 \,\} \qquad et \qquad \{\, z \in \mathbf{C} \mid z^2 = -1 \,\} \ ,$$

on s'aperçoit que ce n'est pas automatique que ces deux définitions de $f[X]$ coïncident. L'écriture simplifiée introduit dans [2.4] et utilisé dans (5.8) suggère que c'est la même chose, mais cela ne constitue pas une preuve (au contraire, c'est peut-être une preuve que la simplification n'est pas autorisée).

Ⓟ **5.12 Lemme.** *Soit A et B deux ensembles et soit $f : A \to B$ une application. Si C est un ensemble vérifiant $f[A] \subset C$, alors pour tout $X \subset A$ on a l'égalité*

$$\{\, b \in B \mid \exists a \in X : b = f(a) \,\} = \{\, c \in C \mid \exists a \in X : c = f(a) \,\} \ .$$

Ⓟ **5.13 La restriction d'une application.** *Soit A et B deux ensembles et soit $f : A \to B$ une application de A dans B. Si $X \subset A$ est un sous-ensemble, alors l'ensemble $f|_X \subset X \times B$ défini comme*

$$f|_X = f \cap (X \times B)$$

est une application de X dans B, appelée la restriction de f à X.

Ⓟ **5.14 Lemme.** *Soit $f : B \to A$ une application de B dans A et soit C, D deux ensembles. Alors on a l'implication*

$$D \subset C \subset B \qquad \Longrightarrow \qquad (f|_C)|_D = f|_D \ .$$

5.15 Proposition. *Soit A et B deux ensembles, soit $f \subset A \times B$ une relation entre A et B, soit $g \subset B \times A$ une relation entre B et A et soit $f^{-1} \subset B \times A$ la relation réciproque de f.*

(i) *Si f est une application bijective, alors on a les égalités*

$$f \circ f^{-1} = id_B \qquad et \qquad f^{-1} \circ f = id_A \ .$$

(ii) *Si les relations $f \circ g \subset B \times B$ et $g \circ f \subset A \times A$ vérifient les égalités*

$$f \circ g = id_B \qquad et \qquad g \circ f = id_A \ ,$$

alors f et g sont des applications bijectives et on a les égalités $g = f^{-1}$ et $f = g^{-1}$.

6. Ensembles infinis et la construction de N

Avec l'axiome de la réunion on peut former beaucoup d'ensembles finis. Par contre, on a l'impression qu'on n'arrive jamais à construire un ensemble infini. Mais c'est quoi exactement un ensemble infini ? Vers 1880 Dedekind a élaboré une définition pour distinguer un ensemble fini d'un ensemble infini : un ensemble A est infini s'il existe une bijection entre A et une vraie partie $B \subset A$ (c'est-à-dire $B \neq A$). Ou alors, A est un ensemble infini s'il existe une application injective $S : A \to A$ qui n'est pas surjective. Dans sa publication [**Ded87**, §5, 64.] *sur la construction de l'ensemble des entiers naturels, il fait la remarque :*

> *Toutes les autres tentatives de distinguer l'infini du fini dont j'ai eu connaissance ont eu tellement peu de succès me semble-t-il que je pense qu'il m'est permis de m'abstenir de les critiquer.*

L'histoire lui a donné raison, car c'est bien cette définition qu'on utilise depuis pour distinguer un ensemble fini d'un ensemble infini.

Définition. Soit A un ensemble. On dit que A est *un ensemble fini* si toute application injective $f : A \to A$ est forcément bijective. Par contraposée on dit que A est *un ensemble infini* s'il existe une application injective $f : A \to A$ qui n'est pas surjective.

Dès qu'on a donné cette définition, il faut se poser la question s'il existe de tels ensembles. Il est facile de montrer que les ensembles $\emptyset$ et $\{\emptyset\}$ sont finis, mais il est plus difficile de trouver un exemple d'un ensemble infini. La preuve donnée par Dedekind de l'existence *d'un ensemble infini n'est plus acceptée aujourd'hui. Pire, on ne peut pas le montrer à partir des axiomes qu'on a vu jusqu'à maintenant. C'est pourquoi on a introduit un axiome intitulé "axiome de l'infini." Avant d'énoncer cet axiome, notons tout de suite que cet axiome ne dit pas directement qu'il existe un ensemble muni d'une application vers lui-même qui est injective mais pas surjective. Une raison pour ne pas le faire ainsi (mais certainement pas la raison initiale) est que l'expression en termes primitives est très longue : s'il faut expliciter les couples, l'ensemble produit et les conditions d'être une application injective mais pas surjective, on obtient une formule de plusieurs lignes.*

Dans l'approche qu'on suit ici, on définit d'abord une opération *S qui à un ensemble A associe un nouvel ensemble $S(A)$, appelé le successeur de A. On pourrait le voir comme une application de la collection de tous les ensembles vers elle-même, mais l'esprit de la définition est le même que la définition des opérations d'union $\cup$ et de l'ensemble des parties $\mathcal{P}$: $S(A)$ est une abréviation pour un ensemble qui est complètement déterminé par l'ensemble A. Cette opération S va fonctionner comme une application injective mais pas surjective. La définition paraît peut-être arbitraire, mais on peut la justifier dans le contexte des ordinaux (voir §28).*

6.1 Définition du successeur d'un ensemble. Soit A un ensemble. Alors *le successeur de* A, noté $S(A)$ est l'ensemble

$$S(A) \stackrel{\text{déf}}{=} A \cup \{A\} \equiv \cup\{A, \{A\}\} \ .$$

Selon l'axiome de la paire, si A est un ensemble, alors $\{A\}$ est un ensemble et si A et $\{A\}$ sont des ensembles, alors $\{A, \{A\}\}$ est un ensemble. L'application de l'axiome de la réunion nous garantit alors que $S(A)$ est bien un ensemble.

Soit maintenant A un ensemble et $a \in A$ un de ses éléments. Alors a est un ensemble et on peut appliquer l'opération de successeur pour obtenir un nouvel ensemble $S(a)$. Cet ensemble appartient ou n'appartient pas à l'ensemble initiale A. Supposons que $S(a)$ appartient à A pour tout élément $a \in A$. Alors on peut définir une application $f : A \to A$ par

$$f = \big\{\, c \in A \times A \mid \exists a \in A : c = \big(a, S(a)\big) \,\big\} \qquad \textit{ou} \qquad \forall a \in A : f(a) = S(a) \ .$$

ou encore, avec l'argument de [2.4] pour simplifier l'écriture,

$$f = \{\, (a, S(a)) \mid a \in A \,\} \ . \tag{6.2}$$

Pour l'instant on ne sait rien sur l'injectivité et/ou surjectivité de f. Mais on peut faire la remarque que l'ensemble $S(a)$ contient toujours un élément, à savoir a lui-même. En particulier l'ensemble $S(a)$ n'est jamais l'ensemble vide. Donc, si A contient l'ensemble vide comme élément, alors l'application f ne peut pas être surjective car l'ensemble vide n'appartient pas à l'image de l'application f. Avec ces préparations on a obtenu l'axiome de l'infini, qui dit qu'il existe un tel ensemble A.

(Z7) Axiome de l'infini. $\exists\, A \ : \ \emptyset \in A$ et $\forall a \in A : S(a) \in A$.

Remarque. L'énoncé de l'axiome de l'infini est légèrement différent des autres axiomes dans le sens que cet axiome utilise trois autres axiomes pour être formulé, à savoir l'axiome de l'ensemble vide et, pour pouvoir parler de $S(a)$, l'axiome de la paire (deux fois) et l'axiome de la réunion.

Malgré son nom, l'axiome de l'infini ne dit pas explicitement qu'il existe un ensemble infini, car on n'a pas montré que l'application $f : A \to A$ définie par $f(a) = S(a)$ est injective. Pire, dans l'état actuel des choses on ne peut pas le montrer. Pourtant, une analyse superficielle pourrait faire croire que l'opération S est injective dans le sens $S(A) = S(B) \Rightarrow A = B$, mais quand on regarde de plus près, on trouve un petit problème. L'égalité $S(A) = S(B)$ veut dire, par définition du successeur, qu'on a l'égalité

$$A \cup \{A\} = B \cup \{B\} \ .$$

L'élément $A \in S(A)$ appartient donc à $S(B) = B \cup \{B\}$ et l'élément $B \in S(B)$ appartient à $S(A) = A \cup \{A\}$. Pour l'élément A on a donc deux possibilités : $A \in B$ ou $A \in \{B\}$ et pour l'élément B on a aussi deux possibilités : $B \in A$ ou $B \in \{A\}$. Les possibilités $A \in \{B\}$ ou $B \in \{A\}$ nous disent tout de suite qu'on a $A = B$.

Mais il reste la possibilité qu'on est dans le cas où on a $A \in B$ et $B \in A$. Une telle situation paraît bizarre, mais sans axiome supplémentaire on ne peut ni l'exclure, ni en déduire l'égalité $A = B$. Heureusement on peut quand même montrer, à partir de l'axiome de l'infini, qu'il existe un ensemble infini (dans le sens de Dedekind), à savoir l'ensemble des entiers naturels.

Les successeurs de 0**.** Soit A un ensemble. On dit que A a *contient les successeurs de* 0 si elle vérifie les deux conditions

$$\emptyset \in A \qquad \text{et} \qquad \forall a \in A : S(a) \in A \ .$$

Un ensemble *minimal* contenant les successeurs de 0 est un ensemble A contenant les successeurs de 0 qui vérifie la condition supplémentaire que si B est un autre ensemble contenant les successeurs de 0, alors on a l'inclusion $A \subset B$.

Ⓟ **6.3 Unicité d'un ensemble minimal contenant les successeurs de** 0**.** *Si A et B sont deux ensembles minimaux contenant les successeurs de* 0*, alors $A = B$.*

Ⓟ **6.4 Existence d'un ensemble minimal contenant les successeurs de** 0**.** *Il existe un ensemble minimal contenant les successeurs de* 0*.*

Une remarque concernant la preuve de [6.4] s'impose : la méthode utilisé pour construire l'ensemble minimal est très classique. On s'intéresse pour des ensembles avec une certaine propriété et on en cherche un qui est minimal (par rapport au nombre d'éléments ou, plus précisément, par rapport à l'inclusion). Alors on en prend un, on considère l'ensemble de tous les sous-ensembles qui ont cette propriété et on prend l'intersection. Avec de la chance cette intersection a, elle aussi, la propriété voulue et elle sera minimal. Par exemple, cette idée est utilisée en algèbre linéaire quand on parle du sous-espace vectoriel engendré par un sous-ensemble (c'est le plus petit sous-espace vectoriel qui contient le sous-ensemble), elle est utilisé en topologie quand on parle de la topologie engendrée par une collection de sous-ensembles (c'est la plus petite topologie qui contient la collection) et elle est utilisée en théorie de la mesure quand on parle de la tribu engendrée par une collection de sous-ensembles (c'est la plus petite tribu qui contient la collection).

6.5 Définition. Avec [6.4] et [6.3] on a montré qu'il existe un unique ensemble minimal contenant les successeurs de 0. Les éléments de cet ensemble, qu'on note avec le symbole **N**, sont appelés des *entiers naturels*. L'ensemble **N** s'appelle bien évidemment *l'ensemble des entiers naturels*. On introduit aussi des noms alternatifs pour certains ensembles :

$$0 \overset{\text{déf}}{=} \emptyset \quad , \quad 1 \overset{\text{déf}}{=} S(0) = \{\emptyset\} \quad \text{et} \quad 2 \overset{\text{déf}}{=} S(1) = \{\emptyset, \{\emptyset\}\} \ .$$

Il nous reste à montrer que $\mathbf{N}$ *est bien un ensemble infini dans le sens de Dedekind. Pour cela il suffit de montrer que l'application* $f : \mathbf{N} \to \mathbf{N}$ *donnée par* $f(n) = S(n) \equiv n \cup \{n\}$ *est injective mais pas surjective. La non-surjectivité est déjà montrée (*$\emptyset \in \mathbf{N}$ *et* $\forall n : S(n) \neq \emptyset$*), mais l'injectivité est restée en suspens. Pour le montrer il nous faut deux résultats préliminaires. Le premier est qu'on dispose de la preuve par récurrence et le deuxième est une propriété particulière des entiers naturels.*

Ⓟ **6.6 La preuve par récurrence.** *Soit* $E \subset \mathbf{N}$ *un ensemble vérifiant les deux propriétés*

$$0 \in E \qquad et \qquad \forall n \in \mathbf{N} : n \in E \Rightarrow S(n) \in E \ .$$

Alors on a l'égalité $E = \mathbf{N}$.

Ⓟ **6.7 Lemme.** *Soit* m *et* n *deux entiers naturels. Si* m *appartient à* n*, alors* m *est aussi un sous-ensemble de* n *:*

$$\forall m, n \in \mathbf{N} : m \in n \Rightarrow m \subset n \ .$$

Ⓟ **6.8 L'ensemble N est infini.** *Soit* m *et* n *deux entiers naturels. Si on a* $S(m) = S(n)$*, alors on a* $m = n$*. En particulier* $\mathbf{N}$ *est un ensemble infini dans le sens de Dedekind.*

Remarque. Dans la preuve de [6.8] on n'a pas écarté la possibilité qu'on a $m = n$ en même temps que $m \in n$ ou $n \in m$. Dans un tel cas on aurait donc $m \in m$. Dans [8.8] on montrera que cela ne peut pas arriver (pour un entier naturel au moins), mais à ce stade il nous suffit la conclusion $m = n$. Pour le moment il faut donc vivre avec la possibilité qu'un entier naturel peut être élément de lui-même.

7. Dedekind, Peano et Landau

La définition de l'ensemble des entiers naturels de Dedekind, telle qu'il la donne dans **[Ded87]** *en 1887, est quasiment identique à la définition présentée dans §6. La seule vraie différence est qu'il ne commence pas avec l'élément privilégié* $0 = \emptyset$*, mais avec* 1*. Son point de départ est un ensemble* N *muni d'une application injective* $S : N \to N$*. Il définit une* chaine *comme un sous-ensemble* K *de* N *tel que* $S(K) \subset K$*. Aujourd'hui on dirait que c'est un sous-ensemble stable sous l'application* S*. Pour un sous-ensemble quelconque* $L \subset N$ *il définit la chaine associée à* L *comme l'intersection de tous les chaines dans* N *qui contiennent* L *et il montre que c'est la plus petite chaine contenant* L*. Pour besoin de la cause, on note cet ensemble ici comme* C_L*. Finalement il définit un* système de nombres N *comme étant un ensemble sur lequel est définie une application* S *et qui contient un élément* $1 \in N$ *vérifiant les quatre conditions*

(α) $S(N) \subset N$ *(autrement dit,* S *est une application de* N *dans* N*),*

(β) $N = C_{\{1\}}$ *(autrement dit,* N *est la plus petite chaine contenant* 1*),*

(γ) $1 \notin S(N)$ *et*

(δ) l'application $S : N \to N$ *est injective.*

Les conditions (α), (γ) et (δ) disent que N *est un ensemble infini (dans le sens de Dedekind) : l'application* $S : N \to N$ *est injective mais pas surjective. Avec la condition supplémentaire (β) Dedekind parle d'un ensemble infini simple. Cette condition (β) dit que* N *ne contient pas un ensemble plus petit qui est stable par* S *et qui contient l'élément privilégié* 1*. C'est l'équivalent de notre condition d'ensemble minimal contenant les successeurs de* 0*. Et comme on a vu dans [6.6], cette condition est la condition de récurrence.*

En 1891 Peano reprend le travail de Dedekind et publie un article **[Pea91]** *sur le concept d'un nombre. Dans cet article il présente une approche axiomatique des entiers naturels sans référence à une construction explicite de* $\mathbf{N}$*. Son idée était que on part de trois symboles* $\mathbf{N}$*,* 0 *et* S *qui satisfont* 6 *axiomes.*[1]

Les axiomes de Peano.

(P0) $\mathbf{N}$ est un ensemble.

(P1) $0 \in \mathbf{N}$.

(P2) S est une opération qui à $n \in \mathbf{N}$ associe un autre élément $S(n)$ de $\mathbf{N}$.

(P3) $\forall E : [\, 0 \in E \text{ et } \forall n : n \in E \Rightarrow S(n) \in E \,] \Rightarrow \mathbf{N} \subset E$.

(P4) $\forall n, m : [\, n, m \in \mathbf{N} \text{ et } S(n) = S(m) \,] \;\Rightarrow\; n = m$.

(P5) $\forall n : n \in \mathbf{N} \;\Rightarrow\; S(n) \neq 0$.

Les trois premiers axiomes nous donnent la nature de ces trois symboles : $\mathbf{N}$ *est un ensemble,* 0 *est un élément de* $\mathbf{N}$ *et* S *est une application qui envoie les éléments*

1. On donne ici la forme qu'on trouve dans **[Pea08]**, y compris la numérotation de 0 à 5 ; on a seulement adapté les notations. Dans l'article original **[Pea91]**, le symbole 0 était remplacé par le symbole 1.

de $\mathbf{N}$ *dans* $\mathbf{N}$ *(ce qui laisse la possibilité que le domaine de définition de l'application* S *est plus grand que* $\mathbf{N}$*). (P4) dit que l'application* S *est injective et (P5) dit que* 0 *n'est pas dans l'image de* S*. Si on compare ces axiomes avec les propriétés de Dedekind, on s'aperçoit vite que c'est la même chose : (P0) et (P1) sont dans les prémisses de Dedekind, (P2) est la condition* (α)*, (P4) est la condition* (δ) *et (P5) est la condition* (γ)*. La seule différence avec les propriétés de Dedekind se trouve dans l'axiome (P3), qui correspond à la propriété* (β) *de Dedekind, mais la formulation est différente. Là où Dedekind parle d'un ensemble infini simple en disant que* N *est la chaine associée à l'élément* 1*, Peano écrit explicitement la propriété de récurrence. Comme on l'a vu, la propriété de récurrence est une conséquence directe des propriétés de Dedekind. De ce point de vue il n'y a donc pas une grande différence entre Dedekind et Peano. Mais le point de vue de Peano est complètement différent : il ne cherchait pas à* construire *l'ensemble des entiers naturels, mais à le* caractériser *par des axiomes. Comme Dedekind, il montre que ces propriétés permettent de construire toutes les opérations sur* $\mathbf{N}$ *(addition, multiplication, relation d'ordre) et de démontrer leurs propriétés usuelles. Mais il montre en plus que ces propriétés sont indépendantes dans le sens que, dès qu'on laisse de coté un d'entre eux, il existe d'autres ensembles que les entiers naturels qui satisfont aux axiomes qui restent. Par exemple, si on laisse tomber la condition de l'injectivité de* S*, on peut prendre pour* $\mathbf{N}$ *un ensemble à deux éléments* $\{0,1\}$ *avec l'application constante* 1*. Ou si on laisse tomber la condition que* 0 *n'est pas dans l'image de* S*, on peut toujours prendre un ensemble à deux éléments* $\{0,1\}$*, mais avec l'application* $S(0)=1$ *et* $S(1)=0$*. Et si on laisse tomber la propriété de récurrence, on peut prendre un ensemble infini plus grand comme les entiers relatifs avec l'application* S *définie par* $S(n)=n+1$ *pour* $n\geq 0$ *et* $S(n)=n-1$ *pour* $n<0$*.*

Ⓟ **7.1 Proposition.** *L'ensemble* $\mathbf{N}$ *définie dans [6.5] avec l'opération* S *définie dans [6.1] et l'élément* $0=\emptyset\in\mathbf{N}$ *vérifie les axiomes de Peano.*

Mais le travail n'est pas fini quand on dispose d'un ensemble $\mathbf{N}$ *vérifiant les axiomes de Peano. Il faut définir les différentes structures sur* $\mathbf{N}$ *comme l'addition, la multiplication et la relation d'ordre. Dedekind commence avec la relation d'ordre et poursuit avec l'addition et la multiplication. Peano commence avec l'addition et la multiplication et utilise l'addition pour définir la relation d'ordre. L'idée pour l'addition est déjà fortement suggéré par le nom "successeur" pour l'opération* S *: on définit* $n+1$ *comme étant* $S(n)$ *:*

$$\forall n\in\mathbf{N}: n+1 \stackrel{déf}{=} S(n) \ ,$$

où 1 *est l'autre nom pour l'ensemble* $\{\emptyset\}=S(\emptyset)=S(0)\in\mathbf{N}$*. Le reste de l'addition se fait par récurrence :*

$$\forall m\in\mathbf{N}: n+S(m)=S(n+m) \ . \tag{7.2}$$

Beaucoup de mathématiciens pensent qu'avec cette formule on a bien défini l'addition. Malheureusement il y a un petit problème important qu'on oublie facilement : cette formule en soi *ne montre pas l'existence de l'addition ! Il faut, une fois pour toute, montrer qu'une définition par récurrence définit vraiment quelque chose. Ce*

n'est que seulement avec ce résultat supplémentaire qu'on peut définir une application sur $\mathbf{N}$ *par récurrence.*

Pour bien expliquer la situation, il faut d'abord donner le point de départ. On commence avec un ensemble A*, une application* $f : A \to A$ *et un élément particulier* $a_0 \in A$*. Et on veut définir une application (suite)* $b : \mathbf{N} \to A$ *par les formules*

$$b(0) = a_0 \qquad et \qquad \forall n \in \mathbf{N} : b\big(S(n)\big) = f\big(b(n)\big) \ . \tag{7.3}$$

En lisant ces formules, on se dit qu'on connaît $b(0)$ *et si on connaît* $b(n)$*, alors on connaît* $b(S(n))$*. Par récurrence on connaît donc toute la suite. Où est l'erreur ? L'erreur est dans l'hypothèse de récurrence ! On utilise la propriété d'un entier* n *qui dit que la valeur* $b(n)$ *de la fonction* b *au point* $n \in \mathbf{N}$ *est connue. Mais, du moment qu'on emploie l'expression "la fonction* b*," on a implicitement supposé que cet objet existe. Et une fonction est un objet* global*. On ne peut pas dire qu'une fonction est définie en un point et que peut-être elle n'est pas (encore) définie en un autre point. Si une fonction n'est pas définie dans un point, ce n'est pas une fonction sur le domaine en considération, mais sur un domaine plus petit.*[2] *Écrire la propriété "*$b(n)$ *est définie" présuppose donc que la fonction* b *existe et c'est exactement cela qu'on veut montrer. On tombe donc dans un cercle vicieux.*

Dedekind a reconnu ce problème dans **[Ded87]** *et l'a résolu. Sa solution repose sur une définition préalable d'une relation d'ordre sur* $\mathbf{N}$*, ce qui permet de définir, pour chaque* $n \in \mathbf{N}$*, l'ensemble* Z_n *par*[3]

$$Z_n = \{m \in \mathbf{N} \mid 0 \leq m \leq n\} \ .$$

À l'aide de cet ensemble on prend l'hypothèse

$$\textit{il existe une fonction } b_n : Z_n \to A \textit{ vérifiant} \tag{7.4}$$

$$b_n(0) = a_0 \qquad et \qquad \forall m \in Z_n : m < n \Rightarrow b_n\big(S(m)\big) = f\big(b_n(m)\big) \ . \tag{7.5}$$

Il n'est pas difficile de montrer que cette propriété est vrai pour $n = 0$ *et si elle est vraie pour* n*, elle l'est pour* $S(n)$*. Par récurrence on aura donc montré qu'elle est vrai pour tout entier naturel* $n \in \mathbf{N}$*. Mais, même quand on sait qu'il existe pour tout* $n \in \mathbf{N}$ *une fonction* b_n *avec les propriétés voulues sur l'ensemble* $Z_n \subset \mathbf{N}$*, on n'en peut pas déduire,* sans argument supplémentaire*, que cette propriété est vraie pour l'ensemble* $\mathbf{N}$ *lui-même. La complétion de l'argument consiste à définir une fonction* $b : \mathbf{N} \to A$ *par*

$$\forall n \in \mathbf{N} : b(n) = b_n(n) \ .$$

Ensuite il faut remarquer (démontrer) que si on a l'inclusion $Z_m \subset Z_n$*, alors la fonction* b_m *définie sur* Z_m *coïncide sur* Z_m *avec la fonction* b_n *définie sur* Z_n *:*

$$b_n|_{Z_m} = b_m \ .$$

Il s'ensuit que la fonction b *vérifie les conditions (7.3).*

Peano, contrairement à Dedekind, ne parle pas du tout de ce problème et définit directement l'addition par la formule (7.2), sans se poser la question si une telle formule garantit l'existence (et il utilise l'addition pour définir la relation d'ordre). Landau a commis la même omission, au moins dans un premier temps. Il en témoigne dans le préface de son livre **[Lan51]** *sur les fondations de l'analyse dans*

2. Par contre, il est bien possible qu'on ne connaît pas une expression explicite pour la valeur d'une fonction dans un point donné ; cela arrive notamment avec l'axiome du choix où on affirme l'existence d'une fonction sans avoir une expression explicite pour les valeurs prises dans chaque point.

3. Bien sûr, chez Dedekind l'ensemble Z_n commence à 1, pas à 0.

lequel il construit les différentes systèmes de nombres $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ *et* $\mathbf{C}$ *à partir des axiomes de Peano. Il raconte qu'un de ses collègues qui avait utilisé son manuscript lui avait fait la remarque qu'il avait commis une erreur et qu'il fallait un axiome supplémentaire pour le rectifier. Landau avoue tout de suite (dans son préface) que l'erreur était bien là, mais qu'un axiome supplémentaire n'était pas du tout nécessaire. Il poursuit son histoire avec la remarque qu'il avait élaboré avec son collègue Von Neumann une solution selon l'idée de Dedekind, mais qu'à la dernière minute on lui a informé d'une solution beaucoup plus simple, trouvée par le mathématicien Kalmár. Et c'est cette solution qu'il présente dans* [**Lan51**]. *L'avantage de sa solution est qu'elle ne nécessite pas une construction laborieuse de la relation d'ordre sur* $\mathbf{N}$ *telle que c'est fait dans* [**Ded87**]. *Par contre, elle repose fortement sur le fait que pour la définition de l'addition et de la multiplication dans* $\mathbf{N}$, *l'ensemble* A *d'une suite récurrente générale est aussi l'ensemble* $\mathbf{N}$. *Sa solution pour montrer l'existence d'une suite récurrente à valeurs dans* $\mathbf{N}$ *est essentiellement une récurrence double.*

La "solution" qu'on présente ici ne repose ni sur une relation d'ordre sur $\mathbf{N}$, *ni sur le cas particulier que l'ensemble* A *est l'ensemble* $\mathbf{N}$ *lui-même. Elle repose seulement sur les axiomes de Peano et la définition d'une application comme un sous-ensemble du produit cartésien vérifiant certaines conditions. Mais avant d'énoncer ce résultat, on discute quelques généralisations. Il arrive souvent qu'on a un ensemble* P *(qu'on considère comme un ensemble de paramètres) et qu'on veut définir, pour tout élément* $p \in P$, *une application* $\varphi_p : \mathbf{N} \to A$ *par les conditions*

$$\varphi_p(0) = a_p \qquad et \qquad \varphi_p\big(S(n)\big) = f_p\big(\varphi_p(n)\big) \ ,$$

où a_p *est une condition initiale qui dépend du paramètre* $p \in P$ *et où l'application* f_p *dépend, elle aussi, du paramètre. Si on voit la correspondance* $p \mapsto a_p$ *comme une application* $g : P \to A$ *et si on voit les familles d'applications* φ_p *et* f_p *comme des applications sur* $P \times \mathbf{N}$ *et* $P \times A$ *respectivement (les deux dans* A*), on est donc à la recherche d'une application* $\varphi : P \times \mathbf{N} \to A$ *vérifiant*

$$\forall p \in P : \varphi(p, 0) = g(p) \qquad et \qquad \forall p \in P \ \forall n \in \mathbf{N} : \varphi(p, S(n)) = f(p, \varphi(p, n)) \ .$$

Une autre situation qui arrive de temps en temps est que la relation de récurrence a une dépendance explicite de n. *Autrement dit, l'élément suivant* $\varphi(S(n))$ *ne dépend pas seulement de l'élément précédent* $\varphi(n)$, *mais aussi de la valeur explicite de* n. *Un exemple simple est la définition par récurrence de* $n!$ *(*n *factoriel) comme la suite* $\varphi : \mathbf{N} \to \mathbf{N}$ *définie par les conditions*

$$\varphi(0) = 1 \qquad et \qquad \varphi(n+1) = (n+1) \times \varphi(n) \ .$$

Dans une telle situation on a une condition initiale $a_0 \in A$ *et une application* $f : \mathbf{N} \times A \to A$ *et on cherche à définir une application* $\varphi : \mathbf{N} \to A$ *vérifiant*

$$\varphi(0) = a_0 \qquad et \qquad \varphi\big(S(n)\big) = f\big(n, \varphi(n)\big) \ .$$

Dans l'exemple ci-dessus on a $A = \mathbf{N}$, $a_0 = 1$ *et l'application* $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ *donnée par*

$$f(n, a) = (n+1) \times a \ .$$

Un autre exemple sera donné dans la preuve de [17.7], où on construit la suites des décimales d'un nombre réel. Quand on combine ces deux généralisations en une, on obtient la définition par récurrence générale [7.6].

Ⓟ **7.6 Définition par récurrence générale.** *Soit* A *et* P *deux ensembles et soit* $g : P \to A$ *et* $f : (P \times \mathbf{N}) \times A \to A$ *deux applications. Alors il existe une et une*

seule application $\varphi : P \times \mathbf{N} \to A$ *vérifiant*

$$\forall p \in P : \varphi(p,0) = g(p) \qquad \textit{et}$$
$$\forall p \in P\ \forall n \in \mathbf{N} : \varphi\big(p, S(n)\big) = f\big((p,n), \varphi(p,n)\big) \quad . \tag{7.7}$$

Dans la preuve de [7.6] on utilise une deuxième fois la technique décrite après la preuve de l'existence de l'ensemble $\mathbf{N}$ *[6.4] : la technique pour obtenir un objet minimal. L'ensemble* $\mathcal{F}$ *contient tous les sous-ensembles de* $(P \times \mathbf{N}) \times A$ *qui ont la propriété de récurrence et on définit* φ *comme l'intersection de* $\mathcal{F}$*. La partie difficile de la preuve consiste à montrer que l'élément minimal est une* application *de* $P \times \mathbf{N}$ *dans* A*.*

Ⓟ **7.8 Définitions par récurrence simplifiées.**

(i) *Soit* A *et* P *deux ensembles,* $g : P \to A$ *et* $f : P \times A \to A$ *deux applications. Alors il existe une et une seule application* $\varphi : P \times \mathbf{N} \to A$ *vérifiant*

$$\forall p \in P : \varphi(p,0) = g(p) \quad \textit{et} \quad \forall p \in P\ \forall n \in \mathbf{N} : \varphi\big(p, S(n)\big) = f\big(p, \varphi(p,n)\big) \quad .$$

(ii) *Soit* A *un ensemble,* $a_0 \in A$ *un élément et* $f : \mathbf{N} \times A \to A$ *une application. Alors il existe une et une seule application* $\varphi : \mathbf{N} \to A$ *vérifiant*

$$\varphi(0) = a_0 \qquad \textit{et} \qquad \forall n \in \mathbf{N} : \varphi\big(S(n)\big) = f\big(n, \varphi(n)\big) \quad .$$

(iii) *Soit* A *un ensemble,* $a_0 \in A$ *un élément et* $f : A \to A$ *une application. Alors il existe une et une seule application* $\varphi : \mathbf{N} \to A$ *vérifiant*

$$\varphi(0) = a_0 \qquad \textit{et} \qquad \forall n \in \mathbf{N} : \varphi\big(S(n)\big) = f\big(\varphi(n)\big) \quad .$$

Ⓟ **7.9 Tous les entiers sauf 0 ont un prédécesseur.**

$$\mathbf{N} = \{\, n \in \mathbf{N} \mid n = 0 \ \textit{ou}\ \exists k \in \mathbf{N} : n = S(k) \,\} \quad .$$

Ⓟ **7.10 Proposition.** *Soit* A *un ensemble. Alors* A *est un ensemble infini si et seulement s'il existe une application injective* $g : \mathbf{N} \to A$*.*

Chapitre 2

Des nombres

8. Les opérations sur N

Dans §6 on a défini l'ensemble **N** *des entiers naturels, mais pour l'instant on n'en sait pas plus. En particulier on ne connaît pas les opérations usuelles d'addition et multiplication, ni comment comparer deux entiers naturels. Notre première tâche est donc de* définir *ces opérations. Mais une simple définition ne suffit pas : il faut* aussi *montrer que ces opérations qu'on vient de définir ont bien les propriétés connues et qu'on utilise tout le temps (comme par exemple le fait qu'on a l'égalité* $2+5=5+2$*, ou* $2\times(3+1)=2\times 3+2\times 1$*). Ce qui rend cette tâche un peu moins évidente qu'on pourrait croire est le fait qu'on connaît ces opérations tellement bien et qu'on a tellement l'habitude de les utiliser, qu'on ne se rend plus compte quand on le fait. Il faut donc être très vigilant de ne pas utiliser des propriétés qu'on n'a pas encore démontré. Un exemple type de ce qui arrive est la "simplification"*

$$x+a=y+a \quad \Longrightarrow \quad x=y \ .$$

Le réflexe naturel est de le faire en soustrayant la quantité a *des deux côtés de l'égalité initiale. Mais on ne connaît pas l'opération de soustraction dans* **N** *! Et, même si on la connaissait, il fallait vérifier qu'on a le droit de l'appliquer, car la soustraction n'est pas définie sur tous les couples d'entiers naturels : on ne connaît pas (encore) les nombres négatifs.*

On commence donc avec la définition de ce qu'on entend par une opération (interne) sur un ensemble A*. On verra que c'est un autre nom pour une application de* $A\times A$ *dans* A*. De là on peut se poser la question pourquoi on introduit un autre nom pour un object qu'on connaît déjà. La raison n'est pas qu'on le fait pour rendre les mathématiques plus opaque, au contraire. L'idée d'attacher plusieurs noms à un même objet (en occurence une application de* $A\times A$ *dans* A*) aide à fixer les idées qui vont nous guider dans la discussion et dans les explications. Par exemple : quand on parle du* nombre 2*, cela suggère automatiquement qu'on peut faire une addition avec, ou d'autres genres de calculs. Mais si on parle de* l'ensemble 2*, on a plutôt tendance à penser à un ensemble avec deux éléments. Il s'agit bien dans ces deux cas du même ensemble, mais le nom qu'on donne nous oriente dans nos pensées.*

8.1 Définition d'une opération interne. Si A est un ensemble, alors une *opération interne (sur* A*)* est une application $p : A\times A\to A$. Dans la quasi totalité des cas, une opération interne est notée par un symbole entre les deux arguments, comme par exemple un $+$, un $\times$ ou un $\star$. On écrit "donc", avec $a,b\in A$:

$$a+b \quad \text{pour} \quad p(a,b) \ .$$

Si $\star : A \times A \to A$ est une opération interne sur A, on dit qu'elle est *associative* si elle vérifie la condition

$$\forall a, b, c \in A : a \star (b \star c) = (a \star b) \star c \ .$$

On dit qu'elle est *commutative* si elle vérifie la condition

$$\forall a; b \in A : a \star b = b \star a \ .$$

Et on dit qu'un élément $e \in A$ est *un élément neutre* pour l'opération interne $\star$ si on a la propriété

$$\forall a \in A : a \star e = e \star a = a \ .$$

Ⓟ **8.2 Lemme.** *Si une opération interne $\star$ sur un ensemble A admet un élément neutre, alors cet élément est unique.*

Définition de l'addition. On applique [7.8.i] avec $A = P = \mathbf{N}$ et les applications $g : \mathbf{N} \to \mathbf{N}$ et $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ définies par

$$g(k) = k \qquad \text{et} \qquad f(k, \ell) = S(\ell) \ .$$

Alors on obtient une application $\varphi : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ vérifiant

$$\varphi(k, 0) = k \qquad \text{et} \qquad \varphi\big(k, S(\ell)\big) = S\big(\varphi(k, \ell)\big) \ ,$$

qui sera l'opération interne d'addition sur $\mathbf{N}$. Il est d'usage de le noter par le symbole $+$ entre ses arguments :

$$k + \ell \overset{\text{déf}}{=} \varphi(k, \ell) \ .$$

Avec cette notation, la formule qui définit l'addition par récurrence s'écrit comme

$$k + 0 = k \qquad \text{et} \qquad k + S(\ell) = S(k + \ell) \ . \tag{8.3}$$

Nota Bene. Il est tentant d'écrire la définition de l'addition sous la forme

$$k + 0 = k \qquad \text{et} \qquad k + (\ell + 1) = (k + \ell) + 1 \ , \tag{8.4}$$

mais cette façon de l'écrire est une définition circulaire, car on ne sait pas ce que c'est $k+1$. Il faut donc impérativement passer par la formulation (8.3). Avec $1 = S(0)$, on en déduit directement qu'on a $k + 1 = S(k)$, ce qui permet de réécrire (8.3) comme (8.4), mais (8.4) ne devient pas pour autant une *définition*.

Ⓟ **8.5 Lemme.** *L'addition $+ : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ vérifie les propriétés*

(i) $\forall k, m, n \in \mathbf{N} : (k + m) + n = k + (m + n)$ *(associativité),*

(ii) $\forall n \in \mathbf{N} : n + 0 = 0 + n = n$ *(élément neutre),*

(iii) $\forall n \in \mathbf{N} : n + 1 = 1 + n = S(n)$,

(iv) $\forall m, n \in \mathbf{N} : m + n = n + m$ *(commutativité).*

Connaître l'opération interne d'addition sur $\mathbf{N}$ et ses propriétés est intéressant mais savoir additionner des entiers n'est pas très utile en soi. On veut résoudre des équations et pour cela on a besoin d'outils. Le résultat suivant est le premier qui

va permettre de "résoudre" des équations dans **N**. *À vrai dire, ce résultat ne sert pas vraiment dans la pratique. Dans la pratique on se sert de propriétés plus performantes, valables pour "tous" les nombres. Par contre, pour montrer ces résultats plus performantes, on a besoin de ces résultats préliminaires dans* **N**.

Ⓟ **8.6 Lemme.** *Soit k, m et n trois entiers naturels. Alors on a les implications suivantes :*

(i) $m+k=n+k \;\Rightarrow\; m=n$ *et*

(ii) $m+n=0 \;\Rightarrow\; m=n=0$.

Ⓟ **8.7 Corollaire.** *Pour tout $k\in\mathbf{N}$ on a $S(k)\equiv k+1\neq k$.*

8.8 Remarque. Dans la preuve de [6.7] on était confronté avec la possibilité qu'un entier naturel $k\in\mathbf{N}$ pourrait appartenir à lui-même. Cela nous n'a pas empêché de finir la preuve, mais cette possibilité n'était pas écartée. Analysons la situation. Pour $k\in\mathbf{N}$ on a, par définition, $S(k)=k\cup\{k\}$ et donc a fortiori $k\subset S(k)$. Pour avoir l'égalité $S(k)=k$, il suffit donc d'avoir l'inclusion dans l'autre sens, ce qui sera le cas seulement si on a l'inclusion $\{k\}\subset k$, c'est-à-dire $k\in k$. On a donc l'équivalence

$$S(k)=k \qquad\Longleftrightarrow\qquad k\in k\ .$$

Avec [8.7] il s'ensuit qu'un entier naturel $k\in\mathbf{N}$ ne peut pas appartenir à lui-même : $k\notin k$.

Définition de la multiplication. En utilisant l'addition on peut maintenant définir la multiplication par récurrence. On applique [7.8.i] avec $A=P=\mathbf{N}$ et les applications $g:\mathbf{N}\to\mathbf{N}$ et $f:\mathbf{N}\times\mathbf{N}\to\mathbf{N}$ définies par

$$g(k)=0 \qquad\text{et}\qquad f(k,\ell)=k+\ell\ .$$

Alors on obtient une application $\varphi:\mathbf{N}\times\mathbf{N}\to\mathbf{N}$ vérifiant

$$\varphi(k,0)=0 \qquad\text{et}\qquad \varphi(k,S(\ell))=k+\varphi(k,\ell)$$

qui sera l'opération interne de multiplication sur **N**. Il est d'usage de le noter par le symbole $\times$ entre ses arguments :

$$k\times\ell \overset{\text{déf}}{=} \varphi(k,\ell)\ .$$

Avec cette notation, la formule qui définit la multiplication par récurrence s'écrit comme

$$k\times 0=0 \qquad\text{et}\qquad k\times S(\ell)=k+(k\times\ell)=(k\times\ell)+k\ . \tag{8.9}$$

Ⓟ **8.10 Lemme.** *La multiplication $\times:\mathbf{N}\times\mathbf{N}\to\mathbf{N}$ vérifie les propriétés*

(i) $\forall n\in\mathbf{N}: n\times 0=0=0\times n$,

(ii) $\forall n\in\mathbf{N}: n\times 1=n=1\times n$ *(élément neutre),*

(iii) $\forall k,m,n\in\mathbf{N}: k\times(m+n)=(k\times m)+(k\times n)$ *(distributivité à gauche),*

(iv) $\forall k,m,n\in\mathbf{N}: (k+m)\times n=(k\times n)+(m\times n)$ *(distributivité à droite),*

(v) $\forall k, m, n \in \mathbf{N} : k \times (m \times n) = (k \times m) \times n$ *(associativité),*

(vi) $\forall m, n \in \mathbf{N} : m \times n = n \times m$ *(commutativité).*

Si $\star : A \times A \to A$ est une opération interne sur l'ensemble A, il n'y a aucune raison de croire que cette opération est associative. Il suffit de penser à la soustraction dans $\mathbf{Z}$, où on n'a pas l'égalité $3 - (2 - 1) = (3 - 2) - 1$. Par contre, si l'opération interne est associative, l'ordre dans lequel on effectue les opérations n'a pas d'importance. La propriété d'associativité nous dit que l'expression

$$a \star b \star c$$

a un sens, car les deux façons de mettre des parenthèses pour donner un sens à cette formule (à savoir $a \star (b \star c)$ et $(a \star b) \star c$) donnent le même résultat. Le même raisonnement montre qu'on a l'égalité

$$(a \star b) \star (c \star (d \star e)) = (a \star ((b \star c) \star d)) \star e \ ,$$

pour cinq éléments $a, b, c, d, e \in A$, car on peut appliquer l'associativité à répétition comme

$$\begin{aligned}(a \star b) \star (c \star (d \star e)) &= (a \star b) \star ((c \star d) \star e) = ((a \star b) \star (c \star d)) \star e \\ &= (a \star (b \star (c \star d))) \star e = (a \star ((b \star c) \star d)) \star e \ .\end{aligned}$$

Bien que la liste de toutes les possibilités de mettre des parenthèses dans l'expression $a \star b \star c \star d \star e$ pour en donner un sens est longue (il y en a 24), on s'imagine facilement qu'on arrive à montrer que toutes ces possibilités donnent le même résultat. On peut donc écrire $a \star b \star c \star d \star e$ sans crainte d'ambiguïté dans le résultat (bien qu'il y a ambiguïté dans l'ordre dans lequel il faut effectuer les opérations).

De là, il est facile d'imaginer que c'est vrai pour toute suite (finie) d'éléments de A séparés par le symbole de l'opération interne associative. Il est effectivement possible de montrer que, mettre de deux façons différentes des parenthèses ne change pas le résultat. La preuve est assez longue, sans trop d'intérêt et se fait par récurrence sur la longueur de la suite. Dorénavant on accepte ce résultat, bien qu'on ne l'a pas démontré explicitement.

8.11 Omission des parenthèses/priorité des opérations. Si $\star : A \times A \to A$ est une opération interne *associative* sur l'ensemble A, alors on peut omettre les parenthèses dans une expression où interviennent plusieurs opération $\star$ de suite, du style $a \star b \star c \star d$, car l'ordre dans lequel on effectue ces opérations n'a pas d'importance. On écrit donc

$$a \star b \star c \star d \star e \qquad \text{au lieu de (par exemple)} \qquad (a \star b) \star \big(c \star (d \star e)\big) \ .$$

L'avantage d'une telle omission est que cela améliore la lisibilité de la formule. Le même argument est utilisé quand on dispose de *deux* opérations interne *associative* $\star$ et $\blacksquare$ sur A. On décide qu'un des deux a priorité sur l'autre (disons $\blacksquare$ sur $\star$). Et alors on omet les parenthèses dans une expression où interviennent plusieurs opérations $\star$ et $\blacksquare$, du style $a \star b \blacksquare c \blacksquare d \star e$. La priorité de $\blacksquare$ sur $\star$ dit alors qu'il faut d'abord effectuer les opérations $\blacksquare$, et seulement après les opérations $\star$. On écrit donc

$$a \star b \blacksquare c \blacksquare d \star e \qquad \text{au lieu de (par exemple)} \qquad \big(a \star \big(b \blacksquare (c \blacksquare d)\big)\big) \star e \ .$$

Par contre, si l'opération non-prioritaire doit s'effectuer avant l'opération prioritaire, on ne peut pas omettre les parenthèses :

$$(a \star b) \blacksquare c \overset{\text{en général}}{\neq} a \star (b \blacksquare c) \overset{\text{par priorité}}{=} a \star b \blacksquare c \ .$$

Les opération d'addition et de multiplication sont deux opérations interne associative sur **N**. Il est coutume d'accorder la priorité à la multiplication sur l'addition. La convention sur l'omission des parenthèses nous permet alors d'écrire les propriétés de distributivité [8.10.iii/iv] comme

$$k \times (m+n) = k \times m + k \times n \qquad \text{et} \qquad (k+m) \times n = k \times n + m \times n \ .$$

Comme pour l'addition, une fois qu'on connaît la multiplication dans **N**, *on veut résoudre des équations qui font intervenir une multiplication. Et comme pour l'addition, les résultats qui vont suivre sont les précurseurs indispensables de résultats plus performants.*

Ⓟ **8.12 Lemme.** $\forall m, n \in \mathbf{N}\ \exists k \in \mathbf{N} : (m + k = n)$ *ou* $(n + k = m)$.

Ⓟ **8.13 Lemme.** *Soit* k, m *et* n *trois éléments de* **N**. *Alors on a les équivalences*

(i) $m \times n = 0 \ \Leftrightarrow\ m = 0$ *ou* $n = 0$.

(ii) $m \times n = 1 \ \Leftrightarrow\ m = n = 1$.

(iii) $k \times m = k \times n \ \Leftrightarrow\ m = n$ *ou* $k = 0$.

À part les opérations internes d'addition et multiplication, la description des entiers naturels ne sera pas complet sans sa relation d'ordre. Il y a plusieurs façons de définir cette relation d'ordre sur **N**. *Avec notre définition de* **N** *via l'axiome de l'infini (Z7), la définition "naturel" est de dire qu'on a* $m \leq n$ *si et seulement si* $m \subset n$. *Autrement dit, la relation d'ordre n'est rien d'autre que l'inclusion. Par contre, avec cette définition il sera nettement plus difficile de montrer les liens entre la relation d'ordre et les operations d'addition et multiplication dont on se sert dans des calculs. On opte donc ici pour l'approche par les axiomes de Peano, ce qui veut dire qu'on définit la relation d'ordre en termes de l'addition. Ce ne sera que beaucoup pus tard qu'on montrera, dans [28.19], que notre définition de la relation d'ordre via l'addition coïncide avec l'inclusion. D'autre part, ce n'est que par commodité qu'on a repoussé la preuve de l'égalité de ces deux définitions, car le lecteur intéressé pourrait facilement le montrer lui-même par récurrence.*

Ⓟ **8.14 La relation d'ordre sur N.** *La relation* $\leq$ *sur* **N** *définie par la formule*

$$\forall m, n \in \mathbf{N} \quad : \quad m \leq n \quad \Longleftrightarrow \quad \exists k \in \mathbf{N} : m + k = n$$

est une relation d'ordre total.

Ⓟ **8.15 Lemme.** *Soit* $j, k, \ell \in \mathbf{N}$ *trois entiers naturels. Alors on a les équivalences*

(i) $k \leq \ell \;\Leftrightarrow\; k+j \leq \ell+j$ *et*
(ii) $k \times j \leq \ell \times j \;\Leftrightarrow\; k \leq \ell$ *ou* $j = 0$.

Ⓟ **8.16 Il n'y a pas d'entiers entre ℓ et $S(\ell) = \ell + 1$.**

$$\forall k, \ell \in \mathbf{N} \quad : \quad k \leq \ell \iff k < S(\ell) = \ell + 1 \ .$$

Notre discussion sur les entiers naturels $\mathbf{N}$ *ne serait pas complet sans énoncer la propriété fondamentale de son relation d'ordre qui dit que tout ensemble (non-vide) d'entiers contient un plus petit élément. Bien que cette propriété des entiers paraît évidente, c'est une propriété assez exceptionnelle : si on se donne un ensemble muni d'un ordre total, les chances sont très faibles qu'elle a cette propriété. Il suffit de penser aux autres ensembles de nombres (entiers relatifs, rationnels, les réels) pour s'en convaincre. Des ensembles muni d'un ordre qui ont cette propriété seront appelés des ensembles bien ordonnés. Ils seront étudiés en plus de détails d'abord en §19 et ensuite dans §30.*

Ⓟ **8.17 Proposition.** *Soit* $A \subset \mathbf{N}$ *un sous-ensemble non-vide. Alors* A *contient un plus petit élément :* $\exists \ell \in A \ \forall k \in A : \ell \leq k$.

Le lecteur attentif aurait pu constater que, dans nos constructions des opérations d'addition et multiplication et de la relation d'ordre, on s'est servi uniquement de la structure *de l'ensemble* $\mathbf{N}$*, c'est-à-dire les propriétés codées dans les axiomes de Peano, mais qu'on n'a jamais utilisé la forme précise de ses éléments comme par exemple* $2 = \{\emptyset, \{\emptyset\}\}$*. On aurait donc pu effectuer les mêmes constructions à partir de n'importe quel ensemble* $\mathbf{N}'$ *muni d'un élément spécial* $0'$ *et une application* S' *ayant les propriétés exprimées par les axiomes de Peano. Quel sera la différence avec la construction sur "notre" triplet* $(\mathbf{N}, 0, S)$ *? Une réponse possible à cette question est : rien ! Mais il faut préciser dans quel sens il n'y a pas de différence. La réponse plus précise devrait être*

> *Tant qu'on ne s'intéresse qu'aux propriétés arithmétiques (les propriétés concernant l'addition, la multiplication et la relation d'ordre), il n'y aura pas de différence.*

Mais comment peut-on justifier cela ? C'est exactement l'idée de Peano : ses axiomes caractérisent l'ensemble $\mathbf{N}$ *complètement dans le sens suivant.*

- *Si* $(\mathbf{N}, 0, S)$ *et* $(\mathbf{N}', 0', S')$ *sont deux triplets vérifiant les axiomes de Peano, alors il existe une unique application bijective* $\varphi : \mathbf{N} \to \mathbf{N}'$ *qui "respecte" le triplet dans le sens*

$$\varphi(0) = 0' \qquad et \qquad \forall n \in \mathbf{N} : \varphi\big(S(n)\big) = S'\big(\varphi(n)\big) \ .$$

De là on en déduit facilement qu'on a les propriétés suivantes.

- *Si* $+'$ *est une opération interne (d'addition) associative et commutative dans* $\mathbf{N}'$ *qui vérifie les conditions*

$$\forall n' \in \mathbf{N}' : n' +' \ 0' = n' \ \text{ et } n' +' \ S'(0') = S'(n') \ ,$$

alors l'application φ ci-dessus respecte l'addition :

$$\forall n, m \in \mathbf{N} : \varphi(m+n) = \varphi(m) +' \varphi(n) \ .$$

- *Si $\times'$ est une opération interne (de multiplication) sur $\mathbf{N}$, associative, commutative avec les propriétés de distributivité sur l'addition $+'$, avec $1' = S'(0')$ comme élément neutre, alors l'application φ respecte la multiplication :*

$$\forall n, m \in \mathbf{N} : \varphi(m \times n) = \varphi(m) \times' \varphi(n) \ .$$

- *Si $\leq'$ est une relation d'ordre total sur $\mathbf{N}'$ ayant la propriété*

$$\forall n' \in \mathbf{N}' : n' \leq' S'(n') \ ,$$

alors l'application φ respecte la relation d'ordre :

$$\forall m, n \in \mathbf{N} : m \leq n \ \Leftrightarrow \ \varphi(m) \leq' \varphi(n) \ .$$

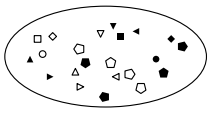
La conclusion de ces résultats est que, si on définit (sur $\mathbf{N}'$) les opérations d'addition et de multiplication et la relation d'ordre dans un sens compatible avec l'idée que l'application S' désigne le successeur (d'un entier naturel), alors la bijection φ transforme "automatiquement" ces opérations dans $\mathbf{N}$ en les opérations correspondantes dans $\mathbf{N}'$. Tout calcul qui n'utilise que ces trois ingrédients peut donc être passé de $\mathbf{N}$ à $\mathbf{N}'$ et vice-versa. Autrement dit, pour tout raisonnement qui ne fait intervenir que ces trois ingrédients (et d'autres choses qu'on en déduit), on peut — sans crainte de contradiction — ajouter des primes à tous les symboles (éléments, sous-ensembles, opérations), ou les enlever. Par contre, dès qu'on utilise d'autres opérations, cette garantie sera absente. Par exemple, dans "notre" $\mathbf{N}$ on a la propriété $2 \in 3$ et $2 \subset 4$. Avec un autre triplet $(\mathbf{N}', 0', S')$ vérifiant les axiomes de Peano, ces propriétés seront fort probablement fausses.

En réalité, dans la pratique de tous les jours, on ne s'intéresse pas tellement à la structure précise de nos nombres entiers naturels ; on se contente de calculer avec. Le raisonnement ci-dessus montre donc que la manière dont on a construit les entiers naturels est sans importances, tant qu'ils obéissent aux axiomes de Peano.

9. Relations d'équivalences

Le collectionneur de billes est une analogie presque parfaite pour bien comprendre les concepts de "relation d'équivalence," "classe d'équivalence," "partition" et "espace quotient." Ce collectionneur a une collection de billes dans un grand sac et un beau jour il décide de les classer. Il se procure une quantité de petites boîtes et il commence à les remplir : une boîte avec ses billes jaunes, une boîte avec ses billes en verre, une boîte avec ces billes de taille standard et cœtera. Il est évident que son critère de sélection ne marche pas, car dans quelle boîte devrait-il mettre une bille jaune en verre de taille standard ? Cette classification n'est donc pas bonne. Pour que ça marche, il faut que le critère est univoque dans le sens qu'on ne peut pas trouver deux boîtes pour mettre la même bille.

Une meilleure façon sera d'utiliser le (seul) critère de couleur : deux billes seront mises dans la même boîte si (et seulement si) elles ont la même couleur. Ainsi notre collectionneur aura une boîte qui contient toutes ses billes jaunes, il aura une boîte qui contient toutes ses billes vertes, et cœtera. Son sac (qui au début contenait ses billes) sera donc remplit de ces boîtes qui contiennent des billes de même couleur. S'il veut bien voir sa collection, il laisse tous ces boîtes ouvertes. Mais il peut aussi fermer les boîtes et coller une étiquette sur chaque boîte avec la caractéristique des billes dedans comme "jaune" ou "vert."



L'ensemble des billes ;
critère de sélection :
même forme et même couleur.

L'idée d'un bon critère de sélection est repris dans la notion d'une relation d'équivalence qui répond à la question si oui ou non il faut mettre deux billes dans une même boîte. Mais elle ne dit pas dans quelle boîte !

9.1 La définition d'une relation d'équivalence sur un ensemble. Soit A un ensemble. Une *relation d'équivalence sur* A est un sous-ensemble $R \subset A \times A$ vérifiant trois conditions. Pour une relation d'équivalence, comme pour une relation d'ordre, il est d'usage de noter le fait qu'un couple $(a, b) \in A \times A$ appartient au sous-ensemble R (qu'on note normalement par $(a, b) \in R$) par aRb :

$$aRb \qquad \overset{\text{déf}}{\Longleftrightarrow} \qquad (a, b) \in R \ .$$

Et, comme pour une relation d'ordre, on utilise fréquemment un symbole autre qu'une lettre pour indiquer une relation d'équivalence ; le symbole utilisé le plus souvent (dans un contexte abstraite) étant $\sim$, ce qu'il faut lire comme "équivalent" ou "similaire," c'est-à-dire qu'on lit $a \sim b$ comme "a équivalent à b" ou "a similaire à b." Mais dans des cas particuliers on trouve une panoplie d'autre symboles comme par exemple $\equiv$ ou $\cong$. En utilisant le symbole $\sim$ pour le sous-ensemble de $A \times A$, les trois propriétés auxquelles $\sim \subset A \times A$ doit satisfaire sont

(i) $\forall a \in A : a \sim a$ (*réflexivité*),

(ii) $\forall a, b \in A : a \sim b \ \Leftrightarrow \ b \sim a$ (*symétrie*) et

(iii) $\forall a, b, c \in A : a \sim b$ et $b \sim c \ \Rightarrow \ a \sim c$ (*transitivité*).

Remarque. Si $R \subset A \times A$ est une relation d'équivalence sur A, alors la condition (ii) de symétrie nous dit que la relation inverse R^{-1} est égale à R.

Si on interprète une relation d'équivalence comme le critère qui dit s'il faut mettre deux billes dans la même boîte, les trois conditions d'une relation d'équivalence deviennent évidentes : bien sûr qu'une bille a est mis dans la même boîte que la (même) bille a ; bien sûr que si on met la bille a dans la même boîte que la bille b, alors la bille b est mis dans la même boîte que la bille a ; et si les billes a et b appartiennent à une même boîte et si les billes b et c appartiennent à une même boîte, alors forcément les billes a et c appartiennent à une même boîte (qui contient donc aussi la bille b). Une fois qu'on a le critère de sélection codé dans une relation d'équivalence, notre collectionneur peut commencer à faire ses boîtes. Il prend une bille, appelons la a, et il cherche toutes *les autres billes dans sa collection qui devraient être mis dans la même boîte que la bille a. Le tas de billes qu'il obtient ainsi est appelé la classe d'équivalence de la bille a.*

9.2 Définition d'une classe d'équivalence. Soit $\sim$ une relation d'équivalence sur un ensemble A et soit $a \in A$ un élément. Alors la *classe d'équivalence de l'élément* a, notée C_a ou $[a]$ est le sous-ensemble de A qui contient tous les éléments qui sont équivalents à a :

$$C_a = \{\, b \in A \mid a \sim b \,\} \ . \tag{9.3}$$

C'est bien un ensemble par l'axiome de séparation.

La définition de la classe d'équivalence C_a d'un élément $a \in A$ est donné dans le même esprit que, par exemple, la définition $\mathrm{Dom}(R)$ du domaine d'une relation R entre deux ensembles A et B [3.4]. Mais ici on le fait seulement pour tous les éléments de l'*ensemble* A (le domaine d'une relation est défini pour tous les relations et la collection de tous les relations n'est pas un ensemble). Ce qui veut dire qu'on a construit une application C sur l'ensemble A, à condition qu'on précise aussi l'ensemble but. Étant donné que chaque C_a est un sous-ensemble de A, il paraît naturel de prendre $\mathcal{P}(A)$, l'ensemble de tous les sous-ensembles de A, comme ensemble but. Et effectivement, on obtient bien une application $C : A \to \mathcal{P}(A)$. Sa définition "officielle" est

$$C = \Big\{\ (a, c) \in A \times \mathcal{P}(A) \mid c = \{\, b \in A \mid a \sim b \,\} \ \Big\} \ . \tag{9.4}$$

Et si on utilise la définition (9.3) pour abréger $\{\, b \in A \mid a \sim b \,\}$ comme C_a, on peut simplifier cette écriture dans l'esprit de [2.4] comme

$$C = \{\, (a, C_a) \in A \times \mathcal{P}(A) \mid a \in A \,\} \ ,$$

ou encore

$$C = \{\, (a, C_a) \mid a \in A \,\} \ .$$

Et si on veut insister sur le fait qu'il s'agit d'une application, on l'écrit sous la forme

$$C : A \to \mathcal{P}(A) \quad , \quad a \mapsto C_a \equiv \{\, b \in A \mid a \sim b \,\} \ .$$

C'est cette façon d'écrire l'application C qui est plus ou moins implicite dans la définition (9.3) : on précise l'image C_a d'un élément quelconque a de A. Et une fois

qu'on a défini cette application, l'écriture C_a est simplement une autre écriture pour l'image $C(a)$ de l'élément $a \in A$ sous l'application C.

Revenons à notre collectionneur. Il a donc pris la bille a et il a trouvé toutes les billes qui devraient être mis dans la même boîte que la bille a. Il les met donc dans une boîte. S'il lui reste des billes, il en prend une, appelons la b, il la met dans une boîte et il refait l'opération : il cherche toutes les billes qui devraient être mis dans la même boîte que la bille b et il les met avec la bille b dans la boîte. Remarquons toute de suite qu'il lui est inutile de vérifier si la première boîte contient des billes qui devraient être mis dans la même boîte que b, car si la première boîte contenait une telle bille, appelons la c, elle devrait être mis dans la même boîte que a et dans la même boîte que b. Et alors, par transitivité d'une relation d'équivalence, b devrait être mis dans la même boîte que a. Ce qui est contraire au fait que la bille b n'était pas dans la boîte qui contient a. Il lui suffit donc de fouiller les billes qui ne sont pas dans la boîte qui contient a.

Une fois la deuxième boîte remplie, il répète cette opération jusqu'à épuisement des billes : s'il lui restent des billes, il en prend une, la met dans une boîte et il cherche toutes les autres billes qui devraient être mis dans la même boîte que celle là. Et comme avant, il lui est inutile de vérifier les billes dans les boîtes déjà remplies, car (par la transitivité d'une relation d'équivalence) ces boîtes ne peuvent pas contenir des billes qui devraient être mis dans une même boîte que la bille qui est restée de coté. Cet argument est exprimé dans le lemme suivant sur les classes d'équivalences.

Ⓟ **9.5 Lemme.** *Soit $\sim$ une relation d'équivalence sur un ensemble A et soit a et b deux éléments de A. Alors les classes d'équivalences correspondantes ne sont pas disjointes si et seulement si elles sont égales, ce qui est le cas si et seulement si a et b sont équivalentes :*

$$C_a \cap C_b \neq \emptyset \qquad \Longleftrightarrow \qquad C_a = C_b \qquad \Longleftrightarrow \qquad a \sim b \ .$$

À la fin de son travail de répartition, notre collectionneur a donc mis toutes ses billes dans des boîtes ; chaque boîte contient des billes qui, selon le critère de sélection, devraient être mis dans une même boîte et deux boîtes différentes ne contiennent pas des billes qui devraient être mis dans une même boîte. Il a créé une partition de sa collection en différentes sous-collections : la sous-collection des billes jaunes, la sous-collection des billes vertes et cætera. Ce qui nous amène à la définition d'une partition d'un ensemble.

Définition d'une partition d'un ensemble. Soit A un ensemble. Une *partition de A* est un ensemble P, sous-ensemble de $\mathcal{P}(A)$, vérifiant deux conditions :

$$\cup P \equiv \bigcup_{X \in P} X = A \qquad \text{et} \qquad \forall X, Y \in P : X \neq Y \ \Rightarrow \ X \cap Y = \emptyset \ .$$

Nota Bene. Si P est une partition de A, alors par [5.1.i] il s'ensuit qu'on a l'implication

$$B \in P \qquad \Longrightarrow \qquad B \subset \cup P = A \ .$$

Les éléments de P sont donc des sous-ensembles de A, c'est-à-dire des éléments de $\mathcal{P}(A)$. On a donc l'inclusion $P \subset \mathcal{P}(A)$. On aurait pu mettre cela comme condition dans la définition d'une partition. On ne le fait pas pour deux raisons : d'abord parce que c'est superflu (comme on vient de voir), mais surtout parce qu'en général on ne *voit* pas une partition comme un sous-ensemble de $\mathcal{P}(A)$, mais plutôt comme un découpage de l'ensemble A avec des frontières.

DESSIN

L'interprétation d'une partition d'un ensemble devrait être évident : si l'ensemble P est une partition d'un ensemble A, les éléments de P sont les boîtes de notre collectionneur de billes contenant les sous-collections de billes jaunes et cætera. Deux boîtes différentes ne contiennent pas une même bille (évidemment) et si on met ensemble le contenu de toutes ces sous-collections, autrement dit, si on vide les boîtes dans le sac, on obtient la collection de billes d'origine. Le travail de triage de notre collectionneur a donc utilisé la relation d'équivalence pour obtenir sa partition en sous-collection. Ceci est exprimé par le lemme suivant.

Ⓟ **9.6 Lemme.** *Soit $\sim$ une relation d'équivalence sur un ensemble A. Alors l'ensemble P définie comme l'image de A sous l'application C, c'est-à-dire l'ensemble de toutes les classes d'équivalence, ou encore*

$$P \overset{déf}{=} \operatorname{Im}(C) \equiv \{\ B \in \mathcal{P}(A) \mid \exists a \in A : B = C_a\}$$

est une partition de A.

Remarque. Avec la simplification d'écriture expliquée dans [2.4], la définition de l'ensemble P est habituellement donné sous la forme

$$P = \{\, C_a \mid a \in A \,\} \ ,$$

ce qui n'est rien d'autre que la simplification de l'écriture de l'image d'une application discutée en [5.8].

Une fois que notre collectionneur a fait ses boîtes de sous-collection de billes selon son critère de tri, il peut fermer ces boîtes et mettre une étiquette dessus pour indiquer le contenu. Ainsi quelqu'un qui ouvre le sac du collectionneur ne voit qu'une collection de boîtes et pas une collection de billes. Dans le fond il n'y a rien qui a changé, ce n'est qu'un changement de point de vue. Il suffit d'ouvrir les boîtes pour voir qu'il s'agit d'une collection de billes.

En mathématiques on distingue ces deux points de vue en utilisant deux noms différents. On parle d'une partition quand on considère les boîtes ouvertes et on parle de l'ensemble quotient quand on considère les boîtes fermées. Mais dans les deux cas

il s'agit du même ensemble ! Et l'action de mettre une bille dans sa boîte est appelée la projection canonique.

Définition de l'ensemble quotient. Soit $\sim$ une relation d'équivalence sur un ensemble A. Alors la partition P donnée par

$$P = \{\, B \in \mathcal{P}(A) \mid \exists a \in A : B = C_a \,\} \equiv \{\, C_a \mid a \in A \,\} \tag{9.7}$$

est appelée *l'espace quotient (de l'ensemble A par la relation d'équivalence $\sim$)*. On le note souvent comme $A/\sim$:

$$A/\sim \stackrel{\text{déf}}{=} P \ .$$

L'application $C : A \to A/\sim \stackrel{\text{déf}}{=} P \subset \mathcal{P}(A)$ déjà définie en (9.4) et qui fait correspondre à chaque $a \in A$ sa classe d'équivalence C_a est appelée *la projection canonique de A sur l'ensemble quotient $A/\sim$*. Pour compliquer la situation pour le lecteur novice, on a tendance à noter cette application par le lettre (grec) π au lieu de C. On dit donc :

$$\text{la projection canonique } \pi : A \to P \text{ est définie par } \pi(a) = C_a.$$

La multiplication des symboles utilisés pour un même objet est, bien sûr, dérangeant pour le novice. Mais que le lecteur soit rassuré : on s'y habitue assez vite.

Une fois que notre collectionneur a bien rangé ses billes dans des boîtes, il lui arrive l'idée de vouloir vendre ses billes. Pour cela il regarde ces billes une à une et décide d'un prix pour chaque bille. Ensuite il colle sur chaque bille une étiquette avec son prix. En mathématique ceci correspond à une fonction f définie sur l'ensemble des billes à valeurs dans $\mathbf{R}$. Mais quand il a mis ses billes dans des boîtes et quand les boîtes sont fermés, personne ne peut voir les prix ! Vient donc le dilemme du collectionneur devenu vendeur : faut-il revoir tout et décider, pour chaque boîte, d'un prix que coutera une bille dans la boîte, ou est ce que le travail déjà fait peut lui servir pour déterminer ce prix ? S'il colle une étiquette avec un prix sur chaque boîte, alors tous les billes dans la boîte couteront autant. Son travail précédent peut lui servir seulement si (par hasard) tous les billes dans une boîte ont déjà le même prix. Mathématiquement cette condition est exprimé dans la notion d'une application compatible avec la relation d'équivalence. Si cette condition est vérifiée, le prix qu'il faut coller sur une boîte s'obtient simplement en prenant (au hasard) une bille dans la boîte, de regarder son prix et de coller ce prix sur la boîte. Vu que toutes les billes dans la boîte ont le même prix, le choix de la bille n'a pas d'importance. Par contre, si ce n'est pas vrai que toutes les billes dans une boîte ont le même prix, alors il n'y aurait pas un prix unique à coller sur la boîte et le collectionneur serait obligé de réfléchir de nouveau sur un prix (par boîte) ou de laisser ses boîtes ouvertes.

L'action de coller un prix sur chaque boîte correspond à une fonction F sur l'ensemble quotient (la partition associée à la relation d'équivalence). L'idée que le prix d'une bille (la valeur de la fonction f) s'obtient en regardant dans quelle boîte elle se trouve et de regarder le prix indiqué sur la boîte correspond à la composition $F \circ C$ de la projection canonique $C : A \to A/\sim$ (regarder dans quelle boîte se trouve la bille) avec l'application F sur l'ensemble quotient (regarder le prix collé sur la boîte). Dans l'autre sens, si on veut savoir quelle prix il faut coller sur une boîte, il suffit de piocher une bille dans la boîte et de regarder quel prix est collé sur cette

bille. Il n'a pas d'importance quelle bille on prend dans la boîte, car elles ont toutes le même prix. À condition bien sûr que la fonction "prix d'une bille" est compatible avec la relation d'équivalence "être dans la même boîte."

Maintenant il y a deux façons d'exprimer ce résultat : une formelle et une informelle. La façon informelle dit que la fonction $F : A/\sim \to \mathbf{R}$ *est* bien définie *par la prescription*

$$F(C_a) = f(a)$$

quand la fonction f *est compatible avec la relation d'équivalence* $\sim$*. Le plus souvent la prescription de* F *est donné dans un énoncé et dans la preuve on démontre que la fonction* f *est compatible avec la relation d'équivalence. L'avantage de cette méthode informelle est qu'elle est très proche de l'idée intuitive. Le désavantage est qu'il faut parler de la fonction* F *avant qu'on sait qu'elle existe. Et comme on a vu avec la définition d'une suite récurrente, cela peut nous induire en erreur. La façon formelle énonce un résultat général qui dit qu'une telle fonction* F *existe si et seulement si la fonction* f *est compatible avec la relation d'équivalence. Et dans la preuve on démontre l'existence d'une telle fonction. Dans la suite il suffit donc d'évoquer ce résultat pour être sûr que* F *existe.*

9.8 Définition. Soit A et X deux ensembles, soit $f : A \to X$ une application et soit $\sim$ une relation d'équivalence sur A. On dit que f *est compatible avec la relation d'équivalence* $\sim$ si elle vérifie la condition

$$\forall a, b \in A : a \sim b \Rightarrow f(a) = f(b) \ .$$

Ⓟ **9.9 Lemme.** *Soit* A *et* X *deux ensembles, soit* $\sim$ *une relation d'équivalence sur* A*, soit* $C : A \to A/\sim$ *la projection canonique et soit* $f : A \to X$ *une application quelconque. Alors il existe une application* $F : A/\sim \to X$ *vérifiant* $f = F \circ C$*, c'est-à-dire*

$$\forall a \in A : f(a) = F(C(a)) \equiv F(C_a) \tag{9.10}$$

si et seulement si f *est compatible avec* $\sim$*. Si cette condition est vérifiée,* F *est unique.*

À part les applications définies sur l'ensemble quotient, on aura aussi besoin dans la suite d'applications définies sur le produit cartésien de l'ensemble quotient $A/\sim$ *avec lui-même ainsi que de sous-ensembles de ce produit et tout cela en termes d'objets analogues déjà définis sur le produit cartésien de l'ensemble* A *avec lui-même.*

On peut pousser l'analogie du vendeur de billes pour comprendre ces démarches. Supposons par exemple que notre vendeur de billes veut accorder une remise pour l'achat simultané de deux billes. Il a son barème de remise selon les deux billes choisies, ce qui correspond avec une fonction r *sur* $A \times A$ *à valeurs dans* $\mathbf{R}$*. Mais quoi dire à l'acheteur quand les boîtes sont fermés ? Faut-il refaire le travail et décider, par couple de boîtes, de la remise accordée ? Une telle liste, indiquant la remise quand on connaît les deux boîtes contenant les billes à acheter, correspondrait à une fonction* R *sur le produit* $(A/\sim) \times (A/\sim)$ *à valeurs dans* $\mathbf{R}$*. Ou est-il possible de se servir de*

sa liste initiale ? Si on peut, alors pour obtenir la nouvelle liste à partir de sa liste des remises selon les billes, on prend deux billes (au hasard) dans les deux boîtes, on regarde la remise accordée et on note cette remise comme la remise associée aux deux boîtes. Pour que cela donne une réponse sans ambiguïtés, il faut que ce résultat ne dépend pas du choix des deux billes. Mathématiquement cela est exprimé par la condition que la fonction r doit être compatible avec la relation d'équivalence. Et comme pour les applications sur A, on a un résultat général qui dit que la fonction R existe si et seulement si r est compatible avec la relation d'équivalence.

Pour illustrer ce qui peut arriver à notre vendeur, imaginons la situation suivante : le critère de sélection pour les boîtes est la couleur des billes. Chaque boîte contient donc des billes d'une même couleur (et pas d'une autre couleur). Et le critère de remise est la différence de taille : plus que la différence de taille entre deux billes est grande, moins élevée sera la remise accordée. Peut-on prédire la remise accordée quand on connaît seulement les deux boîtes qui contiennent les deux billes à acheter ? La réponse dépend de la collection des billes ! Si toutes les billes d'une même couleur ont aussi la même taille, alors ça marche. Sinon on ne peut pas le faire.

Une dernière analogie qui va nous servir dans la suite est l'action promotionnelle du vendeur de billes : pour l'achat simultané de deux billes on peut gagner une boisson gratuite. Mais ce n'est pas n'importe quel couple de billes qui fait gagner la boisson. Comme avant, le vendeur a sa liste de couples qui fait gagner (ce qui correspond à un sous-ensemble g du produit $A \times A$), mais comme toujours, ses boîtes sont fermés. Et l'acheteur veut savoir si oui ou non il gagne s'il achète deux billes dans deux boîtes qu'il indique (ce qui correspondra avec un sous-ensemble G du produit $(A/\sim) \times (A/\sim)$). Pour le savoir, le vendeur prend une bille dans chaque boîte indiquée, regarde sa liste et donne le verdict. Mais pour que le verdict soit sans ambiguïtés, il faut absolument qu'un autre choix de deux billes ne change pas ce verdict. Par exemple si on gagne quand les deux billes ont le même poids, on peut prédire le gagnant si et seulement si les billes dans une boîte ont toutes le même poids. Mathématiquement cela donne la définition d'un sous-ensemble compatible avec la relation d'équivalence.

Les définitions et résultats qui vont suivre sont l'équivalent de [9.8] et [9.9] pour les cas d'une fonction sur $A \times A$ et un sous-ensemble de $A \times A$. Même les preuves sont très similaires, tellement similaires qu'on pourrait avoir l'impression qu'on fait du travail en double. Il est possible de justifier cette impression, mais cela nécessite d'autres résultats intermédiaires dont on n'a pas besoin en formulant ces résultats séparément.

9.11 Définition. Soit A et X deux ensembles, soit $r : A \times A \to X$ une application et soit $\sim$ une relation d'équivalence sur A. On dit que r *est compatible avec la relation d'équivalence* $\sim$ si elle vérifie la condition

$$\forall a, a', b, b' \in A : a \sim a' \text{ et } b \sim b' \Rightarrow r(a, b) = r(a', b') \ .$$

Ⓟ **9.12 Lemme.** *Soit A et X deux ensembles, soit $\sim$ une relation d'équivalence sur A, soit $C : A \to A/\sim$ la projection canonique et soit $r : A \times A \to X$ une application*

quelconque. Alors il existe une application $R : (A/\sim) \times (A/\sim) \to X$ *vérifiant*

$$\forall a, b \in A : r(a,b) = R(C(a), C(b)) \equiv R(C_a, C_b) \tag{9.13}$$

si et seulement si r *est compatible avec* $\sim$*. Si cette condition est vérifiée,* R *est unique.*

9.14 Définition. Soit A un ensemble, soit $g \subset A \times A$ un sous-ensemble et soit $\sim$ une relation d'équivalence sur A. On dit que g *est compatible avec la relation d'équivalence* $\sim$ si elle vérifie la condition

$$\forall a, a', b, b' \in A : a \sim a' \text{ et } b \sim b' \Longrightarrow \big[\ (a,b) \in g \Leftrightarrow (a',b') \in g\ \big]\ .$$

Ⓟ **9.15 Lemme.** *Soit* A *un ensemble, soit* $\sim$ *une relation d'équivalence sur* A*, soit* $C : A \to A/\sim$ *la projection canonique et soit* $g \subset A \times A$ *un sous-ensemble quelconque. Alors il existe un sous-ensemble* $G \subset (A/\sim) \times (A/\sim)$ *vérifiant*

$$\forall a, b \in A : (C(a), C(b)) \equiv (C_a, C_b) \in G \Longleftrightarrow (a,b) \in g \tag{9.16}$$

si et seulement si g *est compatible avec* $\sim$*. Si cette condition est vérifiée,* G *est unique.*

Supposons maintenant que notre collectionneur de billes a fait le tri et mis ses billes dans des boîtes. Et supposons qu'on regarde dans son sac et qu'on voit la collection de boîtes. Peut-on retrouver le critère de tri du collectionneur ? La réponse (peut-être décevant pour certains) est trivialement affirmative : son critère de tri était "deux billes devraient être mis dans une même boîte s'ils se trouvent dans une même boîte." Ce résultat un peu tautologique est exprimé par le lemme suivant.

Ⓟ **9.17 Lemme.** *Soit* P *une partition d'un ensemble* A*. Alors l'ensemble* $\sim\ \subset A \times A$ *défini par*

$$\sim\ = \{\, (a,b) \in A \times A \mid \exists X \in P : a, b \in X \,\}$$

est une relation d'équivalence sur A*. En plus, les classes d'équivalences sont les éléments de* P *(à l'exception de l'ensemble vide qui pourrait appartenir à* P *mais qui n'est pas une classe d'équivalence) :*

$$\forall X \neq \emptyset \quad : \quad X \in P \ \Leftrightarrow\ \exists a \in A : X = \{b \in A \mid a \sim b\}\ .$$

Remarques. • Dans l'énoncé de [9.17] on a déjà utilisé la simplification d'écriture [2.4], car l'écriture officielle de l'ensemble $\sim$ est

$$\sim\ = \{\, C \in A \times A \mid \exists X \in P\ \exists a, b \in X : C = (a,b) \,\}\ .$$

• On a donné la définition de la relation d'équivalence sous sa forme officielle d'un sous-ensemble du produit cartésien $A \times A$. Si on utilise l'écriture habituelle $a \sim b$ pour $(a,b) \in \sim$, la définition de $\sim$ s'écrit comme

$$a \sim b \qquad \overset{\text{déf}}{\Longleftrightarrow} \qquad \exists X \in P : a, b \in X\ .$$

Il n'est même pas nécessaire d'ajouter la condition $a, b \in A$ ou $(a, b) \in A \times A$, car le fait qu'ils appartiennent à un élément de X dans P nous garantit cela : $A = \cup P$ et donc par [1.9] pour tout $X \in P$ on a $X \subset A$.

10. Construction des nombres rationnels positifs

Ce chapitre est, strictement parlant, superflu ; on refait le travail dans §14. On ne donnera donc pas de preuves (sauf une). Mais la construction des nombres rationnels positifs est, en mathématique, l'exemple par excellence pour illustrer les notions de relation d'équivalence et de fonction compatible. La raison est que tout le monde a déjà vu cette construction à l'école primaire et au collège. Bien sûr, on n'utilise pas les mêmes mots, mais à part cela, c'est la même chose. Généralement on parle d'un gateau qu'on partage en parts égales, en moitiés, en tiers ou en quarts. On introduit les notations $\frac{1}{2}$, $\frac{1}{3}$ *et* $\frac{1}{4}$ *pour cela. On parle d'une division et on montre que deux moitiés fait un, que trois sixièmes fait une moitié, ce qu'on note comme* $\frac{2}{2} = 1$ *et* $\frac{3}{6} = \frac{1}{2}$*. Plus généralement on introduit les "fractions"* $\frac{p}{q}$ *pour deux entiers* p *et* q *(*$q \neq 0$*) et on apprend à calculer avec. C'est exactement cette construction et ces règles de calculs qu'on va établir ici dans un langage mathématique. Mais il faut faire attention dans notre raisonnement, car on ne peut utiliser que les opérations déjà définies pour les entiers naturels ; en particulier, on ne dispose pas de l'opération de division (de deux entiers naturels quelconques).*

Définition d'une relation d'équivalence sur $\mathbf{N} \times \mathbf{N}^*$. Sur l'ensemble $\mathbf{N} \times \mathbf{N}^*$ (où $\mathbf{N}^*$ désigne l'ensemble des entiers naturels sauf 0 : $\mathbf{N}^* = \mathbf{N} \setminus \{0\}$) on définit une relation d'équivalence $\sim$ par

$$(a,b) \sim (p,q) \qquad \overset{\text{déf}}{\iff} \qquad a \times q = b \times p \ . \tag{10.1}$$

Dans [10.2] on montrera que $\sim$ est bien une relation d'équivalence. L'ensemble quotient $\mathbf{N} \times \mathbf{N}^*/\sim$ sera noté $\mathbf{Q}_+$:

$$\mathbf{Q}_+ \overset{\text{déf}}{=} \mathbf{N} \times \mathbf{N}^*/\sim \ .$$

Un élément de l'ensemble $\mathbf{Q}_+$ s'appelle un *nombre rationnel positif* et l'ensemble $\mathbf{Q}_+$ lui-même s'appelle bien évidemment *l'ensemble des nombres rationnels positifs*. Pour se conformer à la notation standard, on notera la classe d'équivalence $C_{(a,b)}$ d'un élément $(a,b) \in \mathbf{N} \times \mathbf{N}^*$ par $\frac{a}{b}$:

$$\frac{a}{b} \overset{\text{déf}}{=} C_{(a,b)} \equiv \{(p,q) \in \mathbf{N}^* \times \mathbf{N}^* \mid (p,q) \sim (a,b)\} \ .$$

Pour l'instant on s'abstient de toute interprétation style quotient pour une classe d'équivalence ; pour le moment la notation comme fraction n'est qu'une notation de commodité. Ce ne sera que plus tard qu'on montrera qu'effectivement une classe d'équivalence s'interprète comme un quotient.

Tout lecteur aura reconnu dans la définition de notre relation d'équivalence le fait que deux fractions $\frac{a}{b}$ *et* $\frac{p}{q}$ *représentent le même nombre si et seulement si on a l'égalité* $a \times q = b \times p$*. Dans de telles circonstances l'égalité* $\frac{a}{b} = \frac{p}{q}$ *ne peut pas être interprété comme une égalité de couples d'entiers naturels. Dire qu'elles représentent le même nombre peut être formulé comme étant une relation d'équivalence (ce qu'on a fait), et l'égalité* $\frac{a}{b} = \frac{p}{q}$ *devient l'égalité des classes d'équivalences associées : deux*

éléments/couples sont équivalents si et seulement si leurs classes d'équivalences associées sont égales.

Ⓟ **10.2 Lemme.** *La relation $\sim$ sur $\mathbf{N} \times \mathbf{N}^*$ définie par (10.1) est une relation d'équivalence.*

Une fois qu'on a défini l'ensemble des nombres rationnels positifs, il faut définir les opérations d'addition et multiplication. Et là, nos problèmes commencent, car il faut définir ces opérations sur des classes d'équivalences. Reprenons l'analogie avec le collectionneur de billes : les billes sont les couples d'entiers naturels et les boites sont les classes d'équivalences. Dans notre cas on n'a pas mis des noms sur les boites de billes. (Si on utilise la notion de nombres premiers entre eux, on pourrait donner des noms aux boites, mais cela complique plus la tâche que cela aide.) On n'a donc pas de noms sur les boites et on veut quand même définir l'addition de deux boites. Comment le faire ? L'idée est le même que pour la réduction accordé à la vente simultané de deux billes : on prend une bille dans chaque boite, c'est-à-dire deux couples d'entiers naturels, on applique une procédure sur ces deux couples pour obtenir un troisième couple et on cherche la boite dans laquelle il faut mettre ce couple d'entiers naturels. La grande question es quelle procédure faut-il appliquer aux deux couples ? L'élève au collège pense parfois que la procédure suivante est la bonne : aux couples (a, b) et (p, q) on associe le couple $(a + p, b + p)$. Cet élève écrit "donc" :

$$\frac{a}{b} + \frac{p}{q} = \frac{a+p}{b+q} \quad . \tag{10.3}$$

Il se fait bien sûr rattraper par son professeur de mathématique qui lui dit que c'est faux et qu'il fallait les mettre sur le même dénominateur et écrire

$$\frac{a}{b} + \frac{p}{q} = \frac{a \times q}{b \times q} + \frac{b \times p}{b \times q} = \frac{a \times q + p \times b}{b \times q} \quad . \tag{10.4}$$

Mais pourquoi ? La raison mathématique est que l'opération (10.3) n'est pas compatible avec la relation d'équivalence et que l'opération (10.4) l'est. En termes de nos boites, si quelqu'un pioche d'autres couples dans les mêmes deux boites, applique l'opération (10.3) de l'élève et cherche la boite correspondante au résultat, il ne trouve pas forcément la même boite qu'avec les couples initiales. Par exemple :

$$(1, 2) \sim (2, 4) \text{ et } (1, 3) \sim (3, 9)$$

mais

$$(1 + 1, 2 + 3) = (2, 5) \nsim (5, 13) = (2 + 3, 4 + 9) \quad .$$

L'opération (10.3) ne fournit donc pas une opération sur les boites dans le sens qu'à deux boites on associe une troisième boite. Simplement parce que la troisième boite n'est pas bien déterminé par la procédure. Par contre, si une opération sur les billes/couples d'entiers naturels est telle que, quelque soit le choix des deux couples dans les deux boites, le résultat de l'opération tombe toujours dans la même boite, on aura obtenu une opération sur les boites. On est donc dans la même situation que le vendeur qui veut accorder une remise pour l'achat de deux billes. Les résultats mathématiques correspondants sont donnés dans [9.11] et [9.12].

10.5 L'addition sur $\mathbf{Q}_+$. *L'application* $f : (\mathbf{N} \times \mathbf{N}^*) \times (\mathbf{N} \times \mathbf{N}^*) \to \mathbf{Q}_+$ *définie par*

$$f\big((a,b),(p,q)\big) = \frac{a \times q + p \times b}{b \times q}$$

est compatible avec la relation d'équivalence définie en (10.1). Il existe donc une unique application $+_{\mathbf{Q}} : \mathbf{Q}_+ \times \mathbf{Q}_+ \to \mathbf{Q}_+$, *appelée l'addition dans* $\mathbf{Q}_+$, *vérifiant*

$$\frac{a}{b} +_{\mathbf{Q}} \frac{p}{q} \quad = \quad \frac{a \times q + p \times b}{b \times q} \quad \equiv \quad f\big((a,b),(p,q)\big) \ .$$

On a (provisoirement) ajouté la lettre $\mathbf{Q}$ *en indice pour distinguer cette opération d'addition de l'opération d'addition déjà définie sur* $\mathbf{N}$.

10.6 La multiplication dans $\mathbf{Q}_+$. *L'application* $f : (\mathbf{N} \times \mathbf{N}^*) \times (\mathbf{N} \times \mathbf{N}^*) \to \mathbf{Q}_+$ *définie par*

$$f\big((a,b),(p,q)\big) = \frac{a \times p}{b \times q}$$

est compatible avec la relation d'équivalence définie en (10.1). Il existe donc une unique application $\times_{\mathbf{Q}} : \mathbf{Q}_+ \times \mathbf{Q}_+ \to \mathbf{Q}_+$, *appelée la multiplication dans* $\mathbf{Q}_+$, *vérifiant*

$$\frac{a}{b} \times_{\mathbf{Q}} \frac{p}{q} \quad = \quad \frac{a \times p}{b \times q} \quad \equiv \quad f\big((a,b),(p,q)\big) \ . \tag{10.7}$$

Comme pour l'addition on a ajouté (provisoirement) la lettre $\mathbf{Q}$ *en indice pour distinguer cette opération de multiplication de la multiplication déjà définie sur* $\mathbf{N}$.

Maintenant on a bien défini les nombres rationnels positifs et les deux opérations d'addition et multiplication. Par contre, les entiers naturels ont disparu, car l'ensemble $\mathbf{N}$ *n'est pas un sous-ensemble de* $\mathbf{Q}_+$. *Où sont donc ces entiers naturels ? La réponse est archi-connue : il faut "identifier" les entiers naturels avec les rationnels qui ont un dénominateur* 1. *Autrement dit, il faut (par exemple) identifier l'entier* 5 *avec le rationnel* $\frac{5}{1}$. *Il s'ensuit que le rationnel* $\frac{10}{2}$ *s'identifie également avec l'entier* 5. *Mais comment peut-on formaliser cette notion d'identification en mathématique ? On le fait par une application injective* $\iota : \mathbf{N} \to \mathbf{Q}_+$. *Par [??] on sait que* ι *fournit une bijection entre la source* $\mathbf{N}$ *et son image* $\iota(\mathbf{N})$ *dans* $\mathbf{Q}_+$. *L'idée est qu'on va dire que l'image* $\iota(n)$ *(un nombre rationnel)* représente *l'entier* n. *Et parce que* ι *est injective, il n'existe pas deux nombres rationnels qui représentent le même entier naturel. Bien évidemment il existe beaucoup d'applications injectives de* $\mathbf{N}$ *dans* $\mathbf{Q}_+$, *mais la plupart ne nous convient pas du tout. Car on voudrait bien que l'addition et la multiplication dans les deux ensembles* $\mathbf{N}$ *et* $\mathbf{Q}_+$ *correspondent dans le sens que si (par exemple)* 2 *est identifié avec le rationnel* $\frac{p}{q}$ *et* 5 *avec le rationnel* $\frac{r}{s}$, *alors le rationnel* 2×5 *est identifié avec le rationnel* $\frac{p}{q} \times_{\mathbf{Q}} \frac{r}{s}$. *Plus généralement on demande/exige donc que notre injection* ι *vérifie les conditions (pour tout* $n, m \in \mathbf{N}$*) :*

$$\iota(n+m) = \iota(n) +_{\mathbf{Q}} \iota(m) \qquad et \qquad \iota(n \times m) = \iota(n) \times_{\mathbf{Q}} \iota(m) \ .$$

Et quand on impose ces conditions, on s'aperçoit vite que l'application $\iota : \mathbf{N} \to \mathbf{Q}_+$ *définie par* $\iota(n) = \frac{n}{1}$ *est la seule qui fait cela.*

10.8 Lemme/Définition. *L'application* $\iota : \mathbf{N} \to \mathbf{Q}_+$ *définie par*

$$\iota(n) = \frac{n}{1} \tag{10.9}$$

est une application injective. On l'appelle l'injection canonique de $\mathbf{N}$ *dans* $\mathbf{Q}_+$.

10.10 Compatibilité avec l'addition dans N. *L'addition dans* $\mathbf{Q}_+$ *qu'on vient de définir est compatible avec l'addition déjà définie dans* $\mathbf{N}$ *dans le sens qu'on a*

$$\forall m, n \in \mathbf{N} \quad : \quad \iota(m+n) = \iota(m) \ +_{\mathbf{Q}} \ \iota(n) \ ,$$

où $\iota : \mathbf{N} \to \mathbf{Q}_+$ *est l'injection canonique (10.9).*

10.11 Compatibilité avec la multiplication dans N. *La multiplication dans* $\mathbf{Q}_+$ *qu'on vient de définir est compatible avec la multiplication déjà définie dans* $\mathbf{N}$ *dans le sens qu'on a*

$$\forall m, n \in \mathbf{N} \quad : \quad \iota(m \times n) = \iota(m) \ \times_{\mathbf{Q}} \ \iota(n) \ ,$$

où $\iota : \mathbf{N} \to \mathbf{Q}_+$ *est l'injection canonique (10.9).*

Abus de notation très commode et universellement adopté. Une fois qu'on sait que l'addition et la multiplication dans $\mathbf{N}$ et $\mathbf{Q}_+$ sont compatibles via l'injection canonique $\iota : \mathbf{N} \to \mathbf{Q}_+$, on prend l'habitude de ne plus écrire le symbole $\mathbf{Q}$ en index sur ces opérations et de ne plus écrire le symbole ι de l'injection canonique. On écrit donc

$$(r \times s) \times \frac{p}{q} + (a+b) \times c \qquad \text{au lieu de} \qquad \iota(r \times s) \ \times_{\mathbf{Q}} \ \frac{p}{q} \ +_{\mathbf{Q}} \ \iota(a+b) \ \times_{\mathbf{Q}} \ \iota(c) \ .$$

Autrement dit, on fait l'amalgame entre $\iota(n) \in \mathbf{Q}_+$ et $n \in \mathbf{N}$ et on opte pour l'écriture le plus simple. Le fait que ces opérations sont compatibles via l'injection canonique nous garantit que cet abus est sans danger.

Une fois qu'on a adopté l'abus de notation qui consiste à ne plus écrire l'injection canonique et d'utiliser le même symbole pour les opérations d'addition et multiplications dans $\mathbf{N}$ *et* $\mathbf{Q}_+$*, on est prêt pour interpréter la notation* $\frac{p}{q}$ *pour une classe d'équivalence* $C_{(p,q)}$ *comme un quotient. Mais pour cela il faut d'abord dire ce qu'on entend par "quotient." En mathématiques on parle souvent de quotient ; on l'a déjà fait quand on a introduit "l'espace quotient" dans le contexte de relations d'équivalence. Mais dans le contexte de nombres on entend par quotient l'opération inverse pour la multiplication. Plus précisément, si on veut résoudre une équation*

$$a \times x = b \ , \tag{10.12}$$

on dit que la solution pour x *est le quotient de* b *et de* a*, qu'on notera* b/a *:*

$$a \times x = b \qquad \Longleftrightarrow \qquad x = b/a \ .$$

Il est bien connu que si a*,* b *et* x *sont des éléments de* $\mathbf{N}$*, alors l'équation (10.12) n'a pas toujours des solutions. Autrement dit, l'opération de prendre le quotient n'est pas une opération sur* $\mathbf{N}$*. Mais il est également bien connu que dans* $\mathbf{Q}$ *il existe toujours*

une solution (avec le caveat que a doit être non-nul). Non seulement si a et b sont des entiers, mais même si a et b sont des éléments de $\mathbf{Q}_+$. Mais prenons pour l'instant deux entiers a et b. Alors dans $\mathbf{Q}_+$ on peut faire le calcul

$$a \times \frac{b}{a} = \frac{a \times b}{a} = \frac{b}{1} = b \ .$$

Officiellement on aurait dû l'écrire et justifier comme

$$i(a) \ {}_{\times_{\mathbf{Q}}} \ \frac{b}{a} \overset{(10.9)}{=} \frac{a}{1} \ {}_{\times_{\mathbf{Q}}} \ \frac{b}{a} \overset{(10.7)}{=} \frac{a \times b}{1 \times a} \overset{(10.1)}{=} \frac{b}{1} \overset{(10.9)}{=} i(b) \ ,$$

mais arrivé au lycée il n'y a plus personne qui sent l'obligation de donner ces explications "évidentes." Ce que ce calcul montre est que l'équation (10.12) avec a et b dans $\mathbf{N}$ ($a \neq 0$) a une solution dans $\mathbf{Q}_+$ donné par $x = \frac{b}{a}$:

$$\forall a, b \in \mathbf{N}, a \neq 0 \quad : \quad a \times x = b \qquad \Longleftrightarrow \qquad x = \frac{b}{a} \in \mathbf{Q}_+ \ .$$

Si on compare ce résultat avec notre idée que la solution est donné par le quotient de b et a, alors on voit immédiatement que la fraction $\frac{b}{a}$ est *le quotient de b et a :*

$$b/a = \frac{b}{a} \ . \tag{10.13}$$

Mais on peut aller plus loin en prenant a et b pas dans $\mathbf{N}$ mais dans $\mathbf{Q}_+$. Si on a $a = \frac{p}{q}$ et $b = \frac{r}{s}$ deux éléments de $\mathbf{Q}_+$ avec $\frac{r}{s} \neq 0$ (ce qui est équivalent avec $r \neq 0$), on peut faire le calcul suivant dans $\mathbf{Q}_+$:

$$\frac{p}{q} \times \frac{q \times r}{p \times s} = \frac{p \times q \times r}{q \times p \times s} = \frac{r}{s} \ ,$$

ce qui montre que la solution de l'équation (10.12) est donné par $x = \frac{q \times r}{p \times s}$:

$$\frac{p}{q} \times x = \frac{r}{s} \qquad \Longleftrightarrow \qquad x = \frac{q \times r}{p \times s} = \frac{r}{s} \times \frac{q}{p} \ .$$

La comparaison avec la notation d'un quotient pour cette solution nous donne l'égalité

$$x = \frac{r}{s} \Big/ \frac{p}{q} = \frac{r}{s} \times \frac{q}{p} \ , \tag{10.14}$$

ce qui nous donne la règle bien connue que diviser (prendre le quotient) par une fraction est la même chose que multiplier par la fraction réciproque. Avec la notation d'une fraction (une classe d'équivalence !) comme un quotient (10.13) on peut donc écrire (10.14) de deux façons équivalentes :

$$(r/s)/(p/q) = (r/s) \times (q/p) \qquad ou \qquad \frac{\frac{r}{s}}{\frac{p}{q}} = \frac{r}{s} \times \frac{q}{p} \ ,$$

mais il ne faut jamais oublier que l'opération quotient n'est ni commutatif ni associatif : a/b n'est pas la même chose que b/a et $(a/b)/c$ n'est pas la même chose que $a/(b/c)$. Il faut donc bien prendre soin des parenthèses (ou la taille des barres horizontales dans un quotient) quand on écrit une formule avec plusieurs quotients.

11. Construction de Z

Dans ce sous-chapitre on reprend notre fil conducteur avec la construction des entiers relatifs $\mathbf{Z}$. *Une idée directeur dans la justification de cette construction est la soustraction. Dans* $\mathbf{N}$ *on ne dispose pas de cette opération, opération "inverse" à l'opération d'addition dans le sens qu'une soustraction annule l'opération d'addition. Il faut donc "élargir" l'ensemble des entiers naturels avec d'autres nombres de sorte qu'on puisse faire cette opération de soustraction. Le problème majeur est ce qu'on entend par élargir. L'idée naturel est de prendre la réunion de* $\mathbf{N}$ *avec un autre ensemble pour le compléter en* $\mathbf{Z}$. *Mais quel autre ensemble ? On dira "les nombres négatifs," mais cela n'a pas de sens. Ou "les entiers naturels non-nuls précédés d'un signe moins," ce qui est aussi dénudé de sens. Bien qu'on pouvait donner un sens à cette idée en considérant les deux ensembles* $\mathbf{N} \times \{0\}$ *et* $\mathbf{N}^* \times \{1\}$ *en disant que si la deuxième composante détermine le signe :* 0 *pour "positif" et* 1 *pour "négatif." On pourrait donc dire, avec nos connaissances de l'ensemble* $\mathbf{Z}$ *acquises au collège, qu'on a les représentations/identifications*

$$2 \cong (2,0) \qquad et \qquad -3 \cong (3,1) \ .$$

Cette définition est parfaitement correct mais elle a un très grand désavantage : on aura des difficultés à définir les opérations d'addition et de multiplication, car il faut toujours distinguer les deux cas (deuxième composante 0 *ou* 1*). Et cela devient encore pire quand on veut montrer les propriétés usuelles de ces deux opérations.*

L'approche "standard" est tout autre : on définit $\mathbf{Z}$ *comme un ensemble quotient de* $\mathbf{N} \times \mathbf{N}$ *par rapport à une relation d'équivalence. Cette méthode a plusieurs avantages : les définitions de l'addition et multiplication deviennent plus naturel et facile (sans qu'il faut distinguer des cas à chaque coin de rue) et elle se généralise directement à des situations plus complexes. Par contre, il y a (évidemment) aussi un désavantage : les entiers naturels ne sont plus une partie de* $\mathbf{Z}$. *Et pourtant, tout le monde sait que les entiers naturels peuvent être décrits comme*

$$\mathbf{N} = \{\, n \in \mathbf{Z} \mid n \geq 0 \,\} \subset \mathbf{Z} \ .$$

Comment sortir de cette impasse ? La solution est une procédure qu'on utilise (très) souvent en mathématique : on va identifier *les éléments de* $\mathbf{N}$ *avec des éléments de* $\mathbf{Z}$. *Bien sûr, on peut le faire de beaucoup de façons différentes, mais il y en a un qui est mieux que les autres : celle qui respecte toutes les propriétés/opérations des entiers naturels. Regardons un exemple. Une identification n'est rien d'autre qu'une application injective* $\varphi : \mathbf{N} \to \mathbf{Z}$ *qu'on interprète comme la règle qu'on identifie* $k \in \mathbf{N}$ *avec* $\varphi(k) \in \mathbf{Z}$. *Une possibilité d'une telle injection est l'application* $\varphi : \mathbf{N} \to \mathbf{Z}$ *définie par*

$$\varphi(k) = -2k \ .$$

Avec cette application on identifie donc par exemple l'entier naturel 5 *avec l'entier relatif* -10. *Et oui, cette application est bien injective. Mieux encore, cette application respecte l'addition :*

$$\varphi(k+\ell) = \varphi(k) + \varphi(\ell) \ .$$

Mais elle ne respecte pas la multiplication :

$$\varphi(2 \times 3) = \varphi(6) = -12 \neq 24 = (-4) \times (-6) = \varphi(2) \times \varphi(3) \ .$$

Si on cherche une application injective $\varphi : \mathbf{N} \to \mathbf{Z}$ *qui respecte les deux opérations d'addition et multiplication, il est facile de se convaincre qu'il n'y a qu'une seule*

façon de le faire : prendre l'identité. Mais cela présuppose qu'on sait déjà que $\mathbf{N}$ *est un sous-ensemble de* $\mathbf{Z}$*. Quand on ne le sait pas encore, quand on a une définition de* $\mathbf{Z}$ *pour laquelle* $\mathbf{N}$ *n'est pas un sous-ensemble, alors il faut inventer cette application injective/identification. Et notre raisonnement heuristique ci-dessus suggère qu'il n'y aura qu'une seule qui respectera les deux opérations d'addition et multiplication. C'est cet aspect d'unicité qui motive la dénomination "injection canonique" pour cette identification.*

Une fois qu'on a bien compris que $\mathbf{N}$ *et* $\mathbf{Z}$ *sont deux ensembles "vraiment" différent, mais qu'on peut identifier le premier comme un sous-ensemble du deuxième sans qu'on puisse voir la différence en ce qui concerne l'addition, la multiplication et la relation d'ordre (à ne pas oublier !), alors on effectue un tour de passe-passe : on oublie l'identification et on va dire que* $\mathbf{N}$ *est un sous-ensemble de* $\mathbf{Z}$ *! Une autre façon de voir ce tour de passe-passe est de dire qu'on oublie la définition initiale de l'ensemble* $\mathbf{N}$ *des entiers naturels et qu'on la remplace par une "nouvelle" définition de* $\mathbf{N}$ *qui dit que* $\mathbf{N}$ *est le sous-ensemble de* $\mathbf{Z}$ *constitué de l'image de "l'ancien"* $\mathbf{N}$ *par l'injection canonique.*

Encore une autre façon de voir la situation est d'oublier la construction initiale de $\mathbf{N}$ *et de se concentrer sur le nouvel ensemble* $\mathbf{Z}$*, muni des deux opération d'addition et de multiplication et d'une relation d'ordre total. Dans cet ensemble* $\mathbf{Z}$ *on peut donc définir le sous-ensemble* $\mathbf{N}$ *comme étant les éléments "positifs," c'est-à-dire, plus grand ou égale à l'élément neutre pour l'addition. Et on peut montrer que ce sous-ensemble vérifie les axiomes de Peano. Mais bon, comme ça on tourne un peu en rond.*

Revenons sur la construction de $\mathbf{Z}$*. L'explication/analogie qu'on utilise souvent pour expliquer l'idée derrière la définition de* $\mathbf{Z}$ *comme ensemble quotient de* $\mathbf{N} \times \mathbf{N}$ *par rapport à une relation d'équivalence est l'idée de l'argent qu'on possède. On peut indiquer la quantité d'argent qu'on possède par un entier naturels (par exemple le nombre de centimes d'euro qu'on possède). Normalement cette quantité est toujours positive, donc représentée par un entier naturel. Mais on peut aussi avoir des dettes (chez des copains, un marchand ou la banque). Dans ce cas il faut diminuer la quantité d'argent qu'on possède avec notre dette pour savoir de combien d'argent on dispose vraiment. Et bien sûr, les deux nombres "argent en ma possession" et "ma dette" sont deux entiers naturels. Par exemple si j'ai* 25 *dans ma poche et une dette de* 12*, ma fortune n'est en réalité que* $13 = 25 - 12$*. Et si je rembourse une partie de ma dette, disons* 6*, j'aurai* $25 - 6 = 19$ *dans ma poche et une dette de* $12 - 6 = 6$*. Et ma fortune est toujours* $19 - 6 = 13$*. Si on note* P *la quantité d'argent dans ma poche et* D *ma dette, ma fortune réelle* F *est donnée par* $F = P - D$*. Mais si on ne dispose pas de la soustraction, je n'aurai pas la possibilité d'écrire* $P - D$ *et je serai obligé de continuer à mesurer ma fortune en termes des deux nombres* P *et* D*. Mais comme on vient de voir dans notre exemple, ma fortune réelle n'a pas changé quand j'ai remboursé une partie de ma dette, c'est-à-dire que le couple* (P, D) *et le couple* $(P - 6, D - 6)$ *représentent tous les deux la même fortune. Ainsi est née la notion de la relation d'équivalence. Sauf qu'on n'a pas le droit (toujours pas) d'utiliser la soustraction. Mais ce problème n'est qu'illusoire, car on peut facilement voir que deux couples* (P, D) *et* (P', D') *représentent le même capital si on a*

$$P - D = P' - D' \qquad \Longleftrightarrow \qquad P + D' = P' + D \ .$$

Écrite de cette façon, on n'utilise plus la soustraction. Et les "nombres négatifs" ? Ce sont les couples où la dette est plus grande que ce qu'on a dans sa poche !

11.1 Définition d'une relation d'équivalence sur $\mathbf{N}\times\mathbf{N}$. Sur l'ensemble $\mathbf{N}\times\mathbf{N}$ on définit une relation d'équivalence $\sim$ par

$$(a,b)\sim(p,q) \quad \overset{\text{déf}}{\Longleftrightarrow} \quad a+q=b+p \ . \tag{11.2}$$

Dans [11.3] on montrera que c'est bien une relation d'équivalence. L'ensemble quotient $(\mathbf{N}\times\mathbf{N})/\!\sim$ sera noté par $\mathbf{Z}$:

$$\mathbf{Z} \overset{\text{déf}}{=} (\mathbf{N}\times\mathbf{N})/\!\sim \ .$$

Un élément de l'ensemble $\mathbf{Z}$ s'appelle un *entier relatif* et l'ensemble $\mathbf{Z}$ lui-même s'appelle bien évidemment *l'ensemble des entiers relatifs*. Pour cette relation d'équivalence on note la classe d'équivalence d'un couple (a,b) par $[\![\,a,b\,]\!]_{\mathbf{Z}}$:

$$[\![\,a,b\,]\!]_{\mathbf{Z}} \overset{\text{déf}}{=} \{(p,q)\in\mathbf{N}\times\mathbf{N} \mid (p,q)\sim(a,b)\} \ .$$

Ⓟ **11.3 Lemme.** *La relation $\sim$ sur $\mathbf{N}\times\mathbf{N}$ définie par (11.2) est une relation d'équivalence.*

Ⓟ **11.4 Lemme/Définition.** *L'application $\iota:\mathbf{N}\to\mathbf{Z}$ définie par*

$$\iota(n)=[\![\,n,0\,]\!]_{\mathbf{Z}} \tag{11.5}$$

est injective. On l'appelle l'injection canonique de $\mathbf{N}$ dans $\mathbf{Z}$.

Ⓟ **11.6 L'addition dans Z.** *L'application $f:(\mathbf{N}\times\mathbf{N})\times(\mathbf{N}\times\mathbf{N})\to\mathbf{Z}$ définie par*

$$f\big((a,b),(p,q)\big)=[\![\,a+p,b+q\,]\!]_{\mathbf{Z}}$$

est compatible avec la relation d'équivalence définie en (11.2). Par [9.12] il existe donc une unique application $+_{\mathbf{Z}}:\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$, appelée l'addition dans $\mathbf{Z}$, *vérifiant*

$$[\![\,a,b\,]\!]_{\mathbf{Z}} +_{\mathbf{Z}} [\![\,p,q\,]\!]_{\mathbf{Z}} \quad = \quad [\![\,a+p,b+q\,]\!]_{\mathbf{Z}} \quad \equiv \quad f\big((a,b),(p,q)\big) \ .$$

On a (provisoirement) ajouté la lettre $\mathbf{Z}$ en indice pour distinguer cette opération de l'opération d'addition déjà définie sur $\mathbf{N}$.

Ⓟ **11.7 Compatibilité avec l'addition dans N.** *L'addition dans $\mathbf{Z}$ qu'on vient de définir est compatible avec l'addition déjà définie dans $\mathbf{N}$ dans le sens qu'on a*

$$\forall m,n\in\mathbf{N} \quad : \quad \iota(m+n)=\iota(m)\ +_{\mathbf{Z}}\ \iota(n) \ ,$$

où $\iota:\mathbf{N}\to\mathbf{Z}$ est l'injection canonique (11.5).

Ⓟ **11.8 La multiplication dans Z.** *L'application $f:(\mathbf{N}\times\mathbf{N})\times(\mathbf{N}\times\mathbf{N})\to\mathbf{Z}$ définie par*

$$f\big((a,b),(p,q)\big)=[\![\,a\times p+b\times q,a\times q+b\times p\,]\!]_{\mathbf{Z}}$$

est compatible avec la relation d'équivalence définie en (11.2). Par [9.12] il existe donc une unique application $\times_{\mathbf{Z}}:\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$, appelée la multiplication dans $\mathbf{Z}$, *vérifiant*

$$[\![\,a,b\,]\!]_{\mathbf{Z}} \times_{\mathbf{Z}} [\![\,p,q\,]\!]_{\mathbf{Z}} \quad = \quad [\![\,a\times p+b\times q,a\times q+b\times p\,]\!]_{\mathbf{Z}} \quad \equiv \quad f\big((a,b),(p,q)\big) \ .$$

Comme pour l'addition on a ajouté (provisoirement) la lettre $\mathbf{Z}$ en indice pour distinguer cette opération de l'opération de multiplication déjà définie sur $\mathbf{N}$.

À première vu la formule pour la multiplication peut paraître étrange, mais si on pense à l'idée qu'un couple (P, D) représente ma fortune sous la forme $F = P - D$, alors la multiplication de deux "fortunes" (P_1, D_1) et (P_2, D_2) devient :

$$F_1 \times F_2 = (P_1 - D_1) \times (P_2 - D_2) = (P_1 \times P_2 + D_1 \times D_2) - (P_1 \times D_2 + P_2 \times D_1) \ ,$$

ce qui représente la fortune sous forme d'un couple argent dans la poche et dettes :

$$F_1 \times F_2 \cong (P_1 \times P_2 + D_1 \times D_2, P_1 \times D_2 + P_2 \times D_1) \ .$$

Et on voit apparaître notre formule pour la multiplication.

Ⓟ **11.9 Compatibilité avec la multiplication dans N.** *La multiplication dans* **Z** *qu'on vient de définir est compatible avec la multiplication déjà définie dans* **N** *dans le sens qu'on a*

$$\forall k, \ell \in \mathbf{N} \quad : \quad \iota(k \times \ell) = \iota(k) \ \times_{\mathbf{Z}} \ \iota(\ell) \ ,$$

où $\iota : \mathbf{N} \to \mathbf{Z}$ est l'injection canonique (11.5).

11.10 La relation d'ordre sur Z. *La relation $\preccurlyeq \subset (\mathbf{N} \times \mathbf{N}) \times (\mathbf{N} \times \mathbf{N})$ définie par*

$$(a, b) \preccurlyeq (p, q) \qquad \Longleftrightarrow \qquad a + q \leq b + p$$

est compatible avec la relation d'équivalence (11.2). Par [9.15] il existe donc une relation $\leq_{\mathbf{Z}}$ sur **Z** *vérifiant*

$$[\![\, a, b \,]\!]_{\mathbf{Z}} \leq_{\mathbf{Z}} [\![\, p, q \,]\!]_{\mathbf{Z}} \qquad \Longleftrightarrow \qquad a + q \leq b + p \ .$$

Cette relation $\leq_{\mathbf{Z}}$ sur **Z** *est une relation d'ordre total ; comme pour l'addition et la multiplication on a ajouté (provisoirement) la lettre* **Z** *en indice pour distinguer cette relation d'ordre de la relation d'ordre déjà définie sur* **N**.

11.11 Compatibilité avec la relation d'ordre dans N. *La relation d'ordre dans* **Z** *qu'on vient de définir est compatible avec la relation d'ordre déjà définie dans* **N** *dans le sens qu'on a*

$$\forall m, n \in \mathbf{N} \quad : \quad m \leq n \qquad \Longleftrightarrow \qquad \iota(m) \leq_{\mathbf{Z}} \iota(n) \ ,$$

où $\iota : \mathbf{N} \to \mathbf{Z}$ est l'injection canonique (11.5).

Abus de notation très commode et universellement adopté. Une fois qu'on sait que l'addition, la multiplication et la relation d'ordre dans **N** et **Z** sont compatibles via l'injection canonique $\iota : \mathbf{N} \to \mathbf{Z}$, on prend l'habitude de ne plus écrire le symbole **Z** en index sur ces opérations et de ne plus écrire le symbole ι de l'injection canonique. On écrit donc

$$[\![\, 2, 5 \,]\!]_{\mathbf{Z}} \leq 2 \qquad \text{au lieu de} \qquad [\![\, 2, 5 \,]\!]_{\mathbf{Z}} \leq_{\mathbf{Z}} \iota(2) \quad \text{ou} \quad [\![\, 2, 5 \,]\!]_{\mathbf{Z}} \leq_{\mathbf{Z}} [\![\, 2, 0 \,]\!]_{\mathbf{Z}} \ .$$

Et pour des entiers naturels a, b, c, d, p, q, r, s on écrit

$$(r \times s) \times [\![\, p, q \,]\!]_{\mathbf{Z}} + (a + [\![\, b, c \,]\!]_{\mathbf{Z}}) \times d$$

au lieu de

$$\iota(r \times s) \ \times_{\mathbf{Z}} \ [\![\, p, q \,]\!]_{\mathbf{Z}} \ +_{\mathbf{Z}} \ (\iota(a) \ +_{\mathbf{Z}} \ [\![\, b, c \,]\!]_{\mathbf{Z}}) \ \times_{\mathbf{Z}} \ \iota(d) \ .$$

Le fait que ces opérations sont compatibles via l'injection canonique nous garantit que cet abus est sans danger. Le fait qu'on n'écrit pas l'injection canonique veut dire qu'on voit les entiers naturels comme un sous-ensemble des entiers relatifs. Strictement parlant ceci n'est certainement pas vrai : un entier naturel n'est pas égal à une classe d'équivalence de couples d'entiers naturels (car c'est ça, un entier relatif !). Mais on fait l'identification pour simplifier l'écriture. Et, plus que l'écriture est simple, plus qu'il est facile de comprendre les énoncés. Le prix à payer est qu'il faut être conscient de cet abus au moment où cela risque de devenir une source d'erreurs et/ou de malentendus. Ceci s'applique en particulier aux preuves des propriétés de $\mathbf{Z}$ *qu'on rencontrera dans la suite. Ces propriétés se divisent en deux catégories : celles pour lesquelles on a besoin de la structure explicite de* $\mathbf{Z}$ *pour le montrer, et les autres qu'on peut montrer en utilisant uniquement des propriétés déjà montrées. On pourrait donc dire qu'il y a des propriétés "essentielles" — celles qui nécessitent la connaissance explicite de* $\mathbf{Z}$ *— et des propriétés "dérivées" — celles qu'on peut déduire en utilisant d'autres propriétés, sans recours à la structure explicite de* $\mathbf{Z}$.

Une fois qu'on a noté cette différence entre propriétés essentielles et dérivées[1] *on s'aperçoit qu'on rencontre souvent ces mêmes propriétés essentielles et qu'on répète souvent les mêmes preuves pour démontrer les propriétés dérivées. Au lieu de répéter ces "mêmes" preuves pour des ensembles différentes, on donne des noms à ces propriétés essentielles et on montre une fois pour toutes les propriétés dérivées. C'est ainsi qu'on arrive à la définition d'un groupe, un anneau (qu'on va voir ci-dessous) ou un corps (qu'on va découvrir dans [14]). Ces structures sont "cumulatif" dans le sens que le suivant a plus de propriétés que le précédent. Le nombre de propriétés dérivées pour un corps sera donc (en principe) plus grand que pour un anneau. Par exemple, dans l'anneau* $\mathbf{Z}$ *il n'y a pas de garanti qu'on peut résoudre une équation de la forme* $ax = b$, *tandis que dans le corps* $\mathbf{Q}$ *c'est automatique, car vrai pour tout corps (à condition que* $a \neq 0$*).*

11.12 Lemme. *L'addition* $+_{\mathbf{Z}} : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ *vérifie les propriétés*

(i) $\forall m, n \in \mathbf{Z} : m + n = n + m.$

(ii) $\forall k, m, n \in \mathbf{Z} : (k + m) + n = k + (m + n),$

(iii) $\forall n \in \mathbf{Z} : n + 0 = n,$

(iv) $\forall n \in \mathbf{Z}\ \exists m \in \mathbf{Z} : n + m = 0.$

Ce n'est pas (totalement) vrai que les propriétés que vérifie l'addition dans $\mathbf{Z}$ *sont à la base de la définition d'un groupe. L'origine de la notion de groupe se trouve plutôt dans le domaine des symétries d'un objet, comme un triangle, un tétraèdre ou un cristal de sel. Autrement dit, dans un contexte d'application/bijections qu'on fait subir un objet. Mais le fait que l'addition dans* $\mathbf{Z}$ *a ces même propriétés confirme l'idée que la notion d'un groupe est omniprésent en mathématique.*

11.13 Définition. Soit G un ensemble muni d'une opération interne $\blacksquare : G \times G \to G$. On dit que $(G, \blacksquare)$ est un *groupe* si cette opération vérifie les trois conditions

1. Ces noms, je les ai inventés pour cette discussion ; ils n'ont aucune valeur mathématique !

(G1) $\forall g,h,k \in G : g \blacksquare (h \blacksquare k) = (g \blacksquare h) \blacksquare k$ (*associativité*),

(G2) $\exists e \in G\ \forall g \in G : g \blacksquare e = e \blacksquare g = g$ (*existence d'un élément neutre*) et

(G3) $\forall g \in G\ \exists h \in G : h \blacksquare g = g \blacksquare h = e$ (*existence d'un élément symétrique*).

Si l'opération $\blacksquare$ vérifie en plus la condition

(G4) $\forall g,h \in G : g \blacksquare h = h \blacksquare g$ (*commutativité*),

alors on dit que $(G, \blacksquare)$ est un *groupe abélien* (on dit aussi un groupe commutatif).

L'exemple type d'un groupe est l'ensemble $\mathrm{Gl}(n,\mathbf{R})$ *des matrices carrées d'ordre* n *inversibles muni de la multiplication de matrices. On ne peut pas les additionner (ça restera une matrice carré mais sans la garantie que la somme sera inversible) et ce groupe n'est pas commutatif. C'est même tellement "typique" qu'on a développé toute une théorie qui essaye de réaliser tout groupe comme (sous) groupe de matrices : la théorie des représentations de groupes.*

11.14 Lemme. *Soit* $(G, \blacksquare)$ *un groupe. Alors l'élément neutre* e *est unique et pour tout* $g \in G$ *il n'existe qu'un seul élément symétrique. Il existe donc une unique application* $\sigma : G \to G$*, appelée l'application du symétrique, vérifiant la condition*

$$\forall g \in G : g \blacksquare \sigma(g) = \sigma(g) \blacksquare g = e \ .$$

En plus, elle vérifie les conditions

(i) $\sigma(e) = e$,

(ii) $\forall g \in G : \sigma\big(\sigma(g)\big) = g$ *et*

(iii) $\forall g,h \in G : \sigma(g \blacksquare h) = \sigma(h) \blacksquare \sigma(g)$.

Remarque. Si on revient à la définition officielle d'une application [4.1], on devrait formuler le résultat [11.14] en disant que l'ensemble

$$\sigma = \{\, (g,h) \in G \times G \mid g \blacksquare h = e = h \blacksquare g \,\} \subset G \times G$$

est une application $\sigma : G \to G$.

Définitions/terminologie. • Soit $(G, \blacksquare)$ un groupe. On dit que G *est un groupe abélien additif* (on dit aussi que le groupe G a *une structure additive*) si on écrit l'opération interne par un $+$; on aurait donc dû dire que $(G,+)$ est un groupe abélien. Et on dit que G *est un groupe multiplicatif* (on dit aussi que le groupe G a *une structure multiplicative*) si on écrit l'opération par un $\times$, un $\cdot$, ou par rien du tout. Dans le premier cas on aurait donc dû dire que $(G,\times)$ est un groupe, dans le deuxième cas on aurait dû dire que $(G,\cdot)$ est un groupe, et dans le troisième cas on n'aurait pas pu l'écrire ! L'habitude veut qu'on omet souvent le symbole $\cdot$ de la "multiplication", mais quand on veut indiquer l'opération (sans nom), on est obligé de mettre un symbole, ce qui est donc le "$\cdot$".

Notons tout de suite que ces "définitions" n'ont aucun contenu mathématique supplémentaire. Ajouter le qualificatif "additif" ou "multiplicatif" à un groupe ne donne pas d'information mathématique, mais une information sur notre façon d'écrire

l'objet (en occurence l'opération). Avec comme seule exception que le qualificatif "additif" sous-entend (généralement) que le groupe est abélien. En particulier on omet souvent de préciser que le groupe est abélien quand on dit qu'il est additif (ou que G a une structure additive).

• Dans un groupe abstrait G on désigne l'élément neutre (souvent) par la lettre e et on parle de l'application du symétrique ; pour $g \in G$ on appelle $\sigma(g)$ l'élément *symétrique* de g (ou simplement *le symétrique* de g. Mais il existe d'autres noms pour ces objets dépendant du contexte.

— Si la structure du groupe est additive (c'est-à-dire qu'on note l'opération interne par un $+$, qu'on appelle addition, et qu'on sous-entend que G est abélien), on désigne l'élément neutre le plus souvent par 0 ou par 0_G (un "zéro" avec ou sans G en indice). Il n'est donc pas anormal de voir apparaître le même symbole 0 dans plusieurs sens dans une même formule (et si on veut éviter à tout prix des malentendus, on rajoute en indice le groupe auquel ce 0 appartient). Quant-au symétrique, on parle plutôt de l'élément *opposé*. Et dans un tel cas, on note l'application du symétrique par le signe moins $-$ et on dit que $-g$ est l'opposé de g. Pour les nombres, c'est bien l'opposé par rapport à l'élément neutre pour l'addition (le 0).

— Si la structure est multiplicative (c'est-à-dire qu'on note l'opération interne par $\times$ ou $\cdot$ ou simplement en juxtaposant les deux éléments), on désigne l'élément neutre souvent par le symbole 1 ou une variante comme $\mathbf{1}$ ou $\mathbb{1}$, éventuellement avec un G en indice. Quant-au symétrique, on parle plutôt de l'élément *inverse*. Dans un tel cas on note l'application du symétrique (l'inverse) par un -1 en exposant : $\sigma(g) \equiv g^{-1}$.

— S'il s'agit d'un groupe d'applications (bijectives), au quel cas l"opération interne est la composée d'applications $\circ$, on désigne l'élément neutre souvent par une sorte d'abréviation du mot "identité" comme I ou id. Et au lieu de symétrique on parle le plus souvent de l'élément (l'application !) *réciproque*, qu'on note comme dans le cas multiplicatif par un -1 en exposant.

Dans l'exemple du groupe $\mathrm{Gl}(n, \mathbf{R})$ *des matrices carrées d'ordre n inversibles la structure est bien "multiplicative" et l'élément symétrique est bien noté avec -1 en exposant. Dans ce contexte le résultat [11.14.iii] se traduit comme la règle classique (bien connue ?) que l'inverse d'un produit de matrices est le produit des inverses* dans l'autre sens *: pour deux matrices carrées inversibles A et B on a*

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1} \ .$$

11.15 Corollaire. *L'ensemble* $\mathbf{Z}$ *muni de l'opération* $+_{\mathbf{Z}}$ *est un groupe abélien avec* 0 *comme élément neutre.*

11.16 Corollaire de [11.14]/notation. *L'application du symétrique σ dans* $\mathbf{Z}$ *est notée* $- : \mathbf{Z} \to \mathbf{Z}$ *et pour $n \in \mathbf{Z}$ on dit que $\sigma(n) \equiv -n$ est* l'opposé *de n. On a donc les propriétés*

(i) $-0 = 0$,

(ii) $\forall n \in \mathbf{Z} : n + (-n) = 0 = (-n) + n$,

(iii) $\forall m, n \in \mathbf{Z} : -(m + n) = (-m) + (-n)$ *et*

(iv) $\forall n \in \mathbf{Z} : -(-n) = n$.

11.17 Remarque. Une autre façon de définir l'opposé dans **Z** est de considérer l'application $f : \mathbf{N} \times \mathbf{N} \to \mathbf{Z}$ définie par

$$f\big((a, b)\big) = [\![\, b, a \,]\!]_{\mathbf{Z}}$$

et de constater que cette application est compatible avec la relation d'équivalence définie en (11.2). Par [9.9] il existe donc une unique application $M_{\mathbf{Z}} : \mathbf{Z} \to \mathbf{Z}$ vérifiant

$$M_{\mathbf{Z}}(\, [\![\, a, b \,]\!]_{\mathbf{Z}}) \quad = \quad [\![\, b, a \,]\!]_{\mathbf{Z}} \quad \equiv \quad f\big((a, b)\big) \ .$$

Le calcul

$$\begin{aligned} [\![\, m, n \,]\!]_{\mathbf{Z}} \ +_{\mathbf{Z}} \ M_{\mathbf{Z}}(\, [\![\, m, n \,]\!]_{\mathbf{Z}}) &= [\![\, m, n \,]\!]_{\mathbf{Z}} \ +_{\mathbf{Z}} \ [\![\, n, m \,]\!]_{\mathbf{Z}} \\ &= [\![\, m + n, m + n \,]\!]_{\mathbf{Z}} = [\![\, 0, 0 \,]\!]_{\mathbf{Z}} = \iota(0) \ . \end{aligned}$$

et l'unicité dans [11.16] montrent qu'on doit avoir l'égalité

$$M_{\mathbf{Z}}(\, [\![\, m, n \,]\!]_{\mathbf{Z}}) = -[\![\, m, n \,]\!]_{\mathbf{Z}} \ , \tag{11.18}$$

c'est-à-dire que prendre l'opposé (l'application du symétrique σ !) et l'application $M_{\mathbf{Z}}$ coïncident.

D'autres exemples de l'abus de notation. En poursuivant les exemples de l'abus de notation de ne pas distinguer les opérations (d'addition et de multiplication) dans **Z** de celles dans **N** et de ne pas écrire l'injection canonique, on remarque qu'on écrit -2 pour l'élément $-\iota(2)$, un élément qui est formellement donné par

$$-2 = [\![\, 0, 2 \,]\!]_{\mathbf{Z}} = \big\{\, (a, b) \in \mathbf{N} \times \mathbf{N} \ \big|\ (a, b) \sim \big(\, \emptyset \,,\, \{\emptyset, \{\emptyset\}\,\}\big) \,\big\}$$

Et on écrit

$$-3 \leq 2 \qquad \text{au lieu de} \qquad -\,\iota(3) \leq_{\mathbf{Z}} \iota(2) \quad \text{ou} \quad [\![\, 0, 3 \,]\!]_{\mathbf{Z}} \leq_{\mathbf{Z}} [\![\, 2, 0 \,]\!]_{\mathbf{Z}} \ .$$

La soustraction dans Z. C'est avec la propriété [11.12.iv] qu'on peut définir la soustraction dans **Z**, une opération qu'on n'avait pas dans **N**. Elle est définie comme

$$\forall m, n \in \mathbf{Z} : m - n \ \stackrel{\text{déf}}{=} \ m + (-n) \ ,$$

où $-n$ est l'opposé (le symétrique) de n, écrit avec l'opération, unaire $-$. On vérifie aisément (à l'aide de [11.12]) qu'on a la propriété

$$x + m = n \qquad \Longleftrightarrow \qquad x = n - m \ .$$

À l'aide de la soustraction (ou de l'opposé) on peut interpréter une classe d'équivalence comme une soustraction de deux entier naturels. Ainsi on retrouve notre analogie initiale que notre capital se calcule comme la différence entre l'argent qu'on

a dans la poche P et nos dettes D. Pour cela on fait le calcul suivant avec m et n deux entiers naturels

$$\begin{aligned}[[\,m,n\,]]_{\mathbf{z}} &= [[\,m,0\,]]_{\mathbf{z}} \,+_{\mathbf{z}}\, [[\,0,n\,]]_{\mathbf{z}} = [[\,m,0\,]]_{\mathbf{z}} \,+_{\mathbf{z}}\, M_{\mathbf{Z}}\big([[\,n,0\,]]_{\mathbf{z}}\big) \\ &\equiv \iota(m) \,+_{\mathbf{z}}\, \sigma\big(\iota(n)\big) = \iota(m) - \iota(n)\ .\end{aligned}$$

Mais attention : on utilise le symbole $-$ (le symbole pour "moins") dans deux sens différentes ! On l'a d'abord défini comme l'opération unaire de l'opposé $-:\mathbf{Z}\to\mathbf{Z}$. Et ensuite on l'a aussi définie comme une opération binaire $-:\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$ (autrement dit, une opération interne sur $\mathbf{Z}$). Si on garde le symbole σ pour l'opération du symétrique (unaire), alors les deux opérations sont liées par les formules

$$m-n = m+\sigma(n) \qquad et \qquad \sigma(n) = 0-n\ .$$

Connaissance de l'un entraîne dont la connaissance de l'autre. Ici on a d'abord défini l'opération unaire pour en déduire l'opération interne de soustraction (ce qui est la voie logique dans le contexte d'un groupe). Mais, en guise d'exercice, le lecteur intéressé pourrait définir l'opération interne de soustraction directement comme l'addition, sans passer par le symétrique/opposé.

Plus généralement, si $(G,\blacksquare)$ est un groupe, ce sont les propriétés de l'opération $\blacksquare$ qui permettent de résoudre $x\in G$ d'une équation $a\blacksquare x = b$ ou $x\blacksquare a = b$. Dans le premier cas on raisonne comme suit :

$$a\blacksquare x = b \quad\Rightarrow\quad x = e\blacksquare x = \big(\sigma(a)\blacksquare a\big)\blacksquare x = \sigma(a)\blacksquare(a\blacksquare x) = \sigma(a)\blacksquare b\ ,$$

et dans le deuxième cas on raisonne comme :

$$x\blacksquare a = b \quad\Rightarrow\quad x = x\blacksquare e = x\blacksquare\big(a\blacksquare\sigma(a)\big) = (x\blacksquare a)\blacksquare\sigma(a) = b\blacksquare\sigma(a)\ .$$

Bien évidemment dans le cas d'un groupe commutatif ces deux équations sont les mêmes, comme leurs solutions. Et on reconnaît la forme des solutions qu'on a trouvé dans $\mathbf{Z}$ pour l'équation $x+a=b$ comme $x=b+(-a)$. C'est le fait que dans un groupe non-commutatif il faut distinguer les deux équations $a\blacksquare x=b$ et $x\blacksquare a=b$ et donc le fait que leurs solutions sont différentes, qui fait qu'on préfère écrire la soustraction sous la forme d'une addition avec l'opposé.

11.19 Lemme. *La multiplication $\times:\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$ vérifie les propriétés*

(i) $\forall m,n\in\mathbf{Z} : m\times n = n\times m$.

(ii) $\forall k,m,n\in\mathbf{Z} : k\times(m\times n) = (k\times m)\times n$,

(iii) $\forall k,m,n\in\mathbf{Z} : k\times(m+n) = (k\times m)+(k\times n)$,

(iv) $\forall n\in\mathbf{Z} : n\times 1 = n$,

11.20 Définition. Soit A un ensemble muni de deux opérations internes : $+ : A\times A\to A$ et $\times : A\times A\to A$. On dit que $(A,+,\times)$ est un *anneau* si les conditions suivantes sont satisfaites :

(A0) $(A,+)$ est un groupe abélien additif (et on note 0_A l'élément neutre pour $+$),

(A1) $\forall a,b,c\in A : a\times(b+c) = (a\times b)+(a\times c)$ et $(b+c)\times a = (b\times a)+(c\times a)$ (*distributivité à gauche et à droite de $\times$ sur $+$*) et

(A2) $\forall a,b,c\in A : a\times(b\times c) = (a\times b)\times c$ (associativité de $\times$).

(A3) $\exists 1_A\in A\ \forall a\in A : a\times 1_A = 1_A\times a = a$ (*existence d'un élément neutre pour $\times$*).

On dit que $(A, +, \times)$ est un *anneau commutatif* si c'est un anneau où l'opération $\times$ est commutative :

(A4) $\forall a, b \in A : a \times b = b \times a$.

Si $(A, +, \times)$ est un anneau commutatif et $a \in A$, alors on dit que *a est un diviseur de zéro* si $a \neq 0_A$ et s'il existe $b \neq 0_A$ tel que $a \times b = 0_A$. On dit que $(A, +, \times)$ est un *anneau intègre* si c'est un anneau commutatif unitaire sans diviseurs de zéro, c'est-à-dire que l'opération $\times$ vérifie la condition :

(A5) $\forall a, b \in A : a \times b = 0_A \ \Rightarrow \ a = 0_A$ ou $b = 0_A$.

11.21 Corollaire. *L'ensemble $\mathbf{Z}$ muni des deux opérations $+$ et $\times$ est un anneau commutatif avec 0 l'élément neutre pour l'addition $+$ et 1 l'élément neutre pour la multiplication $\times$.*

On vient de voir que les propriétés d'un anneau commutatif sont les propriétés qu'on vient de montrer pour $\mathbf{Z}$. Et bientôt on montrera que $\mathbf{Z}$ est même un anneau intègre. La question se pose donc si les autres définitions (avec moins de propriétés) sont vraiment utiles et/ou s'il existe vraiment des exemples avec moins de propriétés. La réponse est affirmative dans les deux cas. Pour la notion d'anneau les deux exemples types sont l'ensemble des entiers relatifs $\mathbf{Z}$ et l'ensemble $\mathrm{M}(n, \mathbf{R})$ de tous les matrices carrés d'ordre n (à coefficients réels) muni de l'addition et multiplication de matrices. Le premier est un anneau intègre, mais le deuxième est "seulement" un anneau ; la multiplication des matrices n'est pas commutative et il existe des diviseurs de zéro. Notons en passant que dans ces deux exemples il est tout-à-fait naturel de noter les éléments neutres pour les deux opérations par 0 et par 1. Pour $\mathbf{Z}$ c'est exactement cela, mais même pour les matrices c'est (presque) cela : l'élément neutre pour l'addition est la matrice dont tous les éléments sont 0 et l'élément neutre pour la multiplication est la matrice diagonale avec que des 1 sur la diagonale. Un autre exemple classique d'anneau est l'ensemble des entiers modulo n (on parle de $\mathbf{Z}/n\mathbf{Z}$). Dans le cas $n = 6$ par exemple on calcule modulo 6 dans l'ensemble $A = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Ceci est un anneau commutatif avec $\bar{0}$ l'élément neutre pour l'addition et $\bar{1}$ l'élément neutre pour la multiplication, mais ce A n'est pas intègre, car on a $\bar{2} \times \bar{3} = \bar{6} \equiv \bar{0}$.

Remarque sur la définition d'un anneau. Dans la littérature ancienne la définition d'un anneau est légèrement différente dans le sens qu'on n'exige pas l'existence d'un élément neutre pour l'opération $\times$. Dans ces cas on parle d'un anneau *unitaire* quand l'anneau contient un tel élément. Le fait que les anneaux "intéressants" contiennent toujours un élément neutre pour l'opération $\times$ a motivé ce changement de définition. Un exemple d'un anneau sans élément neutre pour la deuxième opération interne est l'ensemble des entiers relatifs pairs (muni de l'addition et la multiplication pour les deux opérations internes).

Remarque sur la notation/terminologie. Le lecteur attentif aura remarqué que pour un groupe G on a noté l'élément neutre pour l'opération concerné par

la lettre e, mais que dans un anneau on le note comme 0_A, c'est-à-dire avec le symbole "zéro" pourvu d'un A en indice. Et qu'on note l'élément neutre pour la deuxième opération d'un anneau comme 1_A avec le symbole "un" avec un A en indice. La question naturelle est pourquoi on n'a pas utilisé une lettre pour les éléments neutres dans un anneau *ou* pourquoi on n'a pas utilisé le zéro pour l'élément neutre dans un groupe ? La réponse est probablement double. C'est d'abord le poids de l'histoire. Mais on peut donner des justifications plus rationnelles. Dans la nature mathématiques on rencontre beaucoup de groupes et l'écriture de leur élément neutre est divers, bien qu'on trouve souvent soit 0 soit 1. Mais le fait qu'on trouve souvent ces *deux* "chiffres" pour l'élément neutre dans un groupe fait qu'on va vite se tromper si on utilise l'un des deux pour le cas général. Par contre, pour la plupart des anneau qu'on rencontre d'une façon naturelle en mathématique, la notation pour ces deux éléments neutre (un pour chaque opération) est déjà (très) souvent le 0 (ou quelque chose qu'on assimile à un zéro) pour la première opération et le 1 (ou quelque chose qu'on assimile à un "un") pour la deuxième. Et donc notre "intuition" ne sera pas perturbé si dans le cas général on utilise ces deux symboles pour ces deux éléments.

Remarque pour les comparateurs. Dans la littérature on trouve la notion de diviseur de zéro aussi pour des anneaux non-commutatifs, au quel cas il faut distinguer un diviseur de zéro à gauche d'un diviseur de zéro à droite.

11.22 Omission des parenthèses/priorité des opérations II. Un anneau est muni de deux opérations internes associatives $+$ et $\times$ et donc la convention [8.11] de supprimer les parenthèses quand une même opération intervient plusieurs fois s'applique. Et il est coutume d'accorder la priorité à la deuxième opération $\times$, ce qui permet de supprimer d'avantage de parenthèses. Par contre, dans un anneau on dispose d'une troisième opération interne : la "soustraction", c'est-à-dire, l'opération qui permet de résoudre $x \in A$ d'une équation du type $x + a = b$ sous la forme

$$x = b - a \overset{\text{déf}}{=} b + (-a) \equiv b + \sigma(a) \ ,$$

où σ (ou l'opération unaire $-$) désigne l'opération de l'opposé (par rapport à l'opération $+$). Cette opération n'est pas associative et ne "profite" pas de la suppression de parenthèses (au contraire). De plus, le fait qu'on utilise le symbole $-$ dans deux sens différents — comme opération binaire dans $b - a$ ou comme opération unaire d'opposé dans $-a$ — complique les choses. Néanmoins, il n'est pas rare de voir qu'on utilise la soustraction dans ces deux sens dans le cadre d'un anneau. De toute façon, il est "interdit" d'écrire sans parenthèses une expression du type

$$a - b + c \qquad \text{ou} \qquad a - b - c \ ,$$

car le placement des parenthèses change le sens :

$$(a - b) + c = a - (b - c) \neq (a - b) - c = a - (b + c) \ .$$

Par contre, du moment qu'on utilise le symbole $-$ comme une opérateur unaire, alors il aura priorité sur tous les opérations binaire, et cela sans ambiguïté. On pourrait donc écrire

$$a + -b + c \quad \text{pour "simplifier" l'expression} \quad a + (-b) + c \equiv (a - b) + c \ ,$$

mais, vu l'usage du même symbole $-$ pour l'opération binaire, il est (fortement) recommandé de ne pas utiliser cette "simplification."

Revenons maintenant sur les entiers relatifs et plus généralement sur les nombres. Le lecteur sait probablement depuis longtemps que multiplier un nombre par zéro donne toujours zéro, quelque soit le nombre (que ce soit un entier relatif, un rationnel, un réel ou un nombre complexe). Et on sait aussi que "moins un nombre" est la même chose que ce nombre multiplié par "moins un". Ces propriétés ne sont pas spécifiques pour les entiers, mais sont une conséquence générale dans un anneau (ou plus générale encore).

Ⓟ **11.23 Lemme.** *Soit $(A,+)$ un groupe abélien avec 0_A comme élément neutre et σ comme application du symétrique et soit $\times$ une deuxième opération interne sur A.*

(i) *Si on a la condition de distributivité (A1), alors on a la propriété*

$$\forall a \in A : a \times 0_A = 0_A \times a = 0_A \ .$$

(ii) *Si on a les conditions de distributivité (A1) et d'existence d'un élément neutre 1_A pour $\times$ (A3), alors on a les propriétés*

$$\sigma(1_A) \times \sigma(1_A) = 1_A \qquad et \qquad \forall a \in A : \sigma(a) = \sigma(1_A) \times a = a \times \sigma(1_A) \ .$$

Ⓟ **11.24 Corollaire.** *Soit $(A,+,\times)$ un anneau, 0_A l'élément neutre pour l'opération $+$ et 1_A l'élément neutre pour l'opération $\times$. Si on a l'égalité $0_A = 1_A$, alors A ne contient qu'un seul élément.*

11.25 Nota Bene. Dans la définition d'un anneau $(A,+,\times)$, les deux opérations ne sont pas interchangeables. La différence se trouve dans la condition de distributivité, qui n'est pas symétrique en $+$ et $\times$. Une conséquence importante de cette différence est que l'élément neutre $0_A \in A$ pour l'opération $+$ joue un role particulier pour l'opération $\times$: $a \times 0_A = 0_A \times a = 0_A$ pour tout $a \in A$ [11.23.i], ce qui n'est pas vrai pour l'élément neutre pour $\times$ (s'il existe) vis-à-vis l'opération $+$.

11.26 Corollaire de [11.23]. *Soit $m \in \mathbf{Z}$ un entier relatif. Alors on a les égalités*

(i) $m \times 0 = 0$,

(ii) $-m = \big(-1\big) \times m$ *et*

(iii) $(-1) \times (-1) = 1$.

Ⓟ **11.27 Proposition.** *Soit $m,n \in \mathbf{Z}$ deux entiers relatifs. Alors on a l'équivalence*

$$m \leq n \qquad \Longleftrightarrow \qquad n - m \in \mathbf{N} \ .$$

Ⓟ **11.28 Proposition.** **Z** *est un anneau intègre. On a donc (aussi) la propriété*

$$\forall m,n,p \in \mathbf{Z} \quad : \quad p \times m = p \times n \quad \Longrightarrow \quad m = n \ ou \ p = 0 \ .$$

Ⓟ **11.29 Proposition.** *Soit $m,n,p \in \mathbf{Z}$ trois entiers relatifs. Alors on a les propriétés*

(i) $\quad m \leq n \quad \Longleftrightarrow \quad m + p \leq n + p$ *et*

(ii) $m, n \geq 0 \implies m \times n \geq 0$.

Après les définitions d'un groupe et d'un anneau, qui encodent les propriétés "essentielles" de l'addition et de la multiplication (dans $\mathbf{Z}$*), on continue avec l'introduction de la compatibilité entre les opérations et une relation d'ordre. Les propriétés "dérivées" seront réutilisées dans le cadre des nombres rationnels et réels.*

Définition. Soit $(A, +, \times)$ un anneau intègre, soit 0_A l'élément neutre pour $+$ et soit $\leq$ une relation d'ordre total sur A. Alors on dit que $\leq$ *est compatible avec la structure d'anneau* si on a les deux propriétés

(i) $\forall a, b, c \in A : a \leq b \iff a + c \leq b + c$,

(ii) $\forall a, b \in A : a, b \geq 0_A \implies a \times b \geq 0_A$.

11.30 Corollaire. *La relation d'ordre* $\leq$ *sur* $\mathbf{Z}$ *est compatible avec la structure d'anneau.*

Avec [11.29.i] on sait qu'on peut additionner deux inégalités larges ou strictes et obtenir une égalité large ou strict. On sait aussi qu'il est "dangereux" de multiplier deux inégalités entre nombres (entiers, rationnels ou réels) et que le résultat est incertain. Par contre, si on prend ses précautions, on peut multiplier deux inégalités et obtenir un résultat cohérent. C'est probablement moins connu que les conditions et résultats concernant la multiplication d'inégalités ne sont pas réservés aux nombres, mais s'appliquent dès qu'on a une relation d'ordre total compatible avec la structure d'anneau. Dans [11.31] on rassemble quelques uns de ces résultats (le lecteur pourrait facilement en déduire d'autres). On peut résumer ces résultats vaguement comme suit :

l'élément neutre pour la multiplication est toujours strictement positif

prendre l'opposé change le sens de l'inégalité

multiplier par un élément positif préserve le sens de l'inégalité

un carré est toujours positif.

Dans [11.32] on transcrit ces résultats (ceux dont on aura besoin plus tard) dans le cas des entiers relatifs.

11.31 Lemme. *Soit* $(A, +, \times)$ *un anneau intègre et soit* $\leq$ *une relation d'ordre total sur* A *compatible avec la structure d'anneau. Soit* $a, b, c \in A$*, soit* 0_A *l'élément neutre dans* A *pour l'opération* $+$*, soit* 1_A *l'élément neutre pour l'opération* $\times$ *et soit* $- : A \to A$ *l'application du symétrique pour* $+$*. Alors on a les propriétés suivantes.*

(i) $a < b \iff a + c < b + c$;

(ii) $1_A > 0_A$ *et* $-1_A < 0_A$;

(iii) $a \leq b \iff -a \geq -b$;

(iv) $a \geq 0_A$ *et* $b \leq c \implies a \times b \leq a \times c$;
(v) $a > 0_A$ *et* $b < c \implies a \times b < a \times c$;
(vi) $a \leq 0_A$ *et* $b \leq c \implies a \times b \geq a \times c$;
(vii) $a < 0_A$ *et* $b < c \implies a \times b > a \times c$;
(viii) $a > 0_A$ *et* $a \times b \leq a \times c \implies b \leq c$;
(ix) $a \neq 0_A \implies a \times a > 0_A$.

Nota Bene. La condition que l'anneau est intègre dans [11.31] est essentielle pour les résultats avec une inégalité stricte.

11.32 Corollaire/sélection de [11.31]. *Soit $m, n, p \in \mathbf{Z}$ trois entiers relatifs. Alors on a les propriétés*

(i) $p \geq 0$ *et* $m \leq n \implies p \times m \leq p \times n$,
(ii) $p > 0$ *et* $m < n \implies p \times m < p \times n$,
(iii) $p > 0$ *et* $p \times m \leq p \times n \implies m \leq n$,
(iv) $m < 0 \iff -m > 0$,
(v) $m \neq 0 \implies m^2 > 0$.

C'est avec [11.32.iv] et [11.27] qu'on (re)trouve l'autre façon de "définir" les entiers relatifs dont on a parlé dans l'introduction : $\mathbf{Z}$ est la réunion des entiers naturels $\mathbf{N}$ avec les nombres négatifs (sous-entendu les entiers naturels négatifs). Car prenons $m \in \mathbf{Z}$, alors parce que la relation d'ordre est total, on a $m \geq 0$ ou $m < 0$. Dans le premier cas on aura selon [11.27] $m \in \mathbf{N}$, c'est-à-dire que m est un entier naturel. Et dans le deuxième cas on aura par [11.32.iv] $-m > 0$ et donc par [11.27] $-m \in \mathbf{N}$, ce qui veut dire qu'il existe $n \in \mathbf{N}$ tel que $m = -n$: m est un entier naturel précédé d'un signe moins. Et donc un entier relatif est soit un entier naturel, soit un entier naturel précédé par le signe moins. C'est avec cette remarque qu'on peut complètement oublier la construction de $\mathbf{Z}$ comme l'ensemble des classes d'équivalences de $\mathbf{N} \times \mathbf{N}$; il suffit d'utiliser le signe moins et les entiers naturels pour pouvoir désigner tous les entiers relatifs.

Ⓟ **11.33 Proposition.** *Soit $B \subset \mathbf{Z}$ un sous-ensemble non-vide et minoré. Alors B contient un plus petit élément. En formule :*

$$\big(B \neq \emptyset \text{ et } \exists m \in \mathbf{Z}\ \forall n \in B : m \leq n \big) \implies \big(\exists m_o \in B\ \forall n \in B : m_o \leq n \big) .$$

Dans §8 on a défini/construit trois structures — les opérations internes d'addition et de multiplication et la relation d'ordre — sur les entiers naturels en se basant uniquement sur les axiomes de Peano sans avoir recours à la structure explicite de $\mathbf{N}$ tel qu'on l'avait construit dans §6. Et on a argumenté qu'on ne peut pas voir la différence, tant qu'on n'utilise que ces trois structures (ainsi que d'autres objets

qu'on peut en déduire). Autrement dit, en ce qui concerne les structures qu'on a définies sur $\mathbf{N}$*, cet ensemble est complètement caractérisé par les axiomes de Peano. La situation pour* $\mathbf{Z}$ *n'est pas totalement analogue, car on ne caractérise pas* $\mathbf{Z}$ *par des axiomes, mais presque, car on dit que* $\mathbf{Z}$ *est le plus petit anneau contenant* $\mathbf{N}$*. L'idée derrière cette description de* $\mathbf{Z}$ *est intuitivement assez simple. Si un anneau* A *contient* $\mathbf{N}$*, il doit contenir aussi les opposés des éléments de* $\mathbf{N}$*, car un anneau est un groupe (abélien) pour l'addition. Et* $\mathbf{N}$ *complété par ces opposés, c'est exactement* $\mathbf{Z}$*. Mais quelle est l'interprétation rigoureuse de cet adage ? Que veut dire exactement "contenant* $\mathbf{N}$*" et que veut dire "le plus petit" ?*

Commençons avec "contenant $\mathbf{N}$*." On dit qu'un anneau* $(A, +, \times)$ *contient* $\mathbf{N}$ *s'il existe une application injective* $f : \mathbf{N} \to A$ *qui respecte l'addition et la multiplication dans le sens qu'on a pour tout* $m, n \in \mathbf{N}$ *:*

$$f(m+n) = f(m) + f(n) \qquad et \qquad f(m \times n) = f(m) \times f(n) \ .$$

La notion du "plus petit" doit être interprété dans le sens suivant : si A *est un anneau contenant* $\mathbf{N}$*, alors* A *contient* $\mathbf{Z}$*. Plus précisément, on affirme que, si on a une application injective* $f : \mathbf{N} \to A$ *qui respecte l'addition et la multiplication, alors il existe une application injective* $g : \mathbf{Z} \to A$ *qui respecte l'addition et la multiplication telle que pour tout* $m \in \mathbf{N}$*, c'est-à-dire* $m \geq 0$*, on a* $g(m) = f(m)$ *(on dit aussi que l'application* g *prolonge* f*). L'ensemble* $\mathbf{Z}$ *qu'on vient de construire a bien cette propriété (mais on ne l'a pas montré).*

Mais que se passe-t-il quand on a un autre anneau $\mathbf{Z}'$ *avec cette même propriété ? La réponse est qu'on ne peut pas voir la différence, comme on ne pouvait pas voir la différence entre deux ensembles qui vérifient les axiomes de Peano. Plus précisément, supposons qu'on a un anneau* $\mathbf{Z}'$ *qui contient* $\mathbf{N}$ *et qui a aussi la propriété d'être le plus petit. On a donc en particulier une application injective* $f' : \mathbf{N} \to \mathbf{Z}'$ *qui respecte les opérations. Maintenant parce que* $\mathbf{Z}$ *a la propriété d'être le plus petit, il existe une application injective* $g : \mathbf{Z} \to \mathbf{Z}'$ *respectant les opérations qui prolonge* f'*. Mais parce que* $\mathbf{Z}'$ *a aussi la propriété d'être le plus petit, il existe une application injective* $g' : \mathbf{Z}' \to \mathbf{Z}$ *respectant les opérations qui prolonge l'injection canonique* $\iota : \mathbf{N} \to \mathbf{Z}$*. Les composées* $g' \circ g : \mathbf{Z} \to \mathbf{Z}$ *et* $g \circ g' : \mathbf{Z}' \to \mathbf{Z}'$ *sont donc des applications injectives qui respectent les opérations, la première prolongeant l'injection canonique et la deuxième prolongeant l'application* f*. On en déduit que ces deux composées sont l'identité, donc que* g *et* g' *sont bijectives et qu'elles respectent les opérations d'addition et de multiplication. Mais elles respectent aussi la relation d'ordre pour la simple raison que, selon [11.27], la relation d'ordre sur* $\mathbf{Z}$ *est complètement définie en termes de son sous-ensemble* $\mathbf{N}$ *(mieux : l'image de* $\mathbf{N}$ *par l'injection canonique). Et là on se trouve dans la même situation que dans le cas de deux ensembles vérifiant les axiomes de Peano : une bijection qui respecte "tous" les structures (opérations interne, relation d'ordre). Et donc, tant qu'on n'utilise que ces structures, on ne peut pas voir la différence.*

Mais il y a mieux encore ! Une fois qu'on sait qu'on ne peut pas voir la différence, rien ne nous empêche de prétendre que $\mathbf{Z}$ *est bien construit à partir de* $\mathbf{N}$ *comme on vient de le faire, car de toute façon on ne peut pas voir la différence ! À condition bien sûr qu'on ne parle que de ces trois structures (et leurs dérivées). Ceci s'applique en particulier à la construction qu'on va faire dans §13, où on généralisera l'opération externe de* $\mathbf{N}$ *sur un monoide en une action externe de* $\mathbf{Z}$ *sur un groupe.*

12. Multiples et puissances avec un entier naturel

Si a et b sont deux quantités qu'on peut additionner, alors $a+b$ est une troisième quantité. Mais dans des telles circonstances on peut aussi additionner a avec lui-même et former $a+a$, ou bien répéter l'opération n fois ($n \in \mathbf{N}^*$) et considérer l'addition répétée

$$\underbrace{a+a+\cdots+a}_{n\ fois} \quad .$$

Et même quand les entiers n'appartiennent pas à l'ensemble qui contient ce a, on a quand même l'habitude de dire que ce résultat est "n fois a" et d'écrire

$$\underbrace{a+a+\cdots+a}_{n\ fois} = n \cdot a \quad . \tag{12.1}$$

Par contre, quand on n'additionne pas mais quand on multiplie, on obtient les multiplications répétées

$$\underbrace{a \cdot a \cdot \ \cdots \ \cdot a}_{n\ fois} \quad .$$

Et dans une telle circonstance on ne parle pas de n fois a, mais plutôt de "a à la puissance n," ce qu'on écrit comme

$$\underbrace{a \cdot a \cdot \ \cdots \ \cdot a}_{n\ fois} = a^n \quad . \tag{12.2}$$

On voit que les multiples de a et les puissance de a partent du même idée : une opération répétée. Cette idée est formalisée dans [12.8] où on montre que la procédure d'une opération répétée s'applique dans des circonstances assez générales et a des propriétés "agréables." Mais avant qu'on puisse énoncer ce résultat, il faut d'abord définir le cadre.

Définition. Soit A un ensemble et soit $\blacksquare : A \times A \to A$ une opération interne. On dit que $(A, \blacksquare)$ est un *monoïde* si cette opération vérifie les deux conditions

(G1) $\forall a, b, c \in A : a \blacksquare (b \blacksquare c) = (a \blacksquare b) \blacksquare c$ (*associativité*) et

(G2) $\exists e \in A\ \forall a \in A : a \blacksquare e = e \blacksquare a = a$ (*existence d'un élément neutre*).

Si l'opération $\blacksquare$ vérifie en plus la condition

(G4) $\forall a, b \in A : a \blacksquare b = b \blacksquare a$ (*commutativité*),

alors on dit que $(A, \blacksquare)$ est un *monoïde abélien* (on dit aussi *monoïde commutatif*). Un monoïde est donc presque un groupe, sauf qu'on n'a pas la condition de l'existence d'un inverse.

12.3 Exemples. Si $(G, \blacksquare)$ est un groupe [11.13], alors c'est un monoïde ; et si le groupe est abélien, c'est un monoïde abélien. Si $(A, +, \times)$ est un anneau [11.20], alors $(A, +)$, l'ensemble A muni de l'opération interne $+$, est un monoïde abélien et si en plus A est unitaire, alors $(A, \times)$, l'ensemble A muni de l'opération interne $\times$, est un monoïde. Et si $(C, +, \times)$ est un corps [14.18], alors $(C, +)$ et $(C, \times)$ sont des monoïdes abéliens. Mais l'exemple type d'un monoïde est l'ensemble des applications d'un ensemble vers lui-même.

12.4 Definition. Soit A et B deux ensembles, alors la collection $\mathrm{App}(A,B)$ de toutes les applications de A dans B définie comme

$$\mathrm{App}(A,B) = \{\, f \in \mathcal{P}(A\times B) \mid f \text{ une application } \}$$

est un ensemble par l'axiome de séparation (Z5).

Ⓟ **12.5 Proposition.** *Si A, B et C sont trois ensembles, alors la composition d'applications*

$$(g,f) \mapsto g\circ f$$

est elle-même une application définie sur le produit $\mathrm{App}(B,C)\times\mathrm{App}(A,B)$ à valeurs dans $\mathrm{App}(A,C)$. Plus précisément, l'ensemble

$$C_{\mathrm{omp}} \subset \big(\mathrm{App}(B,C)\times\mathrm{App}(A,B)\big)\times\mathrm{App}(A,C)$$

défini comme

$$\begin{aligned} C_{\mathrm{omp}} &= \{\, ((g,f),g\circ f) \mid f\in\mathrm{App}(A,B) \text{ et } g\in\mathrm{App}(B,C)\,\} \\ &= \{\, X\in(\mathrm{App}(B,C)\times\mathrm{App}(A,B))\times\mathrm{App}(A,C) \mid \\ &\qquad \exists f\in\mathrm{App}(A,B)\ \exists g\in\mathrm{App}(B,C) : X=((g,f),g\circ f)\,\} \end{aligned}$$

est une application $C_{\mathrm{omp}} : \mathrm{App}(B,C)\times\mathrm{App}(A,B)\to\mathrm{App}(A,C)$.

Nota Bene. Dans la suite on notera cette application C_{omp} avec le même symbole $\circ$ qu'on utilise pour la composée de deux relations (un abus de notation, comme il y en a beaucoup). Dans l'énoncé de [12.5] on ne l'a pas fait, car on aurait obtenu une définition circulaire avec le symbole $\circ$.

12.6 Exemple. Soit E un ensemble et regardons l'ensemble $X=\mathrm{App}(E,E)$ de toutes les applications de E dans lui-même, muni de l'opération interne de composition d'applications $\circ : \mathrm{App}(E,E)\times\mathrm{App}(E,E)\to\mathrm{App}(E,E)$. Pour vérifier que le couple $(X,\circ)$, l'ensemble X des applications de E dans E muni de cette opération interne, est un monoïde, on constate d'abord que l'application identité $id\in X$ est l'élément neutre dans X car on a

$$\forall e\in E : (f\circ id)(e) = f\big(id(e)\big) = f(e) = id\big(f(e)\big) = (id\circ f)(e)\ ,$$

ce qui montre (avec [4.3]) qu'on a bien l'égalité $f\circ id = id\circ f = f$ pour tout $f\in X$. Et ensuite le calcul

$$\big(f\circ(g\circ h)\big)(e) = f\big((g\circ h)(e)\big) = f\big(g(h(e))\big) = (f\circ g)\big(h(e)\big) = \big((f\circ g)\circ h\big)(e)$$

montre (avec les mêmes arguments) que cette opération interne est associative.

12.7 Définition d'une opération externe. Soit A et B deux ensembles. Alors une *opération externe de A sur B* est une application $p : A\times B\to B$. Dans la quasi totalité des cas, une opération externe est notée par un symbole entre les deux arguments, comme par exemple un $\times$ ou un $\star$. Pour $a\in A$ et $b\in B$ on écrit donc $a\times b$ ou $a\star b$ au lieu de $p(a,b)$.

12.8 L'opération externe de N sur un monoïde. *Soit $(A, \blacksquare)$ un monoïde avec $e \in A$ son élément neutre, alors il existe une unique opération externe $\star : \mathbf{N} \times A \to A$ de $\mathbf{N}$ sur A qui vérifie*

$$0 \star a = e \qquad et \qquad \forall n \in \mathbf{N} : S(n) \star a = (n \star a) \blacksquare a \ , \tag{12.9}$$

où $e \in A$ désigne l'élément neutre pour l'opération $\blacksquare$ dans A. Cette opération externe a en plus les propriétés suivantes.

(i) $\forall a \in A : 1 \star a = a$,

(ii) $\forall k, \ell \in \mathbf{N}\ \forall a \in A : (k + \ell) \star a = (k \star a) \blacksquare (\ell \star a)$ *et*

(iii) $\forall k, \ell \in \mathbf{N}\ \forall a \in A : (k \times \ell) \star a = k \star (\ell \star a)$.

(iv) $\forall k \in \mathbf{N}^*\ \forall a, b \in A : a \blacksquare b = b \blacksquare a \ \Rightarrow\ k \star (a \blacksquare b) = (k \star a) \blacksquare (k \star b)$.

Écrits sous la forme de [12.8], ces résultat sont peu lisibles, surtout parce qu'on n'a pas l'habitude de les voir de cette manière. Dans la suite on continuera quand même à utiliser le symbole $\star$ pour cette opération externe dans des résultats théoriques. Par contre, dans la pratique (ici et ailleurs) il y a deux façons "standards" de présenter ces résultats, des façons qui dépendent de l'opération $\blacksquare$ sur A. Si l'opération interne est (notée comme) une addition $+$ (au quel cas l'élément neutre est souvent noté comme $\mathbf{0}$), il est d'usage de noter l'opération externe par un point " $\cdot$ ", ou même par rien du tout, ce qui donne les formules (qui définissent cette opération)

$$0 \cdot a = \mathbf{0} \qquad et \qquad (n + 1) \cdot a = (n \cdot a) + a \ .$$

Écrite comme cela on reconnaît facilement la définition de l'addition répétée décrite en (12.1). En plus, avec cette notation les propriétés prennent une forme beaucoup plus connue :

$$1 \cdot a = a \qquad , \qquad (k + \ell) \cdot a = k \cdot a + \ell \cdot a \qquad , \qquad (k \times \ell) \cdot a = k \cdot (\ell \cdot a)$$

ainsi que, dans le cas où on a $a + b = b + a$ (ce qui sera le cas si l'opération $+$ est commutatif) :

$$k \cdot (a + b) = k \cdot a + k \cdot b \ .$$

Notons en passant que dans la deuxième et quatrième égalité on a implicitement utilisé la convention que l'opération externe $\cdot$ a priorité sur l'opération interne $+$, ce qui nous a permis d'omettre des parenthèses dans les membres de droite (voir aussi [8.11]).

Par contre, si l'opération interne est (notée comme) un produit $\times$ (au quel cas l'élément neutre est souvent noté comme $\mathbf{1}$), il est d'usage de noter l'opération externe en exposant, ce qui donne les formules définissantes

$$a^0 = \mathbf{1} \qquad et \qquad a^{n+1} = a^n \times a \ .$$

Et on reconnaît la définition de la multiplication répétée décrite en (12.2). Dans ce cas les propriétés prennent la forme habituelle concernant la manipulation des exposants :

$$a^1 = a \qquad , \qquad a^{k+\ell} = a^k \times a^\ell \qquad , \qquad a^{k \times \ell} = (a^\ell)^k$$

ainsi que, dans le cas où on aura $a \times b = b \times a$ (où il ne faut pas confondre l'opération $\times$ dans $\mathbf{N}$ avec l'opération $\times$ dans A qu'on note ici par le même symbole) :

$$(a \times b)^k = a^k \times b^k \ .$$

Mais ce qu'il ne faut surtout pas oublier, c'est que c'est [12.8] qui justifie notre utilisation de cette opération externe sous ses deux formes habituelles (la manipulation des multiples ou des exposants), pas dans l'autre sens !

12.10 Corollaire. *Soit $(A, \blacksquare)$ un monoïde et soit $\star : \mathbf{N} \times A \to A$ l'opération externe de $\mathbf{N}$ sur A associée. Alors on a les propriétés (de commutativité), valable pour tout $k, \ell \in \mathbf{N}$ et tout $a \in A$:*

$$(k \star a) \blacksquare (\ell \star a) = (\ell \star a) \blacksquare (k \star a) \qquad \text{et} \qquad k \star (\ell \star a) = \ell \star (k \star a) \ .$$

12.11 La multiplication dans N comme opération externe. L'addition $+ : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ est une opération interne qui fait de $\mathbf{N}$ un monoïde. Il existe donc une opération externe $\star$ de $\mathbf{N}$ sur $\mathbf{N}$ associée donnée par les formules de récurrence

$$0 \star \ell = 0 \qquad \text{et} \qquad (k+1) \star \ell = (k \star \ell) + \ell \ .$$

On reconnaît directement la définition de la multiplication dans $\mathbf{N}$. Dans ce cas, les propriétés [12.8.ii] et [12.8.iv] sont les propriétés de la distributivité de la multiplication sur l'addition comme données dans [8.10.iii/iv] et la propriété [12.8.iii] est l'associativité de la multiplication.

12.12 Puissances d'un entier/l'exponentielle. La multiplication $\times : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ est une opération interne qui fait de $\mathbf{N}$ un monoïde. Il existe donc une opération externe $\star$ de $\mathbf{N}$ sur $\mathbf{N}$ associée donnée par les formules (de récurrence)

$$0 \star \ell = 1 \qquad \text{et} \qquad (k+1) \star \ell = (k \star \ell) \times \ell \ .$$

Comme il s'agit d'une multiplication, il est d'usage de noter cette opération externe en exposant :

$$\ell^k \overset{\text{déf}}{=} k \star \ell$$

et de dire que ℓ^k est la puissance k-ième de l'entier ℓ.

Nota Bene. Il faut bien noter que la définition de ℓ^k a comme cas particulier l'égalité $0^0 = 1$; c'est l'initialisation de la définition par récurrence de l'opération externe. Cette formule, qui paraît bizarre à première vue, est bien compatible avec les propriétés de l'opération externe ! On verra dans [25.10.iii] (ce qui repose essentiellement sur [4.11]) que cette formule est aussi cohérente avec d'autres résultats.

Itérées d'une application. Soit E un ensemble et soit $X = \mathrm{App}(E, E)$ l'ensemble de toutes les application de E dans lui-même. Dans [12.6] on a vu que X muni de l'opération interne de composition [12.3] est un monoïde. Il existe donc une opération externe $\star : \mathbf{N} \times X \to X$ définie par les formules

$$0 \star f = id \qquad \text{et} \qquad (k+1) \star f = (k \star f) \circ f \ .$$

Comme dans le cas de puissance d'un entier naturel, on note cette opération en exposant comme

$$f^0 = id \qquad \text{et} \qquad f^{k+1} = (f^k) \circ f \ ,$$

où on reconnaît les itérées d'une fonction $f : E \to E$:

$$f^0 = id \quad , \quad f^1 = f \quad , \quad f^2 = f \circ f \quad , \quad f^3 = f \circ f \circ f \quad , \ldots$$

13. Multiples et puissances avec un entier relatif

Dans §12 on a défini l'action externe de $\mathbf{N}$ *sur un monoïde pour rendre compte d'une opération répétée. Mais quand on pense au cas multiplicatif, où on écrit l'opération répétée avec un entier en exposant, on peut se rappeler que dans ce cas on écrit l'opération du symétrique* aussi *avec le symbole* -1 *en exposant. Quand on ne connaît que les entiers naturels, ceci ne pose pas de problèmes, car le symbole* -1 *n'est pas un entier naturel. Mais quand on connaît les entiers relatifs, on voit apparaître un tel nombre en exposant dans deux sens différents selon le signe, et seulement le nombre* -1 *parmi les négatifs. Le but de ce chapitre est de montrer que ce n'est pas seulement une cohabitation de ces deux notations, mais qu'il y a une cohérence totale : pour un groupe* G*, on peut étendre l'opération externe de* $\mathbf{N}$ *sur* G *(pour rendre compte de l'opération répétée) en une action externe de* $\mathbf{Z}$ *sur* G *qui inclut l'application du symétrique comme l'action (externe) de l'élément* $-1 \in \mathbf{Z}$ *sur* G*. Au final, c'est ce résultat, et seulement ce résultat, qui* justifie *le choix de noter l'élément symétrique avec un* -1 *en exposant (ou dans le cas "additif" de noter l'action de* $\mathbf{N}$ *comme une "multiplication" par* $n \in \mathbf{N}$ *et l'opposé par un signe* $-$ *devant l'élément) !*

Ⓟ **13.1 Lemme.** *Soit* $(G, \blacksquare)$ *un groupe et soit* $\star : \mathbf{N} \times G \to G$ *l'action externe de* $\mathbf{N}$ *sur* G *vu comme monoïde. Si* $\sigma : G \to G$ *est l'application du symétrique [11.14], alors on a la propriété*

$$\forall k \in \mathbf{N}\ \forall g \in G \quad : \quad k \star \sigma(g) = \sigma(k \star g)\ ,$$

et (donc) aussi la propriété

$$\forall k, \ell \in \mathbf{N}\ \forall g \in G \quad : \quad (k \star g) \blacksquare \big(\ell \star \sigma(g)\big) = \big(\ell \star \sigma(g)\big) \blacksquare (k \star g)\ .$$

Si $(G, \blacksquare)$ *est un groupe, alors la notation pour l'application du symétrique* σ *dépend de la façon dont on note l'opération interne* $\blacksquare$*, comme c'est le cas pour la notation de l'opération externe de* $\mathbf{N}$ *sur un monoïde. Si l'opération interne est (notée comme) une addition, alors il est d'usage de noter l'application inverse par un moins :* $\sigma(g) = -g$*. Et si l'opération interne est (notée comme) une multiplication, alors l'application inverse est notée par* -1 *en exposant :* $\sigma(g) = g^{-1}$*. Dans ce contexte, le résultat [13.1] prend les formes*

$$k \cdot (-g) = -(k \cdot g) \text{ cas additif} \qquad ou \qquad (g^{-1})^k = (g^k)^{-1} \text{ cas multiplicatif,}$$

ainsi que

$$(k \cdot g) + \big(\ell \cdot (-g)\big) = \big(\ell \cdot (-g)\big) + (k \cdot g) \qquad ou \qquad g^k \cdot (g^{-1})^\ell = (g^{-1})^\ell \cdot g^k\ .$$

Ces formules suggèrent fortement qu'on peut étendre l'action externe de $\mathbf{N}$ *en une action externe de* $\mathbf{Z}$ *en posant, pour* $k \in \mathbf{N}$ *et donc* $-k \in \mathbf{Z}$*,* $-k \leq 0$ *:*

$$(-k) \star g \overset{déf}{=} \sigma(k \star g) \equiv k \star \sigma(g)\ . \tag{13.2}$$

Dons [13.8] on montrera qu'on peut effectivement faire cela. Mais il faut bien réaliser que l'argument va dans l'autre sens : le fait qu'on puisse étendre l'action externe de

N *en une action externe de* **Z** *vérifiant (13.2) montre que la notation choisie pour l'application inverse est cohérente avec la notation choisie pour l'opération externe.*

Pour pouvoir correctement définir cette opération externe de **Z** *sur un groupe, on a besoin d'un résultat préliminaire concernant l'interprétation d'une application définie sur un produit. C'est essentiellement un changement de point de vue et la plupart des mathématiciens professionnels dira que c'est la même chose. L'idée est la suivante : soit* $f : A \times B \to C$ *une application définie sur le produit cartésien* $A \times B$ *et soit* $a \in A$ *un élément. Alors à l'aide de l'application* f *on peut associer à chaque* $b \in B$ *l'élément* $c = f(a, b) \in C$*. Autrement dit, on a fabriqué une application de* B *dans* C *qui dépend de l'élément* $a \in A$ *choisi au départ. Ou bien, on a créé une application de* A *dans l'ensemble des applications de* B *dans* C*.*

Une analogie dans la "vraie" vie est donnée par les prévisions météo. Sur le site de météo-france on peut consulter les prévisions météo, mais il faut remplir deux cases : "où" et "quand." Autrement dit, on doit dire que (par exemple) on s'intéresse à la prévision météo à Lille pour après-demain, ou qu'on s'intéresse à la prévisions à Marseille pour cette après-midi. Ceci est notre application de deux variables. Mais le site propose un service supplémentaire : en donnant un lieu (par exemple Lille), on peut télécharger toutes les prévisions pour ce lieu, qu'on peut consulter après hors connexion. Sur son ordinateur on aura donc un logiciel qui nous donne, pour chaque moment (dans le futur), la prévision météo pour Lille. Ce logiciel est notre application de B *dans* C *(à "quand" on associe la prévision) qui dépend du choix de l'élément* $a \in A$ *(l'endroit "Lille" choisi). Si on téléchargeait ces logiciels pour tous les endroits possibles, on aurait toutes les information concernant les prévisions météo : on peut choisir un lieu et un moment et on trouvera la prévision météo.*

Le résultat mathématique précis dit que donner une application définie sur un produit $A \times B$ *à valeurs dans* C *est "la même chose" que donner une application définie sur* A *à valeurs dans la collection d'applications de* B *dans* C*. Reste à savoir dans quel sens c'est "la même chose." Intuitivement cela veut dire qu'il existe une procédure qui transforme un point de vue dans l'autre et vice-versa. Et quand on dit "procédure," on pense "application." Cette application/procédure est donc définie sur la collection de toutes les applications définies sur le produit (on applique la procédure à une telle application) et à valeurs dans la collection de toutes les application définies sur* A *et à valeurs dans les applications de* B *dans* C *(le résultat de la procédure doit être une telle application). Et le fait qu'on peut aller dans les deux sens dit que cette application doit être une bijection.*

Ⓟ **13.3 Lemme.** *Soit* A*,* B *et* P *trois ensembles. Alors les applications*

$$\Phi : \mathrm{App}\big(P, \mathrm{App}(A, B)\big) \to \mathrm{App}(P \times A, B) \qquad (13.4)$$

$$\text{et} \qquad \Psi : \mathrm{App}(P \times A, B) \to \mathrm{App}\big(P, \mathrm{App}(A, B)\big)$$

définies par

$$\big(\Phi(F)\big)\big((p, a)\big) = \big(F(p)\big)(a) \qquad \text{et} \qquad \Big(\big(\Psi(G)\big)(p)\Big)(a) = G\big((p, a)\big)$$

sont des bijections vérifiant $\Psi^{-1} = \Phi$ *et* $\Phi^{-1} = \Psi$*.*

Remarque. Si on veut décrire les applications Φ et Ψ en termes d'ensembles, on obtiendra des formules très longues. Faisons le pour l'application Φ, en commençant

par une analyse de la définition de l'application $\Phi(F) : P \times A \to B$ pour une application $F : P \to \mathrm{App}(A, B)$. Officiellement il faut l'écrire comme

$$\Phi(F) = \{\, \big((p,a),b\big) \in (P \times A) \times B \mid b = (F(p))(a) \,\} \tag{13.5}$$

$$= \{\, \big((p,a),b\big) \in (P \times A) \times B \mid (a,b) \in F(p) \,\} \ , \tag{13.6}$$

ce qui utilise déjà la simplification de notation [2.4], car l'écriture complète est donnée par

$$\{\, x \in (P \times A) \times B \mid \exists a \in A, b \in B, p \in P : x = \big((p,a),b\big) \text{ et } (a,b) \in F(p) \,\} \ .$$

Mais $F(p)$ est lui-même une application déterminée par la formule

$$f = F(p) \qquad \Longleftrightarrow \qquad (p,f) \in F \ .$$

On devrait donc écrire (avec les mêmes simplifications)

$$\Phi(F) = \{\, \big((p,a),b\big) \in (P \times A) \times B \mid \exists f \in \mathrm{App}(A,B) : (p,f) \in F \text{ et } (a,b) \in f \,\} \ . \tag{13.7}$$

Une fois qu'on a décortiqué la définition de $\Phi(F)$, on peut attaquer la définition de l'application Φ elle-même :

$$\Phi = \{\, (F,G) \in \mathrm{App}(P, \mathrm{App}(A,B)) \times \mathrm{App}(P \times A, B) \mid G = \text{ expression (13.7)} \,\} \ ,$$

où on a de nouveau utilisé la simplification d'écriture [2.4]. L'écriture complète officielle devient donc

$$\Phi = \Big\{ X \in \mathrm{App}(P, \mathrm{App}(A,B)) \times \mathrm{App}(P \times A, B) \ \Big|\ \exists F \in \mathrm{App}(P, \mathrm{App}(A,B)) \quad \exists G \in \mathrm{App}(P \times A, B) : X = (F,G) \text{ et } G = \big\{\, x \in (P \times A) \times B \mid \exists p \in P\ \exists a \in A\ \exists b \in B\ \exists f \in \mathrm{App}(A,B) : x = \big((p,a),b\big) \text{ et } (p,f) \in F \text{ et } (a,b) \in f \,\big\} \Big\} \ .$$

En voyant cette formule, le lecteur comprendra pourquoi on a introduit les différentes simplifications d'écriture et les raccourcies de notations pour décrire de telles applications : la description de l'application Φ donnée dans l'énoncé de [13.3] est bien plus compréhensible que la formule longue officielle.

Ⓟ **13.8 L'opération externe de $\mathbf{Z}$ sur un groupe.** *Soit $(G, \blacksquare)$ un groupe avec élément neutre $e \in G$ et l'opération du symétrique $\sigma : G \to G$. Alors il existe une unique opération externe $\star_{\mathbf{Z}} : \mathbf{Z} \times G \to G$ de $\mathbf{Z}$ sur G vérifiant*

$$0 \star_{\mathbf{Z}} g = e \qquad \textit{et} \qquad \forall n \in \mathbf{Z} : (n+1) \star_{\mathbf{Z}} g = (n \star_{\mathbf{Z}} g) \blacksquare g \ . \tag{13.9}$$

Cette opération étend l'opération externe [12.8] $\star : \mathbf{N} \times G \to G$ de $\mathbf{N}$ sur G (vu comme monoïde) dans le sens que, si $\iota : \mathbf{N} \to \mathbf{Z}$ est l'injection canonique, alors on a les égalités

$$\forall g \in G\ \forall k \in \mathbf{N} : \iota(k) \star_{\mathbf{Z}} g = k \star g \qquad \textit{et} \qquad \big(-\iota(k)\big) \star_{\mathbf{Z}} g = k \star \sigma(g) \ . \tag{13.10}$$

L'opération externe $\star_{\mathbf{Z}}$ a en plus les propriétés suivantes.

(i) $\forall g \in G : 1 \star_{\mathbf{Z}} g = g$,

(ii) $\forall m, n \in \mathbf{Z}\ \forall g \in G : (m+n) \star_{\mathbf{Z}} g = (m \star_{\mathbf{Z}} g) \blacksquare (n \star_{\mathbf{Z}} g)$,

(iii) $\forall m \in \mathbf{Z}\ \forall g \in G : (-m) \star_{\mathbf{Z}} g = \sigma(m \star_{\mathbf{Z}} g) = m \star_{\mathbf{Z}} \sigma(g)$ *et*

(iv) $\forall m,n\in\mathbf{Z}\ \forall g\in G : (m\times n)\star_{\mathbf{Z}} g = m\star_{\mathbf{Z}}(n\star_{\mathbf{Z}} g)$.

(v) $\forall m\in\mathbf{Z}\ \forall g,h\in G : g\cdot h = h\cdot g \ \Rightarrow\ m\star_{\mathbf{Z}}(g\cdot h) = (m\star_{\mathbf{Z}} g)\cdot(m\star_{\mathbf{Z}} h)$.

Remarque sur la notation. On a rajouté la lettre $\mathbf{Z}$ en indice sur le symbole de l'opération externe de $\mathbf{Z}$ sur G pour bien la distinguer de l'opération externe de $\mathbf{N}$ sur G. Dans le même esprit on (ré)écrit l'injection canonique $\iota : \mathbf{N}\to\mathbf{Z}$ pour bien distinguer les entiers naturels des entiers relatifs. Et rappelons nous qu'un entier relatif est une classe d'équivalence de couples d'entiers naturels [11.1]. Par contre, on n'a pas été cohérent avec la notation, car on a noté les entiers naturels 0 et 1 tels quels, au lieu de les noter comme $\iota(0)$ et $\iota(1)$ qu'on aurait dû faire.

On vient de montrer que, si l'opération externe existe, *alors elle est donnée par les formules (13.10). Il est donc tentant de montrer l'existence en définissant $\star_{\mathbf{Z}}$ par ces formules. Bien que cela donne (forcément) la bonne opération, il est difficile de montrer les propriétés de l'opération $\star_{\mathbf{Z}}$ avec cette définition, car il faut à chaque fois distinguer les entiers positifs des entiers négatifs (et quand on a une somme, il faut aussi distinguer le signe de la somme). La construction qu'on va utiliser fait intervenir (à part l'opération $\star$ de $\mathbf{N}$ sur G) la construction de $\mathbf{Z}$ à partir de $\mathbf{N}$ comme classes d'équivalence de couples d'entiers naturels. Avant d'entamer la construction formelle, commençons avec les idées soujacentes.*

Rappelons d'abord qu'un entier relatif $n\in\mathbf{Z}$ s'écrit comme $n=[[k,\ell]]_{\mathbf{Z}}$ avec $k,\ell\in\mathbf{N}$ et qu'on a l'égalité

$$[[k,\ell]]_{\mathbf{Z}} = \iota(k)-\iota(\ell) = \iota(k)+(-\iota(\ell))\ .$$

Si la propriété [13.8.ii] est vraie, alors on devrait avoir

$$\begin{aligned}[[k,\ell]]_{\mathbf{Z}}\star_{\mathbf{Z}} g \quad &= \quad (\iota(k)+(-\iota(\ell)))\star_{\mathbf{Z}} g = (\iota(k)\star_{\mathbf{Z}} g)\cdot((-\iota(\ell))\star_{\mathbf{Z}} g)\\ &\overset{(13.10)}{=} (k\star g)\cdot\big(\ell\star\sigma(g)\big)\ .\end{aligned}$$

Pour montrer que cette formule définit bien l'opération externe, il faut, grosso modo, montrer que le résultat ne dépend pas du représentant choisi. Le (petit) problème avec cette idée est que [9.9] est le seul résultat de ce type dont on dispose et qu'il ne s'applique pas (directement). Dans [13.11] on énoncera un résultat adapté à nos besoin sous forme d'exercice. Mais ce n'est pas la voie qu'on va suivre. On appliquera notre changement de point de vue [13.3] qui nous permettra d'appliquer [9.9] directement. L'avantage est qu'on n'invoque pas un résultat dont on n'a besoin qu'une seule fois, mais qu'on utilise le résultat de base [9.9] en combinaison avec le résultat [13.3] qui va servir à d'autres endroits.

13.11 Exercice. En s'inspirant de la preuve de [9.9], démontrer directement l'énoncé suivant, sans utiliser le passage par [13.3].

Soit A, E et X trois ensembles, soit $\sim$ une relation d'équivalence sur A, soit $C : A\to A/\!\sim$ la projection canonique et soit $f : A\times E\to X$ une application quelconque. Alors il existe une application $F : (A/\!\sim)\times E\to X$ vérifiant

$$\forall a\in A\ \forall e\in E : f\big((a,e)\big) = F\big((C(a),e)\big)\equiv F\big((C_a,e)\big)$$

si et seulement si f est compatible avec $\sim$ dans les sens qu'elle vérifie la condition

$$\forall e \in E\ \forall a, b \in A : a \sim b \Rightarrow f\big((a,e)\big) = f\big((b,e)\big)\ .$$

Si cette condition est vérifiée, F est unique.

13.12 La multiplication dans $\mathbf{Z}$ comme opération externe. L'addition $+ : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ est une opération interne qui fait de $\mathbf{Z}$ un groupe abélien. Il existe donc une opération externe $\star$ de $\mathbf{Z}$ sur $\mathbf{Z}$ associée vérifiant les formules données dans [13.8]. Étant donné que ici $\mathbf{Z}$ opère sur lui même, cette opération externe peut aussi être vu comme une opération interne $\star : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$. Mais par [11.19] et [11.26.i] on sait que la multiplication dans $\mathbf{Z}$ vérifie les conditions (13.9). Il s'ensuit, par l'unicité de l'opération externe, qu'elle doit être la multiplication dans $\mathbf{Z}$.

Revenons sur la discussion sur les différentes façons de noter l'application du symétrique σ dans un groupe G avec opération interne $\blacksquare$. Selon [13.8] on a une opération externe $\star$ de $\mathbf{Z}$ sur G. Et si on combine les propriétés [13.8.i] et [13.8.iii] on obtient la propriété

$$\sigma(g) = (-1) \star g\ .$$

C'est cette formule qui nous garantit la cohérence de nos choix concernant l'écriture de l'opération σ dans les différentes circonstances.

L'habitude veut que, si l'opération interne $\blacksquare$ est notée comme une addition $+$, alors l'opération externe est notée comme $\cdot$:

$$\textit{si} \qquad g \blacksquare h \ \textit{s'écrit}\ g + h \qquad \textit{alors} \qquad n \star g \ \textit{s'écrit}\ n \cdot g$$

et la formule pour l'opposé s'écrit

$$\sigma(g) = (-1) \cdot g\ ,$$

justifiant l'écriture $-g$ pour l'opposé de g.

Et si l'opération interne $\blacksquare$ est notée comme un produit $\cdot$, l'habitude veut qu'on note l'opération externe en exposant :

$$\textit{si} \qquad g \blacksquare h \ \textit{s'écrit}\ g \cdot h \qquad \textit{alors} \qquad n \star g \ \textit{s'écrit}\ g^n$$

et dans ce cas, la formule pour l'application du symétrique s'écrit

$$\sigma(g) = g^{-1}\ ,$$

ce qui est exactement l'écriture habituelle pour l'inverse.

Ce qu'il faut bien réaliser c'est que officiellement il faut d'abord *montrer [13.8] (ou [12.8] et leurs conséquences [13.12] ou [12.11]),* avant *qu'on est autorisé de mélanger les notations qu'on utilise d'habitude pour l'opération interne, l'opération du symétrique et l'opération externe.*

Terminons ce chapitre avec un abus de notation qu'il faut abolir mais qui perdure déjà depuis plusieurs siècles. Commençons avec la notation f^{-1} où $f : X \to Y$ désigne une application d'un ensemble X dans un ensemble Y. Cette notation peut s'interpréter de trois *façons différentes, deux courantes et une (fort heureusement)*

moins courante. D'abord comme l'application réciproque, ce qui présuppose que l'application $f : X \to Y$ soit bijective, sinon l'application réciproque n'existe pas. Ensuite comme l'image réciproque, ce qui existe toujours, mais ne s'applique qu'à des sous-ensembles de Y, pas à des éléments de Y. Ces deux notations sont "compatibles" dans le sens que si l'application réciproque existe (si f est bijective), alors l'interprétation comme image réciproque appliquée à un sous-ensemble de Y coïncide avec l'interprétation de l'application réciproque appliquée à ce sous-ensemble. Mais on trouve une troisième interprétation comme "1 sur f", ce qui présuppose qu'on a $Y = \mathbf{R}$ (ou un autre corps) et que f ne prend jamais la valeur 0, au quel cas ceci désigne la fonction $1/f : X \to \mathbf{R}$, définie comme

$$(f^{-1})(x) \equiv \Big(\frac{1}{f}\Big)(x) = \frac{1}{f(x)} \equiv \big(f(x)\big)^{-1} \ .$$

Déjà la notation $1/f$ est un peu malheureuse bien que sans ambiguïté, mais la notation f^{-1} pour cette fonction est à abolir, car elle confond l'opération du symétrique dans l'ensemble des applications bijectives (à savoir la réciproque) avec l'application du symétrique dans $\mathbf{R}^*$ pour la multiplication (à savoir l'inverse). Imaginons que $f : \mathbf{R}_+ \to \mathbf{R}_+$ désigne la fonction "carré" : $f(x) = x^2$. Comment faut-il interpréter la fonction f^{-1} ? Comme l'application réciproque, c'est-à-dire comme $f^{-1}(x) = \sqrt{x}$, ou comme l'application $1/f$, c'est-à-dire $f^{-1}(x) = x^{-2}$? C'est pour éviter cette ambiguïté qu'il faut abolir l'interprétation de f^{-1} comme la fonction $1/f$ et donc :

$$f^{-1}(x) \qquad \textit{désigne l'application réciproque appliquée à } x$$

$$f(x)^{-1} \qquad \textit{désigne la valeur } \frac{1}{f(x)} \ .$$

Comme dit, fort heureusement on ne voit pas très souvent cette interprétation, mais on la trouve. Une origine possible de cette mauvaise notation pourrait être comme suit. Depuis longtemps on écrit la fonction carré comme $f(x) = x^2$ et très souvent on parle de la fonction x^2 au lieu de la donner un nom explicite comme f. Dans cette même veine on a pris l'habitude d'écrire la fonction qui à $x \in \mathbf{R}$ associe la valeur $(\sin x)^2$ comme $\sin^2$. Ainsi on écrit l'égalité de Pythagore comme

$$\sin^2(x) + \cos^2(x) = 1 \ .$$

De là à écrire la fonction $1/\sin$ comme $\sin^{-1}$ n'est qu'un tout petit pas. Mais, comme pour la notation f^{-1}, la notation f^2 est ambigue, car faut-il l'interpréter comme f appliqué deux fois, ce qui s'applique quand $f : X \to X$ est une application d'un ensemble vers lui-même, ou faut-il l'interpréter comme le carré de la valeur (comme dans Pythogore), ce qui s'applique quand f prend ses valeurs dans $\mathbf{R}$ (ou un autre ensemble qui permet de prendre un carré). Pour éviter cette ambiguïté, il faut donc abolir cet abus de notation, cette interprétation de l'écriture f^2 comme le carré et se restreindre à l'unique interprétation comme application répétée. Cette exhortation n'est pas récente, car le célèbre mathématicien Carl Friedrich Gauss déjà se plaignait de cette interprétation. Le 23 septembre 1839 il écrivit à son élève et ami Heinrich Christian Schumacher (voir [**GS65**, lettre 657(290), pp291–293]*) :*

> *La même chose s'applique à l'écriture $\sin^2 \phi$. Je trouve que cette écriture est contraire à une quelconque analogie, car par analogie un 2 en exposant est surtout une abréviation pour la double écriture du symbole juste avant et donc $\sin^2 \phi = \sin(\sin \phi)$. L'écriture $\sin^2 \phi$ est effectivement utilisée par des personnes de renom,*

comme Laplace et Poisson, et est en soi écrite avec de bonnes intentions, car on veut éviter la mauvaise interprétation de lire $\sin(\phi^2)$ *quand on veut dire* $(\sin\phi)^2$*, ce qui est possible quand on écrit simplement* $\sin\phi^2$*. Mais dans* 1000 *cas cette interprétation ne se produit pas une seule fois et donc un malentendu ne peut pas se produire, et quand ceci en potentiellement possible, il serait mieux de l'éviter en utilisant des parenthèses (comme ci-dessus), que par une écriture qui est contraire à toute analogie. Je me rappelle qu'à un moment Herschel s'est prononcé explicitement contre l'écriture* $\sin^2\phi$*. Bessel, qui à ma connaissance tient à ce que l'on écrive correctement les formules, ne l'écrit jamais ainsi.*

14. Construction de Q

Là où les entiers relatifs sont "inventés" pour pouvoir résoudre x d'une équation de la forme $x + a = b$, on "invente" les nombres rationnels pour pouvoir résoudre x d'une équation de la forme $a \times x = b$. Jusqu'à un certain point on fera exactement la même chose que dans la construction de **Z**, *simplement en remplaçant l'opération d'addition par l'opération de multiplication. Mais bien évidemment l'analogie ne tient pas longtemps, car les opérations d'addition et de multiplication n'ont pas le même statut ; on l'a déjà remarqué pendant la construction de* **Z** *avec la différence de comportement entre le* 0 *(élément neutre pour l'addition) par rapport à la multiplication d'un côté et le comportement de* 1 *(élément neutre pour la multiplication) par rapport à l'addition de l'autre (voir [11.25]).*

Par contre, même si les formules ne se ressemblent pas partout, la démarche est identique à la démarche pour la construction de **Z** *à partir de* **N**. *On définit* **Q** *comme un ensemble quotient de* $\mathbf{Z} \times \mathbf{Z}^*$ *par rapport à une relation d'équivalence, on définit les deux opérations d'addition et multiplication sur* **Q** *ainsi qu'une relation d'ordre total. Parallèlement on définit l'identification de* **Z** *avec un sous-ensemble de* **Q** *via une application injective (canonique) et on montre que cette identification est compatible avec les deux opérations et la relation d'ordre. On montre également les propriétés usuelles de ces opérations et les relations qu'elles ont avec la relation d'ordre. À la fin on rencontre quelques différences : dans* **Z** *tout ensemble minoré admet un plus petit élément, ce qui n'est plus vrai dans* **Q**. *Par contre, dans* **Q** *il y a un élément entre deux éléments (différents) quelconque, ce qui n'est pas vrai dans* **Z**.

Définition de l'ensemble Q. Sur l'ensemble $\mathbf{Z} \times \mathbf{Z}^*$ (avec $\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$) on définit une relation d'équivalence $\sim$ par

$$(a, b) \sim (p, q) \qquad \overset{\text{déf}}{\Longleftrightarrow} \qquad a \times q = b \times p \ . \tag{14.1}$$

Dans [14.2] on montrera que c'est bien une relation d'équivalence. L'ensemble quotient $(\mathbf{Z} \times \mathbf{Z}^*)/\!\sim$ sera noté par **Q** :

$$\mathbf{Q} \overset{\text{déf}}{=} (\mathbf{Z} \times \mathbf{Z}^*)/\!\sim \ .$$

Un élément de l'ensemble **Q** s'appelle un *nombre rationnel* et l'ensemble **Q** lui-même s'appelle bien évidemment *l'ensemble des nombres rationnels*. Pour cette relation d'équivalence on note la classe d'équivalence d'un couple (a, b) par $\frac{a}{b}$, comme on le faisait pour les nombres rationnels positifs :

$$\frac{a}{b} \overset{\text{déf}}{=} \{(p, q) \in \mathbf{Z} \times \mathbf{Z}^* \mid (p, q) \sim (a, b)\} \ .$$

Ⓟ **14.2 Lemme.** *La relation $\sim$ sur $\mathbf{Z} \times \mathbf{Z}^*$ définie par (14.1) est une relation d'équivalence.*

Nota Bene. On peut remarquer que la relation $\sim$ sur $\mathbf{Z} \times \mathbf{Z}^*$ est parfaitement bien définie sur l'ensemble plus grand $\mathbf{Z} \times \mathbf{Z}$. Si on interprète un nombre rationnel comme un quotient, on sait bien qu'on n'a pas le droit de diviser par 0, mais pour la relation

$\sim$ ça ne pose pas de problèmes. Par contre, exclure le 0 de la deuxième coordonnée est nécessaire pour montrer que $\sim$ est une relation d'équivalence. L'adage qu'on ne peut pas diviser par 0 se traduit ici donc sous la forme qu'il faut exclure le 0 (de la deuxième composante) pour obtenir une relation d'équivalence.

14.3 Lemme/Définition. *L'application* $\iota : \mathbf{Z} \to \mathbf{Q}$ *définie par*

$$\iota(n) = \frac{n}{1} \tag{14.4}$$

est injective. On l'appelle l'injection canonique de $\mathbf{Z}$ *dans* $\mathbf{Q}$.

Ⓟ **14.5 L'addition dans Q.** *L'application* $f : (\mathbf{Z} \times \mathbf{Z}^*) \times (\mathbf{Z} \times \mathbf{Z}^*) \to \mathbf{Q}$ *définie par*

$$f\big((a,b),(p,q)\big) = \frac{a \times q + b \times p}{b \times q}$$

est compatible avec la relation d'équivalence définie en (14.1). Par [9.12] il existe donc une unique application $+_{\mathbf{Q}} : \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$, *appelée* l'addition dans $\mathbf{Q}$, *vérifiant*

$$\frac{a}{b} +_{\mathbf{Q}} \frac{p}{q} \quad = \quad \frac{a \times q + b \times p}{b \times q} \quad \equiv \quad f\big((a,b),(p,q)\big) \ .$$

On a (provisoirement) ajouté la lettre $\mathbf{Q}$ *en indice pour distinguer cette opération de l'opération d'addition déjà définie sur* $\mathbf{Z}$.

14.6 Compatibilité avec l'addition dans Z. *L'addition dans* $\mathbf{Q}$ *qu'on vient de définir est compatible avec l'addition déjà définie dans* $\mathbf{Z}$ *dans le sens qu'on a*

$$\forall m, n \in \mathbf{Z} \quad : \quad \iota(m+n) = \iota(m) +_{\mathbf{Q}} \iota(n) \ ,$$

où $\iota : \mathbf{Z} \to \mathbf{Q}$ *est l'injection canonique (14.4).*

14.7 La multiplication dans Q. *L'application* $f : (\mathbf{Z} \times \mathbf{Z}^*) \times (\mathbf{Z} \times \mathbf{Z}^*) \to \mathbf{Q}$ *définie par*

$$f\big((a,b),(p,q)\big) = \frac{a \times p}{b \times q}$$

est compatible avec la relation d'équivalence définie en (14.1). Par [9.12] il existe donc une unique application $\times_{\mathbf{Q}} : \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$, *appelée* la multiplication dans $\mathbf{Q}$, *vérifiant*

$$\frac{a}{b} \times_{\mathbf{Q}} \frac{p}{q} \quad = \quad \frac{a \times p}{b \times q} \quad \equiv \quad f\big((a,b),(p,q)\big) \ . \tag{14.8}$$

Comme pour l'addition on a ajouté (provisoirement) la lettre $\mathbf{Q}$ *en indice pour distinguer cette opération de l'opération de multiplication déjà définie sur* $\mathbf{Z}$.

14.9 Compatibilité avec la multiplication dans Z. *La multiplication dans* $\mathbf{Q}$ *qu'on vient de définir est compatible avec la multiplication déjà définie dans* $\mathbf{Z}$ *dans le sens qu'on a*

$$\forall m, n \in \mathbf{Z} \quad : \quad \iota(m \times n) = \iota(m) \times_{\mathbf{Q}} \iota(n) \ ,$$

où $\iota : \mathbf{Z} \to \mathbf{Q}$ *est l'injection canonique (14.4).*

Ⓟ **14.10 La relation d'ordre sur $\mathbf{Q}$.** *La relation $\preccurlyeq \subset (\mathbf{Z}\times\mathbf{Z}^*)\times(\mathbf{Z}\times\mathbf{Z}^*)$ définie par*

$$(a,b)\preccurlyeq(p,q) \qquad\Longleftrightarrow\qquad a\times b\times q\times q\leq p\times q\times b\times b$$

est compatible avec la relation d'équivalence (14.1). Par [9.15] il existe donc une unique relation $\leq_{\mathbf{Q}}$ sur $\mathbf{Q}$ vérifiant

$$\frac{a}{b}\leq_{\mathbf{Q}}\frac{p}{q} \qquad\Longleftrightarrow\qquad a\times b\times q\times q\leq p\times q\times b\times b\ . \tag{14.11}$$

Cette relation $\leq_{\mathbf{Q}}$ sur $\mathbf{Q}$ est une relation d'ordre total ; comme pour l'addition et la multiplication on a ajouté (provisoirement) la lettre $\mathbf{Q}$ en indice pour distinguer cette relation d'ordre de la relation d'ordre déjà définie sur $\mathbf{Z}$.

Remarque pour les curieux. Bien qu'il est tentant de vouloir simplifier la définition (14.11) en divisant par $b\times q$, une petite réflexion montre que ce n'est pas possible, car le résultat dépendra du signe de $b\times q$. Par contre, si on avait défini $\mathbf{Q}$ comme des classes d'équivalences dans $\mathbf{Z}\times\mathbf{N}^*$ au lieu de $\mathbf{Z}\times\mathbf{Z}^*$ (c'est-à-dire en ne prenant que des dénominateurs strictement positifs), on airait pu simplifier cette définition par une telle division. Mais il y a deux raisons pour ne pas le faire. D'abord parce que cette simplification de la définition de la relation d'ordre introduit une complication dans la détermination du symétrique/inverse par rapport à la multiplication. Une sorte de conservation de problèmes. Et ensuite parce que la même construction s'applique à un anneau intègre commutatif A (en particulier à l'anneau des polynômes) en considérant des classes d'équivalences dans $A\times A^*$ et qu'en général un tel anneau (intègre commutatif) n'est pas pourvu d'une relation d'ordre qui permettra de remplacer A^* par des éléments strictement positifs.

14.12 Compatibilité avec la relation d'ordre dans $\mathbf{Z}$. *La relation d'ordre dans $\mathbf{Q}$ qu'on vient de définir est compatible avec la relation d'ordre déjà définie dans $\mathbf{Z}$ dans le sens qu'on a*

$$\forall m,n\in\mathbf{Z}\quad:\quad m\leq n\qquad\Longleftrightarrow\qquad \iota(m)\leq_{\mathbf{Q}}\iota(n)\ ,$$

où $\iota:\mathbf{Z}\to\mathbf{Q}$ est l'injection canonique (14.4).

Abus de notation très commode et universellement adopté. Ici, où on a construit $\mathbf{Q}$ à partir de $\mathbf{Z}$, on va agir exactement comme on l'a fait après la construction de $\mathbf{Z}$ à partir de $\mathbf{N}$: une fois qu'on sait que l'addition, la multiplication et la relation d'ordre dans $\mathbf{Z}$ et $\mathbf{Q}$ sont compatibles via l'injection canonique $\iota:\mathbf{Z}\to\mathbf{Q}$, on prend l'habitude de ne plus écrire le symbole $\mathbf{Q}$ en index sur ces opérations et de ne plus écrire le symbole ι de l'injection canonique. Pour des entiers relatifs a,b,c,d,p,q,r,s on écrit donc

$$(r\times s)\times\frac{p}{q}\leq\left(a+\frac{b}{c}\right)\times d$$

au lieu de

$$\iota(r\times s)\ \times_{\mathbf{Q}}\ \frac{p}{q}\leq_{\mathbf{Q}}(\iota(a)\ +_{\mathbf{Q}}\ \frac{b}{c})\ \times_{\mathbf{Q}}\ \iota(d)\quad\text{ou}\quad\left(\frac{r}{1}\ \times_{\mathbf{Q}}\ \frac{s}{1}\right)\ \times_{\mathbf{Q}}\ \frac{p}{q}\leq_{\mathbf{Q}}\left(\frac{a}{1}\ +_{\mathbf{Q}}\ \frac{b}{c}\right)\ \times_{\mathbf{Q}}\ \frac{d}{1}\ .$$

Comme pour l'abus analogue dans la construction de $\mathbf{Z}$ *à partir de* $\mathbf{N}$*, cet abus est accompagné de l'avertissement qu'il ne faut pas l'utiliser quand il y a risque de confusion. Comme dans le cas précédent, cela se produit surtout dans quelques preuves concernant les propriétés de* $\mathbf{Q}$ *et il faut donc distinguer les propriétés "essentielles" des propriétés "dérivées."*

14.13 Lemme. *L'addition* $+ : \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$ *vérifie les propriétés*

(i) $\forall m, n \in \mathbf{Q} : m + n = n + m.$

(ii) $\forall k, m, n \in \mathbf{Q} : (k + m) + n = k + (m + n),$

(iii) $\forall n \in \mathbf{Q} : n + 0 = n,$

(iv) $\forall r \in \mathbf{Q}\ \exists s \in \mathbf{Q} : r + s = 0,$

14.14 Corollaire. *L'ensemble* $\mathbf{Q}$ *muni de l'opération* $+$ *est un groupe abélien avec* 0 *comme élément neutre.*

Arrivé à la conclusion que $(\mathbf{Q}, +)$ *est un groupe abélien, on est confronté avec un petit problème : dans un groupe il existe une (unique) application du symétrique. Mais dans* $(\mathbf{Z}, +)$ *on a aussi une (unique) application du symétrique. Quel est le lien entre le symétrique dans* $\mathbf{Z}$ *et celui dans* $\mathbf{Q}$ *? La réponse est qu'ils sont compatibles et ce résultat est une conséquence d'un résultat beaucoup plus général, valable pour tout couple de groupes avec une application "compatible" entre les deux.*

Définition. Soit $(G, \blacksquare)$ et $(H, *)$ deux groupes et soit $f : G \to H$ une application. On dit que f est un *morphisme de groupes* ou simplement *homomorphisme* si elle vérifie la condition

$$\forall a, b \in G : f(a \blacksquare b) = f(a) * f(b)\ .$$

Autrement dit, f est un morphisme de groupes si les opérations $\blacksquare$ dans G et $*$ dans H sont compatibles via f.

14.15 Lemme. *Soit* $f : G \to H$ *un morphisme de groupes, soit* σ_G *l'application du symétrique dans* G *et soit* σ_H *celle dans* H*. Alors ces deux applications sont compatibles via* f *dans le sens qu'on a :*

$$\forall a \in G : \sigma_H\big(f(a)\big) = f\big(\sigma_G(a)\big)\ .$$

14.16 Corollaire de [14.6], [14.15] et [11.14]. *L'injection canonique* $\iota : \mathbf{Z} \to \mathbf{Q}$ *est un morphisme de groupes (pour les opérations d'addition). Si on note par* $-_{\mathbf{Q}}$ *l'application du symétrique dans* $\mathbf{Q}$ *pour l'opération* $+_{\mathbf{Q}}$ *(on l'appelle l'opposé et on a très provisoirement rajouté le symbole* $\mathbf{Q}$ *en indice pour le distinguer de l'opposé déjà défini dans* $\mathbf{Z}$*) on a la compatibilité*

$$\forall m \in \mathbf{Z} \quad : \quad \iota(-m) = -_{\mathbf{Q}}\, \iota(m)\ ,$$

ce qui nous permet d'étendre notre abus de notation en supprimant l'indice $\mathbf{Q}$. *Avec cet abus de notation on les propriétés*

(i) $-0 = 0 \in \mathbf{Q}$,

(ii) $\forall r \in \mathbf{Q} : r + (-r) = 0 = (-r) + r$,

(iii) $\forall r, s \in \mathbf{Q} : -(r+s) = (-r) + (-s)$ *et*

(iv) $\forall r \in \mathbf{Q} : -(-r) = r$.

Remarque. Une autre façon de définir l'opposé dans $\mathbf{Q}$ est de considérer l'application $f : \mathbf{Z} \times \mathbf{Z}^* \to \mathbf{Q}$ définie par

$$f\big((a,b)\big) = \frac{-a}{b}$$

et de constater que cette application est compatible avec la relation d'équivalence définie en (14.1). Par [9.9] il existe donc une unique application $M_{\mathbf{Q}} : \mathbf{Q} \to \mathbf{Q}$ vérifiant

$$M_{\mathbf{Q}}\Big(\frac{a}{b}\Big) \quad = \quad \frac{-a}{b} \quad \equiv \quad f\big((a,b)\big) \ .$$

Le calcul

$$\frac{a}{b} + M_Q\Big(\frac{a}{b}\Big) = \frac{a}{b} + \frac{-a}{b} = \frac{a \times b + (-a) \times b}{b \times b} = \frac{0}{b \times b} = 0$$

et l'unicité du symétrique dans [14.16] montrent qu'on doit avoir l'égalité

$$\frac{-a}{b} \equiv M_Q\Big(\frac{a}{b}\Big) = -\ \frac{a}{b} \ ,$$

c'est-à-dire que prendre l'opposé et l'application $M_{\mathbf{Q}}$ coïncident.

Définition. Comme pour les entiers relatifs, on définit l'ensemble $\mathbf{Q}^*$ comme les rationnels différents de l'élément neutre pour l'addition 0 :

$$\mathbf{Q}^* \ \stackrel{\text{déf}}{=} \ \mathbf{Q} \setminus \{\, 0 \,\} \equiv \{\, r \in \mathbf{Q} \mid r \neq 0 \,\} \ .$$

14.17 Lemme. *La multiplication* $\times : \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$ *vérifie les propriétés*

(i) $\forall m, n \in \mathbf{Q} : m \times n = n \times m$.

(ii) $\forall k, m, n \in \mathbf{Q} : k \times (m \times n) = (k \times m) \times n$,

(iii) $\forall k, m, n \in \mathbf{Q} : k \times (m + n) = (k \times m) + (k \times n)$,

(iv) $\forall r \in \mathbf{Q} : r \times 1 = r$,

(v) $\forall r \in \mathbf{Q}^* \ \exists s \in \mathbf{Q}^* : r \times s = 1$.

14.18 Définition. Un *corps* est un anneau commutatif $(K, +, \times)$ tel que tout élément autre que $0_K \in K$ (l'élément neutre pour l'opération $+$) admet un symétrique par rapport à l'opération $\times$. Autrement dit, si $1_K \in K$ est l'élément neutre pour l'opération $\times$, alors on a (doit avoir) la propriété

(K1) $\forall k \in K \setminus \{0_K\} \ \exists \ell \in K : k \cdot \ell = \ell \cdot k = 1_K$.

14.19 Lemme. *Soit $(K,+,\times)$ un corps. Alors $(K,+,\times)$ est un anneau intègre et l'ensemble $K^*=K\setminus\{0_K\}$ muni de l'opération $\times$ est un groupe commutatif avec 1_K comme élément neutre.*

Définitions. Si $(K,+,\times)$ est un corps, $(K^*,\times)$ est un groupe commutatif et en tant que tel on dispose d'une application du symétrique qui est notée par un -1 en exposant : $K^*\to K^*$, $k\mapsto k^{-1}$ et qu'on appelle "l'inverse" dans K. Elle a (donc) les propriétés

$$1_K^{-1}=1_K \qquad \text{et} \qquad \forall k\in K^* : k\times k^{-1}=1_K \text{ et } (k^{-1})^{-1}=k \ .$$

Omission des parenthèses/priorité des opérations III. Comme un anneau, un corps est muni de deux opérations internes associatives et donc la convention [8.11]/[11.22] de supprimer les parenthèses quand une même opération intervient plusieurs fois s'applique, ainsi que la convention que l'opération $\times$ a priorité sur l'opération $+$. Comme pour un anneau, dans un corps on dispose également de l'opération de soustraction $-$ (liée à l'opération unaire d'opposé) qui n'est pas associative et qui ne permet pas de supprimer des parenthèses. Mais dans un corps on dispose maintenant d'une quatrième opération : l'inverse (qui s'applique partout sauf en 0_K). Comme opération unaire elle a priorité sur tous les opérations binaires (associatives ou non).

14.20 Corollaire. *L'ensemble $\mathbf{Q}$ muni des deux opérations $+$ et $\times$ est un corps avec 0 l'élément neutre pour l'addition et 1 l'élément neutre pour la multiplication.*

14.21 Corollaire de [14.19] et [11.14]. *L'application du symétrique dans $\mathbf{Q}^*$ pour l'opération $\times$ est notée par le symbole -1 en exposant : $\mathbf{Q}^*\to\mathbf{Q}^*$, $r\mapsto r^{-1}$ et appelée* l'inverse *dans $\mathbf{Q}^*$. Elle a (donc) les propriétés*

$$1^{-1}=1 \qquad \textit{et} \qquad \forall r\in\mathbf{Q}^* : r\times(r^{-1})=1 \textit{ et } (r^{-1})^{-1}=r \ .$$

Remarque. Comme pour l'application du symétrique pour l'addition, on aurait pu construire l'application du symétrique pour la multiplication (sur $\mathbf{Q}^*$) directement sans passer par la case d'un corps. Pour cela on constate d'abord qu'on a l'équivalence

$$\frac{p}{q}\in\mathbf{Q}^* \qquad \Longleftrightarrow \qquad p\neq 0 \ .$$

Ensuite on définit l'application $g:\mathbf{Z}^*\times\mathbf{Z}^*\to\mathbf{Q}$ par

$$g(p,q)=\frac{q}{p} \ .$$

On constate que cette application est compatible avec la relation d'équivalence définie en (14.1). Par [9.9] il existe donc une unique application $I_{\mathbf{Q}}:\mathbf{Q}^*\to\mathbf{Q}$ vérifiant

$$I_{\mathbf{Q}}\Big(\frac{p}{q}\Big) \quad = \quad \frac{q}{p} \quad \equiv \quad g\big((p,q)\big) \ .$$

Le calcul

$$\frac{p}{q}\times I_Q\Big(\frac{p}{q}\Big)=\frac{p}{q}\times\frac{q}{p}=\frac{p\times q}{q\times p}=\frac{0}{1\times 1}=1$$

et l'unicité du symétrique dans [14.21] montrent qu'on doit avoir l'égalité

$$\frac{q}{p} \equiv I_Q\Big(\frac{p}{q}\Big) = \Big(\frac{p}{q}\Big)^{-1} \ ,$$

c'est-à-dire que prendre l'inverse et l'application $I_{\mathbf{Q}}$ coïncident (sur $\mathbf{Q}^*$).

Le lecteur attentif aura remarqué que le texte ci-dessus concernant l'application du symétrique pour la multiplication ressemble drôlement au texte concernant l'application du symétrique pour l'addition et que ce texte était déjà une copie presque conforme au texte concernant l'application du symétrique pour l'addition dans $\mathbf{Z}$. *On continue avec l'imitation avec la remarque qu'on peut utiliser l'inverse (l'application du symétrique pour la multiplication) pour résoudre* x *d'une équation de la forme* $x \times r = s$ *avec* $r \neq 0$ *:*

$$x \times r = s \qquad \Longleftrightarrow \qquad x = s \times r^{-1} \ .$$

Ainsi on peut définir la division dans $\mathbf{Q}$, *qu'on note par le symbole* $/$, *par*

$$r/s \overset{déf}{=} r \times s^{-1} \ ,$$

ce qui est l'analogue directe de la définition de la soustraction $r - s = r + (-s)$. *Et comme pour la soustraction, la division n'est ni commutative ni associative.*

Mais on peut pousser l'analogie encore plus loin. On a vu que dans la construction de $\mathbf{Z}$ *comme classes d'équivalences dans* $\mathbf{N} \times \mathbf{N}$ *on pouvait identifier la classe* $[\![m, n]\!]_{\mathbf{Z}}$ *comme la soustraction* $m - n$. *Pour un élément de* $\mathbf{Q}$ *vu comme classe d'équivalence dans* $\mathbf{Z} \times \mathbf{Z}^*$ *on peut faire la même chose avec la division : en faisant le calcul*

$$\frac{p}{q} = \frac{p}{1} \times_{\mathbf{Q}} \frac{1}{q} = \frac{p}{1} \times_{\mathbf{Q}} I_{\mathbf{Q}}\Big(\frac{q}{1}\Big) = p \times_{\mathbf{Q}} q^{-1} \equiv p/q \ ,$$

on voit que la classe d'équivalence $\frac{p}{q}$ *est égale à la division (le quotient)* p/q. *Une fois qu'on a vu cette formule, notre écriture pour la classe d'équivalence du couple* $(p, q) \in \mathbf{Z} \times \mathbf{Z}^*$ *sous la forme du* p *au-dessus le* q *et séparé par une barre horizontale devient "évidente" : on remplace la barre oblique* $/$ *par une barre horizontale et on pousse le* q *en-dessous de la barre.*

14.22 Corollaire de [11.23] et [14.19]. *Soit* $r, s \in \mathbf{Q}$ *deux nombres rationnelles. Alors on a les propriétés*

(i) $r \times 0 = 0$,

(ii) $-r = -1 \times r$ *et*

(iii) $r \times s = 0 \ \Leftrightarrow \ r = 0$ *ou* $s = 0$.

14.23 Propposition. *Soit* $r, s, t \in \mathbf{Q}$ *trois nombres rationnels. Alors on a les propriétés*

(i) $\quad r \leq s \quad \Longleftrightarrow \quad r + t \leq s + t$ *et*

(ii) $\quad r, s \geq 0 \quad \Longrightarrow \quad r \times s \geq 0$.

14.24 Corollaire. *La relation d'ordre $\leq$ sur $\mathbf{Q}$ est compatible avec la structure d'anneau.*

14.25 Corollaire de [14.23] et [11.31]. *Soit $r, s, t, u \in \mathbf{Q}$ quatre nombres rationnels. Alors on a les implications/équivalences*

(i) $r < s \implies r + t < s + t$,
(ii) $r < 0 \implies -r > 0$,
(iii) $r \geq 0$ *et* $s \leq t \implies r \times s \leq r \times t$,
(iv) $r > 0$ *et* $s < t \implies r \times s < r \times t$,
(v) $r > 0 \implies r^{-1} > 0$.

Jusqu'ici les propriétés de $\mathbf{Q}$ ressemblent aux propriétés de $\mathbf{Z}$. Mais l'analogie s'arrête quelque part. Par exemple, le propriété [11.33] de $\mathbf{Z}$ que tout sous-ensemble non-vide et minoré admet un plus petit élément n'est plus vrai dans $\mathbf{Q}$. Il suffit de penser à $\{ q \in \mathbf{Q} \mid q > 0 \}$. D'autre part, $\mathbf{Q}$ a une propriété que $\mathbf{Z}$ ne possède pas : entre deux éléments distincts de $\mathbf{Q}$ il y a toujours un troisième. Et pour finir, on montrera que $\mathbf{Q}$ est archimédien (la définition suivra). C'est une propriété qui pour $\mathbf{Q}$ n'a pas beaucoup d'importance, mais qui jouera un rôle important dans la caractérisation des nombres réels.

14.26 Toujours un rationnel entre deux rationnels. *Soit $r, s \in \mathbf{Q}$ deux rationnels vérifiants $r < s$. Alors il existe un rationnel $t \in \mathbf{Q}$ vérifiant $r < t < s$:*

$$\forall r, s \in \mathbf{Q} \ : \ r < s \quad \Rightarrow \quad \left[\ \exists t \in \mathbf{Q} : r < t < s \ \right] .$$

Définition. Soit $(K, +, \times)$ un corps et soit $\leq$ un ordre total sur K. On dit que K *est archimédien* si pour tout $a \in K$ il existe $n \in \mathbf{N}$ tel que

$$a < n \star 1_K \equiv \underbrace{1_K + \cdots + 1_K}_{n \text{ fois}} ,$$

où 1_K désigne l'élément neutre pour l'opération $\times$ et où $\star$ désigne l'opération externe de $\mathbf{N}$ sur K associée à l'addition $+$ [12.8].

Remarques pour les comparateurs. • Une autre façon pour dire qu'un corps totalement ordonné est archimédien est la condition que l'ensemble

$$L = \{ n \star 1_K \mid n \in \mathbf{N} \}$$

n'est pas borné, c'est-à-dire qu'il n'existe pas $a \in K$ tel que pour tout $x \in L$ on a $x \leq a$.

• La notion d'être archimédien existe aussi pour des groupes et des anneaux totalement ordonnés, aux quels cas la définition est (légèrement) différente. L'existence d'un inverse pour les éléments non-nuls dans un corps permet de montrer l'équivalence entre la notion dans un groupe ou anneau avec la définition donnée ci-dessus pour un corps.

Ⓟ **14.27 $\mathbf{Q}$ est archimédien.** *Pour tout $r \in \mathbf{Q}$ il existe $k \in \mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q}$ tel que $k > r$.*

Une fois qu'on a construit le corps des nombres rationnels, on arrive à la question : et si on le faisait d'une autre façon ? Car si on pense à la discussion/construction des rationnels positifs tenue dans §10, on s'aperçoit facilement qu'il y a une autre façon de construire $\mathbf{Q}$. On peut commencer avec la construction de $\mathbf{Q}_+$ des nombres rationnels positifs comme ensemble quotient de $\mathbf{N} \times \mathbf{N}^*$ par rapport à une relation d'équivalence (dont l'expression est identique à celle pour la construction de $\mathbf{Q}$ à partir de $\mathbf{Z}$). Et ensuite construire $\mathbf{Q}$ à partir de là comme on a construit $\mathbf{Z}$ à partir de $\mathbf{N}$, à savoir comme ensemble quotient de $\mathbf{Q}_+ \times \mathbf{Q}_+$ par rapport à une relation d'équivalence (dont l'expression est identique à celle pour la construction de $\mathbf{Z}$ à partir de $\mathbf{N}$). La réponse est la même que pour $\mathbf{Z}$ et $\mathbf{N}$: tant qu'on ne s'intéresse qu'aux trois structures addition, multiplication et relation d'ordre, on ne peut pas voir la différence. Par analogie avec $\mathbf{Z}$ on le fait par la caractérisation de $\mathbf{Q}$ comme le plus petit corps qui contient $\mathbf{N}$. Et comme pour $\mathbf{Z}$, l'idée intuitive est assez simple : si un corps K contient $\mathbf{N}$, ça doit contenir les opposés des éléments de $\mathbf{N}$ car K muni de l'addition est un groupe (abélien). Et donc K contient $\mathbf{Z}$. Mais un corps contient aussi les inverses de tous les éléments non-nuls, donc tous les éléments de la forme $1/n$ avec $n \in \mathbf{Z}^*$. En utilisant qu'on peut multiplier les éléments de K on en déduit que tous les rationnels appartiennent à K, c'est-à-dire que K contient $\mathbf{Q}$.

Ainsi on arrive à la description plus précise : un corps K contient $\mathbf{N}$ s'il existe une application injective $f : \mathbf{N} \to K$ qui respecte les opérations d'addition et de multiplication. Dire que $\mathbf{Q}$ est le plus petit corps qui contient $\mathbf{N}$ veut dire que si K contient $\mathbf{N}$, alors il existe une application injective $g : \mathbf{Q} \to K$ qui respecte les opérations et qui prolonge f. Ensuite on argumente comme dans le cas des entiers $\mathbf{Z}$ pour montrer que si on a un autre corps $\mathbf{Q}'$ avec cette même propriété de minimalité, alors il existe une application bijective $g : \mathbf{Q} \to \mathbf{Q}'$ qui respecte les opérations ainsi que la relation d'ordre.

15. Construction de R par coupures de Dedekind

La construction des nombres réels par coupures de Dedekind ne suit pas le même schéma que les constructions de $\mathbf{Z}$ *à partir de* $\mathbf{N}$ *ou de* $\mathbf{Q}$ *à partir de* $\mathbf{Z}$*. L'idée intuitive de Dedekind est assez simple à comprendre (mais un petit peu plus difficile à mettre en place rigoureusement). Si on a une idée intuitive de la droite réelle, alors on peut dire que chaque réel* $r \in \mathbf{R}$ *coupe cette droite en deux morceaux : les nombres à gauche et les nombres à droite. Pour l'instant on laisse planer le doute à quel côté il faut mettre le nombre* r *lui-même (comme le faisait Dedekind !). Ce qu'on peut remarquer est que les deux parties ne sont pas vides : il y a bien des nombres à gauche et des nombres à droite de* r*. Et chaque élément à gauche est strictement plus petit que chaque élément à droite. Et si on restreint son attention aux nombres rationnels, on le même résultat : un réel* r *coupe l'ensemble* $\mathbf{Q}$ *en deux morceaux non-vides — la partie à gauche* G *et la partie à droite* D *— tels que chaque élément de la partie de gauche est strictement plus petit que chaque élément de la partie de droite. On aura donc les propriétés*

$$G \cap D = \emptyset \quad , \quad G \cup D = \mathbf{Q} \quad , \quad \forall a \in G \; \forall b \in D : a > b \; .$$

Dedekind a tourné cette propriété dans l'autre sens en le prenant comme définition de $\mathbf{R}$ *: l'ensemble* $\mathbf{R}$ *est l'ensemble de toutes les possibilités de couper* $\mathbf{Q}$ *en deux morceaux vérifiant ces propriétés. Par exemple, le nombre réel* $\sqrt{2}$ *correspond à la coupure* $G, D \subset \mathbf{Q}$ *définie par*

$$G = \{\, x \in \mathbf{Q} \mid x^2 < 2 \text{ ou } x < 0 \,\} \quad \text{et} \quad D = \{\, x \in \mathbf{Q} \mid x > 0 \text{ et } x^2 > 2 \,\} \; .$$

On peut constater que G *n'a pas de plus grand élément et que* D *n'a pas de plus petit élément. Par contre, si on coupe* $\mathbf{Q}$ *à un endroit rationnel, il faut décider de quel côté on le met : à gauche (au quel cas l'ensemble de gauche aura un plus grand élément) ou à droite (au quel cas l'ensemble de droite aura un plus petit élément). Comme dit, Dedekind laisse planer le doute sur quel côté on devrait mettre un tel élément, ou plutôt, il définit implicitement une relation d'équivalence sur les coupures qui identifie ces deux possibilités. Bien que cette "solution" est (très) élégante, elle pose des petits ennuis pour les preuves et constructions qu'on veut effectuer. Pour éviter ces ennuis, on a opté de mettre un tel élément à gauche. La conséquence est que l'ensemble de droite n'aura jamais un plus petit élément (et l'ensemble de gauche aura un plus grand élément si et seulement si la coupure se fait à un nombre rationnel ; on montre le "si" dans (15.2)). Et parce que l'ensemble de gauche est (forcément) le complémentaire de l'ensemble de droite, on ne parle pas de cet ensemble à gauche, mais seulement de l'ensemble à droite (sans le donner ce nom).*

Définitions. Une *coupure (de Dedekind) de* $\mathbf{Q}$ est un sous-ensemble x de $\mathbf{Q}$ (c'est-à-dire $x \subset \mathbf{Q}$ ou $x \in \mathcal{P}(\mathbf{Q})$) vérifiant trois conditions :

(C1) $\emptyset \neq x \neq \mathbf{Q}$	x est ni vide ni $\mathbf{Q}$ entier ;
(C2) $\forall r, s \in \mathbf{Q} : r \in x$ et $r \leq s \Rightarrow s \in x$	x se remplit vers la droite ;
(C3) $\forall r \in x \; \exists s \in x : s < r$	x n'a pas de plus petit élément.

L'ensemble $\mathbf{R}$ est défini comme l'ensemble de toutes les coupures de $\mathbf{Q}$:

$$\mathbf{R} = \{\, x \in \mathcal{P}(\mathbf{Q}) \mid x \text{ vérifie les conditions (C1), (C2) et (C3)} \,\} \; .$$

Un élément de $\mathbf{R}$ est aussi appelé un *(nombre) réel* et $\mathbf{R}$ est appelé *l'ensemble des (nombres) réels* ou *la droite réelle*.

Notation/Nota Bene. Pour $r \in \mathbf{Q}$ on introduit l'abréviation $]r, \infty[$ pour l'ensemble $\{s \in \mathbf{Q} \mid r < s\}$ (c'est un cas particulier ce qu'on appelle généralement *un intervalle*) :

$$]r, \infty[\stackrel{\text{déf}}{=} \{s \in \mathbf{Q} \mid s > r\} \ .$$

Cette notation est certainement bien connu par la plupart des lecteurs, mais il faut faire attention, car ici cet intervalle est un sous-ensemble de l'ensemble $\mathbf{Q}$ des *rationnels*. Il ne s'agit pas d'un intervalle de nombres réels ! Avec cette notation on peut abréger la définition de $\mathbf{Q}_+^*$ comme $\mathbf{Q}_+^* =]0, \infty[$.

Ⓟ **15.1 Définition.** *Pour tout $r \in \mathbf{Q}$ l'ensemble $]r, \infty[\in \mathcal{P}(\mathbf{Q})$ est une coupure de $\mathbf{Q}$. En plus, l'application $\iota : \mathbf{Q} \to \mathbf{R}$ définie par*

$$\iota(r) =]r, \infty[\tag{15.2}$$

est injective. On l'appelle l'injection canonique de $\mathbf{Q}$ dans $\mathbf{R}$.

Ⓟ **15.3 La relation d'ordre sur R.** *La relation $\leq_{\mathbf{R}}$ sur $\mathbf{R}$ définie par*

$$x \leq_{\mathbf{R}} y \qquad \Longleftrightarrow \qquad y \subset x$$

est une relation d'ordre total sur $\mathbf{R}$.

Ⓟ **15.4 Compatibilité avec la relation d'ordre dans Q.** *La relation d'ordre dans $\mathbf{R}$ qu'on vient de définir est compatible avec la relation d'ordre déjà définie dans $\mathbf{Q}$ dans le sens qu'on a*

$$\forall r, s \in \mathbf{Q} \quad : \quad r \leq s \qquad \Longleftrightarrow \qquad \iota(r) \leq_{\mathbf{R}} \iota(s) \ ,$$

où $\iota : \mathbf{Q} \to \mathbf{R}$ est l'injection canonique (15.2).

Ⓟ **15.5 Lemme.** *Soit $x \subset \mathbf{Q}$ une coupure. Alors on a l'égalité*

$$x = \{\, r \in \mathbf{Q} \mid \iota(r) >_{\mathbf{R}} x \,\} \ .$$

Le lecteur aura remarqué que, contrairement aux constructions des structures sur $\mathbf{N}$, $\mathbf{Z}$ et $\mathbf{Q}$, on n'a pas commencé avec la construction des opération d'addition et de multiplication, mais avec la relation d'ordre. L'explication est double : d'abord la définition de la relation d'ordre est (beaucoup) plus simple que la définition de l'addition et surtout de la multiplication. Et ensuite parce que la relation d'ordre sur $\mathbf{R}$ a une particularité très importante qui distingue les réels des rationnels : tout sous-ensemble non-vide et minoré de $\mathbf{R}$ possède une borne inférieure. Ce qui est surprenant, c'est que la preuve de cette propriété est assez facile quand on définit $\mathbf{R}$ par les coupures de Dedekind (contrairement à la situation quand on construit $\mathbf{R}$ comme l'ensemble des classes d'équivalence de suite de Cauchy dans $\mathbf{Q}$).

Définitions. • Soit $\leq$ une relation d'ordre total sur un ensemble E, soit $A \subset E$ un sous-ensemble non-vide et soit $m \in E$ un élément. On dit que m *est un minorant de* A si tout élément de A est plus grand que ou égalé à m :

$$\forall a \in A : m \leq a$$

et on dit que A *est minoré* s'il existe un minorant de A.

• On dit que m *est la borne inférieure de* A, aussi appelé *le plus grand minorant* et noté $\inf A$, si m est le plus grand élément de l'ensemble des minorants de A. Autrement dit, si m est un minorant de A et si tout autre minorant de A est plus petit que ou égalé à m :

(BI1) $\forall a \in A : m \leq a$ et

(BI2) $\forall e \in E : \big(\forall a \in A : e \leq a \big) \ \Rightarrow \ e \leq m.$

Il est immédiat de la formulation comme plus grand élément de l'ensemble des minorants (et l'anti-symétrie d'une relation d'ordre) que la borne inférieure est unique, *si elle existe*.

• On dit que E *possède la propriété de la borne inférieure* si pour tout sous-ensemble non-vide minoré $A \subset E$ il existe une borne inférieure.

Remarque. La condition (BI2) est souvent formulé comme disant que tout élément strictement plus grand que m n'est pas un minorant, ce qui donne la condition équivalente (BI2') :

(BI2') $\forall e \in E : e > m \ \Rightarrow \ \big(\exists a \in A : a < e \big).$

L'équivalence avec la condition (BI2) se démontre en utilisant la tautologie logique

$$(p \Rightarrow q) \Longleftrightarrow \big(\neg q \Rightarrow \neg p\big)$$

qui dit qu'un implication $p \Rightarrow q$ est équivalente à l'implication inverse des négations $\neg q \Rightarrow \neg p$ et la tautologie

$$\neg\big(\forall a : p(a)\big) \Longleftrightarrow \exists a : \neg p(a)$$

qui dit qu'en échangeant un quantificateur avec la négation, alors le quantificateur change de sens.

Ⓟ **15.6 R a la propriété de la borne inférieure.** *Soit $A \subset \mathbf{R}$ un sous-ensemble non-vide minoré de $\mathbf{R}$. Alors A possède une borne inférieure.*

Ⓟ **15.7 $\iota[\mathbf{Q}]$ est dense dans R.** *Soit $x, y \in \mathbf{R}$ deux réels. Si on a $x <_{\mathbf{R}} y$, alors il existe $r \in \mathbf{Q}$ tel que $x <_{\mathbf{R}} \iota(r) <_{\mathbf{R}} y$.*

On peut résumer une partie de ce qu'on vient de faire comme suit. On part d'un ensemble totalement ordonné $\mathbf{Q}$ *et on construit l'ensemble totalement ordonné* $\mathbf{R}$ *comme l'ensemble des coupures (de Dedekind) de* $\mathbf{Q}$. *Ensuite on constate qu'il existe une injection canonique $\iota : \mathbf{Q} \to \mathbf{R}$ qui respecte la relation d'ordre et qu'elle n'est pas surjective (la coupure représentant $\sqrt{2}$ n'est pas dans l'image de* $\mathbf{Q}$*). Il est donc tentant de répéter l'opération : on définit l'ensemble* $\mathbf{S}$ *comme l'ensemble des*

coupures de **R** *qu'on muni d'une relation d'ordre total et on définit une injection canonique de* **R** *dans* **S**. *La surprise est que cette injection canonique sera bijective ! Autrement dit, toute coupure de* **R** *est nécessairement déterminé par un élément de* **R**. *Pour exprimer cette propriété de* **R** *on dit que "***R** *est complet." La preuve de cette propriété est une conséquence très simple de la propriété de la borne inférieure.*

Une fois qu'on a prononcé le mot "complet," il faut tout de suite signaler que la définition officielle est tout autre. La notion d'un espace métrique complet signifie que toute suite de Cauchy dans cet espace converge. Et dans un espace métrique arbitraire la notion de coupure n'a plus de sens, ni par ailleurs la notion de borne inférieure. Mais on peut démontrer que pour les nombres réels, les trois propriétés (i) de la borne inférieure, (ii) toute coupure est déterminé par un réel et (iii) toute suite de Cauchy converge, sont équivalentes.

Ⓟ **15.8 R est complet.** *Soit* C *un sous-ensemble de* $\mathbf{R}$ *vérifiant les conditions d'une coupure de* $\mathbf{R}$, *c'est-à-dire*

(C1') $\emptyset \neq C \neq \mathbf{R}$,

(C2') $\forall x, y \in \mathbf{R} : x \in C$ *et* $x \leq_{\mathbf{R}} y \;\Rightarrow\; y \in C$ *et*

(C3') $\forall x \in C \; \exists y \in C : y <_{\mathbf{R}} x$.

Alors il existe $z \in \mathbf{R}$ *tel que* $C = \{\, x \in \mathbf{R} \mid z <_{\mathbf{R}} x \,\}$.

Ⓟ **15.9 L'addition sur R.** *Si* x *et* y *sont deux réels, alors l'ensemble* $z \subset \mathbf{Q}$ *défini comme*

$$z \overset{déf}{=} \{\, r + s \mid r \in x \text{ et } s \in y \,\}$$

est une coupure de $\mathbf{Q}$ *qu'on note comme* $z = x +_{\mathbf{R}} y$. *L'application* $+_{\mathbf{R}} : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ *ainsi obtenue s'appelle* l'opération d'addition dans $\mathbf{R}$.

Remarque. Officiellement on devrait dire que l'ensemble $+_{\mathbf{R}} \subset (\mathbf{R} \times \mathbf{R}) \times \mathbf{R}$ défini par

$$+_{\mathbf{R}} = \big\{\, \big((x,y),z\big) \mid x, y \in \mathbf{R} \text{ et } z = \{r + s \mid r \in x \text{ et } s \in y\} \,\big\}$$

est une application de $\mathbf{R} \times \mathbf{R}$ dans $\mathbf{R}$ et qu'on note l'image d'un élément (x, y) par $x +_{\mathbf{R}} y$:

$$\big((x,y),z\big) \in +_{\mathbf{R}} \qquad \Longleftrightarrow \qquad z = x +_{\mathbf{R}} y \;.$$

Ⓟ **15.10 Compatibilité avec l'addition dans Q.** *L'addition dans* $\mathbf{R}$ *qu'on vient de définir est compatible avec l'addition déjà définie dans* $\mathbf{Q}$ *dans le sens qu'on a*

$$\forall r, s \in \mathbf{Q} \quad : \quad \iota(r + s) = \iota(r) +_{\mathbf{R}} \iota(s) \;,$$

où $\iota : \mathbf{Q} \to \mathbf{R}$ *est l'injection canonique (15.2).*

Un début d'abus de notation (toujours très commode et universellement adopté). Comme pour la construction de $\mathbf{Z}$ à partir de $\mathbf{N}$ et la construction de $\mathbf{Q}$ à partir de $\mathbf{Z}$, on utilise le fait que la relation d'ordre et l'addition sont compatibles via l'injection canonique $\iota : \mathbf{Q} \to \mathbf{R}$ pour supprimer le $\mathbf{R}$ en indice sur ces deux opérations et pour ne plus écrire le symbole pour l'injection canonique. Ceci veut

dire que chaque fois qu'on voit une formule dans laquelle on mélange des nombres rationnels et réels, il faut rajouter l'injection canonique pour les nombres rationnels et rajouter l'indice $\mathbf{R}$ sur les opérations (sauf bien sûr quand ces opérations se trouvent "à l'intérieur" d'une application de l'injection canonique). Par contre, quand il y a risque de confusion (surtout dans certaines preuves des propriétés des opérations sur $\mathbf{R}$), on reviendra sur la notation officielle.

Le but de cet abus est toujours le même : alléger la notation pour améliorer la lisibilité. On n'a pas attendu la définition de la multiplication sur $\mathbf{R}$ pour une raison très simple : la définition de la multiplication est un peu plus laborieuse que celle de l'addition et nécessite plusieurs étapes et des résultats sur l'addition. Et parce que ces résultats deviennent beaucoup plus lisible/reconnaissable avec l'abus de notation, on l'introduit dès maintenant.

Ⓟ **15.11 Lemme préliminaire.** *Soit $x \in \mathbf{R}$ tel que $x \notin \iota[\mathbf{Q}]$. Alors l'ensemble $y \subset \mathbf{Q}$ défini par*

$$y = \{\, s \in \mathbf{Q} \mid -s \notin x \,\}$$

est une coupure.

Ⓟ **15.12 Lemme préliminaire.** *Soit $x \in \mathbf{R}$ et $t \in \mathbf{Q}_+^*$. Alors il existe $r \in x$ et $s \in \mathbf{Q} \setminus x$ tel que $r - s = t$.*

Ⓟ **15.13 Lemme.** *L'addition $+ : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ vérifie les propriétés*

(i) $\forall x, y \in \mathbf{R} : x + y = y + x$.

(ii) $\forall x, y, z \in \mathbf{R} : (x + y) + z = x + (y + z)$,

(iii) $\forall x \in \mathbf{R} : x + 0 = x$,

(iv) $\forall x \in \mathbf{R}\ \exists y \in \mathbf{R} : x + y = 0$.

15.14 Corollaire. *L'ensemble $\mathbf{R}$ muni de l'opération $+$ est un groupe abélien avec 0 comme élément neutre.*

15.15 Corollaire de [15.10], [14.15] et [11.14]. *L'injection canonique $\iota : \mathbf{Q} \to \mathbf{R}$ est un morphisme de groupes pour les opérations d'addition dans $\mathbf{Q}$ et $\mathbf{R}$. Si on note par $-_{\mathbf{R}}$ l'application du symétrique dans $\mathbf{R}$ pour l'opération $+_{\mathbf{R}}$ (on l'appelle l'opposé et on a très provisoirement rajouté le symbole $\mathbf{R}$ en indice pour le distinguer de l'opposé déjà défini dans $\mathbf{Q}$) on a la compatibilité*

$$\forall r \in \mathbf{Q} \quad : \quad \iota(-r) = -_{\mathbf{R}}\, \iota(r) \ ,$$

ce qui nous permet d'étendre notre abus de notation en supprimant l'indice $\mathbf{R}$. Avec cet abus de notation on les propriétés

(i) $-0 = 0 \in \mathbf{R}$,

(ii) $\forall x \in \mathbf{R} : x + (-x) = 0 = (-x) + x$,
(iii) $\forall x, y \in \mathbf{R} : -(x + y) = (-x) + (-y)$ *et*
(iv) $\forall x \in \mathbf{R} : -(-x) = x$.

Remarque. Si on regarde la preuve de [15.13.iv], on s'aperçoit que l'élément $-_{\mathbf{R}}\, x$ est donné par

$$-_{\mathbf{R}}\, x = \begin{cases} \{\, s \in \mathbf{Q} \mid -s \notin x \,\} & x \notin \iota[\mathbf{Q}] \\ \{\, s \in \mathbf{Q} \mid -s \notin x \,\} \setminus \{-r\} = \,]-r, \infty[& x = \iota(r) \in \iota[\mathbf{Q}] \ . \end{cases}$$

Dans la pratique, la connaissance de cette formule explicite pour l'élément $-_{\mathbf{R}}\, x$ n'a aucun intérêt.

Ⓟ **15.16 Proposition.** *Soit $x, y, z \in \mathbf{R}$ trois nombres réels. Alors on a l'implication*

$$x \leq y \qquad \Longrightarrow \qquad x + z \leq y + z$$

15.17 Corollaire[2] **de [15.16] et [11.31].** *Soit $x, y, z \in \mathbf{R}$ trois (nombres) réels. Alors on a les propriétés*

(i) $x < y \quad \Longrightarrow \quad x + z < y + z$;
(ii) $x < 0 \quad \Longleftrightarrow \quad -x > 0$.

Définition. Comme pour les entiers relatifs et les rationnels on définit l'ensemble $\mathbf{R}^*$ comme les réels différents de l'élément neutre pour l'addition $\iota(0)$:

$$\mathbf{R}^* = \mathbf{R} \setminus \{\iota(0)\} = \{\, x \in \mathbf{R} \mid x \neq \iota(0) \,\} \ .$$

On introduit aussi les ensembles $\mathbf{R}_+$ et $\mathbf{R}_+^*$ comme les ensembles des réels positifs et strictement positifs :

$$\mathbf{R}_+ = \{\, x \in \mathbf{R} \mid x \geq_{\mathbf{R}} \iota(0) \,\} \qquad \text{et} \qquad \mathbf{R}_+^* = \mathbf{R}_+ \cap \mathbf{R}^* = \{\, x \in \mathbf{R} \mid x >_{\mathbf{R}} \iota(0) \,\} \ .$$

Ⓟ **15.18 La multiplication dans $\mathbf{R}_+$.** *Pour $x, y \in \mathbf{R}_+$ l'ensemble $z \subset \mathbf{Q}$ défini comme*

$$z \overset{déf}{=} \{\, r \times s \mid r \in x \ \textit{et}\ s \in y \,\}$$

est une coupure de $\mathbf{Q}$ vérifiant $z \geq_{\mathbf{R}} \iota(0)$. On le note comme $z = x \times'_{\mathbf{R}_+} y$. L'application ainsi obtenue $\times'_{\mathbf{R}_+} : \mathbf{R}_+ \times \mathbf{R}_+ \to \mathbf{R}_+$ s'appelle l'opération de multiplication sur $\mathbf{R}_+$.

Remarque. Officiellement on devrait dire que l'ensemble $\times'_{\mathbf{R}_+}$, sous-ensemble de $(\mathbf{R}_+ \times \mathbf{R}_+) \times \mathbf{R}_+$, défini par

$$\times'_{\mathbf{R}_+} = \left\{\, \big((x, y), z\big) \mid x, y \in \mathbf{R}_+ \ , \ z = \{r \times s \mid r \in x \ , \ s \in y\} \,\right\}$$

2. Je triche un tout petit peu, car proprement parlant on ne peut pas encore appliquer [11.31]. Mais si on regarde bien la preuve de [11.31], on s'aperçoit que pour les trois premiers résultats on n'utilise que la propriété énoncé dans [15.16].

est une application de $\mathbf{R}_+ \times \mathbf{R}_+$ dans $\mathbf{R}_+$ et qu'on prend l'habitude d'écrire l'appartenance à cet ensemble comme

$$\big((x,y),z\big) \in \times'_{\mathbf{R}_+} \qquad \Longleftrightarrow \qquad z = x \times'_{\mathbf{R}_+} y \ .$$

La multiplication dans R. Une fois qu'on connaît la multiplication $\times'_{\mathbf{R}_+}$ dans $\mathbf{R}_+$, on étend cette opération sur tout $\mathbf{R}$ par la procédure suivante. Pour $x, y \in \mathbf{R}$ on définit $x \times_{\mathbf{R}} y$ par

$$x \times_{\mathbf{R}} y = \begin{cases} x \times'_{\mathbf{R}_+} y & x, y \geq \iota(0) \\ -_{\mathbf{R}} \big((-_{\mathbf{R}} x) \times'_{\mathbf{R}_+} y \big) & x < \iota(0) \text{ et } y \geq \iota(0) \\ -_{\mathbf{R}} \big(x \times'_{\mathbf{R}_+} (-_{\mathbf{R}} y) \big) & x \geq \iota(0) \text{ et } y < \iota(0) \\ (-_{\mathbf{R}} x) \times'_{\mathbf{R}_+} (-_{\mathbf{R}} y) & x, y < \iota(0) \ , \end{cases} \tag{15.19}$$

où à droite on a utilisé la multiplication déjà définie dans [15.18]. Ceci est possible car par [15.17.ii] on ne multiplie à droite que des réels positifs.

Remarque. Si on veut être très correct, on devrait définir l'application $\times_{\mathbf{R}}$ comme

$$\begin{aligned} \times_{\mathbf{R}} = & \Big\{ \big((x,y), x \times'_{\mathbf{R}} y\big) \mid x, y \in \mathbf{R}_+ \Big\} \\ & \cup \Big\{ \big((x,y), -_{\mathbf{R}} \big(x \times'_{\mathbf{R}} (-_{\mathbf{R}} y)\big)\big) \mid x \in \mathbf{R}_+, y \in \mathbf{R}, y <_{\mathbf{R}} \iota(0) \Big\} \\ & \cup \Big\{ \big((x,y), -_{\mathbf{R}} \big((-_{\mathbf{R}} x) \times'_{\mathbf{R}} y\big)\big) \mid x \in \mathbf{R}, x <_{\mathbf{R}} \iota(0), y \in \mathbf{R}_+ \Big\} \\ & \cup \Big\{ \big((x,y), (-_{\mathbf{R}} x) \times'_{\mathbf{R}} (-_{\mathbf{R}} y)\big) \mid x, y \in \mathbf{R}, x, y <_{\mathbf{R}} \iota(0) \Big\} \ . \end{aligned}$$

Ⓟ **15.20 Compatibilité avec la multiplication dans Q.** *La multiplication dans* $\mathbf{R}$ *qu'on vient de définir est compatible avec la multiplication déjà définie dans* $\mathbf{Q}$ *dans le sens qu'on a*

$$\forall r, s \in \mathbf{Q} \quad : \quad \iota(r \times s) = \iota(r) \times_{\mathbf{R}} \iota(s) \ ,$$

où $\iota : \mathbf{Q} \to \mathbf{R}$ *est l'injection canonique (15.2).*

Abus de notation, suite.

Ⓟ **15.21 Lemme préliminaire.** *Soit* $x \in \mathbf{R}$ *un réel tel que* $x >_{\mathbf{R}} \iota(0)$ *et* $x \notin \iota[\mathbf{Q}]$. *Alors l'ensemble* $y \subset \mathbf{Q}$ *défini par*

$$y = \{ s^{-1} \mid s \in \mathbf{Q}_+^* \setminus x \}$$

est une coupure vérifiant $y \geq_{\mathbf{R}} \iota(0)$.

Ⓟ **15.22 Lemme.** *La multiplication* $\times : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ *vérifie les propriétés*

(i) $\forall x, y \in \mathbf{R} : x \times y = y \times x$.

(ii) $\forall x, y, z \in \mathbf{R} : x \times (y \times z) = (x \times y) \times z$,

(iii) $\forall x, y, z \in \mathbf{R} : x \times (y + z) = (x \times y) + (x \times z)$,
(iv) $\forall x \in \mathbf{R} : x \times 1 = x$,
(v) $\forall x \in \mathbf{R}^* \; \exists y \in \mathbf{R}^* : x \times y = 1$.

15.23 Corollaire. *L'ensemble* $\mathbf{R}$ *muni des deux opérations* $+$ *et* $\times$ *est un corps avec* 0 *comme élément neutre pour* $+$ *et* 1 *comme élément neutre pour* $\times$.

15.24 Corollaire de [14.19] et [11.14]. *L'application du symétrique dans* $\mathbf{R}^*$ *pour l'opération* $\times_{\mathbf{R}}$ *est notée par le symbole* $^{-1_{\mathbf{R}}}$ *en exposant :* $\mathbf{R}^* \to \mathbf{R}^*$, $x \mapsto x^{-1_{\mathbf{R}}}$ *et appelée l'inverse dans* $\mathbf{R}^*$. *On ajoute (très provisoirement) le symbole* $\mathbf{R}$ *dans le* -1 *en exposant pour le distinguer de l'opération correspondant dans* $\mathbf{Q}^*$. *Cette opération d'inverse dans* $\mathbf{R}^*$ *est compatible avec l'opération d'inverse déjà définie dans* $\mathbf{Q}^*$ *dans le sens qu'on a*

$$\forall r \in \mathbf{Q}^* \quad : \quad \iota(r^{-1}) = \big(\iota(r)\big)^{-1_{\mathbf{R}}} \ ,$$

ce qui permet d'étendre notre abus de notation en supprimant l'indice $\mathbf{R}$. *Avec cet abus de notation on a les propriétés*

(i) $1^{-1} = 1$,
(ii) $x \times (x^{-1}) = 1 = (x^{-1}) \times x$,
(iii) $(x \times y)^{-1} = y^{-1} \times x^{-1}$,
(iv) $(x^{-1})^{-1} = x$.

Remarque. Si on regarde la preuve de [15.22.v], on s'aperçoit que l'élément $x^{-1_{\mathbf{R}}}$ est donné, dans le cas $x >_{\mathbf{R}} \iota(0)$, par la formule

$$x^{-1_{\mathbf{R}}} = \begin{cases} \{\, s^{-1} \mid s \in \mathbf{Q}_+^* \setminus x \,\} & x \notin \iota[\mathbf{Q}] \\ \{\, s^{-1} \mid s \in \mathbf{Q}_+^* \setminus x \,\} \setminus \{r^{-1}\} & x = \iota(r) \in \iota[\mathbf{Q}^*] \end{cases}$$

et que pour $x <_{\mathbf{R}} \iota(0)$ cet élément est donné par

$$x^{-1_{\mathbf{R}}} = \begin{cases} -_{\mathbf{R}} \{\, s^{-1} \mid s \in \mathbf{Q} \,,\, s \notin -_{\mathbf{R}} x \,,\, s > 0 \,\} & x \notin \iota[\mathbf{Q}] \\ -_{\mathbf{R}} \Big(\{\, s^{-1} \mid s \in \mathbf{Q} \,,\, s \notin -_{\mathbf{R}} x \,,\, s > 0 \,\} \setminus \{-r^{-1}\} \Big) & x = \iota(r) \in \iota[\mathbf{Q}^*] \ . \end{cases}$$

Mais comme pour l'opération "moins", la connaissance de ces formules explicites n'a aucun intérêt dans la pratique.

15.25 Corollaire de [11.23] et [14.19]. *Soit* $x, y \in \mathbf{R}$ *deux nombres réels. Alors on a les propriétés*

(i) $x \times 0 = 0$,
(ii) $-x = -1 \times x$ *et*
(iii) $x \times y = 0 \;\Leftrightarrow\; x = 0$ *ou* $y = 0$;

15.26 Corollaire. *La relation d'ordre sur* $\mathbf{R}$ *est compatible avec la structure d'anneau.*

15.27 Corollaire de [11.31] et [15.26]. *Soit $a, b, c, d \in \mathbf{Q}$ quatre (nombres) réels. Alors on a les implications/équivalences*

(iv)	$a, b > 0$	$\Longrightarrow$	$a \times b > 0$
(v)	$\left[\ a \leq b \text{ et } c \geq 0\ \right]$	$\Longrightarrow$	$a \times c \leq b \times c$
(vi)	$\left[\ a \leq b \text{ et } c < 0\ \right]$	$\Longrightarrow$	$a \times c \geq b \times c$
(vii)	$\left[\ a < b \text{ et } c > 0\ \right]$	$\Longrightarrow$	$a \times c < b \times c$
(viii)	$\left[\ 0 \leq a < b \text{ et } 0 \leq c < d\ \right]$	$\Longrightarrow$	$a \times c < b \times d$
(ix)	$a > 0$	$\Longleftrightarrow$	$a^{-1} > 0$.

Ⓟ **15.28 R est archimédien.** *Soit $x, y \in \mathbf{R}$ tels que $x > 0$ et $y \geq 0$. Alors il existe $k \in \mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$ tel que $k \times x > y$.*

16. Le symbole $\sum$

Pour donner les détails de cette preuve on commence donc avec une définition rigoureuse du symbole $\sum$. L'idée de base est l'écriture

$$\sum_{i=k}^{m} t(i) = t(k) + t(k+1) + \cdots + t(m-1) + t(m) \ ,$$

où ni la partie gauche ni la partie droite est bien définie. Évidemment on a deux entiers k et m vérifiant $k \leq m$ et des réels $t(k), \ldots, t(m)$, mais le reste n'est pas (encore) défini. Commençons avec quelques cas particuliers :

$$\sum_{i=k}^{k} t(i) = t(k) \quad , \quad \sum_{i=k}^{k+1} t(i) = t(k) + t(k+1) \quad , \tag{16.1}$$

$$\sum_{i=k}^{k+2} t(i) = t(k) + t(k+1) + t(k+2) \ ,$$

où la partie de droite est parfaitement bien définie. Il est immédiat qu'on a les égalités

$$\sum_{i=k}^{k+1} t(i) = \sum_{i=k}^{k} t(i) + t(k+1) \qquad \textit{et} \qquad \sum_{i=k}^{k+2} t(i) = \sum_{i=k}^{k+1} t(i) + t(k+2) \ ,$$

ce qui suggère que le cas général se définit par récurrence.

16.2 Définition. Soit $t : \mathbf{N} \to \mathbf{R}$ une suite de réels. Alors pour tout $k \in \mathbf{N}$ on définit une suite $s_k : \mathbf{N} \to \mathbf{R}$ par récurrence par les formules

$$s_k(0) = t(k) \qquad \text{et} \qquad s_k(n+1) = s_k(n) + t(k+n+1) \ . \tag{16.3}$$

Ceci est une application de [7.6] avec $P = \mathbf{N}$, $g : P \to \mathbf{R}$ définie par $g(k) = t(k)$ et $f : (P \times \mathbf{N}) \times \mathbf{R} \to \mathbf{R}$ définie par $f\big((k,n),a\big) = a + t(k+n+1)$. La valeur $s_k(n)$ ne dépend pas seulement de k et de n, mais aussi de la suite t. Une meilleure notation serait donc $S(k,n,t)$ pour bien indiquer de quoi dépend cette valeur. Mais c'est la notation qui utilise le symbole $\sum$ qui est préférée et le réel $s_k(n)$ est habituellement notée comme

$$s_k(n) = \sum_{i=k}^{k+n} t(i) \ ,$$

où le symbole i (qui apparaît deux fois) est "formel" et peut être remplacé par n'importe quel autre symbole. Dans cette notation on voit, à part le symbole formel i, les entiers k et n, ainsi que la suite t. Le symbole $\sum$ (le sigma majuscule, la lettre "s" dans l'alphabet grec) représente l'opération interne d'addition : "s" pour "somme," car la même procédure est utilisée dans d'autre circonstances avec d'autres opérations (voir ci-dessous). L'entier k en-dessous du symbole $\sum$ (avec le $i = k$) s'appelle *la borne inférieure de la somme* et l'entier $m = k+n$ au-dessus du symbole $\sum$ s'appelle *la borne supérieure de la somme*. Par construction la borne supérieure d'une somme est donc un entier plus grand ou égal à la borne inférieure de la somme.

On a donc l'écriture

$$\text{si } k \leq m, \text{ alors } \sum_{i=k}^{m} t(i) \text{ veut dire } \sum_{i=k}^{k+n} t(i) \text{ avec } n = m - k.$$

Parfois on met les bornes inférieur et supérieur tous les deux en bas comme

$$\sum_{k \leq i \leq m} t(i) \text{ ce qui veut dire la même chose que } \sum_{i=k}^{m} t(i) \ .$$

L'avantage de la notation $\sum_{i=k}^{k+n} t(i)$ *par rapport à la notation* $S(k,n,t)$ *ne se voit pas dans le cas général (la deuxième notation est même plus courte que la première) mais dans les cas particuliers où on connaît une formule/expression pour les termes de la suite* t*. Si par exemple la suite* t *est donnée par*

$$\forall i \in \mathbf{N} : t(i) = i \ ,$$

alors on peut écrire

$$\sum_{i=k}^{n+k} i$$

sans avoir besoin d'utiliser le symbole t*. Dans la même veine on peut écrire*

$$\textit{considérons la valeur } \sum_{i=k}^{k+n} i^2 \ ,$$

au lieu de dire

$$\textit{soit } t : \mathbf{N} \to \mathbf{R} \textit{ la suite définie par } \forall i \in \mathbf{N} : t(i) = i^2 \textit{ et considérons } \sum_{i=k}^{k+n} t(i) \ .$$

Dans ces cas le fait de pouvoir écrire directement la valeur de $t(i)$ *permet d'éviter l'introduction d'un nom pour une suite particulière.*

Comme on a dit, la définition de la somme $\sum_{i=k}^{m} t(i)$ *est un cas particulier d'une situation beaucoup plus générale où on considère un ensemble* A *muni d'une opération interne* $\star : A \times A \to A$ *[8.1] et une suite* $t : \mathbf{N} \to A$ *à valeurs dans* A*. Alors pour tout* $k \in \mathbf{N}$ *on définit une suite* $s_k : \mathbf{N} \to A$ *par récurrence par les formules*

$$s_k(0) = t(k) \qquad et \qquad s_k(n+1) = s_k(n) \star t(k+n+1) \ .$$

Comme pour la définition de la somme, ceci est une application de [7.6], ici avec $P = \mathbf{N}$*,* $g : P \to A$ *définie par* $g(k) = t(k)$ *et* $f : (P \times \mathbf{N}) \times A \to A$ *définie par* $f((k,n),a) = a \star t(k+n+1)$*. Et la notation habituelle pour la valeur* $s_k(n)$ *ressemble aussi celle d'une somme : on remplace le symbole* $\sum$ *par un symbole qui ressemble au symbole de l'opération (souvent juste une version plus grande), ce qui fait qu'on note pour le cas de l'opération* $\star$ *la valeur de* $s_k(n)$ *comme*

$$s_k(n) = \overset{n+k}{\underset{i=k}{\star}} t(i) \ .$$

Une application du cas plus général est quand on considère l'opération de multiplication dans $\mathbf{R}$ *au lieu de l'addition. Dans ce cas on utilise le symbole* $\prod$ *(le pi*

majuscule, la lettre "p" dans l'alphabet grec, "p" pour "produit") dans la notation pour $s_k(n)$*, ce qui donne*

$$s_k(n) = \prod_{i=k}^{k+n} t(i) \ .$$

Si on l'applique à la suite particulière $t(i) = i$*, on obtient la définition du factoriel :*

$$n! = \prod_{i=1}^{n} t(i) \equiv \prod_{i=1}^{n} i$$

avec les cas particuliers $1! = 1$*,* $2! = 2$ *et* $3! = 6$*.*

Certains résultats qu'on va démontrer pour les sommes (de suites à valeurs dans $\mathbf{R}$*) sont aussi valables dans le cas général. On l'indiquera au fur et à mesure.*

Ⓟ **16.4 Lemme.** *Soit* $t, u : \mathbf{N} \to \mathbf{R}$ *deux suites à valeurs dans* $\mathbf{R}$ *et soit* $k, m \in \mathbf{N}$ *deux entiers vérifiant* $k \leq m$*. Alors on a l'implication*

$$\Big(\ \forall i \in \mathbf{N} : k \leq i \leq m \Rightarrow t(i) \leq u(i) \ \Big) \quad \Longrightarrow \quad \sum_{i=k}^{m} t(i) \leq \sum_{i=k}^{m} u(i) \ .$$

16.5 Corollaire. *Soit* $t, u : \mathbf{N} \to \mathbf{R}$ *deux suites à valeurs dans* $\mathbf{R}$ *et soit* $k, m \in \mathbf{N}$ *deux entiers vérifiant* $k \leq m$*. Alors on a l'implication*

$$\Big(\ \forall i \in \mathbf{N} : k \leq i \leq m \Rightarrow t(i) = u(i) \ \Big) \quad \Longrightarrow \quad \sum_{i=k}^{m} t(i) = \sum_{i=k}^{m} u(i) \ .$$

L'importance de ce corollaire est qu'il dit que la valeur $\sum_{i=k}^{m} t(i)$ *ne dépend que des valeurs de la suite pour les indices comprises entre* k *et* m*. Ceci est particulièrement intéressant quand on ne dispose pas de toute la suite mais seulement d'un bout comme dans*

$$\sum_{i=2}^{10} \sqrt{(i-2) \times (10-i)} \ . \tag{16.6}$$

Quand on veut définir une suite $t : \mathbf{N} \to \mathbf{R}$ *par*

$$\forall i \in \mathbf{N} : t(i) = \sqrt{(i-2) \times (10-i)} \ ,$$

on a un problème, car pour $i > 10$ *ou* $i < 2$ *on prend la racine carré d'un nombre négatif. Pour ces cas il faut donc "inventer" d'autres valeurs, mais lesquelles ? Selon [16.5] ce choix n'a pas d'importance pour la valeur de (16.6). On prend une suite* $u : \mathbf{N} \to \mathbf{R}$ *au hasard et on définit la suite* $t : \mathbf{N} \to \mathbf{R}$ *par*

$$t(i) = \begin{cases} u(i) & i < 2 \text{ ou } i > 10 \\ \sqrt{(i-2) \times (10-i)} & 2 \leq i \leq 10 \ . \end{cases}$$

Chaque choix pour u *donnera les mêmes valeurs pour* $t(i)$ *avec* $2 \leq i \leq 10$ *et donc par [16.5] on obtiendra le même résultat pour* $\sum_{i=2}^{10} t(i) \equiv \sum_{i=2}^{10} \sqrt{(i-2) \times (10-i)}$*.*

Remarquons aussi que ce corollaire est vrai dans le cas général et donne l'implication

$$\Big(\forall i \in \mathbf{N} : k \leq i \leq m \Rightarrow t(i) = u(i) \Big) \quad \Longrightarrow \quad \coprod_{i=k}^{m} t(i) = \coprod_{i=k}^{m} u(i) \ .$$

Seulement on doit le montrer directement (une petite variation sur la preuve de [16.4]), car dans le cas général on ne dispose pas d'une relation d'ordre (et si on en dispose, ce n'est pas sûr qu'on a l'équivalent de [15.16] pour l'opération interne $\star$, ingrédient essentiel dans la preuve de [16.4]).

Ⓟ **16.7 Lemme.** *Soit $t : \mathbf{N} \to \mathbf{R}$ une suite de réels et soit $k, m, n \in \mathbf{N}$ trois entiers vérifiant $k \leq m < n$, alors on a l'égalité*

$$\left(\sum_{i=k}^{m} t(i) \right) + \left(\sum_{i=m+1}^{n} t(i) \right) = \sum_{i=k}^{n} t(i) \ .$$

Ce résultat reste vrai dans le cas général avec une opération interne $\star : A \times A \to A$ et une suite $t : \mathbf{N} \to A$, à condition que cette opération soit associative. Avec cette condition même la preuve ne nécessite que des changements cosmétiques et donne la formule

$$\left(\coprod_{i=k}^{m} t(i) \right) \star \left(\coprod_{i=m+1}^{n} t(i) \right) = \coprod_{i=k}^{n} t(i) \ .$$

Ⓟ **16.8 Lemme.** *Soit $b \in \mathbf{R}^*$ un réel non-nul. Alors pour tout $k, m \in \mathbf{N}$ vérifiant $k \leq m$ on a l'égalité*

$$\sum_{i=k}^{m} \frac{b-1}{b^i} = \frac{b^{m-k+1} - 1}{b^m} \ .$$

Ce premier résultat pour une suite particulière montre déjà l'utilité de la notation : au lieu d'introduire la suite $t : \mathbf{N} \to \mathbf{R}$ comme

$$\forall i \in \mathbf{N} : t(i) = \frac{b-1}{b^i}$$

et de parler de la valeur $\sum_{i=k}^{m} t(i)$, on parle directement de la valeur $\sum_{i=k}^{m} \frac{b-1}{b^i}$. Remarquons aussi que c'est bien une suite géométrique (de raison $\frac{1}{b}$ et de premier terme $\frac{b-1}{b^k}$), mais qu'il est plus judicieux de la voir comme une suite téléscopique de terme $t(i) = \frac{1}{b^{i-1}} - \frac{1}{b^i}$. En connaissant la formule pour la somme d'une suite géométrique et en utilisant les petits points, on obtient bien l'égalité

$$\begin{aligned} (16.9) \quad & \left(\frac{1}{b^{k-1}} - \frac{1}{b^k} \right) + \left(\frac{1}{b^k} - \frac{1}{b^{k+1}} \right) + \cdots + \left(\frac{1}{b^{m-1}} - \frac{1}{b^m} \right) \\ & = \frac{1}{b^{k-1}} - \frac{1}{b^m} = \frac{b-1}{b^k} \cdot \frac{1 - \left(\frac{1}{b}\right)^{m-k+1}}{1 - \frac{1}{b}} \ . \end{aligned}$$

17. Le développement décimal d'un réel

Ⓟ **17.1 Proposition/Définition.** *L'ensemble* $\mathrm{Ent} \subset \mathbf{R} \times \mathbf{Z}$ *défini comme*

$$\mathrm{Ent} \overset{déf}{=} \{\, (x,n) \in \mathbf{R} \times \mathbf{Z} \mid n \leq x < n+1 \,\}$$

est une application $\mathrm{Ent} : \mathbf{R} \to \mathbf{Z}$. *Elle associe à chaque réel* $x \in \mathbf{R}$ *un entier* $n = \mathrm{Ent}(x)$ *qui vérifie* $n \leq x < n+1$ *et qu'on appelle* la partie entière de x.

Ⓟ **17.2 Lemme.** *Soit* $b \in \mathbf{R}$ *tel que* $b > 1$. *Alors on a l'égalité*

$$\inf \{\, b^{-n} \mid n \in \mathbf{N} \,\} = 0 \ .$$

Si $x \in \mathbf{R}_+$ *est un nombre réel positif, alors son "développement décimal" est l'écriture de* x *sous la forme*

$$x = a_n\, a_{n-1} \ldots a_2\, a_1\, a_0 \ ,\ d_1\, d_2\, d_3 \ldots$$

où les a_i *et* d_j *sont des chiffres appartenant à l'ensemble* $\{0,1,\ldots,8,9\}$. *Par exemple le chiffre* a_3 *représente les milliers et* d_2 *les centièmes. Plus précisément, on prétend qu'on a l'égalité*

$$\begin{aligned} x &= a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0 \\ &\qquad + \frac{d_1}{10} + \frac{d_2}{10^2} + \frac{d_3}{10^3} + \cdots \\ &= \sum_{i=0}^{n} a_i \times 10^i + \sum_{j=1}^{\infty} \frac{d_j}{10^j} \ . \end{aligned}$$

Sous-entendu est l'idée que la première somme (sur i*) représente la partie entière de* x *et que la deuxième somme (sur* j*) représente la partie "fractionnelle" de* x. *On utilise le symbole* $\sum$ *parce que les (trois) petits points sont (très) ambigus. La signification du symbole* $\sum$ *pour la somme sur* i *a été rigoureusement dfdéfinie en §16. Par contre, l'utilisation du symbole* $\sum$ *pour la somme sur* j *n'a pas été définie, car on n'a pas définie ce que c'est une somme infinie. Pour éviter une discussion sur la convergence de séries, on le fera dans ce texte par l'utilisation d'un sup sur des sommes finies.*

Avec une bonne interprétation du symbol $\sum$ *dans les deux cas, on arrive à la situation suivante : on décompose un réel positif* $x \in \mathbf{R}_+$ *en sa partie entière* $n = \mathrm{Ent}(x) \in \mathbf{N}$ *et sa partie fractionnelle* $f = x - n$, *c'est-à-dire :*

$$x = n + f \qquad , \qquad n \in \mathbf{N} \quad et \quad 0 \leq f < 1 \ .$$

Ensuite on "trouve" la suite des décimales $d_j \in \{0,1,\ldots,9\}$, $j \in \mathbf{N}^*$ *et on pense qu'il y a une bijection entre les réels* f *vérifiant* $0 \leq f < 1$ *d'une part et les suites des décimales* d_j *d'autre part. Et que le lien est donné par la formule*

$$f = \sum_{j=1}^{\infty} \frac{d_j}{10^j} \ . \tag{17.3}$$

Malheureusement la situation est un petit peu plus compliquée que cela, car l'écriture "décimale" n'est pas unique ; par exemple,

$$0,099999\ldots \qquad et \qquad 0,100000\ldots$$

représentent tous les deux le nombre $\frac{1}{10}$. *Plus précisément, ces deux suites de décimales produisent la même valeur pour* f *dans (17.3) (dans l'interprétation standard d'une série). Pour rétablir une écriture unique on peut introduire le* développement décimal réduit *qui consiste à exclure les développements qui se terminent par la suite constante* 9. *Et c'est avec cette précision qu'on arrive à montrer rigoureusement l'idée que les suites des décimales sont en bijection avec les réels entre* 0 *et* 1.

17.4 Lemme. *Soit* $A \subset \mathbf{R}$ *un ensemble, soit* $x \in \mathbf{R}$ *fixe et soit* $A_x \subset \mathbf{R}$ *l'ensemble définie comme*

$$A_x = \{\, y \in \mathbf{R} \mid \exists a \in A : y = a + x \,\} \equiv \{\, a + x \mid a \in A \,\} \ .$$

Alors A *est majoré si et seulement si* A_x *est majoré. Si c'est le cas on a l'égalité*

$$\sup A_x = x + \sup A \ .$$

On a maintenant suffisamment de résultats préliminaire pour pouvoir attaquer le problème du développement décimal. Ce développement est intimement lié à l'écriture des entiers naturels en base dix. Ceci veut dire qu'on décrit un entier quelconque par une suite finie de chiffres qui appartiennent à l'ensemble de dix éléments $\{0, 1, \ldots, 9\}$. *Plus précisément, pour un entier* $n \in \mathbf{N}$ *on écrit*

$$n = \sum_{i=0}^{m} a_i \times (9+1)^i \tag{17.5}$$

avec $a_i \in \{0, 1, \ldots, 9\}$. *On n'entre pas ici dans l'analyse précise de cette écriture d'un entier naturel. Elle est semblable (mais pas analogue) à l'analyse du développement décimal d'un réel. Par contre, il n'y a rien de spécial dans le choix du nombre dix qui sert comme base pour cette écriture (sauf que l'homme a dix doigts aux deux mains). L'ordinateur utilise la base binaire et pour l'écriture d'une adresse MAC d'un ordinateur on utilise la base hexadécimale. Parce que on aura besoin plus tard d'une telle écriture en d'autres bases, on donne la description du développement décimal dans une base quelconque* $b \in \mathbf{N}$, $b \geq 2 \equiv S\big(S(\emptyset)\big)$.

Mais il y un piège qu'il faut éviter : quel que soit la base b *qu'on utilise, cet entier s'écrit* toujours *comme* 10 *dans cette base ! Car l'écriture* 10 *veut dire qu'on a zéro "unités" et une fois la base* b *:*

$$b = 1 \times b^1 + 0 \times b^0 \ .$$

C'est pourquoi on a soigneusement évité dans le paragraphe précédent d'écrire 10, *mais qu'on a toujours parlé de "dix," car dix est le nombre qui vient après neuf (dix est le successeur de neuf), et* 10 *est une écriture ambigue qui dépend de la base. Il est donc impossible de dire qu'on utilise la base 16, car cela voudrait dire qu'on a l'égalité*

$$b = 16 = 1 \times b^1 + 6 \times 1 = b + 6 \ .$$

Ceci explique pourquoi on a écrit $9 + 1$ *au lieu de* 10 *dans (17.5) ; on aurait pu écrire aussi* $S(9)$, *le successeur de* 9. *Et même si on avait écrit* 10, *on serait obligé de l'interpréter comme le successeur de* 9, *car (17.5) nous donne la définition de l'écriture en base dix. Utiliser la notation pour le définir est un cercle vicieux.*

Définition. Pour un entier $b \in \mathbf{N}$ vérifiant $b \geq 2$ on définit l'ensemble $B_b \subset \mathbf{N}$ par

$$B_b = \{0, 1, \ldots, b-1\} = \{\, n \in \mathbf{N} \mid n < b \,\} \ .$$

L'ensemble $\mathcal{DR}_b$ des *suites réduites en base b* est l'ensemble des applications de $\mathbf{N}^*$ dans B_b qui n'ont pas une queue constante égale à $b-1$:

$$\mathcal{DR}_b = \{\, d : \mathbf{N}^* \to B_b \mid \forall n \in \mathbf{N}^* \ \exists m \in \mathbf{N}^* : m \geq n \text{ et } d(m) \neq b-1 \,\} \ .$$

Si l'ensemble des entiers naturels $\mathbf{N}$ *est construit comme on l'a fait dans §6, alors l'ensemble* B_b *n'est rien d'autre que l'ensemble* b *lui-même. Une esquisse de preuve par récurrence est donnée dans le schéma*

$$0 = \emptyset = \{n \in \mathbf{N} \mid n < 0\}$$

et

$$b = \{n \in \mathbf{N} \mid n < b\} \quad \Longrightarrow \quad S(b) = b \cup \{b\} = \{n \in \mathbf{N} \mid n < b\} \cup \{b\}$$
$$= \{n \in \mathbf{N} \mid n \leq b\} \overset{[8.16]}{=} \{n \in \mathbf{N} \mid n < S(b)\} \ .$$

Avec ce résultat, [6.7] devient un corollaire. Mais il faut bien faire attention à des boucles dans le raisonnement. On avait besoin de [6.7] pour montrer que l'application du successeur sur $\mathbf{N}$ *est injective. Avec cela on a montré que l'ensemble* $\mathbf{N}$ *ainsi construit vérifie les axiomes de Peano. Et à l'aide des axiomes de Peano on a construit la relation d'ordre sur* $\mathbf{N}$*. Dans §28 on donnera une toute autre preuve de l'égalité* $b = \{n \in \mathbf{N} \mid n < b\}$ *qui ne dépend pas des axiomes de Peano. Avec cette nouvelle preuve, on a le droit de voir [6.7] comme un corollaire. Mais dans l'approche de §28 on n'en aura plus besoin.*

Ⓟ **17.6 Lemme.** *Soit* $d \in \mathcal{DR}_b$ *une suite réduite en base* b*. Alors on a l'encadrement*

$$0 \leq \sup \left\{ \sum_{j=1}^{n} \frac{d(j)}{b^j} \;\middle|\; n \in \mathbf{N} \right\} < 1 \ .$$

Ⓟ **17.7 Proposition.** *L'application* $f_b : \mathcal{DR}_b \to \{\, x \in \mathbf{R} \mid 0 \leq x < 1 \,\}$ *définie par*

$$f_b(d) = \sup \left\{ \sum_{j=1}^{n} \frac{d(j)}{b^j} \;\middle|\; n \in \mathbf{N} \right\}$$

est une bijection.

Ⓟ **17.8 L'argument de la diagonale de Cantor.** *Il n'existe pas une surjection de* $\mathbf{N}^*$ *dans* $[0, 1[\subset \mathbf{R}$.

Chapitre 3

Des choix

18. L'axiome du choix

Les sept axiomes qu'on a vu jusqu'à maintenant sont les sept axiomes de base que tous les mathématiciens utilisent tous les jours. Les six premiers sont utilisés quand on écrit des ensembles : l'axiome de l'ensemble vide et l'axiome d'extensionnalité sont à la base du raisonnement mathématique, l'axiome de la paire est utilisé dès qu'on écrit un ensemble comme une liste d'élément sous la forme $\{a, b, c\}$*, l'axiome de séparation est utilisé dès qu'on écrit un ensemble comme un sous-ensemble défini par un critère sous la forme* $\{a \in A \mid p(a)\}$*, l'axiome de la réunion est utilisé dès qu'on parle de réunion ou intersection, l'axiome de l'ensemble des parties est aussi fréquemment utilisé (et nous on l'a utilisé pour définir le produit cartésien). Et "last but not least," l'axiome de l'infini entre en jeu dès qu'on utilise les entiers naturels* $\mathbf{N}$ *ou les systèmes de nombres dérivés comme* $\mathbf{Z}$*,* $\mathbf{Q}$*,* $\mathbf{R}$ *(ou* $\mathbf{C}$*).*

Par contre, l'axiome du choix, dont on parle souvent, est beaucoup moins utilisé, bien qu'on l'utilise souvent, même sans s'en rendre compte. Comme son nom l'indique, cela concerne des choix et intervient quand on a des enesmbles non-vides et qu'on choisit un élément. Regardons deux exemples pour bien comprendre le problème.

Le premier exemple concerne l'énoncé que si B *est un ensemble non-vide et* A *un ensemble quelconque, alors il existe une application* $f : A \to B$*. La preuve est simple : on choisit un élément* b *dans* B *et on définit l'application* f *comme*

$$f = \{\, p \in A \times B \mid \exists a \in A : p = (a, b) \,\} \equiv \{\, (a, b) \mid a \in A\} \equiv A \times \{b\} \ ,$$

ce qui est l'application constante b*. On a donc montré l'existence d'une application.*

Dans le deuxième exemple on considère une suite d'ensembles non-vides $X_n \subset \mathbf{R}$ *(des sous-ensembles de* $\mathbf{R}$*), autrement dit, on a une application* $g : \mathbf{N} \to \mathcal{P}(\mathbf{R}) \setminus \{\emptyset\}$ *avec* $g(n) = X_n$*. Étant donné que les* X_n *ne sont pas vides, on choisit, pour chaque* $n \in \mathbf{N}$*, un élément* $x_n \in X_n$*. Autrement dit, on se donne une application* $f : \mathbf{N} \to \mathbf{R}$ *telle que* $x_n \equiv f(n) \in g(n) \equiv X_n$*.*

Dans les deux exemples on prononce les mots "on choisit", mais il y a une grande différence : dans le premier exemple le raisonnement se justifie avec nos sept axiomes, tandis que le raisonnement dans le deuxième exemple ne se justifie pas avec nos sept axiomes ! L'origine du problème est semblable au problème qu'on a rencontré pour la définition d'une suite récurrente. Quand on écrit x_n *on a déjà implicitement supposé qu'il existe une* application *définie sur* $\mathbf{N}$*. Et le fait qu'un ensemble* $X_n \equiv g(n)$ *n'est pas vide ne garantit pas l'existence d'une application. On devrait écrire*

$$\forall n : n \in \mathbf{N} \ \Rightarrow \ \exists x : x \in g(n) \ .$$

On n'a pas le droit de mettre une dépendance fonctionelle sur le symbole x (style x_n ou $x(n)$). On ne peut donc pas définir l'application $f : \mathbf{N} \to \mathbf{R}$ par $f(n) = x_n$; ce serait une tautologie, car on aurait déjà supposé l'existence d'une fonction en utilisant l'écriture fonctionnelle x_n. Ce même problème ne se produit pas dans le premier exemple, car là on n'utilise que l'unique symbole b qui désigne un élément de B.

Quand on a un nombre fini d'ensembles non-vides, on peut utiliser des symboles différentes pour le choix d'un élément dans chacun de ces ensembles. Mais dès que le nombre d'ensembles non-vides n'est plus fini, on ne peut plus faire cela. Pourtant, il semble naturel qu'on puisse choisir un élément dans chacun de ces ensembles. C'est ce que dit l'axiome du choix : si on a un ensemble B et une famille de sous-ensembles non-vides $X_i \subset B$ indexée par un ensemble I (c'est-à-dire qu'on a une fonction $g : I \to \mathcal{P}(B) \setminus \{\emptyset\}$ avec $g(i) = X_i$ pour tout $i \in I$), alors on peut choisir un élément $x_i \in X_i$ pour tout $i \in I$, c'est-à-dire qu'il existe une fonction (qu'on appelle une fonction de choix*) $f : I \to B$ telle que $x_i \equiv f(i) \in g(i) \equiv X_i$ pour tout $i \in I$.*

(Z8)=(C) Axiome du choix.

$$\forall B, I, g \ : \ g : I \to \mathcal{P}(B) \setminus \{\emptyset\} \quad \Longrightarrow \quad \exists f : I \to B \quad \forall i \in I : f(i) \in g(i) \ .$$

La formulation de l'axiome du choix qu'on a donné ici est la forme qu'on utilise le plus souvent. Il existe des variantes plus ou moins ressemblantes, dont une qu'il faut mentionner, car c'est la forme plus officielle qui ne parle pas de fonctions, mais seulement d'ensembles et qui dit que si on a un ensemble A dont tous les éléments sont des ensembles non-vides 2 à 2 disjoints, alors il existe un ensemble (qu'on appelle un ensemble de choix*) qui contient un et un seul élément de chaque élément de A.*

Ⓟ **18.1 Proposition.** *L'axiome du choix est équivalent à la propriété*

$$\forall A \ : \ \Big[\ \big[\ \forall a \in A : a \neq \emptyset \ \big] \ \textit{et} \ \big[\ \forall a, b \in A : a \neq b \ \Rightarrow \ a \cap b = \emptyset \ \big] \ \Big] \tag{18.2}$$
$$\Longrightarrow \quad \big[\ \exists C \subset \cup A \quad \forall a \in A \quad \exists c : a \cap C = \{c\} \ \big] \ .$$

Le lecteur pourrait croire qu'on doit invoquer systématiquement l'axiome du choix, chaque fois qu'on veut obtenir une fonction de choix f dans la situation décrite par l'axiome du choix. Heureusement ce n'est pas toujours le cas. L'exemple classique qu'on donne souvent pour décrire les deux cas de figures (oui ou non besoin de l'axiome du choix) est l'exemple des chaussures et des chaussettes. Quand on a une infinité de paires de chaussures, il est facile de choisir une chaussure dans chaque paire : on choisit (par exemple) la chaussure gauche. Et on n'a pas besoin d'invoquer l'axiome du choix pour le faire. Par contre, si on dispose d'une infinité de paires de chaussettes, il n'y a pas de règle pour choisir une chaussette dans chaque paire : les deux sont identiques. Et dans cette situation on aura besoin d'invoquer l'axiome du choix pour faire ce choix pour tous les paires de chaussettes.

Un exemple plus mathématique est le cas où on a une famille de sous-ensembles non-vides des entiers naturels $\mathbf{N}$*, c'est-à-dire une application* $g : I \to \mathcal{P}(\mathbf{N})\setminus\{\emptyset\}$*. On sait que chaque sous-ensemble de* $\mathbf{N}$ *qui n'est pas vide possède un plus petit élément. On peut donc "choisir" celui pour obtenir notre fonction de choix* $f : I \to \mathbf{N}$ *:*

$$\forall i \in I : f(i) = \text{ le plus petit élément de } g(i) \ .$$

Si on veut le mettre sous la forme officielle et sans utiliser des mots dans la description, on pourrait écrire

$$f = \{\, (i,n) \in I \times \mathbf{N} \mid n \in g(i) \text{ et } \forall k \in g(i) : n \leq k \,\} \ .$$

Le fait que cet ensemble est bien une application de I *dans* $\mathbf{N}$ *utilise (évidemment) le fait qu'un élément* $n \in \mathbf{N}$ *vérifiant* $n \in g(i)$ *et* $\forall k \in g(i) : n \leq k$ *existe et est unique pour tout sous-ensemble non-vide* $g(i) \subset \mathbf{N}$ *[8.17]. Dans cette situation on n'a donc pas besoin de l'axiome du choix. Mais la situation change si on remplace l'ensemble* $\mathbf{N}$ *par l'ensemble des réels* $\mathbf{R}$*, c'est-à-dire qu'on regarde une famille de sous-ensembles non-vides de* $\mathbf{R}$*, ou encore une application* $g : I \to \mathcal{P}(\mathbf{R}) \setminus \{\emptyset\}$*. Dans un sous-ensemble non-vide de* $\mathbf{R}$ *il n'existe pas forcément un plus petit élément. La méthode utilisé dans le cas* $\mathbf{N}$ *ne s'applique donc pas et on a besoin d'invoquer l'axiome du choix pour obtenir une fonction de choix* $f : I \to \mathbf{R}$ *vérifiant* $f(i) \in g(i)$*.*

On a donc besoin de l'axiome du choix dans les situations où on ne dispose pas d'un algorithme pour déterminer un élément (unique) dans chaque ensemble non-vide. Ce phénomène montre aussi un autre aspect de l'axiome du choix : c'est le seul axiome qui ne détermine pas d'une façon unique, l'ensemble dont l'existence est annoncée. Tous les autres axiomes déterminent complètement (à l'aide de l'axiome d'extensionnalité) l'ensemble dont l'existence est garantie.

Malgré le fait que l'énoncé de l'axiome du choix paraît naturel, certains mathématiciens préfèrent ne pas l'utiliser. Comme décrit dans **[Her06]***, il y a des bonnes raisons pour utiliser l'axiome du choix et il y a des bonnes raison pour le refuser. Côté positif on peut penser au résultat que tout espace vectoriel admet une base, même en dimenion infinie, et que le cardinal d'une telle base est un invariant de l'espace, ou au théorème de Hahn-Banach en analyse fonctionelle. Côté négatif on peut penser au paradoxe de Banach-Tarski qui dit (entre autres) qu'on peut couper une boule pleine de* $\mathbf{R}^3$ *en* 5 *morceaux et les rassembler de telle façon qu'on obtient deux boules pleines, chacune de même taille que la boule initiale ; on a donc doublé le volume. C'est en particulier le côté négatif qui a poussé les mathématiciens à tenter de trouver d'autres axiomes qui pourraient remplacer l'axiome du choix, mais sans ces conséquences troublantes. Un de ces axiomes alternatifs est* l'axiome du choix dénombrable*, qui est similaire à l'axiome du choix, sauf qu'on restreint l'ensemble* I *à être l'ensemble* $\mathbf{N}$ *des entiers naturels.*

(CD) Axiome du choix dénombrable.

$$\forall B, g \ : \ g : \mathbf{N} \to \mathcal{P}(B) \setminus \{\emptyset\} \quad \Longrightarrow \quad \exists f : \mathbf{N} \to B \quad \forall i \in I : f(i) \in g(i) \ .$$

L'axiome du choix dénombrable est suffisamment "faible" pour éviter les résultats troublants qui se déduisent avec l'axiome du choix général. Mais on perd aussi les résultats agréables comme l'existence d'une base pour un espace vectoriel arbitraire ou le théorème de Hahn-Banach. Dans la suite on indiquera avec un "(C)" ou un

"(CD)" dans la marge les résultats qui dépendent de l'axiome du choix (général) ou de l'axiome du choix dénombrable.

Si on revient à l'axiome du choix (standard, non dénombrable), il y a un autre endroit où on l'utilise, le plus souvent sans s'en rendre compte : la définition d'un produit arbitraire d'ensembles. Si on pense à un produit de cinq ensembles, c'est rare qu'on utilise cinq symboles différents pour les décrire ; le plus souvent on utilise le même symbole indexé par les chiffres de 1 à 5 comme $A_1, \dots, A_5$ et un élément de ce produit s'écrit comme $(a_1, a_2, a_3, a_4, a_5)$ avec $a_i \in A_i$. Si on essaye à deviner comment on définit ce cinquetuplet, on arrive vite à l'idée que c'est une application définie sur l'ensemble $I = \{1, 2, 3, 4, 5\}$ telle que l'image de $i \in I$ appartient à A_i. D'où l'idée d'un produit générale avec un ensemble I d'indices et pour tout $i \in I$ un ensemble A_i. Avec ces ingrédients on définit l'ensemble produit $\prod_{i\in I} A_i$ comme l'ensemble des applications définies sur I telles que l'image de $i \in I$ appartient à A_i. Si on doit préciser (et on le doit) dans quelle ensemble une telle application prend ses valeurs, c'est dans l'ensemble $B = \cup_{i\in I} A_i$, la réunion des A_i.

Définition. Soit I et B deux ensembles et soit $g : I \to \mathcal{P}(B)$ une application. Si on note $A_i = g(i)$ pour chaque $i \in I$, alors *le produit des ensembles A_i (quand i parcourt l'ensemble I)*, noté $\prod_{i\in I} A_i$, est défini comme l'ensemble

$$\begin{aligned}\prod_{i\in I} A_i &\overset{\text{déf}}{=} \{f : I \to B \mid \forall i \in I : f(i) \in A_i\} \\ &\equiv \{\, f \in \mathcal{P}(I \times B) \mid f : I \to B \text{ et } \forall i \in I : f(i) \in A_i \,\} \ .\end{aligned}$$

Étant donné qu'une application est complètement déterminée par les images des éléments dans son domaine de définition, on écrit parfois/souvent une telle fonction sous forme d'une liste de ses valeurs. En particulier pour $I = \{1, 2, 3, 4, 5\}$ on écrit

$$\big(f(1), f(2), f(3), f(4), f(5)\big)$$

au lieu d'écrire simplement f. Et si la liste devient trop longue ou quand on ne connaît pas vraiement un ordre sur l'ensemble I, on raccourci la liste sous la forme $\big(f(i)\big)_{i\in I}$. Il suffit maintenant de remplacer $f(i)$ par a_i pour retrouver l'écriture classique pour un multiplet ou une suite de nombres.

18.3 Proposition. *Soit I et B deux ensembles, soit $g : I \to \mathcal{P}(B)$ une application et notons $g(i) = A_i$. S'il existe $i \in I$ tel que $A_i = \emptyset$, alors $\prod_{i\in I} A_i = \emptyset$.*

18.4 Proposition. *L'axiome du choix est équivalent à l'énoncé que pour tout ensemble I et toute application $g : I \to \mathcal{P}(B) \setminus \{\emptyset\}$ le produit $\prod_{i\in I} A_i$ est non-vide, où on a noté $g(i) = A_i$.*

Terminons ce chapitre avec deux exemples empruntés de l'analyse pour montrer que l'axiome du choix facilite les choses mais n'est pas nécessairement indispensable : la notion de limite d'une suite et la limite d'une fonction définie sur $\mathbf{R}$. Soit donc $a : \mathbf{N} \to \mathbf{R}$ une suite de réels, soit $f : \mathbf{R} \to \mathbf{R}$ une application et soit $b, \ell \in \mathbf{R}$ deux

réels. Alors on a les définitions

(18.5)
$$\lim_{n\to\infty} a(n) = \ell \qquad \Longleftrightarrow \qquad \forall \varepsilon > 0 \; \exists N \in \mathbf{N} \; \forall n \in \mathbf{N} : n \geq N \;\Rightarrow\; |a(n) - \ell| < \varepsilon$$

(18.6)
$$\lim_{x\to b} f(x) = \ell \quad \Longleftrightarrow \quad \forall \varepsilon > 0 \; \exists \delta > 0 \; \forall x \in \mathbf{R} : 0 < |x - b| < \delta \;\Rightarrow\; |f(x) - \ell| < \varepsilon \;.$$

Dans les deux cas, le fait que le quantificateur existentiel vient après *le quantificateur universel implique que le N, respectivement le δ, dépend de ε. Dans certains cas on a besoin d'avoir connaissance des ces nombres pour tout les ε en même temps. Autrement dit, on a besoin d'une application qui nous donne le N, respectivement le δ, en fonction de ε.*

Dans le cas d'une suite on peut utiliser la technique de la preuve de l'axiome du choix à l'aide du théorème du bon ordre pour obtenir une telle application sans *l'axiome du choix. Pour cela on définit d'abord l'application $g : \mathbf{R}_+^* \to \mathcal{P}(\mathbf{N})$ par*

$$g(\varepsilon) = \{\, N \in \mathbf{N} \mid \forall n \in \mathbf{N} : n \geq N \;\Rightarrow\; |a(n) - \ell| < \varepsilon \,\}$$

et on constate que la définition de la limite de la suite nous garantit que $g(\varepsilon)$ n'est pas vide. On peut donc définir la fonction $f : \mathbf{R}_+^* \to \mathbf{N}$ en prenant l'élément minimal dans chaque $g(\varepsilon)$:

$$f(\varepsilon) = \min\big(g(\varepsilon)\big) \;.$$

Par définition on aura donc la propriété

$$\forall \varepsilon > 0 \; \forall n \in \mathbf{N} : n \geq f(\varepsilon) \;\Rightarrow\; |a(n) - \ell| < \varepsilon \;.$$

Dans le deuxième cas cette approche ne marche pas, car $\mathbf{R}$ n'est pas bien ordonné par l'ordre naturel : on peut toujours définir l'application $g : \mathbf{R}_+^* \to \mathcal{P}(\mathbf{R}_+^*)$ par

$$g(\varepsilon) = \{\, \delta \in \,]0, \infty[\mid \forall x \in \mathbf{R} : 0 < |x - b| < \delta \;\Rightarrow\; |f(x) - \ell| < \varepsilon \,\} \;,$$

mais on ne peut plus parler du plus petit élément dans chaque $g(\varepsilon)$. Penser à la borne inférieure n'est pas une bonne idée non plus, car on ne peut pas exclure la possibilité que la borne inférieure soit 0.

Il est évident que l'axiome du choix peut nous fournir une application $f : \mathbf{R}_+^* \to \mathbf{R}_+^*$ telle que $f(\varepsilon) \in g(\varepsilon)$, mais dans ce cas ce n'est pas nécessaire. La remarque cruciale pour le faire sans *l'axiome du choix est l'implication*

(18.7)
$$\forall \delta, \delta' \in \mathbf{R}_+^* : \big[\; \delta \in g(\varepsilon) \;\textit{et}\; \delta' < \delta \;\big] \;\Rightarrow\; \delta' \in g(\varepsilon) \;,$$

ce qui est "évident," car on a les implications

$$|x - b| < \delta' \;\textit{et}\; \delta' < \delta \;\Rightarrow\; |x - b| < \delta \;\Rightarrow\; |f(x) - \ell| < \varepsilon \;.$$

La définition nous garantit que $g(\varepsilon)$ n'est pas vide. Si cet ensemble est majoré, alors la borne supérieure existe (mais n'appartient pas forcément à $g(\varepsilon)$). Si $g(\varepsilon)$ n'est pas borné, alors forcément $g(\varepsilon) = \mathbf{R}_+^*$ car si m n'est pas un majorant, il est dedans :

$$\forall m \in \mathbf{R}_+^* \;:\; \big[\; \exists \delta \in g(\varepsilon) : \delta > m \quad \overset{(18.7)}{\Longrightarrow} \quad m \in g(\varepsilon) \;\big] \;.$$

On peut donc définir une fonction $f : \mathbf{R}_+^* \to \mathbf{R}_+^*$ par

$$f(\varepsilon) = \tfrac{1}{2} \cdot \sup\, g(\varepsilon) \quad \textit{si } g(\varepsilon) \textit{ est majoré} \qquad \textit{et} \qquad f(\varepsilon) = 1 \quad \textit{dans le cas contraire.}$$

Si $g(\varepsilon)$ n'est pas majoré, alors on a $f(\varepsilon) = 1 \in \mathbf{R}_+^* = g(\varepsilon)$. Et si $g(\varepsilon)$ est majoré, on prend $\delta' \in g(\varepsilon)$, donc $\sup\, g(\varepsilon) \geq \delta' > 0$. Il s'ensuit qu'on a les inégalités strictes $0 < \frac{1}{2} \cdot \sup\, g(\varepsilon) < \sup\, g(\varepsilon)$. Par définition de la borne supérieure il existe donc $\delta \in g(\varepsilon)$ tel que $\frac{1}{2} \cdot \sup\, g(\varepsilon) < \delta$. Avec (18.7) il s'ensuit qu'on a bien $f(\varepsilon) = \frac{1}{2} \cdot \sup\, g(\varepsilon) \in g(\varepsilon)$.

Ainsi on a donc trouvé une fonction f vérifiant $f(\varepsilon) \in g(\varepsilon)$ sans recours à l'axiome du choix.

19. La trinité du choix

19.1 Définitions. Soit E un ensemble, $\leq$ une relation d'ordre (partiel) sur E, soit $<$ la relation d'ordre stricte associée, soit $A \subset E$ un sous-ensemble et $m \in E$ un élément. On dit que m est un *majorant de* A si on a la propriété

$$\forall a \in A : a \leq m \qquad \text{(majorant de } A\text{)} \ .$$

En particulier un majorant de A est comparable avec tous les éléments de A. On dit que m est un *élément maximal de* A si m appartient à A ($m \in A$) et s'il n'y a pas d'élément plus grand dans A :

$$\forall a \in A : m \not< a \qquad \text{(élément maximal de } A\text{)} \ .$$

On dit que m est un (le) *plus grand élément de* A si m appartient à A et si tous les éléments de A sont plus petits que m :

$$\forall a \in A : a \leq m \qquad \text{(plus grand élément de } A\text{)} \ .$$

En particulier le plus grand élément de A est comparable avec tous les éléments de A, ce qui n'est pas (forcément) le cas pour un élément maximal.

Les notions de minorant, élément minimal et plus petit élément sont définies de façon analogue : m est un *minorant de* A si on a

$$\forall a \in A : m \leq a \qquad \text{(minorant de } A\text{)} \ ,$$

et si m appartient à A on dit qu c'est un *élément minimal de* A si on a

$$\forall a \in A : a \not< m \qquad \text{(élément minimal de } A\text{)}$$

et que m est le *plus petit élément de* A si on a

$$\forall a \in A : m \leq a \qquad \text{(plus petit élément de } A\text{)} \ .$$

On pourrait aussi dire que ce sont les notions de majorant, élément maximal et plus grand élément pour la relation inverse $\geq \equiv \leq^{-1}$.

19.2 Lemme. *Soit $(E, \leq)$ un ensemble partiellement ordonné, soit $A \subset E$ un sous-ensemble et soit $m \in E$ un élément.*

(i) *Si m est un plus grand élément de A (donc $m \in A$) et si $m' \in A$ est aussi un plus grand élément de A, alors $m = m'$, ce qui justifie de parler de "***le** *plus grand élément".*

(ii) *Si m est le plus grand élément de A, alors m est un élément maximal de A et un majorant de A.*

(iii) *Si l'ordre $\leq$ est total, alors m est un élément maximal de A si et seulement si m est le plus grand élément de A.*

Des résultats analogues sont valables pour les notions de minorant, élément minimal et plus petit élément.

Il est bien connu qu'un sous-ensemble n'admet pas toujours un majorant et même s'il existe un majorant, l'existence du plus grand élément n'est pas assuré. Il suffit de penser à l'ensemble $\mathbf{N} \subset \mathbf{R}$ qui n'admet pas de majorant (dans $\mathbf{R}$), ou à l'intervalle $]0, 1[\subset \mathbf{R}$ qui admet un majorant, mais n'a pas de plus grand élément. Pour apprécier la différence entre un élément maximal et le plus grand élément, on peut penser

à l'ensemble $E = \mathcal{P}(\{0,1,2\})$ des sous-ensembles de l'ensemble $X = \{0,1,2\}$ à trois éléments. On muni E de la relation d'ordre partiel donnée par l'inclusion [3.13] et on considère le sous-ensemble $A \subset E$ défini par

$$A = \{\ \{0\}, \{0,1\}, \{0,2\}\ \}\ .$$

L'élément $X \in E$ est un majorant de A (tous les éléments de A sont inclus dans X) et $\{0\}$ est le plus petit élément de A (il est inclu dans tous les éléments de A). En plus, les éléments $\{0,1\}$ et $\{0,2\}$ sont tous les deux des éléments maximaux de A, mais A ne contient pas un (le) plus grand élément : il n'y a pas un élément dans A qui contient tous les éléments de A comme sous-ensemble.

Un exemple un petit peu plus intéressant, et en plus un exemple qui montre l'intérêt de la recherche d'un élément maximal dans un ensemble partiellement ordonné, est le cas d'un espace vectoriel E (sur $\mathbf{R}$). Rappelons qu'un sous-ensemble $L \subset E$ est dit libre *ou* indépendant *s'il n'existe pas de liaisons non-triviales entre les éléments de L :*

$$\forall n \in \mathbf{N}^*\ \forall x_1, \dots, x_n \in L\ \forall \lambda_1, \dots, \lambda_n \in \mathbf{R} : \sum_{i=1}^{n} \lambda_i\, x_i = 0\ \Rightarrow\ \lambda_1 = \cdots = \lambda_n = 0\ .$$

Un sous-ensemble $G \subset E$ est dit générateur *si tout élément de E s'écrit comme une combinaison linéaire finie d'éléments de G :*

$$\forall e \in E\ \exists n \in \mathbf{N}^*\ \exists x_1, \dots, x_n \in B\ \exists \lambda_1, \dots, \lambda_n \in \mathbf{R} : e = \sum_{i=1}^{n} \lambda_i\, x_i\ . \tag{19.3}$$

Et finalement, on dit qu'un sous-ensemble $B \subset E$ est une base *pour E si B est à la fois libre et générateur. La grande question est de savoir si un espace vectoriel admet toujours une base (sans restriction sur la dimension). Pour faire le lien entre l'existence d'une base et un élément maximal dans un ensemble (partiellement) ordonné, on introduit l'ensemble $\mathcal{L} \subset \mathcal{P}(E)$ de tous les systèmes libres dans E :*

$$\mathcal{L} = \{\, L \subset E \mid L \text{ est libre} \,\}\ .$$

La remarque importante à faire est qu'un élément maximal B dans $\mathcal{L}$ est une base de E et réciproquement. Pour le voir, supposons que B est un élément maximal dans $\mathcal{L}$ et que ce n'est pas générateur. Alors il existe $e \in E$ tel qu'il n'existe pas un $n \in \mathbf{N}^*$ et cætera. Avec ce e on définit $L = B \cup \{e\}$ et on montre que $L \in \mathcal{L}$. Pour cela il faut montrer que L est libre. Prenons donc $x_1, \dots, x_n \in L$ et $\lambda_1, \dots, \lambda_n \in \mathbf{R}$ et supposons qu'on a $\sum_{i=1}^{n} \lambda_i\, x_i = 0$. Si aucun des x_i est égal à e, ils sont tous dans B, qui est un système libre (car élément de $\mathcal{L}$), donc tous les λ_i sont nuls. Si l'élément e se trouve parmi les x_i, on peut supposer sans perte de généralité que c'est x_1. Si $\lambda_1 = 0$, alors on a $\sum_{i=2}^{n} \lambda_i\, x_i = 0$. Mais les x_i avec $i \geq 2$ sont dans B, qui est libre, donc les λ_i sont nuls pour $i \geq 2$. Et si $\lambda_1 \neq 0$, on peut réécrire l'égalité $\sum_{i=1}^{n} \lambda_i\, x_i = 0$ comme

$$e \equiv x_1 = \sum_{i=2}^{n} \frac{-\lambda_i}{\lambda_1}\, x_i\ ,$$

ce qui est contraire à l'hypothèse sur $e \in E$. Il s'ensuit que L appartient à $\mathcal{L}$. Mais $B \subset L$ et $B \neq L$, ce qui contredit la maximalité de B dans $\mathcal{L}$. La conclusion est qu'un élément maximal de $\mathcal{L}$ est une base.

Réciproquement, si B est une base, B appartient à $\mathcal{L}$ car c'est libre. Mais en plus c'est maximal, car s'il existait $L \in \mathcal{L}$ tel que $B \subset L$ et $B \neq L$, alors il existe

$e \in L \backslash B$. Mais B est générateur, donc il existe $x_1, \ldots, x_n \in B \subset L$ et $\lambda_1, \ldots, \lambda_n \in \mathbf{R}$ tels qu'un a

$$e = \sum_{i=1}^{n} \lambda_i \, x_i \qquad \Longleftrightarrow \qquad (-1)\, e + \sum_{i=1}^{n} \lambda_i \, x_i = 0 \ ,$$

ce qui contredit le fait que L est libre. La conclusion est donc que B est un élément maximal dans $\mathcal{L}$.

Ainsi on a traduit la recherche d'une base pour un espace vectoriel E en une question sur l'existence d'un élément maximal dans l'ensemble partiellement ordonné $\mathcal{L}$. Et il est évident que l'ensemble $\mathcal{L}$ n'est pas totalement ordonné et qu'un élément maximal n'est pas unique : il existe des bases différentes et deux bases différentes sont incomparables pour la relation d'inclusion.

Avec en tête l'exemple d'une base d'un espace vectoriel comme élément maximal, on s'intéresse donc à la question s'il existe des critères pour décider si un ensemble partiellement ordonné admet un élément maximal. Le critère le plus connu pour décider de l'existence d'un élément maximal est le "lemme de Zorn". Malgré son nom, Zorn n'a jamais parlé d'un lemme. Dans l'article concerné [**Zor35**] *de 1935 il parle d'un "principe de maximum," et ceci dans le contexte où la relation d'ordre est l'inclusion (d'ensembles). En plus, il ne le démontre pas, il en donne des applications. Mais il promet de publier un autre article avec la preuve que ce principe est équivalent à l'axiome du choix, article qui ne sera jamais fait. Et il ignorait qu'un énoncé très analogue (aussi dans le contexte où la relation d'ordre est l'inclusion) se trouve déjà dans une publication de Kuratowski* [**Kur22**] *de 1922. Et d'autres variantes d'un tel "principe de maximum" étaient déjà publiées dès 1907, entre autres par Hausdorff. Le lecteur interessé peut trouver une étude plus détaillé de l'histoire de ce lemme dans* [**Cam78**] *; il trouvera une études de l'équivalence des ces principes dans* [**RR63**] *et* [**Kel55**].

(AC) **19.4 Lemme de Zorn.** *Soit $(X, \leq)$ un ensemble (partiellement) ordonné. Si tout sous-ensemble totalement ordonné C de X admet un majorant, alors X admet un élément maximal.*

Pour montrer le lemme de Zorn, on a, comme indiqué ci-dessus, besoin de l'axiome du choix. Mais on peut aussi déduire l'axiome du choix du lemme de Zorn, ce qui montre l'équivalence des ces deux propriétés. On démontrera cette équivalence en passant par une troisième propriété, connue sous le nom du "théorème du bon ordre". Cette propriété ne s'intéresse pas pour l'existence d'un élément maximal, mais cherche à savoir si tout sous-ensemble admet un plus petit élément, comme c'est le cas pour $\mathbf{N}$.

Définition. Soit $(E, \leq)$ un ensemble *totalement* ordonné. On dit que la relation $\leq$ est un *bon ordre* ou que E est *bien ordonné (par $\leq$)* si tout sous-ensemble non-vide $A \subset E$ admet un élément minimal :

$$\forall A \subset E \quad : \quad A \neq \emptyset \quad \Rightarrow \quad \Big[\, \exists m \in A : \forall a \in A : a \not< m \, \Big] \ .$$

19.5 Corollaire [8.17]. *La relation d'ordre sur* $\mathbf{N}$ *est un bon ordre.*

19.6 Lemme. *Soit* E *un ensemble et* $\leq \subset E \times E$ *une relation vérifiant les conditions*

(i) $\forall x, y \in E : x \leq y \text{ et } y \leq x \;\Rightarrow\; x = y,$

(ii) $\forall x, y, z \in E : x \leq y \text{ et } y \leq z \;\Rightarrow\; x \leq z$ *et*

(iii) $\forall A \subset E : A \neq \emptyset \;\Rightarrow\; \big[\exists m \in A : \forall a \in A : m \leq a\big]$.

Alors $\leq$ *est un bon ordre sur* E.

19.7 Lemme. *Soit* $\leq$ *un bon ordre sur un ensemble* E *et soit* $A \subset E$ *un sous-ensemble. Alors la relation d'ordre induite sur* A *est un bon ordre.*

Ⓟ **19.8 Lemme.** *Soit* $(E, \leq)$ *un ensemble bien ordonné. Alors il existe une (unique) application* $\min : \mathcal{P}(E) \setminus \{\emptyset\} \to E$ *qui a chaque sous-ensemble non-vide* $A \subset E$ *associe l'élément minimal de* A *:*

$$m = \min(A) \qquad \Longleftrightarrow \qquad m \in A \text{ et } \forall a \in A : m \leq a \ .$$

19.9 Corollaire/Définition. *Soit* $(E, \leq)$ *un ensemble bien ordonné. Alors il existe une unique application* $S_E : E \to E$*, appelée* l'application successeur (direct) dans E*, vérifiant*

$$\forall a \in E : a < S_E(a) \qquad \text{et} \qquad \forall a, b \in E : a < b \Rightarrow S_E(a) \leq b \ .$$

19.10 Le théorème du bon ordre. *Soit* E *un ensemble, alors il exists un bon ordre sur* E.

Ⓟ **19.11 Lemme.** *Soit* $< \subset E \times E$ *une relation quelconque sur un ensemble* E*. Alors les deux propriétés suivantes sont équivalentes.*

(i) $\forall A \subset E : A \neq \emptyset \;\Rightarrow\; \Big[\; \exists a \in A \; \forall x \in A : x \not< a \;\Big].$

(ii) $\forall B \subset E : \Big[\; \forall x \in E \;\big(\; \forall y \in E : y < x \Rightarrow y \in B \;\big) \;\Rightarrow\; x \in B \;\Big] \;\Rightarrow\; B = E.$

Si, dans [19.11], la relation $<$ *est la relation d'ordre stricte associée à une relation d'ordre (partiel), alors la propriété (i) exprime le fait que tout sous-ensemble de* E *admet un élément minimal. La propriété (ii) est connu sous le nom de* récurrence transfinie*. Elle exprime la propriété que si un sous-ensemble a la propriété dite* de récurrence (transfinie)*, alors c'est l'ensemble total. Et la propriété de récurrence transfinie dit que si pour un élément* $x \in E$ *dans l'espace total, tous les éléments "en dessous de* x*" appartiennent au sous-ensemble, alors l'élément* x *lui-même appartient au sous-ensemble.*

Dans [8.17] on a montré que $\mathbf{N}$ *a la propriété (i) (et même la propriété que tout sous-ensemble admet un plus petit élément, car l'ordre est total). Et si on regarde*

bien la preuve, on s'aperçoit vite qu'on montre effectivement la propriété (ii) par récurrence ordinaire. Regardons donc de plus près la propriété de récurrence transfinie dans ce cas. Pour cela on prend un ensemble $B \subset \mathbf{N}$ *et un élément* $n \in \mathbf{N}$ *et on suppose que tous les éléments plus petits que* n *appartiennent à* B*. Si* $n = 0$*, il n'en a pas, donc si on veut en déduire que* $n = 0$ *appartient à* B*, on doit montrer directement que* 0 *appartient à* B*. Et si* n *est plus grand que* 0*, l'ensemble des entiers strictement plus petits que* n *est l'ensemble (non-vide)* $\{0, 1, \ldots, n-1\}$*. La propriété de récurrence transfinie dit alors qu'il faut en déduire que* n *appartient à* B*. Mais si* $n > 0$*, il existe* $m \in \mathbf{N}$ *tel que* $n = m + 1$ *et l'ensemble* $\{0, 1, \ldots, n-1\}$ *s'écrit comme* $\{0, 1, \ldots, m\}$*. La propriété de récurrence transfinie dit donc qu'il faut montrer les choses suivantes :*

$$0 \in B \qquad et \qquad \forall m \in \mathbf{N} : \{0, 1, \ldots, m\} \subset B \;\Rightarrow\; m + 1 \in B \;\; .$$

Si on compare cette condition avec la propriété de récurrence ordinaire dans $\mathbf{N}$*, qu'on peut écrire sous la forme*

$$0 \in B \qquad et \qquad \forall m \in \mathbf{N} : \{m\} \subset B \;\Rightarrow\; m + 1 \in B \;\; ,$$

alors on voit que c'est quasiment la même chose, sauf que la propriété de récurrence transfinie est plus générale : si on a l'implication $\{m\} \subset B \;\Rightarrow\; m + 1 \in B$*, on a certainement l'implication* $\{0, 1, \ldots, m\} \subset B \;\Rightarrow\; m + 1 \in B$*. Étant donné qu'on a montrer la propriété du plus petit élément [8.17] à l'aide de la récurrence ordinaire, ces deux propriétés sont donc équivalentes dans* $\mathbf{N}$*. Mais l'analyse qu'on a fait dans* $\mathbf{N}$ *avec la dichotomie* $n = 0$ *ou* n *admet un prédécesseur direct* $n = m + 1$ *(il n'y a pas d'élément entre* m *et* $n = m + 1$*), cette analyse on ne peut pas le faire dans un ensemble ordonné quelconque, car il est nullement garanti qu'un prédécesseur direct existe. Pour cela il suffit de penser à deux copies de* $\mathbf{N}$ *mises l'une après l'autre dans le sens que les éléments de la deuxième copie sont tous plus grand que tous les éléments de la première copie.*

DESSIN

Formellement on regarde donc l'ensemble $\mathbf{N} \times \{1, 2\}$ *avec la relation d'ordre* $\leq$ *définie par*

$$(n, i) \leq (m, j) \qquad \Longleftrightarrow \qquad i < j \;\; ou \;\; \left[\; i = j \;\; et \; n \leq m \; \right] \;\; ,$$

où à droite on utilise la relation d'ordre déjà définie sur $\mathbf{N} \supset \{1, 2\}$*. Dans ce cas, l'élément* $0 \cong (0, 2)$ *dans la deuxième copie n'a pas de prédécesseur immédiat : dans la deuxième copie il n'y a pas un élément plus petit que* $0 \cong (0, 2)$ *et si on prend un* $n \cong (n, 1)$ *dans la première copie, ce ne peut être un prédécesseur direct, car on a les inégalités*

$$(n, 1) < (n + 1, 1) < (0, 2) \;\; .$$

Cet exemple donne aussi une explication pour l'adjectif "transfinie" : on peut franchir le cap de l'infini. Si on commence avec le 0 *dans la première copie de* $\mathbf{N}$ *et si on applique systématiquement le successeur, on reste toujours dans la première copie et on ne passe jamais dans la deuxième.*

Une autre façon de voir la différence entre la récurrence ordinaire et la récurrence transfinie est de constater qu'avec la récurrence ordinaire on démontre d'abord que le plus petit élément (à savoir 0*) appartient au sous-ensemble et que si on prend un élément de l'ensemble total vérifiant une hypothèse (à savoir qu'il est dans le sous ensemble), alors son successeur (direct) est dans le sous-ensemble. On montre donc que tous les successeurs directs sont dans le sous-ensemble. Si on veut appliquer*

ce principe à un ensemble ordonné quelconque, on ne sait pas quoi faire pour les éléments qui ne sont ni le plus petit, ni le successeur direct d'un autre élément. Et dans notre exemple, le $0 \cong (0,2)$ *dans la deuxième copie n'est pas le successeur direct d'un élément.*

Par contre, avec la récurrence transfinie, on prend un élément quelconque dans l'ensemble total vérifiant une hypothèse (à savoir que tous ses prédécesseurs sont dans le sous-ensemble) et on en déduit que l'élément lui-même est dans le sous-ensemble. De cette façon on démontre donc que tous les éléments sont dans le sous-ensemble, pas seulement les successeurs directs. Les éléments qui ne sont pas le successeur direct d'un autre élément ne sont donc pas oubliés.

Comme on a vu dans [19.11], la propriété de récurrence transfinie s'applique en principe avec n'importe quelle relation dans E*. Mais il n'est pas facile de trouver des relations qui ont cette propriété et qui ne sont pas des relation d'ordre. Et dès que la relation d'ordre est totale, on est dans la situation d'un ensemble bien ordonné telle qu'on l'a défini. L'utilisation de la récurrence transfinie est donc, dans la pratique, restreint aux ensembles bien ordonnés. Cela explique aussi pourquoi on n'a pas regardé l'ensemble* $\mathbf{R}$ *avec sa relation d'ordre usuelle comme exemple où il n'y a pas un prédécesseur direct : cet ordre n'est pas un bon ordre (le théorème du bon ordre dit qu'il en existe un, mais il n'y a personne qui le connaît). Par contre, le lecteur pourrait se convaincre facilement que l'exemple des deux copies de* $\mathbf{N}$ *l'une après l'autre est bien un ensemble bien ordonné.*

On a vu que pour la récurrence transfinie on parle de l'ensemble des prédécesseurs d'un élément donné. Cette notion est utile même en-dehors la récurrence transfinie. C'est pourquoi on introduit une notation spéciale pour un tel ensemble.

19.12 Définition. Soit $(E, \leq)$ un ensemble totalement ordonné, soit $I \subset E$ un sous-ensemble et $x \in E$ un élément. On dit que I est un *idéal* s'il vérifie la condition

$$\forall a, b \in E : a < b \text{ et } b \in I \Longrightarrow a \in I \ .$$

On définit les ensembles $E_{<x}$ et $E_{\leq x}$ par

$$E_{<x} = \{\, y \in E \mid y < x, \} \qquad \text{et} \qquad E_{\leq x} = \{\, y \in E \mid y \leq x \,\} \ .$$

Ces ensembles sont des idéaux (on dit parfois que $E_{<x}$ est un intervalle initial *ouvert* et $E_{\leq x}$ un intervalle initial *fermé*).

Il est évident que la notion d'idéal a un sens pour un ensemble ordonné quelconque, mais l'intérêt de cette notion dans le cas général est trop limité pour l'inclure dans la définition. Par ailleurs, si on regarde bien la définition des ensembles $E_{<x}$ *et* $E_{\leq x}$ *et si on fait la comparaison avec la définition de l'image réciproque par une relation, on remarque qu'on peut réécrire leurs définitions comme*

$$E_{<x} \ = \ <^{-1}[\,\{x\}\,] \qquad \textit{et} \qquad E_{\leq x} \ = \ \leq^{-1}[\,\{x\}\,] \ .$$

C'est un phénomène qu'on voit régulièrement : on introduit différentes notations pour un même objet qu'on utilisera selon les circonstances. Dans un premier temps la pluralité des notations complique la lecture. Mais les différentes notations sont adaptées aux circonstances et après une courte période de familiarisation une nouvelle notation facilite la lecture.

Dans tout ensemble totalement ordonné $(E, \leq)$ on a les deux idéaux évidents qui sont $I = E$ l'ensemble total et $I = \emptyset$ l'ensemble vide. Et en général ces idéaux ne s'écrivent pas sous la forme $E_{<x}$ ou $E_{\leq x}$ (il suffit de penser à l'ensemble des réels). Mais mêmes des cas non-triviaux ne sont pas forcément de la forme $E_{<x}$ ou $E_{\leq x}$. Un exemple est donné par l'ensemble des rationnels $\mathbf{Q}$ et l'idéal $I \subset \mathbf{Q}$ défini comme

$$I = \{\, q \in \mathbf{Q} \mid q^2 < 2 \,\} \cup \mathbf{Q}_- \ ,$$

ce qu'on écrit d'habitude comme $I = \{\, q \in \mathbf{Q} \mid q < \sqrt{2} \,\}$. Le fait que $\sqrt{2}$ n'appartient pas à $\mathbf{Q}$ entraîne qu'il n'existe pas $x \in \mathbf{Q}$ tel qu'on ait $I = \mathbf{Q}_{<x}$ ou $I = \mathbf{Q}_{\leq x}$.

19.13 Lemme. *Soit $(E, \leq)$ un ensemble bien ordonné et soit $I \subset E$ un idéal. Si $I \neq E$, alors il existe $a \in E$ tel que $I = E_{<a}$.*

19.14 Principe de récurrence transfinie. *Soit E un ensemble, soit $\leq$ un bon ordre sur E et soit $B \subset E$ un sous-ensemble vérifiant la propriété*

$$\forall x \in E \ : \ E_{<x} \subset B \ \Rightarrow \ x \in B \ .$$

Alors $B = E$.

Il y a, dans la récurrence transfinie, un aspect potentiellement troublant pour le novice : la remarque qu'il semble ne pas y avoir un début. Dans la récurrence ordinaire (sur $\mathbf{N}$) on commence à montrer que 0 apppartient au sous-ensemble et ensuite on applique le principe de récurrence : si n appartient, alors $n+1$ appartient. Pour la récurrence transfinie, il n'y a que la propriété de récurrence. Dans un ensemble bien ordonné E il existe un plus petit élément, appelons le e_o. Cet élément n'a pas de prédécesseur : l'ensemble $E_{<e_o}$ est vide. La propriété de récurrence transfinie pour $x = e_o$ nous dit donc qu'il faut montrer l'implication

$$\emptyset \subset B \ \Rightarrow \ e_o \in B \ .$$

Étant donné que la condition $\emptyset \subset B$ est toujours vraie, l'implication est vrai si et seulement si la conclusion est vraie : $e_o \in B$. Et on voit qu'on démontre explicitement que le plus petit élément de E doit appartenir au sous-ensemble B. Mais la formulation est telle, qu'il n'y a pas de différence entre le cas particulier du premier élément et un élément quelconque. Dans la pratique il arrive souvent qu'on ne s'aperçoit pas qu'il y a une différence entre le cas particulier et le cas général, mais parfois on est obligé de traiter le cas particulier du premier élément séparément.

Comme il existe une construction par récurrence (ordinaire) qui permet de construire des application sur $\mathbf{N}$, il existe une construction par récurrence transfinie qui permet de construire des applications $\varphi : E \to A$ sur un ensemble bien ordonné E. Grosso modo, pour construire une application $\varphi : \mathbf{N} \to A$ par récurrence (ordinaire), on fournit la valeur initiale $\varphi(0) = a_0 \in A$ et une application $f : A \to A$ qui dit comment on calcule φ dans un point $n \in \mathbf{N}$ qand on connaît la valeur de φ dans le prédécesseur direct $n-1$ de ce n (pour $n \neq 0$ bien sûr). Ce qui donne en formule

$$\varphi(0) = a_0 \qquad et \qquad n \neq 0 \ \Rightarrow \ \varphi(n) = f\big(\varphi(n-1)\big) \ . \tag{19.15}$$

Dans un ensemble bien ordonné, la notion d'un prédécesseur direct *n'est pas garantie. Pour construire une application $\varphi : E \to A$ sur un ensemble bien ordonné E par*

récurrence transfinie, on remplace l'idée du "prédécesseur direct" par "tous les prédécesseurs." Il faut donc remplacer (19.15) par une formule convenable. La formule qui vient naturellement à l'esprit est la suivante :

$$\varphi(x) = F\big(\ \{\,\varphi(y) \mid y < x\,\}\ \big) \equiv F\big(\ \varphi[E_{<x}]\ \big)\ ,$$

où F est la procédure qui calcule $\varphi(x)$ quand on connaît l'application φ dans tous les prédécesseurs de ce x. Écrit sous cette forme, on exprime l'idée que $\varphi(x)$ dépend de toutes les valeurs $\varphi(y)$ avec $y < x$. Il arrive parfois qu'on n'a pas seulement besoin de ces valeurs, mais aussi de l'ordre dans laquelle elles sont obtenues. On arrive donc à la formule

$$\varphi(x) = F\big(\ \varphi|_{E_{<x}}\ \big)\ , \tag{19.16}$$

qui dit que la valeur de φ en x dépend, via une procédure codée dans l'application F, de la restriction de φ à $E_{<x}$, l'ensemble des prédécesseurs de x. Cette application F doit donc être définie sur la collection de toutes les applications définies sur tous les idéaux $E_{<x}$ à valeurs dans A.

Bien sûr, il n'y a rien qui interdit que la procédure F n'utilise que les valeurs *$\varphi(y)$, $y < x$. Par exemple, on peut interpréter la construction par récurrence classique comme un cas particulier de la construction par récurrence transfinie. Pour mettre (19.15) dans le cadre de la construction transfinie (19.16), il faut donner une application F définie sur l'ensemble de toutes les application à valeurs dans A et définies sur un idéal $\mathbf{N}_{<n}$. Pour le moment on ne s'occupe pas de la question comment il faut définir cet ensemble ; on le fera dans l'énoncé exacte [19.17] de la construction par récurrence transfinie. Soit donc g une telle application. Alors il existe $n \in \mathbf{N}$ tel que g est une application de $\mathbf{N}_{<n}$ à valeurs dans A. Si $n = 0$, alors $\mathbf{N}_{<0} = \emptyset$: il n'y a pas d'éléments dans $\mathbf{N}$ (strictement) plus petit que 0. Donc on a $g : \emptyset \to A$, ce qui implique que $g = \emptyset$ [4.11]. En particulier, (19.16) se réduit à l'équation*

$$\varphi(0) = F(\emptyset)\ .$$

Si on veut avoir $\varphi(0) = a_0$, on doit donc poser $F(\emptyset) = a_0$. Par contre, si $n > 0$, alors $\mathbf{N}_{<n} = \{0, \ldots, n-1\} \neq \emptyset$. On peut donc poser

$$F(g) = f\big(g(n-1)\big)\ ,$$

c'est-à-dire que, pour obtenir la valeur de la procédure F sur l'application g, il faut prendre l'image par f de la dernière valeur prise par l'application g. La formule (19.16) se réduit donc à

$$\varphi(n) = F(\varphi|_{\mathbf{N}_{<n}}) = f\big(\varphi(n-1)\big)\ .$$

Si on applique cela à $n+1$ on obtient bien la formule $\varphi(n+1) = f\big(\varphi(n)\big)$ comme voulu par la construction par récurrence (ordinaire). Et on voit que la dichotomie entre $n = 0$ et $n > 0$ se déplace vers la définition de la procédure F : on ne le voit plus dans la construction par récurrence, mais on le voit dans la définition de F.

Ⓟ **19.17 Construction par récurrence transfinie.** *Soit $(E, \leq)$ un ensemble bien ordonné, soit A un ensemble, soit $\mathcal{H} \subset \mathcal{P}(E \times A)$ défini par*

$$\mathcal{H} = \{\,\psi \in \mathcal{P}(E \times A) \mid \exists y \in E : \psi : E_{<y} \to A\,\}$$

et soit $F : \mathcal{H} \to A$ une application. Alors il existe une et une seule application $\varphi : E \to A$ vérifiant

$$\forall x \in E\ :\ \varphi(x) = F(\varphi|_{E_{<x}})\ .$$

Il existe d'autres preuves de la construction par récurrence transfinie, mais les différences ne sont que superficielles. La façon dont on l'a écrit ici est très proche de la preuve par Dedekind de la construction par récurrence (ordinaire, voir p.41). Sa preuve de l'unicité (sur tout sous-ensemble de la forme $\{1, \dots, n\}$*) correspond à la première étape dans la preuve de [19.17]. Son hypothèse de récurrence correspond à la troisième étape. À ce stade il n'a pas besoin de la deuxième étape, car dans la récurrence ordinaire on n'utilise que le prédécesseur direct, quelque chose qui n'existe pas forcément dans un ensemble bien ordonné quelconque. Et Dedekind termine avec l'équivalent de la deuxième étape pour rassembler les résultats de sa récurrence en une application sur* $\mathbf{N}$ *entier.*

20. Ne fait qu'une

Dans le chapitre précédent on a vu trois énoncés avec des noms différents : l'axiome *du choix, le* lemme *de Zorn et le* théorème *du bon ordre. À l'aide des 7 premiers axiomes de bases, on peut montrer que ces trois énoncés sont équivalents, ce qu'on va faire dans ce chapitre. On le fait d'une façon circulaire en ajoutant une version "améliorée" du lemme de Zorn [20.1]. Le raisonnement consiste "donc" des implications*

$$\begin{array}{ccc} \textit{axiome du choix} & \Rightarrow & \textit{lemme de Zorn renforcé} \\ \Uparrow & & \Downarrow \\ \textit{théorème du bon ordre} & \Leftarrow & \textit{lemme de Zorn} \end{array}$$

20.1 Lemme de Zorn renforcé. *Soit $(X, \leq)$ un ensemble (partiellement) ordonné. Si tout sous-ensemble bien ordonné C dans X admet un majorant, alors X admet un élément maximal.*

L'idée de la preuve du lemme de Zorn (renforcé) à l'aide de l'axiome du choix est relativement facile à comprendre. On commence avec un élément $x_0 \in X$ arbitraire et on construit une chaîne $C \subset X$ (c'est-à-dire un sous-ensemble totalement ordonné) à partir de ce x_0 aussi long que possible. Tant qu'il existe un majorant strict de C (c'est-à-dire un majorant qui n'est pas dans C), on le rajoute. À la fin on aura une chaîne qui n'a plus de majorant strict de C. Par hypothèse du lemme, ce C admet un majorant, qui est donc dans C. Le fait qu'il n'y a pas un majorant strict de C implique que ce majorant de C est un élément maximal de X. L'axiome du choix intervient dans la construction de la chaîne, car s'il y a plusieurs majorants stricts, il faut en choisir un. Et cela à chaque étape de la construction. Il faut donc choisir un élément dans chaque ensemble de majorants stricts de la chaîne en construction. Étant donné qu'on ne connaît pas d'avance ces ensembles, on utilise l'axiome du choix pour choisir dans tout sous-ensemble non-vide de X un élément particulier. On applique donc l'axiome du choix à l'ensemble $\mathcal{P}(X) \setminus \{\emptyset\}$.

Mais si on commence à exécuter cette idée de preuve, on se heurte au problème qu'on ne connaît pas la longueur de la chaîne et que "donc" une construction par récurrence n'aboutit pas forcément. On va donc regarder tous les bouts de chaînes bien ordonné (c'est l'aspect renforcé du lemme) qui sont construits de la façon indiquée. Et pour reconnaître ces bouts de chaînes, on utilise la tautologie qu'un élément de la chaîne est l'élément qui suit tous les éléments qui le précèdent. Et la construction de la chaîne nous dit que cet élément est l'élément choisi dans l'ensemble de tous les majorants stricts de l'ensemble de ces précédants. La partie la plus longue de la preuve est de montrer que tous ces bouts sont le début d'une même *chaîne bien ordonné. Une fois qu'on dispose de l'ensemble de tous ces bouts de chaînes on en prend le plus grand (la réunion de tous les bouts) et on aura notre chaîne recherchée. Son majorant sera un élément maximal de X.*

Ⓟ **20.2 Lemme.** *Soit $(E, \leq)$ un ensemble bien ordonné et soit $\mathcal{J} \subset \mathcal{P}(E)$ une collection d'idéaux :*

$$\forall I \in \mathcal{J} : I \text{ est un idéal de } E.$$

Alors la réunion $\cup\, \mathcal{J}$ est un idéal.

Pour trouver un bon ordre sur un ensemble E avec le lemme de Zorn, il faut le réaliser comme un élément maximal dans un certain ensemble partiellement ordonné $\mathcal{B}$. L'idée est de prendre tous les sous-ensembles de E qu'on peut munir d'un bon ordre ; plus précisément, un élément de $\mathcal{B}$ est un sous-ensemble de E muni d'un bon ordre. On dira qu'un tel sous-ensemble A est plus petit qu'un autre B si on a l'inclusion $A \subset B$ et *si les relations d'ordre coïncident. Par exemple, si $a, b, c \in E$ sont trois éléments distincts, alors on peut munir le sous-ensemble $A = \{a, b\}$ de deux façons d'une relation d'ordre : on peut dire qu'on a $a < b$ et on peut dire qu'on a $b < a$. Cela nous donne* deux *éléments distincts de $\mathcal{B}$; appelons les A_1 pour l'ordre $a < b$ et A_2 pour l'ordre $b < a$. Ces deux ensembles sont donc* incomparable *pour notre relation d'ordre sur $\mathcal{B}$, car, bien qu'on a l'inclusion dans les deux sens, les relations d'ordre ne coïncident pas. Et si on considère l'ensemble $B = \{a, b, c\}$ muni de la relation d'ordre $a < b < c$, alors cet ensemble* avec cette relation d'ordre *est plus grand, dans $\mathcal{B}$, que l'ensemble A_1* avec sa relation d'ordre *$a < b$. Par contre, ce B n'est pas comparable avec A_2, car les relations d'ordre ne correspondent pas.*

L'idée suivante est que si on a un sous-ensemble totalement ordonné $\mathcal{C} \subset \mathcal{B}$ de cette collection $\mathcal{B}$ de sous-ensembles de E muni d'un bon ordre, alors la réunion sera encore un sous-ensemble qu'on peut munir d'un bon ordre. La condition du lemme de Zorn sera donc vérifiée et il existe un élément maximal. Si un élément maximal n'est pas l'ensemble total E, on peut ajouter un élément qu'on déclare plus grand que tous les autres. Ainsi on aura obtenu un sous-ensemble strictement plus grand, ce qui contredit la maximalité. Donc l'élément maximal est l'ensemble total, muni d'un bon ordre *et donc l'ensemble total peut être muni d'un bon ordre.*

Quand on commence à mettre ces idées au propre, on s'aperçoit vite qu'on ne peut pas montrer que la réunion (des éléments d'un sous-ensemble totalement ordonné de $\mathcal{B}$) est de nouveau muni d'un bon ordre (c'est l'aspect "existence d'un élément minimal pour un sous-ensemble non-vide" qui fait défaut). Pour remédier la situation, il faut changer, pas l'ensemble $\mathcal{B}$ même, mais la relation d'ordre sur $\mathcal{B}$ en étant plus restrictif. Si A et B sont deux éléments de $\mathcal{B}$, donc des sous-ensembles de E munis d'un bon ordre, il ne suffit pas d'exiger qu'on a l'inclusion $A \subset B$ et que la restriction de la relation d'ordre sur B au sous-ensemble A est la relation d'ordre sur A, pour pouvoir dire que l'élément A est plus petit que l'élément B dans $\mathcal{B}$. Il faut rajouter la condition que les éléments de B qui ne sont pas dans A sont tous plus grand que tous les éléments de A. Avec cette nouvelle définition d'une relation d'ordre sur $\mathcal{B}$, on peut montrer que la réunion est un sous-ensemble muni d'un bon ordre, ce qui permet de finaliser la preuve.

Quant'à la réalisation explicite de l'ensemble $\mathcal{B}$, on commence avec l'idée qu'un élément de $\mathcal{B}$ est un sous-ensemble $A \subset E$ de l'ensemble total, muni d'une relation

d'ordre $\leq_A$. Mais une relation d'ordre est un sous-ensemble du produit $A \times A$, qui est inclus dans $E \times E$. On a donc deux objets pour caractériser l'élément de $\mathcal{B}$: un sous-ensemble $A \subset E$ et un sous-ensemble $\leq_A \subset E \times E$ vérifiant des conditions (à savoir $\leq_A \subset A \times A$ et d'être un bon ordre sur A). Mais quand on connaît le sous-ensemble $\leq_A \subset E \times E$, on connaît le sous-ensemble $A \subset E$; on peut le définir par exemple comme

$$A = \{\, x \in E \mid (x,x) \in \leq_A \,\} \qquad ou \qquad A = \{\, x \in E \mid \exists y \in E : (x,y) \in \leq_A \,\} \ .$$

Le seul sous-ensemble $\leq_A \subset E \times E$ suffit donc pour caractériser le sous-ensemble $A \subset E$ et *le bon ordre sur A. En plus, la relation d'ordre sur $\mathcal{B}$ (avant la version plus restrictive) se traduit par la simple inclusion de ces relations d'ordre : un sous-ensemble bien ordonné $(A, \leq_A)$ est plus petit qu'un sous-ensemble bien ordonné $(B, \leq_B)$ si et seulement si on a l'inclusion $\leq_A \subset \leq_B$ (comme sous-ensembles de $E \times E$). En suivant les idées décrites ci-dessus, la preuve du théorème du bon ordre à partir du lemme de Zorn n'est pas difficile ; elle est seulement longue à cause des multiples vérifications qu'il faut effectuer.*

La preuve de l'axiome du choix à l'aide du théorème du bon ordre est la généralisation directe de l'exemple décrit p.121, où on a construit une fonction de choix (sans l'axiome du choix) à l'aide du plus petit élément dans chaque sous-ensemble de $\mathbf{N}$. *Pour le cas général on fait la même chose à l'aide du théorème du bon ordre. Selon ce théorème il existe un bon ordre sur n'importe quel ensemble. On en prend un et on définit la fonction de choix comme le plus petit élément dans chaque sous-ensemble.*

La fonction de choix qu'on obtient à l'aide du théorème du bon ordre n'est pas complètement général dans le sens qu'il existe des fonctions de choix qu'on ne peut pas obtenir à l'aide du théorème du bon ordre comme ci-dessus. Plus précisément, la fonction de choix obtenue à l'aide du théorème du bon ordre dépend du choix du bon ordre sur l'ensemble B : si on change le bon ordre, la notion du plus petit élément change et donc la fonction $f = \min \circ g$ aussi. Par contre, il existe des fonctions de choix $f : I \to B$ qui ne s'écrivent pas sous la forme $f = \min \circ g$ pour un bon ordre bien choisi. Un exemple très simple est donné par l'ensemble $I = \{0,1\}$ consistant de deux éléments et une application $g : I \to \mathcal{P}(B) \setminus \{\emptyset\}$ constante : $g(0) = g(1) \subset B$. Une fonction de choix "arbitraire" $f : I \to B$ peut choisir deux éléments différents : $f(0) \neq f(1)$, mais pour n'importe quel bon ordre sur B, les images $(\min \circ g)(0)$ et $(\min \circ g)(1)$ seront toujours les mêmes.

Chapitre 4

Comparer la taille d'ensembles

21. Introduction

Quand on veut comparer la taille de deux ensembles A et B, une idée qui vient à l'esprit (surtout après les travaux de Dedekind et Cantor) est de dire qu'ils ont la même taille s'il existe une bijection $f : A \to B$. Mais comment peut-on donner un nom à la taille d'un ensemble ? Pour un ensemble fini on a résolu ce problème par le cardinal : l'entier naturel qui indique le nombre d'éléments dans l'ensemble, ou encore, l'unique entier naturel qui est en bijection avec l'ensemble. Pour l'instant on n'a pas de noms pour les ensembles infinis, quoi que...peut-être le seul nom "infini" suffit ! Peut-être tous les ensembles infinis sont en bijection l'un avec l'autre. Malheureusement (ou heureusement, ça dépend de son point de vue) ce n'est pas le cas : on peut montrer qu'il y a des ensembles infinis qui ne sont pas en bijection. Et effectivement, on a déjà vu que l'ensemble des nombres réels entre 0 *et* 1 *n'est pas en bijection avec les entiers naturels.*

On revient donc à la case de départ : comment donner un nom à la taille d'un ensemble ? On se rend vite compte que la notion de "même taille" est une relation d'équivalence. Et on pourrait penser à notre description d'une relation d'équivalence comme un collectionneur de billes qui range ses billes dans des boîtes selon la couleur. Quand on ferme ces boîtes, alors chaque boîte représente une couleur. Si on fait la même chose avec la notion de taille, on met tous les ensembles de même taille dans une boîte et quand on ferme la boîte, c'est la boîte qui représente la taille : chaque boîte correspond à une taille unique d'ensembles. C'est un peu un tour de passe-passe, car on n'a pas vraiment donné un nom à la taille. Par contre, on a quand même associé un objet unique à chaque ensemble : la boîte dans laquelle il se trouve avec les autres ensembles de même taille.

Mais malheur ! on n'a pas le droit de le faire ainsi, car le contenu d'une boîte, la collection de tous les ensembles de même taille, n'est pas un ensemble[1]*. On n'a donc pas le droit de parler d'une telle boîte. Heureusement il existe, dans l'axiomatique de Zermelo, (au moins) deux solutions pour contourner ce problème. Et ces deux solutions ont une ressemblance très forte avec la façon dont les élèves apprennent à calculer avec les nombres rationnels (positifs). Officiellement un nombre rationnel positif est une classe d'équivalence de couples d'entiers. Mais dans chaque boîte, c'est-à-dire classe d'équivalence, on arrive à désigner un représentant unique : pour chaque rationnel positif $r \in \mathbf{Q}_+$ il existe un unique couple $(p, q) \in \mathbf{N} \times \mathbf{N}^*$ tel que $r = p/q$ (on devrait écrire $(p, q) \in r$) et tel que le pgcd de p et q soit* 1*. Ainsi on a une écriture unique de chaque rationnel positif comme quotient de deux entiers. Les*

1. Il semble, mais je suis trop ignorant pour en dire plus, que dans l'axiomatique de Bernays-Gödel-Von Neumann on peut parler de collections qui sont plus grandes que des ensembles.

élèves apprennent donc que la réponse

$$\frac{173}{3} \times \frac{2}{173} = \frac{346}{519}$$

est "fausse" ou incomplète et que la réponse

$$\frac{173}{3} \times \frac{2}{173} = \frac{346}{519} = \frac{2}{3}$$

est "juste." Ce qu'on fait est la chose suivante : dans chaque boîte/classe d'équivalence on a choisi un élément type et c'est le nom de cet *élément qu'on met sur la boîte. On a donc une boîte avec le nom* $1/2$ *et une boîte avec le nom* $3/7$*, mais on n'a pas de boîte avec le nom* $3/6$*. Par contre, le couple* $3/6$ *appartient à la boîte avec le nom* $1/2$*. Et le couple* $1/2$ *appartient* aussi *à la boîte avec le nom* $1/2$*. C'est comme le font certains marchands de billes : ils n'écrivent pas le nom "vert" sur la boîte contenant les billes vertes, mais il collent une bille verte sur la boîte pour montrer que c'est ce type de billes qui est dans la boîte.*

D'autre part, quand on avance un peu dans les études scientifiques, quand on a bien appris à calculer avec les nombres rationnels, on laisse tomber cette exigence de "simplification" du quotient. On laisse le couple $3/6$ *sans le "changer" en* $1/2$*. Autrement dit, tant qu'on ne fait pas des calculs "formels" avec des lettres, on continue à écrire des couples d'entiers (sous la forme* p/q *au lieu de* (p, q)*, mais cela n'est qu'une question de notation), sans donner un nom unique à une classe d'équivalence. Ou encore : on calcule avec des couples d'entiers sans faire référence à des classes d'équivalences, donc sans parler des boîtes. Ce qui est d'autant plus justifié par le fait que les opérations avec des boîtes (les nombres rationnels) sont définies en termes des couples d'entiers et qu'on a dû montrer que ces opérations en termes des couples d'entiers induisent bien des opérations sur les boîtes, c'est-à-dire sur l'ensemble des classes d'équivalence.*

Pour la notion de "taille d'un ensemble" la démarche sera analogue. Dans chaque boîte avec les ensembles de même taille (mais ces boîtes ne sont pas des ensembles) on trouve un ensemble type qu'on utilise comme "nom" pour la boîte. Et pour définir des opérations sur ces boîtes, comme l'addition de tailles ou la multiplication de tailles, on définit (a déjà défini) des opérations sur les ensembles et on montre que ces opérations sont compatibles avec la relation d'équivalence "même taille" (qui n'est donc pas une relation d'équivalence sur un ensemble). Un début de ce programme a déjà été fait pour les ensembles finis dans §25, où on a associé à un ensemble fini un entier naturel, appelé "le cardinal de l'ensemble." En termes de nos boîtes, s'il y a un ensemble fini dans la boîte, alors cette boîte contient un unique entier naturel qu'on colle comme nom sur cette boîte. Entre parenthèses, sans l'axiome du choix (dénombrable) on ne peut pas exclure qu'il y a des boîtes avec des ensembles finis qui ne contiennent pas un entier naturel.

Notre programme se déroulera de la façon suivante. On commence, bien évidemment, avec la preuve que la notion de taille est une relation d'équivalence (ou plutôt, a toutes les propriétés d'une relation d'équivalence, car elle n'est pas définie sur un ensemble mais sur la collection de tous les ensembles). Et on introduit une notion de relation d'ordre qui permet de comparer des tailles. Ensuite on montre que le produit cartésien de deux ensembles est compatible avec cette relation d'équivalence, ainsi que la réunion (disjointe) et que ces deux opérations ont toutes les propriétés d'une multiplication et d'une addition associative et commutative avec éléments neutres. Dans §24 on justifiera que l'opération App *(qui à deux ensembles* A *et* B *associe*

l'ensemble $\mathrm{App}(A, B)$ *de toutes les applications de* A *dans* B*) a toutes les propriétés d'une exponentielle.*

Muni de ces résultats, le lecteur ne devrait pas être surpris que, pour des ensembles finis, le passage d'un ensemble à son cardinal (le nombre d'éléments, la taille, un élément de $\mathbf{N}$*) fait correspondre les opérations de réunion (disjointe), produit cartésien et* App *aux opérations d'addition, multiplication et exponentiation définies sur* $\mathbf{N}$*. Par contre, dès qu'on passe aux ensembles infinis, il y a quelques petites surprises en ce qui concerne la relation d'ordre. Pour les entiers naturels on sait que* $n > 1$ *implique* $n \times n > n$*. Mais ce résultat n'est plus vrai pour les ensembles infinis (à condition d'accepter l'axiome du choix) : si on prend un ensemble infini, alors la taille du produit avec lui-même est égale à la taille de l'ensemble. On l'a déjà vu pour l'ensemble* $\mathbf{N}$ *où on a exhibé une bijection entre* $\mathbf{N} \times \mathbf{N}$ *et* $\mathbf{N}$*.*

Pour trouver dans chaque classe d'équivalence un ensemble type unique qu'on peut utiliser comme "nom" de la boîte, on fera un détour par les ordinaux. Les ordinaux sont des ensembles avec des propriétés particulières et parmi les ordinaux il y en a avec des propriétés encore plus particulières et qu'on appelle des cardinaux. Les entiers naturels sont un cas particulier de cardinaux, mais il y en a d'autres (comme l'ensemble $\mathbf{N}$*). À l'aide de l'axiome du choix (et l'axiome de remplacement qu'on n'a pas encore vu) on peut montrer que dans chaque classe d'équivalence (par rapport à la relation "même taille") il y a un unique cardinal. Ce qui nous donne un ensemble représentatif pour la taille de tous les ensembles dans cette boîte/classe d'équivalence. Chaque cardinal représente donc une taille d'ensembles et chaque ensemble est associé à un cardinal de même taille. Et quand on traduit nos opérations de réunion (disjointe), produit cartésien en "applications entre ensembles" en termes des cardinaux, on parlera de l'arithmétique des cardinaux, avec addition, multiplication et exponentiation de cardinaux.*

La seule chose qu'on ne peut pas faire dans toute cette histoire est de dire que nos opérations sont définies sur un ensemble, car même la collection des cardinaux est trop grande pour être un ensemble. Mais cela n'est pas un vrai inconvénient : c'est comme pour les opérations de réunion, intersection ou produit cartésien. Ça ne gêne personne qu'on ne peut pas dire, par exemple, que la réunion est une application

$$\cup : \mathcal{E} \times \mathcal{E} \to \mathcal{E} \ ,$$

où $\mathcal{E}$ *désigne la collection de tous les ensembles. On n'a pas le droit de l'écrire (si on ne veut écrire que des ensembles). Mais personne nous empêche de le penser !*

22. Applications injectives et surjectives

Ⓟ **22.1 Proposition (Cantor-Bernstein-Schröder)** [4]**.** *Soit A et B deux ensembles. S'il existe une injection $f : A \to B$ et une injection $g : B \to A$, alors il existe une bijection $h : A \to B$.*

Une idée pour la preuve[5] *est assez simple : on coupe A et B en deux morceaux*

$$A = X \cup (A \setminus X) \qquad \text{et} \qquad B = Y \cup (B \setminus Y)$$

d'une telle façon qu'on a

$$f[X] = B \setminus Y \qquad \text{et} \qquad g[Y] = A \setminus X \ . \tag{22.2}$$

Si cela marche, on invoque [??] pour en déduire que f établit une bijection entre X et $f[X]$ et g établit une bijection entre Y et $g[Y]$, donc g^{-1} établit une bijection entre $g[Y] = A \setminus X$ et $Y = B \setminus f[X]$. Ensemble ces applications forment donc une bijection entre A et B.

On présentera deux façons différentes de construire de tels ensembles X et Y. Dans la première façon on construit (par récurrence) des approximations successives C_n de X et D_n de Y, basées sur l'observation qu'on a les égalités

$$Y = B \setminus f[X] \qquad \text{et} \qquad X = A \setminus g[Y] \ .$$

On commence avec une première approximation $C_0 = A$. Si c'était le bon choix, on devrait avoir $Y = B \setminus f[C_0]$. On prend donc comme première approximation pour Y l'ensemble $D_0 = B \setminus f[C_0]$. Et si ce D_0 était le bon choix pour Y, on devrait avoir $X = A \setminus g[D_0]$, ce qui suggère de prendre comme deuxième approximation pour X l'ensemble $C_1 = A \setminus g[D_0]$. Et on continue avec ce zig-zag entre A et B pour obtenir une suite d'approximations pour X et Y :

$$\begin{array}{ccc}
C_0 = A & \xrightarrow{\ f\ } & f[C_0] \\
 & & \Downarrow \\
g[D_0] & \xleftarrow{\ g\ } & B \setminus f[C_0] = D_0 \\
\Downarrow & & \\
C_1 = A \setminus g[D_0] & \xrightarrow{\ f\ } & f[C_1] \\
 & & \Downarrow \\
g[D_1] & \xleftarrow{\ g\ } & B \setminus f[C_1] = D_1 \\
\Downarrow & & \\
\cdots & &
\end{array}$$

4. Dans la littérature on retrouve ce résultat sous le nom de "théorème de Cantor-Bernstein" ou de "théorème de Bernstein-Schröder." Ce résultat était mentionné comme question dans un texte de Cantor et des preuves furent publiés indépendamment par Felix Bernstein et E. Schröder (en 1898). En 1911 A. Korselt signalait une erreur dans la preuve de Schröder [**Kor11**] ; il citait aussi une correspondance avec Schröder qui était au courant de l'erreur et qui attribuait ce résultat à Bernstein. La première preuve correcte publiée est donc due à Bernstein. Dedekind l'avait déjà démontré en 1887, mais il n'avait jamais publié son résultat (voir [**Bou07**]).

5. Le lecteur curieux trouvera une autre type de preuve dans [**AZ98**].

Ce qui est remarquable est que ces deux suites "convergent" et donnent une solution pour les ensembles X et Y.

La deuxième façon part de l'observation que si X et Y satisfont (22.2), alors on a l'implication

$$f[X] \subset f[A] \qquad \Longrightarrow \qquad B \setminus f[A] \subset B \setminus f[X] = Y \ ,$$

ainsi que l'implication

$$g[Y] \cap X = \emptyset \quad \Longrightarrow \quad f\big[g[Y]\big] \cap f[X] = \emptyset \quad \Longrightarrow \quad f\big[g[Y]\big] \subset B \setminus f[X] = Y \ .$$

L'ensemble Y doit donc vérifier au moins les deux conditions

$$B \setminus f[A] \subset Y \qquad et \qquad f\big[g[Y]\big] \subset Y \ .$$

Avec cette observation on définit Y comme le plus petit sous-ensemble de B vérifiant les deux conditions ci-dessus. Ce qui est remarquable ici est que si Y est ce plus petit sous-ensemble et si on pose $X = A \setminus g[Y]$, alors on a trouvé une solution pour (22.2).

À titre d'exercice le lecteur pourrait essayer de montrer que ces deux façons de trouver des ensembles X et Y vérifiants (22.2) conduisent au même résultat, mais qu'en toute généralité on n'a pas unicité d'un tel couple.

Remarque. La différence entre les deux constructions données dans la preuve de [22.1] est que la première construction utilise la récurrence, et donc implicitement l'axiome de l'infini, ce qui n'est pas le cas pour la deuxième construction.

Ⓟ **22.3 Lemme.** *Soit A et B deux ensembles non-vides et $f : A \to B$ une injection. Alors il existe une surjection $g : B \to A$ vérifiant $g \circ f = id_A$.*

Si A est un ensemble dénombrable non-vide, il existe (par [22.3]) une application surjective $g : \mathbf{N} \to A$. Cette application peut s'interpréter comme un "dénombrement" de l'ensemble A comme $a_0 = g(0)$, $a_1 = g(1)$, $a_2 = g(2)$, et cætera. Le fait que g est surjective garantit qu'on passe au moins une fois par chaque élément de A. Mais il n'est pas exclu qu'on passe plusieurs fois par le même élément de A.

(AC)Ⓟ **22.4 Proposition.** *L'axiome du choix est équivalent à la propriété que pour toute surjection $g : B \to A$ il existe une injection $f : A \to B$ vérifiant $g \circ f = id_A$.*

(AC)Ⓟ **22.5 Proposition.** *Soit A et B deux ensembles. S'il n'existe pas une injection $f : A \to B$, alors il existe une injection $g : B \to A$.*

23. Définition de la comparaison

Comme on a argumenté dans §21, on dira que deux ensembles ont la même taille quand il existe une bijection entre eux. Pour préparer le changement de perspective que cela représente une relation d'équivalence, on introduit une notation alternative pour dire cela. Et si on parle de comparer des tailles, on voudrait aussi pouvoir dire qu'un ensemble est "plus petit en taille" qu'un autre ensemble. Naïvement un ensemble A est plus petit ou égal à un ensemble B si A a la même taille qu'un sous-ensemble de B. En termes d'applications ceci se traduit comme l'existence d'une injection $f : A \to B$, au quel cas A sera de même taille que l'image $C = f[A] \subset B$. Et pour cette notion on introduit aussi une notation alternative.

→ **23.1 Lemme.** *Soit A et B deux ensembles. Alors il existe une injection $f : A \to B$ si et seulement s'il existe un sous-ensemble $C \subset B$ et une bijection $g : A \to C$.*

Notation alternative. Soit A et B deux ensembles. On écrit $A \approx B$ pour dire qu'il existe une bijection entre A et B :

$$A \approx B \qquad \overset{\text{déf.}}{\iff} \qquad \exists f : A \to B \text{ , } f \text{ une bijection.}$$

Et on écrit $A \precsim B$ pour dire qu'il existe une injection de A dans B :

$$A \precsim B \qquad \overset{\text{déf.}}{\iff} \qquad \exists f : A \to B \text{ , } f \text{ une injection.}$$

On prononce la formule $A \approx B$ comme "A a la même taille que B," et on prononce la formule $A \precsim B$ comme "A est plus petit en taille que B."

23.2 Lemme. *Le symbole $\approx$ a les propriétés d'une relation d'équivalence [9.1] : si A, B et C sont trois ensembles, alors on a*

(i) $A \approx A$,

(ii) $A \approx B \;\Leftrightarrow\; B \approx A$ *et*

(iii) *si* $A \approx B$ *et* $B \approx C$, *alors* $A \approx C$.

23.3 Lemme. *Le symbole $\precsim$ a les propriétés d'une relation compatible (dans le sens [9.14]) avec la relation d'équivalence $\approx$: si A, A', B et B' sont quatre ensembles, alors on a*

$$A \approx A' \text{ et } B \approx B' \qquad \Longrightarrow \qquad [\, A \precsim B \;\Leftrightarrow\; A' \precsim B' \,] \;.$$

23.4 Lemme. *La "relation" induite par le symbole $\precsim$ sur les "classes d'équivalence" du symbole $\approx$ a toutes les propriétés d'une relation d'ordre partiel : si A, B et C sont trois ensembles, alors on a*

(i) $A \precsim A$,

(ii) $[\, A \precsim B$ *et* $B \precsim A \,] \iff A \approx B$ *et*

(iii) *si* $A \precsim B$ *et* $B \precsim C$, *alors* $A \precsim C$.

Une fois qu'on a montré qu'on a une relation d'équivalence et une relation d'ordre, on aborde la question comment les opérations de réunion et de produit cartésien se comportent vis-à-vis ces relations. On commence avec le produit cartésien qui est le plus simple.

23.5 Lemme. *Soit A, A', B et B' quatre ensembles vérifiant $A \precsim A'$ et $B \precsim B'$. Alors on a $A \times B \precsim A' \times B'$.*

23.6 Corollaire. *Le produit cartésien $\times$ est compatible (dans le sens [9.14]) avec la relation d'équivalence $\approx$: si A, A', B et B' sont quatre ensembles vérifiant $A \approx A'$ et $B \approx B'$, alors on a $A \times B \approx A' \times B'$.*

Rappel. Les symboles 0, 1 et 2 sont des abréviations pour les ensembles

$$0 = \emptyset \quad , \quad 1 = \{0\} \equiv \{\emptyset\} \quad , \quad 2 = \{0, 1\} \equiv \big\{ \emptyset, \{\emptyset\} \big\} \ .$$

23.7 Lemme. *Soit A un ensemble.*

(i) $A = \emptyset \iff 0 \approx A$.

(ii) $A \neq \emptyset \iff 1 \precsim A$.

23.8 Lemme. *Soit A, B et C trois ensembles.*

(i) $0 \times A = 0$ *et donc a fortiori* $0 \times A \approx 0$.

(ii) $1 \times A \approx A$.

(iii) $A \times B \approx B \times A$.

(iv) $A \times (B \times C) \approx (A \times B) \times C$.

[23.8] suggère fortement que le produit cartésien (de deux ensembles) joue le rôle d'une multiplication commutatif avec 1 comme élément neutre. Il est donc tout-à-fait naturel de se poser la question s'il existe une opération ensembliste qui fait office d'addition, surtout quand on voit le comportement de l'ensemble vide vis-à-vis la multiplication : s'il existe un équivalent pour l'addition, 0 doit être l'élément neutre. Et la réponse semble être évidente : la réunion. Sauf que la réunion n'a pas les propriétés qu'on attend quand on pense à la taille : si A et B sont deux ensembles finis qui ne sont pas disjoints, alors le nombre d'éléments dans $A \cup B$ n'est pas la somme du nombre d'éléments dans A et le nombre d'éléments dans B. Ça ne marche que si A et B sont disjoints. C'est pour cela qu'on introduit l'opération de la "réunion disjointe." Ce n'est pas une vraie réunion, mais cette opération jouera le rôle d'addition.

23.9 Lemme. *Soit A et B deux ensembles, alors $A \times \{0\} \cap B \times \{1\} = \emptyset$.*

Définition. La *réunion disjointe de deux ensembles A et B*, notée $A \sqcup B$, est définie par

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

Nota Bene. Dans des circonstances "normales" le fait de prendre le produit avec $\{0\}$ et $\{1\}$ garantit qu'il n'y a pas d'intersection entre $A \cup B$ d'une part et $A \sqcup B$ d'autre part. Mais on ne peut pas l'affirmer en général. Il suffit de prendre $B = A \times \{0\}$, au quel cas on aura

$$A \cup B = A \cup A \times \{0\} \qquad \text{et} \qquad A \sqcup B = A \times \{0\} \cup (A \times \{0\}) \times \{1\} \ .$$

Il s'ensuit qu'on a l'inclusion

$$A \times \{0\} \subset \big(A \cup B\big) \cap \big(A \sqcup B\big) \ .$$

Mais attention, ce n'est qu'une inclusion ! Cette intersection peut être plus grande encore. Il suffit de penser que pour un certain $a \in A$ on a aussi $((a,0),1) \in A$, au quel cas ce dernier élément (qui n'appartient pas à $A \times \{0\}$) appartient aussi à $(A \times \{0\}) \times \{1\}$ et donc à cette intersection.

23.10 Lemme. *Soit A, A', B et B' quatre ensembles vérifiant $A \precsim A'$ et $B \precsim B'$. Alors on a $A \sqcup B \precsim A' \sqcup B'$.*

23.11 Corollaire. *La réunion disjointe $\sqcup$ est compatible (dans le sens [9.14]) avec la relation d'équivalence $\approx$: si A, A', B et B' sont quatre ensembles vérifiant $A \approx A'$ et $B \approx B'$, alors on a $A \sqcup B \approx A' \sqcup B'$.*

Il est presque immédiat de voir que l'opération de réunion ordinaire n'est pas compatible avec la relation d'équivalence $\approx$. Il suffit de considérer l'exemple suivant : $A = \{0\}$, $A' = \{1\}$, $B = \{0\}$, $B' = \{2\}$ *et donc* $A \cup B = \{0\}$, $A' \cup B' = \{1,2\}$, *au quel cas on a*

$$A \approx A' \quad , \quad B \approx B' \qquad \text{et} \qquad A \cup B \not\approx A' \cup B' \ .$$

D'autre part, le nom "réunion disjointe" pour l'opération $\sqcup$ est entièrement justifié par [23.12.ii].

23.12 Lemme. *Soit A, B et C trois ensembles.*

(i) $A \cup B \precsim A \sqcup B$.

(ii) *Si* $A \cap B = \emptyset$, *alors* $A \cup B \approx A \sqcup B$.

(iii) $A \sqcup 0 = A$ *et donc a fortiori* $A \sqcup 0 \approx A$.

(iv) $A \sqcup B \approx B \sqcup A$.

(v) $A \sqcup (B \sqcup C) \approx (A \sqcup B) \sqcup C$.

(vi) $A \times (B \sqcup C) \approx (A \times B) \sqcup (A \times C)$.

(vii) $2 \times A \approx A \sqcup A$.

Si on regarde les résultats [23.8] et [23.12] on a bien l'impression que les opérations de "réunion disjointe" et de "produit cartésien" jouent le rôle d'addition et de multiplication avec $0 \equiv \emptyset$ *l'élément neutre pour "l'addition" et* $1 \equiv \{\emptyset\}$ *l'élément neutre pour la "multiplication." Dans §25 on verra que, pour des ensembles finis, ces opérations correspondent vraiment à l'addition et à la multiplication.*

24. L'exponentielle d'ensembles

Dans §23 on a vu que la réunion disjointe et le produit cartésien peuvent jouer le rôle d'addition et de multiplication. Reste la question s'il y a un équivalent pour l'exponentiation. Un début de réponse se trouve dans l'écriture bien connue A^2 pour l'ensemble $A \times A$. Plus généralement on note A^n le produit cartésien n-fois pour $n \in \mathbf{N}^*$. Sauf que...on n'a pas défini un tel produit pour $n > 2$. Par exemple A^3, faut-il le définir comme $A \times (A \times A)$ ou comme $(A \times A) \times A$? Ces deux possibilités ne sont pas les mêmes : pour la première possibilité, un élément est un couple dont la première composante est un élément de A, tandis que pour la deuxième possibilité, un élément est un couple dont la première composante est un élément de $A \times A$. Selon les circonstances, on peut opter pour l'une ou l'autre solution. Et plus généralement on peut définir par récurrence l'ensemble A^n soit par

$$A^1 = A \qquad et \qquad A^{n+1} = A \times A^n \ ,$$

ce qui correspond à la première approche, soit par

$$A^1 = A \qquad et \qquad A^{n+1} = A^n \times A \ ,$$

ce qui correspond à la deuxième approche.

Bien sûr, il y a des bijections "évidentes" entre les deux façons de définir A^n. Et dans la pratique, on n'écrit jamais $((a_0, a_1), a_2)$ ou $(a_0, (a_1, a_2))$ pour un triplet, mais simplement (a_0, a_1, a_2), sans se soucier quelle solution on a pris. Et ce n'est pas seulement par paresse qu'on agit ainsi, mais aussi parce qu'il y a une tout autre façon de définir les n-uplets, éléments de A^n. Naïvement tout le monde sait ce que c'est un n-uplet : un n-uplet est une liste $(a_0, a_1, \dots, a_{n-1})$ telle que pour tout $i \in \{0, \dots, n-1\}$ on a $a_i \in A$. Autrement dit, pour décrire un n-uplet, il faut préciser pour chaque indice $i \in \{0, \dots, n-1\} = n$ un élément $a_i \in A$. Dit comme ça, un n-uplet n'est rien d'autre qu'une application de l'ensemble n (qui a n éléments !) dans A. Et pour obtenir tous les n-uplets, il faut prendre toutes les applications de n dans A. Ce qu'on a donc obtenu peut être vu comme une définition de A^n :

$$A^n \overset{déf.}{=} \mathrm{App}(n, A) \ ,$$

où $\mathrm{App}(n, A)$ désigne l'ensemble de toutes les applications de n dans A [12.4]. En plus, cette façon de voir un n-uplet est cohérente avec l'idée qu'une application de $\mathbf{N}$ dans A se visualise comme une suite infinie $(a_0, a_1, a_2, \dots)$ avec $a_i \in A$ pour tout $i \in \mathbf{N}$.

Notation alternative. Soit A et B deux ensembles. Alors on notera l'ensemble $\mathrm{App}(A, B)$ de toutes les applications de A dans B [12.4] aussi par B^A :

$$B^A \overset{\text{déf}}{=} \mathrm{App}(A, B) \equiv \{\, f \in \mathcal{P}(A \times B) \mid f : A \to B \,\} \ .$$

On a vu que la notation exponentielle B^A d'ensembles est cohérente dans le cas où A est un entier naturel, au quel cas cela représente bien l'ensemble des n-uplets. Mais cette notation est aussi cohérente du point de vue taille. Dans [25.10] on montrera rigoureusement que si A est un ensemble (fini) à n éléments et B un ensemble (fini) à m éléments, alors l'ensemble $B^A = \mathrm{App}(A, B)$ a m^n éléments. Mais on peut

déjà se convaincre que ce résultat est raisonnable en argumentant comme suit : pour chaque élément de A il y a m possibilités dans B pour son image par une application. Étant donné qu'il y a n éléments dans A, on aura donc en total $m \times m \times \cdot \times m$ n-fois, c'est-à-dire m^n applications possibles. Et une troisième argument en faveur de cette notation se trouve dans le comportement de la taille de l'ensemble des applications de A dans B quand on prend des réunions disjointes ou des produits cartésiens (aux bons endroits).

Ⓟ **24.1 Lemme.** *Soit A, B et C trois ensembles avec $B \cap C = \emptyset$. Alors on a*

$$A^{B \cup C} \approx (A^B) \times (A^C) \ .$$

Plus en détails : les applications

$$\Phi : A^{B\cup C} \to A^B \times A^C \qquad et \qquad \Psi : A^B \times A^C \to A^{B\cup C}$$

définies par

$$\Phi(f) = (f|_B, f|_C) \qquad et \qquad \Psi\big((g,h)\big) = g \cup h$$

sont des bijections vérifiant $\Psi = \Phi^{-1}$.

Outre la ressemblance évidente avec la formule $\ell^{m+n} = \ell^m \times \ell^n$ qu'on connaît pour les entiers naturels, il y a une interprétation très visuelle des bijections qui figurent dans [24.1] : la bijection Φ peut être vu comme l'opération de couper une application en deux et la bijection réciproque Ψ peut être vu comme l'opération de recoller deux applications.

DESSIN

24.2 Corollaire. *Soit A, B et C trois ensembles, alors $A^{B \sqcup C} \approx (A^B) \times (A^C)$.*

24.3 Lemme. *Soit A, B et C trois ensembles. Alors on a*

$$(A \times B)^C \approx (A^C) \times (B^C) \ .$$

Plus en détail : les applications

$$\Phi : (A \times B)^C \to A^C \times B^C \qquad et \qquad \Psi : A^C \times B^C \to (A \times B)^C$$

définies par

$$\Phi(f) = (\pi_A \circ f, \pi_B \circ f) \qquad et \qquad \Psi\big((g,h)\big) : c \mapsto \big(g(c), h(c)\big)$$

sont des bijections vérifiant $\Psi = \Phi^{-1}$.

24.4 [13.3]. Lemme-rappel. *Soit A, B et C trois ensembles. Alors on a*

$$(A^B)^C \approx A^{C\times B} \ .$$

Plus en détail : les applications

$$\Phi : (A^B)^C \to A^{C\times B} \qquad et \qquad \Psi : A^{C\times B} \to (A^B)^C$$

définies par

$$\Phi(F) : (c,b) \mapsto \big(F(c)\big)(b) \qquad et \qquad \Psi(G) : c \mapsto \ [\ b \mapsto G\big((c,b)\big)\ ]$$

sont des bijections vérifiant $\Psi = \Phi^{-1}$.

→ **Exercice.** Soit $f : A \to B$ et $g : C \to D$ deux applications. Alors on peut définir l'application $h : A \times C \to B \times D$ par

$$h(a,c) = \big(f(a), g(b)\big) \ .$$

Cette construction nous donne une application

$$\Phi : B^A \times D^C \to (C \times D)^{A\times B}$$

définie par $\Phi(f,g) = h$. Montrer que Φ est injective et que Φ n'est pas surjective quand A et C ont au moins un élément et B et D au moins deux.

Ⓟ **24.5 Lemme.** *Soit A et B deux ensembles.*

(i) *$A^0 = 1$ et donc a fortiori $A^0 \approx 1$, $A^1 \approx A$ et $A^2 \approx A \times A$.*

(ii) *$1^A \approx 1$, $0^0 = 1$ mais si $A \neq 0$, alors $0^A = 0$ et donc a fortiori $0^A \approx 0$.*

(iii) *Si $1 \precsim B$, alors $1 \precsim B^A$. Autrement dit, si B n'est pas vide, alors B^A n'est pas vide non plus.*

24.6 Lemme. *Soit A, A', B et B' quatre ensembles vérifiant $A \precsim A'$ et $B \precsim B'$. Alors on a $A^B \precsim (A')^{B'}$.*

24.7 Corollaire. *L'opération d'exponentielle d'ensembles est compatible (dans le sens [9.14]) avec la relation d'équivalence $\approx$: si A, A', B et B' sont quatre ensembles vérifiant $A \approx A'$ et $B \approx B'$, alors on a $A^B \approx (A')^{B'}$.*

Définition. Soit A un ensemble et $B \subset A$ un sous-ensemble. Alors *la fonction indicatrice de B*, notée $\mathbf{1}_B$ est la fonction $\mathbf{1}_B : A \to 2 = \{0,1\}$ de A dans $\{0,1\}$ définie par

$$\mathbf{1}_B(a) = 1 \text{ si } a \in B \qquad \text{et} \qquad \mathbf{1}_B(a) = 0 \text{ si } a \notin B.$$

Ⓟ **24.8 Lemme.** *Soit A un ensemble et soit $\mathcal{P}(A)$ l'ensemble de toutes les parties de A. Alors on a*

$$\mathcal{P}(A) \approx 2^A \ .$$

Plus en détail, les applications $\Psi : \mathcal{P}(A) \to \{0,1\}^A$ *et* $\Phi : \{0,1\}^A \to \mathcal{P}(A)$ *définies par*

$$\Psi(B) = \mathbf{1}_B \qquad et \qquad \Phi(f) = \{a \in A \mid f(a) = 1\} \ ,$$

sont des bijections vérifiant $\Psi^{-1} = \Phi$.

Ⓟ **24.9 Proposition.** *Soit* A *un ensemble et soit* $\mathcal{P}(A)$ *l'ensemble de toutes les parties de* A. *Alors on il existe une injection* $f : A \to \mathcal{P}(A)$, *mais il n'existe pas de surjection* $f : A \to \mathcal{P}(A)$. *Autrement dit, on a* $A \precsim \mathcal{P}(A)$, *mais on n'a pas* $A \approx \mathcal{P}(A)$ *ou* $\mathcal{P}(A) \precsim A$. *Ou encore, avec [24.8] :*

$$A \precsim 2^A \qquad et \qquad 2^A \not\approx A \ .$$

Ⓟ **24.10 Proposition.** *Soit* $a, b \in \mathbf{R}$ *deux réels vérifiant* $a < b$. *Alors il existe des bijections entre les cinq ensembles* $]a,b[$, $[a,b[$, $]a,b]$, $\mathbf{R}$ *et* $2^{\mathbf{N}^*}$.

Remarque. Si on combine [24.10] et [24.9], on obtient une autre preuve de [17.8] : s'il existait une surjection $\mathbf{N}^* \to [0,1[$, alors en composant avec une bijection $[0,1[\to \{0,1\}^{\mathbf{N}^*}$ et la bijection $\{0,1\}^{\mathbf{N}^*} \to \mathcal{P}(\mathbf{N}^*)$ on obtiendrait une surjection $\mathbf{N}^* \to \mathcal{P}(\mathbf{N}^*)$, ce qui est impossible.

24.11 Corollaire. *On a* $\mathbf{N} \precsim \mathbf{R} \approx 2^{\mathbf{N}}$ *et* $\mathbf{N} \not\approx \mathbf{R}$.

Comme on l'a déjà dit, on interprète [24.11] comme l'énoncé que $\mathbf{R}$ *contient strictement plus d'élément que* $\mathbf{N}$, *que* $\mathbf{R}$ *est strictement plus grand que* $\mathbf{N}$. *Ce qui nous amène directement à la question : y-a-t-il des ensembles qui sont strictement plus grand que* $\mathbf{N}$ *et strictement plus petit que* $\mathbf{R}$ *?* L'hypothèse du continu, *dont le nom vient du fait qu'on appelle (le cardinal de)* $\mathbf{R}$ *le continu, dit que non. Mais on peut démontrer que la question n'est pas décidable : on peut rajouter l'hypothèse du continu aux axiomes ZFC sans créer des contradictions, mais on peut aussi rajouter la négation de l'hypothèse du continu sans créer des contradictions !*

24.12 L'hypothèse du continu. Soit $A \subset \mathbf{R}$, alors on a $A \approx \mathbf{R}$ ou $A \precsim \mathbf{N}$.

25. Ensembles finis

Dans §6 on a défini, en suivant Dedekind, un ensemble infini comme un ensemble pour lequel il existe une application injective mais pas surjective vers lui-même. Par contraposée un ensemble fini est défini comme un ensemble tel que toute application injective vers lui-même est forcément aussi surjective. Le but est maintenant de montrer que pour tout ensemble fini A on peut compter le nombre d'éléments. Plus précisément, on va montrer qu'il existe un unique *entier naturel $n \in \mathbf{N}$ pour lequel il existe une bijection $f : A \to n$. Cet entier naturel n "est" le nombre d'éléments dans A ; on l'appelle "le cardinal" de l'ensemble A et on le note $n = \mathrm{card}(A)$. Une fois qu'on sait qu'on peut compter le nombre d'éléments dans un ensemble fini, on montre qu'on peut calculer avec ce cardinal comme avec les entiers naturels dans le sens suivant. Si A contient n éléments et B en contient m, alors la réunion$A \cup B$ en contient $n + m$ (quand A et B sont disjoints), le produit cartésien $A \times B$ en contient $n \times m$ et l'ensemble des applications de A dans B en contient m^n. Ainsi les trois opérations sur $\mathbf{N}$ (l'addition, la multiplication et l'exponentiation) se retrouvent comme "opérations" sur les ensembles finis. Parmi les résultats annoncés ci-dessus, seul* l'existence *de l'entier n qui est en bijection avec un ensemble fini A ne peut pas être montré sans l'axiome du choix (dénombrable).*

Ⓟ **25.1 Lemme.** *Soit A un ensemble et B un ensemble fini. S'il existe une application injective $f : A \to B$, alors A est aussi un ensemble fini.*

Ⓟ **25.2 Lemme.** *Soit $m, n \in \mathbf{N}$ deux entiers naturels. Alors $n \leq m$ équivaut l'existence d'un injection $f : n \to m$.*

25.3 Corollaire. *Soit $n, m \in \mathbf{N}$ deux entiers naturels. Si $n \neq m$, alors il n'existe pas une bijection $f : m \to n$.*

Ⓟ **25.4 Lemme.** *Soit $n \in \mathbf{N}$ un entier naturel. Alors n est un ensemble fini.*

25.5 Lemme. *Soit A et B deux ensembles et $f : A \to B$ une bijection. Si A est un ensemble fini, alors B l'est aussi.*

25.6 Corollaire. *Soit A un ensemble et soit $m, n \in \mathbf{N}$ deux entiers naturels. S'il existe une bijection $f : A \to n$ et une bijection $g : A \to m$, alors $m = n$.*

25.7 Définition. Soit A un ensemble et $n \in \mathbf{N}$ un entier naturel. On dit que A est un *ensemble fini à n éléments* s'il existe une bijection $f : A \to n$. Par [25.6] cet entier n est unique ; on l'appelle *le cardinal de A*, noté $\mathrm{card}(A)$:

$$\mathrm{card}(A) = n \quad \overset{\text{déf.}}{\Longleftrightarrow} \quad n \in \mathbf{N} \text{ et il existe une bijection } f : A \to n \ .$$

Ⓟ **25.8 Proposition.** *Soit A un ensemble. Alors les deux propriétés suivantes sont équivalentes.*

(i) *Il existe $n \in \mathbf{N}$ et une bijection $f : A \to n$ (ce qui veut dire que A est un ensemble fini à n éléments).*

(ii) *Il existe $m \in \mathbf{N}$ tel que toute application $g : m \to A$ est soit surjective, soit non-injective.*

Ⓟ **25.9 Corollaire.** *Soit A un ensemble et B un ensemble fini à $n \in \mathbf{N}$ éléments. S'il existe une application injective $f : A \to B$, alors il existe $k \in \mathbf{N}$, $k \leq n$ tel que A est un ensemble fini à k éléments. En plus on a $k = n$ si et seulement si f est bijective.*

Ⓟ **25.10 Proposition.** *Soit $n, m \in \mathbf{N}$ deux entiers naturels, soit A un ensemble fini à n éléments et B un ensemble fini à m éléments. Autrement dit :*

$$\operatorname{card}(A) = n \qquad \text{et} \qquad \operatorname{card}(B) = m \ .$$

Alors on a les propriétés suivantes.

(i) *$A \cup B$ est un ensemble fini à $k \leq n+m$ éléments et $k = n+m$ si et seulement si $A \cap B = \emptyset$:*

$$\operatorname{card}(A \cup B) \leq \operatorname{card}(A) + \operatorname{card}(B)$$

et

$$\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B) \qquad \Longleftrightarrow \qquad A \cap B = \emptyset \ .$$

(ii) *$A \times B$ est un ensemble fini à $n \times m$ éléments :*

$$\operatorname{card}(A \times B) = \operatorname{card}(A) \times \operatorname{card}(B) \ .$$

(iii) *B^A est un ensemble fini à m^n éléments :*

$$\operatorname{card}\big(B^A\big) = \operatorname{card}(B)^{\operatorname{card}(A)} \ .$$

Ⓟ **25.11 Lemme.** *Soit $(A, \leq_A)$ un ensemble partiellement ordonné et soit $f : \mathbf{N} \to A$ une application vérifiant*

$$\forall n \in \mathbf{N} : f(n) \leq_A f\big(S(n)\big) \ .$$

Alors on a (aussi) la propriété

$$\forall m, n \in \mathbf{N} : m \leq n \ \Rightarrow \ f(m) \leq_A f(n)$$

(ACD) Ⓟ **25.12 Théorème.** *Soit A un ensemble fini. Alors il existe $n \in \mathbf{N}$ tel que A est un ensemble fini à n éléments.*

26. Ensembles dénombrables

Définition. On dit qu'un ensemble A est *dénombrable* s'il existe une application injective $f : A \to \mathbf{N}$.

→ **26.1 Lemme.** *Soit A un ensemble dénombrable.*

(i) *Si $B \subset A$ est un sous-ensemble, alors B est aussi dénombrable.*

(ii) *Si B est un ensemble et $f : A \to B$ une bijection, alors B est aussi dénombrable.*

26.2 Lemme. *Soit $n \in \mathbf{N}$ un entier naturel. Alors on a l'égalité*

$$n = \{\, k \in \mathbf{N} \mid k < n \,\} \ .$$

En particulier n est un ensemble dénombrable et tout ensemble fini à n éléments A est dénombrable.

Remarque pour les comparateurs. Certains auteurs définissent la notion d'un ensemble dénombrable comme un ensemble A pour lequel il existe une *bijection* entre A et $\mathbf{N}$. En vu de [7.10], ceci entraîne automatiquement que c'est un ensemble infini. Nous adoptons ici un point de vue moins restrictif qui inclut les ensembles finis à n éléments [25.7].

(ACD) Ⓟ **26.3 Lemme.** *Soit A un ensemble dénombrable. S'il n'existe pas une bijection $h : A \to \mathbf{N}$, alors il existe $n \in \mathbf{N}$ tel que A est un ensemble fini à n éléments.*

Ⓟ **26.4 Proposition.** *Il existe une bijection $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$.*

Remarque. La deuxième bijection dans la preuve de [26.4] est souvent utilisée dans le calcul d'un produit de deux séries entières. Sans entrer dans les détails des justifications de ce calcul, on écrit

$$\Big(\sum_{p=0}^{\infty} a_p\, z^p\Big) \cdot \Big(\sum_{q=0}^{\infty} b_q\, z^q\Big) = \sum_{p,q=0}^{\infty} a_p\, b_q\, z^{p+q} = \sum_{n=0}^{\infty} \sum_{q=0}^{n} a_{n-q}\, b_q\, z^n$$
$$= a_0\, b_0\, z^0 + (a_1\, b_0 + a_0\, b_1)\, z^1 + (a_2\, b_0 + a_1\, b_1 + a_0\, b_2)\, z^2 + \cdots$$

où on reconnaît, dans les indices des produits $a_i\, b_j$, les premiers termes de la deuxième application f : $f(m) = (0,0)$, $(1,0)$, $(0,1)$, $(2,0)$, $(1,1)$, $(0,2)$, ….

26.5 Corollaire. *Pour tout $n \in \mathbf{N}^*$ il existe une bijection entre $\mathbf{N}^n$ et $\mathbf{N}$.*

Ⓟ **26.6 Proposition.** *Une réunion (pas forcément disjointe) dénombrable d'ensembles dénombrables est dénombrable. Plus précisément, soit I un ensemble dénombrable,*

soit B un ensemble et soit $\phi : I \to \mathcal{P}(B)$ une application telle que chaque image $A_i \overset{déf}{=} \phi(i) \subset B$ est un ensemble dénombrable :

$$\forall i \in I : A_i \text{ est dénombrable.}$$

Alors la réunion $R \overset{déf}{=} \cup\, \phi[I] \equiv \cup_{i\in I} A_i$ est dénombrable.

Ⓟ **26.7 Corollaire.** *Les ensembles* **Z** *et* **Q** *sont dénombrables.*

27. Arithmétique d'ensembles infinis

On a déjà vu qu'on a "l'égalité" $\mathbf{N} \times \mathbf{N} \approx \mathbf{N}$ *[26.4]. Naïvement on pourrait croire que les ensembles infini ont tous la même taille, mais on sait déjà que ce n'est pas le cas : l'ensemble* $[0,1[$ *des réels entre* 0 *et* 1 *est infini mais on n'a pas* $[0,1[\approx \mathbf{N}$ *par l'argument du diagonale de Cantor [17.8]. L'ensemble* $[0,1[$ *est donc forcément "strictement plus grand en taille" que* $\mathbf{N}$*. Il y a donc au moins deux tailles infinies différentes. En plus, on a vu dans [24.9] qu'on peut en construire (beaucoup) d'autres, simplement en considérant l'ensemble des parties, ce qui est la même chose que prendre l'exponentielle* 2^A *[24.8]. D'autre part, prendre une réunion disjointe ou un produit cartésien n'augmentera pas la taille infinie. La seule façon d'obtenir des ensembles plus grands est donc par l'exponentiation Mais pour le montrer on a besoin de l'axiome du choix.*

27.1 [7.10]. Proposition-rappel. *Un ensemble* A *est un ensemble infini si et seulement si on a* $\mathbf{N} \precsim A$*.*

27.2 Lemme. *Soit* A *un ensemble infini et* B *un ensemble dénombrable. Alors on a* $B \precsim A$*.*

(ACD) **27.3 Proposition.** *Soit* A *un ensemble. Si on a* $2 \precsim A$ *et* $A \approx A \times A$*, alors on a* $\mathbf{N} \precsim A$*.*

Remarque. On peut interpréter [27.3] dans les sens que "l'équation" $A \times A \approx A$ n'a que trois solutions : $A \approx 0$, $A \approx 1$ et $\mathbf{N} \precsim A$. Autrement dit, A est vide, A est un singleton ou A est un ensemble infini.

(AC(ℵ)) **27.4 Théorème.** *Soit* A *un ensemble. Si on a* $\mathbf{N} \precsim A$*, alors* $A \times A \approx A$*.*

27.5 Remarque sur la preuve de [27.4]. Une autre façon de voir l'ensemble $\mathcal{B}$, dans la même veine qu'utilisé dans la preuve que le lemme de Zorn implique le théorème du bon ordre §20, est la suivante. L'application f dans le couple (B, f) est un sous-ensemble de $B \times (B \times B)$. En tant que telle, l'ensemble B est déjà codé dans l'ensemble f comme l'ensemble des premières composantes de f :

$$B = \pi_1[f] \ ,$$

où $\pi_1 : B \times (B \times B) \to B$ est donnée par $\pi_1\big((b,(c,d))\big) = b$. En plus, on a l'inclusion $B \times (B \times B) \subset A \times (A \times A)$. Pour un couple $(B, f) \in \mathcal{B}$ on a donc

$$f \in \mathcal{P}\big(A \times (A \times A)\big) \qquad \text{et} \qquad B = \pi_1[f] \ .$$

On peut donc définir la collection $\mathcal{B}$ comme

$$\mathcal{B} = \{\, f \in \mathcal{P}\big(A \times (A \times A)\big) \mid \exists B \subset A : \mathbf{N} \precsim B \text{ et } f : B \to B \times B \text{ une bijection.} \,\} \ .$$

Quant à la relation d'ordre $(B,f) \preccurlyeq (C,g)$, elle se traduit par la simple inclusion $f \subset g$! D'abord il est évident que cette inclusion implique $B = \pi_1[f] \subset \pi_1[g] = C$. Et on a, par définition d'une application, les équivalences et implication

$$f(a) = (b,c) \quad \Longleftrightarrow \quad \big(a,(b,c)\big) \in f \quad \stackrel{f\subset g}{\Longrightarrow} \quad \big(a,(b,c)\big) \in g \quad \Longleftrightarrow \quad g(a) = (b,c) \ ,$$

ce qui monte qu'on a bien $g|_B = f$.

Une fois qu'on sait que la relation d'ordre est l'inclusion, la recherche d'un majorant pour un sous-ensemble totalement ordonné $\mathcal{C}$ devient aussi plus simple, au moins au début. Car il suffit de poser $F = \cup\mathcal{C}$. Mais le vrai travail commence là, car il faut montrer que ce F, dont on sait a priori seulement que c'est un sous-ensemble de $A \times (A \times A)$ est bien un élément de $\mathcal{B}$.

Commençons avec le plus simple : on définit $M = \pi_1[F]$ et on constate que pour $f \in \mathcal{C}$ on a (par défintion de la réunion) $f \subset F$ et donc

$$\mathbf{N} \precsim \pi_1(f) \precsim \pi_1(F) = M \ .$$

Pour montrer que F est une bijection $F : M \to M \times M$, il faut d'abord établir qu'on a bien l'inclusion $F \subset M \times (M \times M)$. Mais si on a $\big(a,(b,c)\big) \in F \subset A \times (A \times A)$, on a $a \in M$ par définition de M. Et par définition de la réunion il existe $f \in \mathcal{C}$ tel que $\big(a,(b,c)\big) \in f$. En particulier $a \in \pi_1[f] = B$ et donc par définition de $\mathcal{B}$ on a

$$\big(a,(b,c)\big) \in B \times (B \times B) \subset M \times (M \times M) \ .$$

Une fois qu'on sait qu'on a bien $F \subset M \times (M \times M)$, il faut vérifier les propriétés d'une bijection. Faisons le dans l'ordre.

• (i) Pour $a \in M = \pi_1[F]$ il existe (par définition de l'image) $\big(a,(b,c)\big) \in F$.

• (ii) Si on a $\big(a,(b,c)\big), \big(a,(b',c')\big) \in F$, alors par définition de la réunion il existe $f, g \in \mathcal{C}$ avec

$$\big(a,(b,c)\big) \in f \qquad \text{et} \qquad \big(a,(b',c')\big) \in g \ .$$

Mais $\mathcal{C}$ est totalement ordonné, donc on a $f \subset g$ ou $g \subset f$. Dans le premier cas on a donc

$$\big(a,(b,c)\big), \big(a,(b',c')\big) \in g$$

et donc parce que g est un application on doit avoir $(b,c) = (b',c')$. Dans le deuxième cas l'argument est semblable pour la même conclusion.

• (iii) Si on a $\big(a,(b,c)\big), \big(a',(b,c)\big) \in F$, alors de nouveau par définition de la réunion il existe $f, g \in \mathcal{C}$ avec

$$\big(a',(b,c)\big) \in f \qquad \text{et} \qquad \big(a,(b,c)\big) \in g \ .$$

Mais $\mathcal{C}$ est totalement ordonné, donc on a $f \subset g$ ou $g \subset f$. Dans le premier cas on a donc

$$\big(a,(b,c)\big), \big(a',(b,c)\big) \in g$$

et donc parce que g est un application injective on doit avoir $a = a'$. Dans le deuxième cas l'argument est semblable pour la même conclusion.

• (iv) Soit $(b,c) \in M \times M$, ce qui est équivalent à $b, c \in \pi_1[F]$. Alors par définition de la projection il existe

$$\big(b,(x,y)\big), \big(c,(x',y')\big) \in F$$

et donc par définition de la réunion il existe $f, g \in \mathcal{C}$ tels que

$$\big(b,(x,y)\big) \in f \qquad \text{et} \qquad \big(c,(x',y')\big) \in g \ .$$

Mais (pour une dernière fois) $\mathcal{C}$ est totalement ordonné et on a donc $f \subset g$ ou $g \subset f$. Dans le premier cas on a

$$\big(b,(x,y)\big),\big(c,(x',y')\big) \in g$$

et donc en particulier $b,c \in \pi_1[g] = C$. Sachant que $g : C \to C \times C$ est en particulier surjective par définition de $\mathcal{B}$, il existe donc $a \in C$ tel que $g(a) = (b,c)$. On a donc

$$\big(a,(b,c)\big) \in g \subset F \ ,$$

ce qui montre qu'il existe $a \in M$ tel que $\big(a,(b,c)\big) \in F$. Dans le deuxième cas l'argument est analogue avec la même conclusion. Ce qui termine la preuve que F est surjective et donc au final une bijection comme annoncée.

(AC(P)) **27.6 Proposition.** *Soit A et B deux ensembles avec $\mathbf{N} \precsim A$, c'est-à-dire que A est un ensemble infini.*

(i) *Si $B \precsim A$, alors $A \sqcup B \approx A$.*

(ii) *Si on a $1 \precsim B \precsim A$, alors $A \times B \approx A$.*

(iii) *Si on a $2 \precsim B \precsim A$, alors $B^A \approx 2^A$.*

(iv) *Pour tout $n \in \mathbf{N}^*$ on a $A^n \approx A$.*

L'hypothèse du continu dit qu'il n'y a pas une taille d'ensemble strictement entre la taille de $\mathbf{N}$ et la taille de $\mathbf{R}$. Étant donné que la taille de $\mathbf{R}$ est la taille de $2^{\mathbf{N}}$, on peut se poser la question plus générale s'il y a une taille d'ensemble entre la taille d'un ensemble A et la taille de 2^A. Pour les ensembles finis *il est facile de montrer que la réponse est négative pour $A \approx 0$ et $A \approx 1$, et positive pour $2 \precsim A$. Et donc l'hypothèse du continu dit que pour la première taille non finie c'est faux aussi. Et pour les autres ?* L'hypothèse du continu généralisée *dit que c'est faux aussi pour les autres ensembles infinis. Avec l'axiome du choix on peut reformuler l'hypothèse du continue généralisé comme disant que pour tout ensemble A vérifiant $A \approx A \times A$, il n'y a pas de taille entre la taille de A et la taille de 2^A.*

27.7 L'hypothèse du continu généralisée. Soit A un ensemble infini et $B \subset 2^A$. Alors on a $B \approx 2^A$ ou $B \precsim A$.

Chapitre 5

Ordinaux et cardinaux

28. Ordinaux

Ⓟ **28.1 Lemme.** *Soit $\leq$ une relation d'ordre sur un ensemble A, alors la relation $<$ vérifie les propriétés suivantes :*

(i) $\forall a, b \in A : a \not< b$ *ou* $b \not< a$,

(ii) $\forall a, b, c \in A : \big(a < b \text{ et } b < c\big) \Rightarrow a < c$.

Ⓟ **28.2 Lemme.** *Soit $<$ une relation sur A vérifiant les propriétés*

(i) $\forall a, b \in A : a \not< b$ *ou* $b \not< a$,

(ii) $\forall a, b, c \in A : \big(a < b \text{ et } b < c\big) \Rightarrow a < c$.

Alors la relation $\leq$ définie par

$$a \leq b \quad \overset{\text{déf.}}{\Longleftrightarrow} \quad a < b \text{ ou } a = b \ ,$$

est une relation d'ordre sur A et la relation d'ordre stricte associée à cette relation d'ordre $\leq$ est la relation $<$ du départ.

Définition. Un ensemble α est appelé un *ordinal* s'il vérifie les cinq propriétés suivantes.

(O1) $\forall x, y \in \alpha : x \notin y$ ou $y \notin x$.

(O2) $\forall x, y, z \in \alpha : x \in y$ et $y \in z \Rightarrow x \in z$.

(O3) $\forall x, y \in \alpha : x \in y$ ou $x = y$ ou $y \in x$.

(O4) $\forall A \neq \emptyset : A \subset \alpha \Rightarrow \exists x \in A \ \forall y \in A : y \notin x$.

(O5) $\forall y : y \in \alpha \Rightarrow y \subset \alpha$.

Selon [28.2], les conditions (O1) et (O2) disent que $\in$ est la version stricte d'une relation d'ordre sur α. Ensuite, la condition (O3) dit que cette ordre est total et la condition (O4) qu'elle est un bon ordre. Un ensemble vérifiant la condition (O5) est appelé un *ensemble transitif*. En résumant on peut dire qu'un ordinal est un ensemble transitif pour lequel la relation "appartenance" est la version stricte d'un bon ordre. À noter qu'on peut reformuler la condition de transitivité (O5) comme

(O5) $\forall x, y : x \in y$ et $y \in \alpha \Rightarrow x \in \alpha$,

ce qui donne une explication du nom "ensemble transitif" pour un ensemble vérifiant cette propriété.

On a vu (voir [19.6]) que pour une relation d'ordre (version non-stricte) on peut remplacer, dans la définition d'un bon ordre, la condition de l'existence d'un élément minimal par la condition de l'existence d'un plus petit élément. Et que dans la suite on peut oublier la condition de réflexivité et la condition que l'ordre doit être total, car cela devient une conséquence. Tout cela suggère qu'on introduit, dans la définition d'un ordinal, la condition (O4') comme

(O4') $\forall A \neq \emptyset : A \subset \alpha \Rightarrow \exists x \in A\ \forall y \in A : x \in y$ ou $x = y$,

et qu'on enlève la condition (O3). Dans tous les cas, les quatre/cinq conditions ne sont pas indépendantes, car on a les implications suivantes entre eux.

(i) (O4) $\Rightarrow$ (O1).

(ii) (O4') $\Rightarrow$ (O3).

(iii) (O3) et (O4) $\Rightarrow$ (O4').

(iv) (O1) et (O4') $\Rightarrow$ (O4).

(v) (O3), (O4) et (O5) $\Rightarrow$ (O2).

(vi) (O2), (O4) et (O5) $\Rightarrow$ (O3).

Il s'ensuit qu'on peut caractériser un ordinal par trois conditions seulement : au choix par (O2), (O4) et (O5), par (O3), (O4) et (O5) ou par (O1), (O4') et (O5). Et si on accepte l'axiome de fondation (voir §32), on peut même enlever la condition (O4) dans les deux premières variantes.

Remarque. Dans la preuve de l'implication (O2,4,5) $\Rightarrow$ (O3) on peut interpréter certains ingrédients en termes d'une relation d'ordre, car avec (O4) on a (O1) et donc (par (O1,2)) on sait que l'appartenance est la version stricte d'une relation d'ordre. En ces termes, la relation $C(x, y)$ dit que les éléments x et y sont comparables pour cette relation d'ordre. L'élément x_1 est un élément minimal de α qui n'est pas comparable avec tous les autres éléments de α et y_1 est un élément minimal de α qui n'est pas comparable avec x_1. En même temps, l'ensemble A est l'ensemble des éléments de α qui ne sont pas comparables à tous les autres éléments de α et B est l'ensemble des éléments de α qui ne sont pas comparables avec x_1 (par définition de x_1 il y en a). Malheureusement, le reste de la preuve ne s'interprète pas aussi facilement.

Ⓟ **28.3 Lemme.** *Si α est un ordinal, alors on a $\alpha \notin \alpha$.*

Nota Bene. Dans un certain nombre de preuves qui vont suivre, on utilisera les propriétés d'un ordinal. Mais parce qu'on parlera souvent de plusieurs ordinaux en même temps, il faut distinguer de quel ordinal on invoque la propriété concernée. On fera cette distinction en écrivant $(\mathrm{Oi})_\alpha$ si on utilise la propriété (Oi) de l'ordinal α.

Ⓟ **28.4 Lemme.** *Si α et β sont deux ordinaux, alors on a l'équivalence*

$$\alpha \subset \beta \qquad \Longleftrightarrow \qquad \alpha = \beta \text{ ou } \alpha \in \beta \ .$$

Ⓟ **28.5 Lemme.** *Soit α un ordinal et $\beta \in \alpha$. Alors β est un ordinal.*

Ⓟ **28.6 Proposition.** *Soit X un ensemble non vide dont tous les éléments sont des ordinaux. Alors l'intersection $m = \cap X$ est un ordinal appartenant à X.*

Ⓟ **28.7 Corollaire.** *Soit X un ensemble dont tous les éléments sont des ordinaux. Alors l'inclusion est un bon ordre sur X et la relation d'ordre stricte associée est l'appartenance.*

Ⓟ **28.8 Corollaire.** *Soit α et β deux ordinaux. Alors on a une et seulement une des trois possibilités $\alpha \in \beta$ ou $\beta \in \alpha$ ou $\alpha = \beta$.*

Ⓟ **28.9 Corollaire.** *Il n'existe pas un ensemble qui contient tous les ordinaux. Autrement dit, la collection de tous les ordinaux n'est pas un ensemble.*

Étant donné que la notion de collection n'est pas définie, on n'a donc pas le droit de le donner un nom. Si on abuse, on pourrait noter cette collection comme ORD *et écrire $\alpha \in$ ORD pour dire que α est un ordinal. Mais que le lecteur sache bien : on n'a pas le droit d'utiliser le symbole d'appartenance pour cela, car ce symbole n'est défini que pour les ensembles. D'autre part, cette fiction, cet abus de notation, nous permet de résumer d'une façon "facile" un certain nombre de résultats concernant les ordinaux. Car on vient de montrer que* ORD *a toutes les propriétés d'un ordinal, en particulier que* ORD *est bien ordonné par l'inclusion et que la version stricte de cette relation d'ordre est l'appartenance.*

Vérifions les propriétés dans le désordre, en commençant par (O3). Dans (O3) il faut prendre $x, y \in$ ORD, ce qui est une abréviation/abus de notation pour dire que x et y sont des ordinaux. Et donc par [28.8] on a bien la trichotomie désiré. Mais l'exclusivité dans [28.8] nous donne en même temps (O1). La propriété (O2), toujours avec l'interprétation que $x, y, z \in$ ORD veut dire que x, y, z sont des ordinaux, est une conséquence immédiate du fait que z est un ordinal, car par $(O5)_z$ on a $y \subset z$ et donc la condition $x \in y$ donne automatiquement $x \in z$.

Pour les propriétés (O4) et (O5), il faut d'abord déchiffrer ce que veut dire l'inclusion $A \subset$ ORD. La définition [1.1] nous dit que c'est une abréviation pour

$$A \subset \text{ORD} \quad \overset{déf}{\equiv} \quad \forall x : x \in A \ \Rightarrow \ x \in \text{ORD} \ .$$

Et si on traduit $x \in$ ORD comme x un ordinal, on obtient la traduction que $A \subset$ ORD veut dire que A est un ensemble dont tous les éléments sont des ordinaux. Et selon [28.7] A est bien ordonné par la relation d'ordre stricte donnée par l'appartenance. En particulier l'ensemble A lui même admet un élément minimal pour cette relation, ce qui montre la propriété (O4). Et finalement, (O5) n'est rien d'autre que [28.5] : si x est un ordinal ("appartient" à ORD*), alors ses éléments sont des ordinaux, ce qu'on a "résumé" comme $x \subset$ ORD. La remarque que l'inclusion est la relation d'ordre associée à la relation d'ordre stricte $\in$ est, comme dans la preuve de [28.7], une conséquence de [28.4] et [28.3].*

Ⓟ **28.10 Proposition.** *Soit X un ensemble dont tous les éléments sont des ordinaux. Alors $M = \cup X$ est un ordinal vérifiant $x \subset M$ pour tout $x \in X$. En plus, si β est un ordinal vérifiant $x \subset \beta$ pour tout $x \in X$, alors on a $M \subset \beta$.*

Toujours avec la fiction qu'on peut écrire $\alpha \in \mathrm{ORD}$ pour dire que α est un ordinal, on peut interpréter [28.10] comme l'énoncé que ORD *a la propriété de la borne sup. Plus précisément, soit $X \subset \mathrm{ORD}$, c'est-à-dire, soit X un ensemble dont les éléments sont des ordinaux. Alors la première partie de [28.10] dit que $M \in \mathrm{ORD}$ est un majorant de X pour la relation d'ordre donnée par l'inclusion et la deuxième partie dit que si $\beta \in \mathrm{ORD}$ est aussi un majorant de X, alors M est plus petit ou égal à β, autrement dit, M est le plus petit majorant de X.*

Ⓟ **28.11 Corollaire.** *L'ensemble vide est un ordinal.*

Ⓟ **28.12 Proposition.** *Soit α un ordinal et soit $\beta = \cup\alpha$. Alors on a $\alpha = \beta$ ou $\alpha = \beta \cup \{\beta\} \equiv S(\beta)$.*

Dans [6.1] on a introduit l'opération S du successeur d'une façon ad-hoc. Ici on part de la définition d'un ordinal et on s'intéresse à la réunion d'un ordinal. Et dans [28.12] on trouve qu'il n'y a que deux possibilités pour le lien entre un ordinal α et sa réunion $\beta = \cup\alpha$: soit on a égalité, soit α est le successeur de β. On retrouve donc d'une façon "naturelle" l'opération du successeur. On dit que c'est une façon naturelle car on ne l'a pas caché (d'une façon plus ou moins explicite) dans la définition d'un ordinal. On peut toujours contester l'adjectif "naturelle" pour la définition d'un ordinal.

Ⓟ **28.13 Propriétés du successeur.** *Soit A un ensemble.*

(i) *A est un ordinal si et seulement si $S(A)$ est un ordinal.*

(ii) *Si A est un ordinal, alors $A \neq S(A)$ et $A = \cup S(A)$.*

(iii) *Si α et A sont des ordinaux tels que $A \subset \alpha \subset S(A)$, alors $\alpha = A$ ou $\alpha = S(A)$ (il n'y a pas d'ordinaux strictement entre A et $S(A)$).*

Ⓟ **28.14 Proposition.** *Soit α un ordinal. Alors les propriétés suivantes sont équivalentes :*

(i) $\alpha = \cup\alpha$,

(ii) $\forall \beta \in \alpha : S(\beta) \in \alpha$ *et*

(iii) *il n'existe pas un ensemble A tel que $\alpha = S(A)$.*

Définition. Soit α un ordinal différent de $\emptyset$. Alors on dit que α est un *ordinal limite* si on a $\cup\alpha = \alpha$. Dans le cas contraire on dit que α est le *successeur* de $\beta = \cup\alpha$ ou que β est le *prédécesseur direct* de α.

Ⓟ **28.15 Corollaire.** *L'ensemble* $\mathbf{N}$ *des entiers naturels est un ordinal limite.*

Dans §6 on a introduit l'ensemble des entiers naturels via l'axiome de l'infini et l'opération du successeur. Mais on peut récupérer les entiers naturels aussi comme un cas particulier des ordinaux. Pour cela on se sert de l'opération du successeur (qui apparaît naturellement dans le contexte des ordinaux). On rappelle d'abord le fait que l'ensemble vide, qui est le plus petit ordinal, ne peut pas être le successeur d'un ensemble. Pour les ordinaux plus grand (c'est-à-dire qui ne sont pas vide) la question se pose s'ils sont oui ou non le successeur d'un autre ordinal. Avec cette idée on définit un ordinal fini comme un ordinal tel que tout ordinal plus petit ou égal (dans le sens de l'appartenance/inclusion) est le successeur d'un autre (sauf si c'est l'ensemble vide bien sûr).

Définition. Soit α un ordinal. On dit que α est un *ordinal fini* si on a les deux propriétés supplémentaires

(N1) $\alpha = \emptyset$ ou $\exists\beta : \alpha = S(\beta)$ et

(N2) $\forall\gamma \in \alpha : \gamma = \emptyset$ ou $\exists\beta : \gamma = S(\beta)$.

Ⓟ **28.16 Lemme.** *L'ensemble vide est un ordinal fini. Et si α est un ordinal fini, alors tout élément de α ainsi que $S(\alpha)$ est un ordinal fini.*

Ⓟ **28.17 Corollaire.** *Soit α un ensemble. Alors on a l'équivalence*

$$\alpha \in \mathbf{N} \qquad \Longleftrightarrow \qquad \alpha \text{ est un ordinal fini.}$$

Dans [28.17] on a établit qu'un entier naturel n'est rien d'autre qu'un ordinal fini. Mais le mot fini, on l'a déjà utilisé dans le sens de Dedekind pour désigner un ensemble fini. Il y a donc une confusion potentielle entre ces deux utilisation du même mot. Heureusement cette confusion n'est qu'apparente, car un ordinal fini est bien un ensemble fini.

Ⓟ **28.18 Lemme.** *Soit α un ordinal. Alors α est un ordinal fini si et seulement si α, en tant qu'ensemble, est un ensemble fini.*

Dans §6 on a introduit l'ensemble $\mathbf{N}$ des entiers naturels directement à l'aide de l'axiome de l'infini. Ici on vient de voir qu'un élément de $\mathbf{N}$ n'est rien d'autre qu'un

ordinal fini. Et pour définir la notion d'un ordinal fini on n'a pas besoin de l'axiome de l'infini. Pourtant, on a (toujours) besoin de l'axiome de l'infini sous une forme ou autre. Car, bien qu'on peut définir la notion d'un ordinal fini sans recours à l'axiome de l'infini, sans l'axiome de l'infini sous une forme ou autre, on ne peut pas affirmer que la collection de tous les ordinaux finis est un ensemble. L'axiome de l'infini est donc parfois formulé comme : il existe un ordinal qui n'est pas un ordinal fini. Le désavantage de cette formulation est que, pour le formuler en termes primitifs, elle devient très longue (car il faut inclure la définition d'ordinal et la négation d'ordinal fini). Et pour en déduire l'existence des entiers naturels comme le plus petit ordinal non-fini, il faut démontrer un certain nombre de résultats préalablement. Par contre, la définition des entiers naturels comme des ordinaux finis a un avantage par rapport à la définition directe : l'ensemble $\mathbf{N}$ *vu comme l'ensemble des ordinaux finis est automatiquement muni d'un bon ordre (donné par l'inclusion avec l'appartenance comme version stricte). On n'a plus besoin de le construire à l'aide des axiomes de Peano. La seule question qui reste est de savoir si la relation d'ordre qu'on a construit à l'aide des axiomes de Peano est vraiment la même que celle donné par l'inclusion.*

Ⓟ **28.19 Proposition.** *La relation d'ordre sur* $\mathbf{N}$ *définie à l'aide des axiomes de Peano coïncide avec la relation d'ordre des ordinaux (l'inclusion).*

Remarque. La deuxième partie de la preuve de [28.19] est un cas particulier d'un résultat plus général qui dit qu'une application croissante et bijective entre deux ensembles totalement ordonnés (ici l'identité entre $(\mathbf{N}, \subset)$ et $(\mathbf{N}, \leq)$) a nécessairement une réciproque qui l'est aussi. Le lecteur curieux pourrait s'en convaincre lui-même.

29. L'axiome de remplacement

Dans §28 on a défni la notion d'un ordinal et on a vu que c'est un cas particulier d'un ensemble bien ordonné. Dans §30 on veut montrer que les ordinaux sont les archetypes pour les ensembles bien ordonnés. Plus précisément, on introduit la notion d'isomorphisme d'ensembles bien ordonnés comme des bijections qui respectent la relation d'ordre et on montre que pour tout ensemble bien ordonné il existe un unique ordinal qui lui est isomorphe. Malheureusement il y a un piège : sans axiome supplémentaire on ne peut pas boucler la preuve. Car on est confronté à la situation suivante. On a un ensemble A et à chaque élément $x \in A$ on associe un unique ordinal α. Pour décrire la dépendance en $x \in A$ de cet ordinal α on l'écrit comme α_x. Mais cela implique une dépendance fonctionnelle. Le problème est qu'on ne sait pas dans quel ensemble cette application, qui associe l'ordinal α_x à $x \in A$, prend ses valeurs. On ne peut donc pas définir une application $\alpha : A \to B$, car on ne sait pas ce qu'on pourrait mettre comme ensemble B. Évidemment on souhaiterait affirmer que la collection B de tous ces ordinaux, qu'on aimerait écrire comme

$$B = \{\, \alpha_x \mid x \in A \,\} \ ,$$

est un ensemble. Cette écriture ressemble beaucoup à l'écriture simplifiée introduit en [2.4]. Mais contrairement à ce qui se passait là, ici on ne peut pas trouver un ensemble qui contient tous ces α_x ; le candidat "évident" est la collection de tous les ordinaux, mais ce n'est pas un ensemble [28.9].

D'autre part, on a justifié l'introduction des axiomes par le fait qu'il y a des collections qui sont trop grandes pour être appelées "ensemble." Et que les axiomes nous permettent de faire le tri. Mais la collection B qu'on cherche ici n'est certainement pas trop grande, car le candidat idéal pour B contient autant d'éléments que l'ensemble A lui même : on remplace simplement chaque élément de A par un ordinal correspondant. On a donc l'impression que notre collection B devrait être un ensemble, mais qu'il nous manque les moyens de le montrer. Et c'est exactement ce que propose de faire l'axiome de remplacement : justifier que B est bien un ensemble.

L'idée de cet axiome est exactement ce que dit son nom : on part d'un ensemble A et on remplace chaque élément $x \in A$ (un ensemble) par un autre ensemble. Le résultat sera de nouveau un ensemble. Ou encore : on prend un ensemble A, on met tous ses éléments sur une ligne et en face de chaque élément (un ensemble) on met un autre ensemble. L'axiome de remplacement dit que la collection des ensembles qui sont en face des éléments de A est bien un ensemble. On a remplacé simplement chaque élément par l'ensemble en face de lui. La grande question est : comment décrire la recette de remplacement ? L'idée simpliste est de dire qu'il nous faut une application f définie sur A à valeurs dans les ensembles. Mais comme on a constaté ci-dessus, on tombe dans un argument circulaire. Car si on sait montrer que c'est une application, alors on a un ensemble but B pour dire qu'on a une application $f : A \to B$. Et dans ce cas il suffit de dire qu'on applique l'axiome de séparation, car remplacer chaque élément $x \in A$ par son image $y = f(x) \in B$ ne nous donne rien d'autre que l'ensemble $\mathrm{Im}(f) \subset B$. Et si on n'a pas un ensemble but, on ne peut pas parler d'une application tel qu'on l'a définie en [4.1].

Pour contourner ce problème, on utilise une idée analogue à l'idée utilisé pour l'axiome de séparation (Z5) : on décrit une application par une propriété qui relie deux ensembles x et y, ce qui est exprimée par une formule $q(x, y)$ qui ne prend

que les valeurs "vrai" ou "faux." Et comme pour l'axiome de séparation on suppose que dans q on ne parle que d'ensembles et pas d'autres sortes d'objets. Pour qu'une telle formule représente une application, il faut qu'elle a la propriété que pour tout ensemble x appartenant à A il y a exactement un ensemble y qui est lié à ce x :

$$\begin{cases} \forall x \in A \; \exists y \;\; : \;\; q(x,y) \\ \forall x \in A \; \forall y, z \;\; : \;\; [\; q(x,y) \text{ et } q(x,z) \;] \;\Rightarrow y = z \;\; . \end{cases} \tag{29.1}$$

Dans (29.1) la première ligne dit que pour tout ensemble x dans A il existe un ensemble y qui est lié à x et la deuxième ligne dit qu'un tel ensemble est unique. Et si $q(x,y)$ représente une application dans le sens (29.1), alors le résultat de substituer les éléments d'un ensemble A par les images de "l'application" q peut s'écrire comme

$$\{\, y \mid \exists x : x \in A \text{ et } q(x,y) \,\} \;\; ,$$

la collection des ensembles y qui sont lié par q à un élément x de A. L'axiome de remplacement nous dit que ce résultat est effectivement un ensemble. Et comme pour l'axiome de séparation ce n'est pas vraiment un seul axiome, mais un schéma d'axiomes : il y a un axiome pour chaque "application" q reliant deux ensembles.

(F) Axiome de remplacement, première version.

$$\forall A \;\; : \;\; \big(\; \exists B \;\; \forall C \;\; : \;\; C \in B \;\; \Leftrightarrow \;\; [\; \exists x \;\; : \;\; x \in A \text{ et } q(x,C) \;] \;\big) \;\; ,$$

où $q(x,y)$ est une formule ne prenant que les valeurs "vrai" ou "faux" et vérifiant

$$\begin{cases} \forall x \in A \; \exists y \;\; : \;\; q(x,y) \\ \forall x \in A \; \forall y, z \;\; : \;\; [\; q(x,y) \text{ et } q(x,z) \;] \;\Rightarrow y = z \;\; . \end{cases}$$

Par l'axiome d'extensionnalité (Z1) l'ensemble B est unique et complètement déterminé par l'ensemble A et la propriété q. On le note comme :

$$B \;\overset{\text{déf}}{=}\; \{C \mid \exists x : x \in A \text{ et } q(x,C)\} \equiv \{C \mid \exists x \in A : q(x,C)\} \;\; .$$

Remarque. On a indexé l'axiome de remplacement par la lettre "F" et pas par la lettre Z suivie d'un nombre, car cet axiome a été introduit par Abraham Fraenkel et ne figure pas dans la liste initiale des axiomes formulée par Ernst Zermelo.

Changement de notation. Il arrive qu'une relation q qu'on utilise dans l'axiome de remplacement (F) a une forme particulière qui ressemble beaucoup a une vraie fonction. C'est quand on a une "application" explicite, notons le F, définie sur tous les ensembles (donc on ne peut pas l'appeler application) qui détermine l'ensemble qu'on associe à un élément de l'ensemble A. Dans un tel cas la formule $q(x,y)$ s'écrit comme

$$q(x,y) \qquad \overset{\text{déf.}}{\Longleftrightarrow} \qquad y = F(x) \;\; .$$

Si c'est le cas, on simplifie l'écriture pour le résultat de l'axiome de remplacement par

$$B \equiv \{\, C \mid \exists x \in A : q(x,C) \,\} \overset{\text{écr. simpl.}}{\equiv} \{\, F(x) \mid x \in A \,\} \;\; . \tag{29.2}$$

Cette écriture ressemble énormément à l'écriture simplifiée pour l'image d'une application (5.8), sauf qu'ici la procédure F n'est pas une application définie sur un

ensemble. On a donc besoin de l'axiome de remplacement pour justifier que le résultat (29.2) est bien un ensemble. D'autre part, cette écriture reflète bien l'aspect "remplacement" de cet axiome : B est l'ensemble des $F(x)$ quand x parcourt l'ensemble A. Autrement dit, on remplace vraiment chaque élément x de A par l'élément $F(x)$.

L'exemple type est l'opération du successeur S. Imaginons qu'on veut remplacer dans un ensemble A chaque élément par son successeur. Si on ne connaît pas trop bien l'ensemble A, on ne peut pas prédire d'avance dans quel ensemble les images $S(a)$ vont atterrir. On ne peut donc pas dire que S est une *application* définie sur A, ce qui empêche de dire que la collection de tous les successeurs des éléments de A est l'image de cette application. On invoque donc l'axiome de remplacement avec la formule $p(x, y)$ donnée par

$$p(x, y) \qquad \overset{\text{déf.}}{\Longleftrightarrow} \qquad y = S(x) \equiv x \cup \{x\}$$

et on obtient, avec l'écriture simplifiée, l'ensemble

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

La situation est presque identique à la situation dans (6.2), sauf que là on a l'hypothèse supplémentaire que les successeurs $S(a)$ avec $a \in A$ appartienent tous à A. Dans ce cas on obtient donc une vraie application dans le sens [4.1].

Dans [2.4] on a introduit une écriture simplifiée qui cache un peu l'utilisation de l'axiome de séparation (Z5). Et au final, cette écriture simplifiée ressemble beaucoup à l'utilsation de l'axiome de remplacement (F). Et effectivement, dans la plupart des cas, l'écriture simplifiée (qui cache donc l'utilisation de l'axiome de séparation) peut être interprété comme une application de l'axiome de remplacement. (À part les cas (5.8) et (6.2) cités ci-dessus, le lecteur trouvera d'autres instances dans (4.7) et [4.10] ; par contre, l'utilisation de l'axiome de remplacement est déjà nécessaire dans (3.5).) D'autre part, une fois qu'on a accepté l'axiome de remplacement, on n'a plus besoin de l'axiome de séparation : on peut le déduire de l'axiome de remplacement.

Ⓟ **29.3 Proposition.** *L'axiome de séparation (Z5) est une conséquence de l'axiome de remplacement (F).*

Le lecteur attentif aura certainement remarqué qu'on a parlé d'une première version de l'axiome de remplacement, ce qui suggère fortement qu'il y a (au moins) une deuxième version. Et effectivement il y a une deuxième version qui est en apparence plus laxiste. On remplace toujours des éléments d'un ensemble A, mais pas systématiquement. Si on visualise l'ensemble A avec ses éléments sur une ligne, alors en face de chaque élément de A on va, soit mettre un seul autre ensemble, soit rien du tout. La décision si oui ou non on met un ensemble en face, et si oui quel ensemble, est codée par une formule $q(x, y)$ qui ne prend que des valeurs "vrai" ou "faux" et qui relie un élément $x \in A$ à un ensemble y. Pour dire qu'on met au plus un ensemble en face de chaque élément de A, on exige que cette formule q a la propriété

$$\forall x \in A \ \forall y, z \ : \ [\ q(x, y) \ \textit{et}\ q(x, z)\ ] \ \Rightarrow y = z \ . \tag{29.4}$$

Si on compare (29.4) avec (29.1), on voit que la condition que pour tout $x \in A$ il existe un ensemble qui est lié à x a disparu ; seulement l'unicité est maintenu. Avec cette définition on obtient la deuxième version de l'axiome de remplacement.

(F) Axiome de remplacement, deuxième version.

$$\forall A \ : \ \big(\forall x \in A \, \forall y, z \ : \ [\ (q(x,y) \text{ et } q(x,z)\ ] \ \Rightarrow y = z \ \big) \quad \Longrightarrow$$
$$\big(\ \exists B \ \forall C \ : \ C \in B \ \Leftrightarrow \ [\ \exists x \ : \ x \in A \text{ et } q(x,C)\ ] \ \big) \ .$$

Par l'axiome d'extensionnalité (Z1) l'ensemble B est unique et complètement déterminé par l'ensemble A et la propriété q. On le note comme avant

$$B \ \overset{\text{déf}}{=} \ \{C \mid \exists x : x \in A \text{ et } q(x,C)\} \equiv \{C \mid \exists x \in A : q(x,C)\} \ .$$

Il est évident que la première version de l'axiome de remplacement est un cas particulier de la deuxième version : une formule q qui vérifie les conditions requises pour la première version vérifie certainement la condition requise par la deuxième version. D'autre part, un argument analogue à la preuve de [29.3] montre que la première version implique la deuxième version. Les deux versions sont donc équivalentes et c'est une question de gout laquelle on préfère écrire.

La deuxième variante a plusieurs avantages : il y a moins de contraintes pour la formule q, et on en déduit plus facilement l'axiome de séparation (Z5) : pour une formule $p(x)$ il suffit de prendre la formule $q(x,y)$ définie par

$$q(x,y) \qquad \overset{\text{déf.}}{\Longleftrightarrow} \qquad y = x \ \text{ et } p(x)$$

pour obtenir, par l'axiome de rempalcement, l'ensemble

$$\{\, C \mid \exists x \in A : C = x \ \text{ et } p(x)\} \equiv \{\, C \mid C \in A \ \text{ et } p(C)\} \ .$$

Il est immédiat que cet ensemble vérifie les condition de l'axiome de séparation (Z5) et personne ne sera choqué quand on simplifie (a simplifié) l'écriture de cet ensemble comme

$$\{\, C \mid \exists x \in A : C = x \ \text{ et } p(x)\} \equiv \{\, C \mid C \in A \ \text{ et } p(C)\} \equiv \{\, x \in A \mid p(x)\} \ .$$

Par contre, la deuxième version n'est pas totalement en concordance avec son nom : on ne "remplace" pas/plus systématiquement.

À part le fait qu'on a vraiment besoin de l'axiome de remplacement dans §30, on peut aussi l'utiliser pour nous simplifier les définitions d'une relation et donc a fortiori d'une application. Mais il ne faut pas surestimer cette simplification, car ce n'est qu'au niveau de l'écriture de la définition que ça joue, pas dans l'utilisation de ces concepts (presque au contraire, comme on verra). Avec l'axiome de remplacement, on n'a plus besoin de préciser qu'une application est entre deux ensembles, il "suffit" de dire qu'un ensemble f est une application s'il vérifie les deux conditions :

(i) $\forall c \in f \ \exists x, y : c = (x,y) \ \text{ et}$

(ii) $\forall x, y, z \ : \ \big[\, (x,y) \in f \ \text{ et } (x,z) \in f \,\big] \ \Rightarrow \ y = z.$

La première condition dit simplement que tout élément de f doit être un couple ; la deuxième condition dit (comme d'habitude) que deux couples dans f dont les premières composantes sont égales doivent avoir aussi leurs deuxièmes composantes égales.

Si on veut dire que c'est une application d'un ensemble A dans un ensemble B, il faut extraire de l'ensemble f son domaine et son image. Et pour cela on a besoin de l'axiome de remplacement. Pour le domaine de définition on utilise la formule

$$q(x,y) \qquad \overset{déf.}{\Longleftrightarrow} \qquad \exists b : x = (y,b) \ ,$$

ce qui donne pour $\mathrm{Dom}(f)$ *l'écriture*

$$\mathrm{Dom}(f) = \{\, a \mid \exists c \in f : \exists b : (a,b) = c \,\} \ .$$

Étant donné qu'on a l'équivalence logique (une tautologie)

$$\big(\ \exists c \in f : \exists b : (a,b) = c\ \big) \quad \Longleftrightarrow \quad \big(\ \exists b : (a,b) \in f\ \big) \ ,$$

on peut simplifier l'écritue de $\mathrm{Dom}(f)$ *en*

$$\mathrm{Dom}(f) = \{\, a \mid \exists b : (a,b) \in f \,\} \ .$$

Et pour l'image on utilise la formule

$$q(x,y) \qquad \overset{déf.}{\Longleftrightarrow} \qquad \exists a : x = (a,y) \ ,$$

ce qui donne pour $\mathrm{Im}(f)$ *l'écriture*

$$\mathrm{Im}(f) = \{\, b \mid \exists c \in f : \exists a : (a,b) = c \,\} \overset{écr.\ simpl.}{=} \{\, b \mid \exists a : (a,b) \in f \,\} \ .$$

À première vue cette définition d'une application paraît plus simple, mais il suffit de réfléchir un tout petit peu pour se rendre compte qu'il y a un inconvénient : si on a d'abord deux ensembles A et B et qu'ensuite on veut décrire une application f de A dans B, il faut dire que f est une application dans le sens ci-dessus qui vérifie en plus les conditions

$$\mathrm{Dom}(f) = A \qquad \textit{et} \qquad \mathrm{Im}(f) \subset B \ .$$

Et donc, ce qu'on a gagné en raccourci dans la définition, on le perd dans l'écriture après.

30. Ensembles bien ordonnés et ordinaux

Soit $A = S(\mathbf{N})$, alors c'est un ordinal [28.13], donc en particulier un ensemble bien ordonné. Si on considère la relation $\approx$ qui formalise l'idée de taille, on montre facilement qu'on a $A \approx \mathbf{N}$. Une bijection possible $f : A \to \mathbf{N}$ est donnée par

$$\forall n \in \mathbf{N} \subset A : f(n) = S(n) \equiv n + 1 \qquad et \qquad f(\mathbf{N}) = 0 \ .$$

D'autre part, A n'est certainement pas équivalent en tant qu'ensemble bien ordonné *à $\mathbf{N}$, car l'élément $\mathbf{N} \in A$ est l'élément maximal et l'ensemble bien ordonné $\mathbf{N}$ n'a pas d'élément maximal. C'est pourquoi on dit que deux ensembles bien ordonnés sont équivalent* en tant qu'ensemble ordonné *s'il existe une bijection qui respecte l'ordre. Il n'est pas difficile de montrer que cette notion a toutes les propriétés d'une relation d'équivalence, sauf que ce n'est pas définie sur un ensemble mais sur la collection de tous les ensembles. La situation est donc analogue à la situation avec la notion de "même taille" §21, §23. On aimerait donner un nom à chaque classe d'équivalence, sauf qu'on n'a pas le droit de parler de ces classes d'équivalences. Une solution possible est, comme suggéré déjà pour la notion de taille, de trouver dans chaque classe un représentant unique qu'on utilise comme nom pour la classe. Et c'est la notion d'ordinal qui fait l'affaire. À l'aide de l'axiome de remplacement on montre qu'il y a, dans chaque classe d'équivalence d'ensembles bien ordonnées, un unique ordinal. Plus précisément, pour chaque ensemble bien ordonné il existe un unique ordinal qui lui est équivalent et deux ensembles bien ordonnés ne sont équivalents en tant qu'ensemble bien ordonné, que si l'ordinal associé est le même. C'est dans ce sens que les ordinaux sont les archetypes d'ensembles bien ordonnés.*

Définition. Soit $(V, \leq_V)$ et $(W, \leq_W)$ deux ensembles totalement ordonnés. On dit qu'une application $f : V \to W$ est *strictement croissante* si elle vérifie la condition

$$\forall v, v' \in V \ : \ v <_V v' \quad \Longrightarrow \quad f(v) <_W f(v') \ .$$

On dit que l'application $f : V \to W$ est un *isomorphisme (d'ensembles totalement ordonnés)* si elle est strictement croissante, bijective et si l'application réciproque $f^{-1} : W \to V$ est aussi strictement croissante. S'il existe un isomorphisme (d'ensembles totalement ordonnés) entre deux ensemble totalement ordonnés, on dit que ces deux ensembles sont *isomorphes (en tant qu'ensembles totalement ordonnés)*.

30.1 Lemme. *Soit $(V, \leq_V)$, $(W, \leq_W)$ et $(X, \leq_X)$ trois ensembles totalement ordonnés et soit $f : V \to W$ et $g : W \to X$ deux applications strictement croissantes. Alors on a les propriétés suivantes..*

(i) *L'application f est injective.*

(ii) *La composée $g \circ f : V \to X$ est strictement croissante.*

(iii) *Si f est surjective, alors f est bijective et $f^{-1} : W \to V$ est strictement croissante.*

(iv) *Si f est bijective, alors pour tout $a \in V$ la restriction de f à $V_{<_V a} \subset V$ est une bijection strictement croissante entre l'idéal $V_{<_V a}$ de V et l'idéal $W_{<_W f(a)}$ de W.*

Pour tout $a \in V$ on a les inclusions $f[V_{<_V a}] \subset W_{<_W f(a)}$ et $f[V_{\leq_V a}] \subset W_{\leq_W f(a)}$. Si en plus f est surjective, alors ces inclusions sont des égalités.

Dans [28.7] on a vu que l'inclusion définit un bon ordre sur tout ensemble dont les éléments sont des ordinaux et que l'appartenance est la relation d'ordre stricte associée. Par [28.5] les éléments d'un ordinal sont des ordinaux. Il s'ensuit que l'inclusion définit un bon ordre sur tout ordinal. Comme on a dit dans [3.8], on a une liste de symboles qu'on utilise pour indiquer une relation d'ordre. Le symbole de l'inclusion ne figure, en général, pas dans cette liste, bien qu'il indique aussi une relation d'ordre [3.13]. Mais c'est surtout le symbole de l'appartenance qui n'y figure pas. La raison est simple : quand on utilise les symboles de l'appartenance et de l'inclusion, on a tendance a se concentrer sur l'aspect "ensemble" des objets concernés, c'est-à-dire qu'on s'intéresse surtout à l'aspect qui est élément de qui. Et si on utilise un symbole pour une relation d'ordre, on se concentre sur l'aspect de comparaison et on ne s'intéresse pas du tout si les objets concernés sont des ensembles qui contiennent des éléments.

Mais pour un ordinal, ces deux aspects sont confondus, ce qui complique l'interprétation d'un raisonnement : faut-il voir (par exemple) l'appartenance comme une comparaison ou comme la "vraie" appartenance d'un élément dans un ensemble ? Bien-sûr, formellement il n'y a rien qui change. Mais pour comprendre/sentir une preuve, cette différence pourrait être cruciale. On a déjà fait allusion a un tel changement de point de vu dans la preuve des équivalences des différentes définitions possibles d'un ordinal. Pour aider le lecteur à distinguer à quelle moment il est plus utile d'utiliser l'interprétation d'une relation d'ordre, on introduit une notation alternative pour les symboles de l'inclusion et d'appartenance.

30.2 Une notation alternative. On introduit le symbole $\prec$ comme un alternative pour le symbole d'appartencance $\in$: $A \prec B$ veut donc dire la même chose que $A \in B$. Et on introduit le symbole $\preccurlyeq$ comme un alternative pour le symbole de l'inclusion $\subset$: $A \preccurlyeq B$ veut donc dire la même chose que $A \subset B$. On utilisera ces symboles alternatives uniquement dans le contexte d'ordinaux. Mais pas systématiquement, car il y aura des occasions où on veut vraiment voir un ordinal comme un ensemble.

Ⓟ **30.3 Lemme.** *Soit α un ordinal muni du bon ordre $\preccurlyeq$ donné par l'appartenance/inclusion et soit $\beta \in \alpha$ un élément. Alors l'idéal $\alpha_{\prec\beta}$ de α est l'ordinal β : $\alpha_{\prec\beta} = \beta$.*

Ⓟ **30.4 Proposition.** *Soit α et β deux ordinaux (munis de leurs bons ordres $\preccurlyeq$ définis par l'appartenance/inclusion) et soit $f : \alpha \to \beta$ une application strictement croissante. Alors on a les propriétés suivantes.*

(i) $\forall \gamma \in \alpha : \gamma \preccurlyeq f(\gamma)$

(ii) $\alpha \preccurlyeq \beta$.

(iii) *Si f est bijective, alors $\alpha = \beta$ et $f = id$.*

Comme on vient de voir, les possibilités pour une application entre deux ordinaux d'être strictement croissante sont assez limitées et deux ordinaux ne peuvent être isomorphes que s'ils sont égaux et *si l'isomorphisme est l'identité. Ceci n'est certainement pas le cas général, car il suffit de penser à l'ensemble totalement ordonné* $\mathbf{R}$ *et l'application strictement croissante* $f : \mathbf{R} \to]-1,1[$ *définie par*

$$f(x) = \frac{x}{|x|+1} \ ,$$

qui fournit un isomorphisme entre $\mathbf{R}$ *et* $]-1,1[$*. Ou à l'isomorphisme* $f : \mathbf{R} \to \mathbf{R}$ *défini par*

$$f(x) = x + a$$

pour un réel $a \in \mathbf{R}$ *fixé mais arbitraire.*

(AF) **30.5 Théorème.** *Soit* $(W, \leq)$ *un ensemble bien ordonné. Alors il existe un unique ordinal* α *et un unique isomorphisme* $f : W \to \alpha$*.*

La preuve de [30.5] se fait en trois étapes. Dans la première étape, qu'on formule comme un lemme indépendant, on démontre l'unicité. Dans la deuxième étape, qu'on formule aussi comme un lemme indépendant, on démontre un cas particulier de [30.5]. Et la troisième étape est (la fin de) la preuve de [30.5].

Ⓟ **30.6 Lemme.** *Soit* $(W, \leq)$ *un ensemble bien ordonné, soit* α *et* β *deux ordinaux et soit* $f : W \to \alpha$ *et* $g : W \to \beta$ *deux isomorphismes. Alors* $\alpha = \beta$ *et* $f = g$*.*

(AF)Ⓟ **30.7 Lemme.** *Soit* $(W, \leq)$ *un ensemble bien ordonné. Si pour tout* $x \in W$ *il existe un ordinal* α *et un isomorphisme* $f : W_{<x} \to \alpha$*, alors il existe un ordinal* β *et un isomorphisme* $g : W \to \beta$*.*

31. Cardinaux

Dans §23, §24 et §27 on a trouvé des résultats concernant la comparaison des tailles d'ensembles. On l'a fait à l'aide des symboles $\approx$ *et* $\precsim$ *qu'on a interprété comme "même taille" et "plus petit ou égal en taille." Dans §?? on a montré que, pour les ensembles finis, dans chaque classe d'équivalence de* $\approx$ *il existe un unique entier naturel qu'on a appelé le cardinal. Et on a montré que la relation* $\precsim$ *correspond exactement avec la relation d'ordre sur* $\mathbf{N}$ *et que les opérations de réunion disjointe, produit cartésien et exponentiation d'ensembles correspond via ce cardinal avec les opérations d'addition, multiplication et exponentiation définies dans* $\mathbf{N}$.

Ici on va étendre, à l'aide de l'axiome du choix et l'axiome de remplacement, la notion de cardinal à toutes les classes d'équivalence. Plus précisément, on va trouver dans chaque classe d'équivalence de $\approx$ *un unique ordinal d'un type spécial (appelé cardinal) et on va montrer que la relation* $\precsim$ *correspond avec la relation d'ordre* $\preccurlyeq$ *(qui n'est rien d'autre que l'inclusion !) entre ordinaux. Par contre, on va* définir *les opérations d'addition, multiplication et exponentiation de cardinaux à l'aide des opérations de réunion disjointe, produit cartésien et exponentiation d'ensembles. Nos résultats concernant la comparaison de tailles vont nous dire que ces opérations ont les propriétés habituelles. Ainsi le cardinal fait office de nom pour la classe d'équivalence de* $\approx$ *et on interprète le cardinal d'un ensemble (l'unique cardinal qui est dans la même classe d'équivalence) comme "le nombre d'éléments" de l'ensemble. Et les opérations qu'on a définies sur les cardinaux étendent les opérations qu'on connait déjà pour les entiers naturels. Ce qu'il faut bien noter c'est qu'ici on ne fait quasiment rien d'autre que* traduire *les résultats déjà obtenus dans §23, §24 et §27 en termes de cardinaux ; le vrai travail est déjà fait (à part l'introduction du cardinal).*

À noter que la quasi totalité des résultats ici ont besoin de l'axiome du choix et de l'axiome de remplacement, simplement parce qu'on invoque l'existence du cardinal d'un ensemble. Et comme dit ci-dessus, pour pouvoir attribuer un cardinal à un ensemble, on a besoin de ces deux axiomes (en plus des 7 axiomes de base). Pour certains on pourrait éviter l'usage des ces axiomes en mettant dans les hypothèses qu'il existe des cardinaux qui ont la même taille que les ensembles concernés. Mais cela devient très artificielle.

La définition du cardinal d'un ensemble A est au fond assez simple : c'est le plus petit ordinal qui a la même taille que A. Un petit peu plus en détail : on invoque l'axiome du choix sous la forme du théorème du bon ordre pour mettre un bon ordre sur A. Ensuite on invoque l'axiome de remplacement pour trouver un (unique) ordinal α qui est isomorphe à cet ensemble bien ordonné. La collection des ordinaux strictement plus petit que α est bien un ensemble (c'est α lui même), qui de plus est bien ordonné (par l'inclusion). On peut donc trouver le plus petit ordinal qui a la même taille que A. L'ordre de notre présentation sera légèrement différent : on commence à définir ce que c'est un cardinal, on montre quelques propriétés et ensuite on montre que tout ensemble est équivalent (en taille) qu'un unique cardinal.

Définition/Rappel. Pour un ensemble ne contenant que des ordinaux (et donc en particulier pour un ordinal) on sait que l'inclusion est un bon ordre et que l'appartenance est la relation d'ordre stricte associée. Quand on veut insister sur l'aspect

"relation d'ordre," on a introduit des notations alternative pour l'iunclusion et l'appartenance [30.2] : pour deux ordinaux α et β on note alternativement

$$\alpha \prec \beta \quad \overset{\text{déf.}}{\equiv} \quad \alpha \in \beta \qquad \text{et} \qquad \alpha \preccurlyeq \beta \quad \overset{\text{déf.}}{\equiv} \quad \alpha \subset \beta \ .$$

→ **31.1 Lemme.** *Soit α et β deux ordinaux. Alors on a l'équivalence*

$$\beta \preccurlyeq \alpha \quad \equiv \quad \beta \subset \alpha \qquad \Longleftrightarrow \qquad \beta \prec S(\alpha) \quad \equiv \quad \beta \in S(\alpha) \ .$$

Définition. Soit α un ordinal. Alors on a évidemment $\alpha \in S(\alpha)$ ainsi que $\alpha \approx \alpha$. Il s'ensuit que l'ensemble $\{\, \gamma \in S(\alpha) \mid \gamma \approx \alpha \,\}$ n'est jamais vide (car contenant α). Ayant constaté cela, on dit qu'un *cardinal* est un ordinal α qui vérifie la condition

$$\alpha = \min \{\, \gamma \in S(\alpha) \mid \gamma \approx \alpha \,\} \ .$$

Notation. Il est d'usage de noter un cardinal infini par le caractère hébreu $\aleph$ indexé par un ordinal (comme $\aleph_\alpha$). Ces cardinaux $\aleph_\alpha$ ont une définition bien précise, qu'on donnera dans [31.16]. Ici on va, suivant **[Dug66]**, utiliser le caractère $\aleph$ sans indexe pour un cardinal quelconque. Et si on a besoin de plusieurs, on parlera de $\aleph$, $\aleph'$ et $\aleph''$.

Ⓟ **31.2 Lemme.**

(i) *Soit α un ordinal, alors l'ensemble $\aleph$ défini par*

$$\aleph = \min \{\, \gamma \in S(\alpha) \mid \gamma \approx \alpha \,\}$$

est un cardinal vérifiant $\aleph \approx \alpha$.

(ii) *Soit α un ordinal. Alors α est un cardinal si et seulement si pour tout ordinal $\beta \prec \alpha$ il n'existe pas une injection $f : \alpha \to \beta$.*

(iii) *Soit $\aleph$ et $\aleph'$ deux cardinaux. Alors on a l'équivalence*

$$\aleph \approx \aleph' \qquad \Longleftrightarrow \qquad \aleph = \aleph' \ .$$

(iv) *Tout ordinal fini, c'est-à-dire tout entier naturel, est un cardinal.*

(v) **N** *est un cardinal*

(AFC) Ⓟ **31.3 Proposition.** *Soit A un ensemble. Alors il existe un unique cardinal $\aleph$ tel qu'on a $A \approx \aleph$.*

(AFC) **31.4 Définition.** Soit A un ensemble. Alors *le cardinal de A*, noté $\mathrm{card}(A)$ est l'unique cardinal $\aleph$ vérifiant $A \approx \aleph$ dont l'existence est garantie par [31.3] :

$$\mathrm{card}(A) = \aleph \qquad \Longleftrightarrow \qquad A \approx \aleph \text{ et } \aleph \text{ un cardinal.}$$

Nota Bene. Dans [25.7] on a déjà défini la notion de cardinal d'un ensemble fini par l'équivalence (pour un ensemble fini)

$$\mathrm{card}(A) = n \qquad \Longleftrightarrow \qquad A \approx n \text{ et } n \in \mathbf{N} \ .$$

Mais selon [31.2.iv] un élément $n \in \mathbf{N}$ est un cardinal, ce qui montre que la définition [25.7] coïncide avec la définition plus générale [31.4].

(AFC) **31.5 Corollaire.** *Soit A et B deux ensembles. Alors on a les équivalences*

$$\operatorname{card}(A) = \operatorname{card}(B) \iff A \approx B \quad \textit{(il existe une bijection } f : A \to B\textit{)}$$

et

$$\operatorname{card}(A) \preccurlyeq \operatorname{card}(B) \iff A \precsim B \quad \textit{(il existe une injection } f : A \to B\textit{)} \ .$$

Avec [31.3] et [31.5] on a réussi ce qu'on voulait faire : dans chaque collection d'ensembles qui ont la même taille (notre boîte ou classe d'équivalence pour $\approx$) on a trouvé un représentant unique, à savoir un cardinal. En plus, notre idée d'une relation d'ordre (plus petit ou égal en taille), qu'on avait défini comme étant en bijection avec un sous-ensemble, se traduit au niveau des cardinaux vraiment par l'inclusion : pour les ordinaux les symboles $\preccurlyeq$ et $\subset$ sont équivalents. Autrement dit, un ensemble A est en bijection avec un sous-ensemble d'un ensemble B si et seulement si le représentant/cardinal de A est inclu dans le représentant/cardinal de B.

(AFC) **Définition.** Pour définir les trois opération d'addition, multiplication et exponentiation de cardinaux, on utilise l'idée que ces opérations correspondent avec des opérations entre ensembles comme on a vu dans [25.10]. Là on connaissait déjà ces opérations (sur les entiers naturels) et on a fait le lien avec les opérations entre ensembles. Ici on utilise cela pour *définir* ces opérations entre cardinaux en se basant sur les opérations entre ensembles correspondantes. Le fait que la définition du cardinal en général [31.4] coïncide avec la définition du cardinal d'un ensemble fini [25.7] garantit que notre définition de ces trois opérations sur des cardinaux correspond bien avec les opérations correspondantes sur $\mathbf{N}$.

Soit donc $\aleph$ et $\aleph'$ deux cardinaux. Alors pour l'addition on définit le cardinal $\aleph + \aleph'$ comme le cardinal de la réunion disjointe :

$$\aleph + \aleph' = \operatorname{card}(\aleph \sqcup \aleph') \ .$$

Pour la multiplication on se base sur le produit cartésien et on définit le cardinal $\aleph \times \aleph'$ comme le cardinal du produit cartésien :

$$\aleph \times \aleph' = \operatorname{card}(\aleph \times \aleph') \ ,$$

où à gauche le symbole $\times$ désigne le produit de deux cardinaux, tandis qu'à droite le symbole $\times$ (légèrement plus grand) désigne le produit cartésien de deux ensembles.

Pour l'exponentiation on se base sur l'ensemble des applications de $\aleph$ dans $\aleph'$. Sauf qu'ici on tombe tout de suite dans un piège notationnelle : on utilise la même notation pour l'exponentielle de deux cardinaux que pour l'ensemble des application d'un ensemble dans un autre. On définit donc $\aleph^{\aleph'}$, c'est-à-dire "$\aleph$ à la puissance $\aleph'$" comme le cardinal de l'ensemble des applications de $\aleph$ dans $\aleph'$, ce qui est *aussi* noté comme $\aleph^{\aleph'}$. Cela donne donc la définition

$$\aleph^{\aleph'} = \operatorname{card}(\aleph^{\aleph'}) \ ,$$

avec le sous-entendu qu'à gauche on désigne le cardinal "$\aleph$ à la puissance $\aleph'$," tandis qu'à droite on désigne l'ensemble des application de $\aleph$ dans $\aleph'$. Une meilleure définition serait d'écrire

$$\aleph^{\aleph'} = \mathrm{card}\big(\mathrm{App}(\aleph', \aleph)\big) \ .$$

Mais la confusion notationnelle reste, car on peut toujours interpréter la notation $\aleph^{\aleph'}$ comme l'ensemble $\mathrm{App}(\aleph', \aleph)$, ce qui n'est pas un cardinal.

Avec la définition des opérations d'addition, multiplication et exponentiation de cardinaux, on peut maintenant traduire les résultats de §23, §24 et §27 en termes d'égalités et inégalités entre cardinaux.

(AFC) **31.6 Le lien entre les opérations ensemblistes et les opérations sur cardinaux.** *Soit A et B deux ensembles quelconques. Alors on a les propriétés suivantes.*

(i) *Si A est un cardinal, alors* $\mathrm{card}(A) = A$.

(ii) *Si $A \subset B$, alors* $\mathrm{card}(A) \preccurlyeq \mathrm{card}(B)$.

(iii) $\mathrm{card}(A \cup B) \preccurlyeq \mathrm{card}(A) + \mathrm{card}(B)$.

(iv) *Si $A \cap B = \emptyset$, alors* $\mathrm{card}(A \cup B) = \mathrm{card}(A) + \mathrm{card}(B)$.

(v) $\mathrm{card}(A \times B) = \mathrm{card}(A) \times \mathrm{card}(B)$.

(vi) $\mathrm{card}(A^B) = \mathrm{card}(A)^{\mathrm{card}(B)}$.

(vii) $\mathrm{card}(A) = 0 \ \Leftrightarrow \ A = \emptyset$.

(AFC) **31.7 Associativité, commutativité, distributivité et plus.** *Soit A et B deux ensembles quelconques. Alors on a les propriétés suivantes.*

(i) $\mathrm{card}(A) + 0 = \mathrm{card}(A)$.

(ii) $\mathrm{card}(A) \times 0 = 0$.

(iii) $\mathrm{card}(A) \times 1 = \mathrm{card}(A)$.

(iv) $\mathrm{card}(A) + \mathrm{card}(B) = \mathrm{card}(B) + \mathrm{card}(A)$.

(v) $\mathrm{card}(A) \times \mathrm{card}(B) = \mathrm{card}(B) \times \mathrm{card}(A)$.

(vi) $\mathrm{card}(A) \times \big(\mathrm{card}(B) + \mathrm{card}(C)\big) = \big(\mathrm{card}(A) \times \mathrm{card}(B)\big) + \big(\mathrm{card}(A) \times \mathrm{card}(C)\big)$.

(vii) $\mathrm{card}(A)^{\mathrm{card}(B) \times \mathrm{card}(C)} = \big(\mathrm{card}(A)^{\mathrm{card}(B)}\big)^{\mathrm{card}(C)}$.

(viii) $\mathrm{card}(A)^{\mathrm{card}(B) + \mathrm{card}(C)} = \big(\mathrm{card}(A)^{\mathrm{card}(B)}\big) \times \big(\mathrm{card}(A)^{\mathrm{card}(C)}\big)$.

(AFC) **31.8 Quelques cas particuliers.** *Soit A un ensemble. Alors on a l'égalité*

$$2 \times \mathrm{card}(A) = \mathrm{card}(A) + \mathrm{card}(A) \ ,$$

ainsi que les égalités

$$\mathrm{card}(A)^0 = 1 \quad , \quad 0^{\mathrm{card}(A)} = 0 \ \ \textit{si } A \neq \emptyset$$

$$\mathrm{card}(A)^1 = \mathrm{card}(A) \quad , \quad 1^{\mathrm{card}(A)} = 1$$

$$\mathrm{card}(A)^2 = \mathrm{card}(A) \times \mathrm{card}(A) \quad , \quad 2^{\mathrm{card}(A)} = \mathrm{card}\big(\mathcal{P}(A)\big) \ .$$

(AFC) **31.9 "Croissance" des opérations.** *Soit A, B, C et D quatre ensembles vérifiant* $\mathrm{card}(A) \preccurlyeq \mathrm{card}(B)$ *et* $\mathrm{card}(C) \preccurlyeq \mathrm{card}(D)$. *Alors on a aussi les inégalités*

$$\begin{aligned} \mathrm{card}(A) + \mathrm{card}(C) &\preccurlyeq \mathrm{card}(B) + \mathrm{card}(D) \\ \mathrm{card}(A) \times \mathrm{card}(C) &\preccurlyeq \mathrm{card}(B) \times \mathrm{card}(D) \\ \mathrm{card}(C)^{\mathrm{card}(A)} &\preccurlyeq \mathrm{card}(D)^{\mathrm{card}(B)} \quad . \end{aligned}$$

(AFC) **31.10 Une inégalité stricte.** *Soit A un ensemble, alors on a l'inégalité stricte* $\mathrm{card}(A) \prec 2^{\mathrm{card}(A)}$.

(AFC) **31.11 Des égalités pour ensembles infinis.** *Soit A et B deux ensembles avec* $\mathbf{N} \preccurlyeq \mathrm{card}(A)$. *Autrement dit, A est un ensemble infini.*

(i) *Si* $\mathrm{card}(B) \preccurlyeq \mathrm{card}(A)$, *alors* $\mathrm{card}(A) + \mathrm{card}(B) = \mathrm{card}(A)$.

(ii) *Si* $1 \preccurlyeq \mathrm{card}(B) \preccurlyeq \mathrm{card}(A)$, *alors* $\mathrm{card}(A) \times \mathrm{card}(B) = \mathrm{card}(A) \times 1 = \mathrm{card}(A)$.

(iii) *Si* $2 \preccurlyeq \mathrm{card}(B) \preccurlyeq \mathrm{card}(A)$, *alors* $\mathrm{card}(B)^{\mathrm{card}(A)} = 2^{\mathrm{card}(A)}$.

(iv) *Pour tout* $n \in \mathbf{N}^*$ *on a* $\mathrm{card}(A)^n = \mathrm{card}(A)$.

(AFC) **31.12 Proposition.** *Il n'existe pas un ensemble qui contient tous les cardinaux.*

On termine ce chapitre avec un résultat qui est le début de l'étude de ce qu'on appelle les "grands cardinaux." Une façon d'exprimer ce résultat est de dire qu'il y a autant de cardinaux infinis que d'ordinaux. En général on présente ce résultat en disant que pour tout ordinal α il y a un cardinal infini $\aleph_\alpha$, à commencer avec $\aleph_0 = \mathbf{N}$. Ici on a jugé plus facile de montrer la réciproque : pour tout cardinal infini il y a un ordinal qu'on appelle son rang. Une fois qu'on a montré que cette "application" est bijective, dans le sens que pour tout ordinal α il existe un unique cardinal infini dont le rang est α, alors on peut inverser la situation et parler du cardinal infini $\aleph_\alpha$ tel qu'on le trouve dans la litérature.

(AF) **Définition.** Soit $\aleph$ un cardinal infini. Alors on définit $I(\aleph)$ comme l'ensemble des cardinaux infinis strictement plus petit que $\aleph$:

$$I(\aleph) = \{\, \aleph' \in \aleph \mid \aleph' \text{ un cardinal infini} \,\} \quad .$$

C'est bien un ensemble par l'axiome de séparation et contient bien les cardinaux strictement plus petits que $\aleph$, car pour les ordinaux (donc a fortiori pour les cardinaux), la version stricte de la relation d'ordre est l'appartenance [30.2]. Il s'ensuit que $I(\aleph)$ ne contient que des ordinaux et donc, selon [28.7], c'est un ensemble bien ordonné par l'inclusion. Selon [30.5] il existe donc un unique ordinal, qu'on note $\mathcal{R}(\aleph)$, et un unique isomorphisme (d'ensembles bien ordonnés) $f : I(\aleph) \to \mathcal{R}(\aleph)$. On appelle cet ordinal le *rang du cardinal infini* $\aleph$. Dans le cas $\aleph = \mathbf{N}$ on a $I(\mathbf{N}) = \emptyset$ et donc $\mathcal{R}(\mathbf{N}) = 0$.

(AFO) **31.13 Lemme.** *Soit $\aleph$ un cardinal infini et soit $f : I(\aleph) \to \mathcal{R}(\aleph)$ l'unique isomorphisme. Alors on a les porpriétés suivantes.*

(i) $\forall \aleph' \in I(\aleph) : \mathcal{R}(\aleph') = f(\aleph') \in \mathcal{R}(\aleph)$. *En mots : tout cardinal infini strictement plus petit que $\aleph$ a un rang strictement plus petit que $\mathcal{R}(\aleph)$.*

(ii) $\forall \beta \in \mathcal{R}(\aleph) : \mathcal{R}\big(f^{-1}(\beta)\big) = \beta$. *En mots : tout ordinal strictement plus petit que $\mathcal{R}(\aleph)$ est le rang d'un cardinal infini strictement plus petit que $\aleph$.*

(AFO) **31.14 Corollaire.** *Soit $\aleph, \aleph'$ deux cardinaux infinis. Si on a $\aleph \prec \aleph'$, alors on a $\mathcal{R}(\aleph) \prec \mathcal{R}(\aleph')$. En particulier on a l'implication $\mathcal{R}(\aleph) = \mathcal{R}(\aleph') \Rightarrow \aleph = \aleph'$.*

(AFO) **31.15 Proposition.** *Soit α un ordinal. Alors il existe un unique cardinal infini $\aleph$ tel que $\alpha = \mathcal{R}(\aleph)$.*

31.16 Définition. Soit α un ordinal, alors il est d'usage de noter l'unique cardinal dont le rang est α par $\aleph_\alpha$ et de dire que c'est le α-ième cardinal infini. Et après, on n'aura plus besoin de la notion de rang, car on a évidemment $\mathcal{R}(\aleph_\alpha) = \alpha$. En particulier on a $\aleph_0 = \mathbf{N}$, le premier cardinal infini (le zéro-ième).

Une reformulation de l'hypothèse du continu (généralisé). Avec les cardinaux infinis indexés par un ordinal, on peut reformuler l'hypothèse du continu [24.12] comme l'égalité

$$2^{\aleph_0} = \aleph_1$$

et l'hypothèse du continu généralisé [27.7] comme

$$\forall \alpha \text{ un ordinal} : 2^{\aleph_\alpha} = \aleph_{S(\alpha)} \ .$$

32. L'axiome de fondation

L'axiome de fondation prend une place particulière parmi les axiomes de Zermelo. Un mathématicien λ ne travaillant pas dans le domaine de la théorie des ensembles ne s'en sert jamais. En plus, en informatique théorique on le remplace parfois par un axiome opposé (appelé axiome d'anti-fondation). Le but principal de cet axiome est d'exclure qu'il existe des ensembles qui sont élément d'eux même (et d'éviter des boucles). Pour bien expliquer l'idée soujacente, on commence avec une équivalence entre deux propriétés qu'on peut (ou pas) attribuer à une relation sur un ensemble.

(AC) **32.1 Lemme.** *Soit $< \subset E \times E$ une relation quelconque (mais rien ne nous interdit de penser que c'est la version stricte d'une relation d'ordre) sur un ensemble E et considérons les deux propriétés suivantes.*

(i) *Tout sous-ensemble non-vide de E admet "un élément minimal" [19.1], [19.11] :*

$$\forall A \subset E : A \neq \emptyset \;\Rightarrow\; \big[\; \exists a \in A \; \forall x \in A : x \not< a \;\big] \;.$$

(ii) *Il n'existe pas une suite $(a_n)_{n\in\mathbf{N}}$ dans E "strictement décroissante" dans le sens $a_{n+1} < a_n$ pour tout $n \in \mathbf{N}$:*

$$\neg\big[\; \exists f : \mathbf{N} \to E \; \forall n \in \mathbf{N} : f(n+1) < f(n) \;\big] \;.$$

Alors la propriété (i) implique la propriété (ii) et si on accepte l'axiome du choix, alors la propriété (ii) implique la propriété (i).

Bien que les deux propriétés données dans [32.1] s'appliquent à n'importe quelle relation sur un ensemble, il est utile de penser qu'il s'agit de la version stricte d'une relation d'ordre pour l'interpréter. La première condition dit donc que tout sous-ensemble non-vide admet un élément minimal (à ne pas confondre avec un plus petit élément) et la deuxième dit qu'il n'existe pas une suite (infinie) qui est (strictement) décroissante. Une autre façon d'exprimer cela est de dire que si on cherche toujours des éléments "avant" ou "plus petit," alors on doit forcément toucher le fond à un moment donné : il est impossible qu'on puisse descendre toujours plus bas (une suite infinie vérifiant $a_{n+1} < a_n$ pour tout $n \in \mathbf{N}$).

Si on applique cette idée à la "relation" $\in$ d'appartenance, on exprime l'idée qu'il n'existe pas une suite d'ensembles A_n vérifiant $A_{n+1} \in A_n$ pour tout $n \in \mathbf{N}$. Si on réfléchit un petit peu, on commence avec un ensemble A_0. Si A_0 n'est pas vide, il contient au moins un élément, disons $A_1 \in A_0$. Mais les éléments de A_0 sont eux aussi des ensembles. Donc si A_1 n'est pas vide, par le même argument, il existe $A_2 \in A_1$. Et on peut continuer ainsi. L'idée de non-existence d'une telle suite infinie dit donc que ce processus doit s'arrêter, on doit toucher le fond et trouver l'ensemble vide.[1] *Et c'est exactement cela qu'exprime l'axiome de fondation, écrit sous la forme de la propriété (i) que tout ensemble non-vide admet un élément "minimal."*

1. Si on ajoute la notion d'atomes à la théorie, cela devient la propriété qu'à un moment donné on tombe sur un atome, pas forcément sur l'ensemble vide.

(Z10) Axiome de fondation. $\forall A : A \neq \emptyset \;\Rightarrow\; \big[\; \exists a \in A \; \forall x \in A : x \notin a \;\big]$.

Remarque. Si on devient puriste et qu'on ne veut pas invoquer d'autres axiomes pour formuler l'axiome de fondation, on peut l'écrire sous la forme

$$\forall A : \big[\; \exists a_o : a_o \in A \;\big] \;\Rightarrow\; \big[\; \exists a \in A \; \forall x \in A : x \notin a \;\big] \;.$$

Et si on devient moins puriste et qu'on accepte d'utiliser la notion d'intersection, on peut écrire l'axiome de fondation sous la forme

$$\forall A : A \neq \emptyset \;\Rightarrow\; \big[\; \exists a \in A : a \cap A = \emptyset \;\big] \;.$$

Ⓟ **32.2 Lemme.** *Si on accepte l'axiome de fondation, il n'existe pas un ensemble A vérifiant $A \in A$. Et il n'existe pas deux ensembles A et B vérifiant $A \in B$ et $B \in A$.*

Si on a peur d'ensembles qui ont la propriété $A \in A$ (on pourrait penser au paradoxe de Russell !), ou des boucles du style $A \in B \in C \in A$, alors il faut adopter l'axiome de fondation. Mais dans la pratique de tous les jours d'un mathématicien λ (ne travaillant pas en logique ou théorie des ensembles), on n'en a pas besoin. En plus, on a vu qu'il y a des ensembles qui ont cette propriété d'une façon naturelle : les ordinaux et donc a fortiori les entiers naturels.

Chapitre 6

Les preuves

Les preuves de §1

Preuve de [1.2]. Les deux inclusions $A \subset B$ et $B \subset A$ veulent dire par définition qu'on a les propriétés

$$\forall C \ : \ C \in A \ \Rightarrow \ C \in B \qquad \text{et} \qquad \forall C \ : \ C \in B \ \Rightarrow \ C \in A \ .$$

On a donc l'équivalence

$$\forall C \ : \ C \in A \ \Leftrightarrow \ C \in B \ ,$$

ce qui implique selon l'axiome d'extensionnalité qu'on a $A = B$. CQFD

Preuve de [1.3]. Pour montrer l'inclusion $A \subset C$, il faut montrer l'implication

$$D \in A \qquad \Longrightarrow \qquad D \in C \ .$$

Prenons donc $D \in A$. Alors par l'inclusion $A \subset B$ on en déduit qu'on a $D \in B$. Mais alors par l'inclusion $B \subset C$ on en déduit $D \in C$ comme voulu. CQFD

Preuve de [1.4]. Si A et B sont deux ensembles qui ont la propriété de l'axiome de l'ensemble vide, on aura

$$\forall C \ : \ C \notin A \qquad \text{et} \qquad \forall C \ : \ C \notin B \ .$$

On aura donc certainement l'équivalence

$$C \in A \Leftrightarrow C \in B \ ,$$

ce qui entraîne avec l'axiome d'extensionnalité qu'on doit avoir $A = B$. CQFD

Preuve de [1.9]. Prenons $C \in X$. Selon la définition de $\cup A$ on a $C \in \cup A$ si et seulement si on a

$$\exists D \ : \ D \in A \text{ et } C \in D \ .$$

Mais ceci est vrai pour le choix $D = X$, donc $C \in \cup A$ comme voulu. CQFD

Preuve de [1.12]. À l'aide de l'axiome de la réunion on définit d'abord l'ensemble X comme la réunion de A :

$$X = \cup A = \bigcup_{D \in A} D \ .$$

Ensuite on invoque l'axiome de séparation avec l'ensemble X et la propriété $p(x)$ que x appartient à tous les éléments de A pour obtenir l'ensemble B :

$$B = \{\, C \in X \mid \forall D \ : \ D \in A \ \Rightarrow \ C \in D \,\} \ .$$

Par définition de ce B on a l'équivalence

$$C \in B \ \Leftrightarrow \ [\, C \in X \text{ et } (\forall D \ : \ D \in A \ \Rightarrow \ C \in D) \,] \ , \tag{33.1}$$

ce qui nous donne l'implication

$$C \in B \ \Rightarrow \ (\forall D \ : \ D \in A \ \Rightarrow \ C \in D) \ .$$

Pour obtenir l'implication dans l'autre sens on raisonne comme suit. L'hypothèse $A \neq \emptyset$ est équivalent avec $\exists Y : Y \in A$. Si on part de l'hypothèse supplémentaire qu'on a $\forall D : D \in A \ \Rightarrow \ C \in D$, alors on obtient en particulier pour $D = Y$ la conclusion $C \in Y$. Avec [1.9] on a donc $C \in X$. Et donc par définition de B (33.1) on a bien $C \in B$. CQFD

Les preuves de §2

Preuve de [2.1]. On a $y \in \{x, y\} = \{x, z\}$, donc par l'axiome de la paire on a $y = x$ ou $y = z$. Si on a $y = x$, alors on a $z \in \{x, z\} = \{x, y\} = \{y\}$, ce qui implique qu'on a $z = y$. Dans tous les cas on a donc la conclusion $y = z$. CQFD

Preuve de [2.2]. L'implication inverse étant triviale, on suppose qu'on a l'égalité $(a, b) = (c, d)$ et on essaye de montrer qu'on a les égalités $a = c$ et $b = d$. L'égalité de départ nous donne par définition l'égalité

$$\{\,\{a\}, \{a, b\}\,\} = \{\,\{c\}, \{c, d\}\,\} \ . \tag{33.2}$$

Si on regarde l'élément $\{a\}$ dans l'ensemble de gauche, il appartient à l'ensemble de droite, donc on a

$$\{a\} = \{c\} \text{ ou } \{a\} = \{c, d\} \ .$$

Dans le premier cas on a directement $a = c$ et dans le deuxième cas on a $a = c = d$, donc aussi $a = c$. Par [2.1] appliqué avec $x = \{a\} = \{c\}$, $y = \{a, b\}$ et $z = \{c, d\}$ on obtient donc l'égalité

$$\{a, b\} = \{c, d\} \ .$$

Mais on savait déjà qu'on a $a = c$, donc une nouvelle application de [2.1], maintenant avec $x = a = c$, $y = b$ et $z = d$ nous donne $b = d$ comme voulu. CQFD

Preuve de [2.3]. Étant donné que A et B sont des ensembles, $A \cup B$ est un ensemble par l'axiome de la réunion. Par l'axiome de l'ensemble des parties appliqué deux fois il s'ensuit que $\mathcal{P}\big(\mathcal{P}(A \cup B)\big)$ est un ensemble.

L'observation cruciale est maintenant qu'un couple ordonné (a, b) avec $a \in A$ et $b \in B$ appartient à cet ensemble. Pour le voir on remarque d'abord que a et b appartiennent tous les deux à la réunion $A \cup B$. Ensuite on constate que les ensembles $\{a\}$ et $\{a, b\}$ sont des sous-ensembles de cette réunion $A \cup B$, donc appartiennent à $\mathcal{P}(A \cup B)$. Il s'ensuit que l'ensemble $(a, b) = \{\{a\}, \{a, b\}\}$ est un sous-ensemble de $\mathcal{P}(A \cup B)$, donc appartient à $\mathcal{P}\big(\mathcal{P}(A \cup B)\big)$.

Il suffit maintenant d'invoquer l'axiome de séparation pour définir l'ensemble P comme

$$P = \{C \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big) \mid \exists a \in A \ \exists b \in B : C = (a, b)\ \} \ .$$

Il est immédiat de la définition de ce P qu'on a l'implication

$$C \in P \quad \Longrightarrow \quad \exists a \in A \ \exists b \in B : C = (a, b) \ .$$

Pour l'implication inverse il suffit de se rappeler qu'on a $(a, b) \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big)$ pour en déduire qu'on a bien $C \in P$. CQFD

Preuve de [2.7]. Pour montrer l'implication directe, on prend $a \in A$ et $b \in B$. Alors par définition du produit cartésien, on a $C = (a, b) \in A \times B$. Par l'hypothèse $p(C)$ est vrai, c'est-à-dire qu'on a $p\big((a, b)\big)$. Pour l'implication réciproque, on prend $C \in A \times B$. Par définition du produit cartésien, il existe $a \in A$ et $b \in B$ tels que $C = (a, b)$. Par l'hypothèse $p\big((a, b)\big)$ est vrai, c'est-à-dire qu'on a $p(C)$. CQFD

Preuve de [2.8]. Selon la définition du produit cartésien on a l'équivalence

$$C \in \emptyset \times A \quad \Longleftrightarrow \quad \exists a, b \ : \ a \in A \text{ et } b \in \emptyset \text{ et } C = (a, b) \ .$$

Si on prend la négation à chaque coté on obtient l'équivalence

$$C \notin \emptyset \times A \quad \Longleftrightarrow \quad \forall a, b \ : \ a \notin A \text{ ou } b \notin \emptyset \text{ ou } C \neq (a, b) \ .$$

Par définition de l'ensemble vide, la condition $b \notin \emptyset$ est toujours vraie, donc la partie de droite dans cette équivalence est toujours vraie, donc la partie de gauche aussi. Ce qui veut dire, avec l'axiome de l'extensionnalité, que $\emptyset \times A$ est l'ensemble vide. Le même argument s'applique au cas $A \times \emptyset$. CQFD

Preuve de [2.9]. Par définition du produit cartésien on a l'équivalence

$$C \in A \times B \quad \Longleftrightarrow \quad \exists a, b \ : \ a \in A \text{ et } b \in B \text{ et } C = (a, b) \ .$$

Selon les inclusions $A \subset A'$ et $B \subset B'$ on a les implications

$$a \in A \quad \Rightarrow \quad a \in A' \qquad \text{et} \qquad b \in B \quad \Rightarrow \quad b \in B' \ .$$

Ces deux observations combinées nous donnent l'implication

$$C \in A \times B \quad \Longrightarrow \quad \exists a, b \ : \ a \in A' \text{ et } b \in B' \text{ et } C = (a, b) \ ,$$

où la conclusion est équivalent à la condition $C \in A' \times B'$. CQFD

Les preuves de §3

Preuve de [3.3]. Selon l'axiome de séparation on a l'équivalence

$$z \in \{y \in B \mid \exists x : (x,y) \in R\} \iff z \in B \quad \text{et} \quad \exists x : (x,z) \in R \ .$$

L'hypothèse $R \subset C \times D$ nous permet donc de faire le raisonnement

$$\begin{aligned} z \in B \quad \text{et} \quad \exists x : (x,z) \in R \quad &\Rightarrow \quad \exists x : (x,z) \in R \quad \text{et} \quad (x,z) \in C \times D \\ &\Rightarrow \quad \exists x : (x,z) \in R \quad \text{et} \quad z \in D \\ &\Leftrightarrow \quad z \in D \quad \text{et} \quad \exists x : (x,z) \in R \ . \end{aligned}$$

Ainsi on a démontré l'implication

$$z \in \{y \in B \mid \exists x : (x,y) \in R\} \implies z \in \{y \in D \mid \exists x : (x,y) \in R\} \ .$$

La preuve de l'implication dans l'autre sens étant analogue, on a montré l'égalité voulue par double inclusion. CQFD

Preuve de [3.6]. Si R est une relation entre A et B, alors par définition on a

$$\mathrm{Dom}(R) = \{x \in A \mid \exists y : (x,y) \in R\} \overset{(Z5)}{\subset} A$$

et

$$\mathrm{Im}(R) = \{y \in B \mid \exists x : (x,y) \in R\} \overset{(Z5)}{\subset} B \ .$$

Pour l'autre implication, supposons que R est une relation entre C et D vérifiant $\mathrm{Dom}(R) \subset A$ et $\mathrm{Im}(R) \subset B$. Pour en déduire l'inclusion $R \subset A \times B$, on tient le raisonnement :

$$\begin{aligned} X \in R \quad &\overset{R \subset C \times D}{\Leftrightarrow} \quad \exists c \in C \ \exists d \in D : X = (c,d) \in R \\ &\overset{\text{déf. Dom et Im}}{\Rightarrow} \quad \exists c \in \mathrm{Dom}(R) \ \exists d \in \mathrm{Im}(R) : X = (c,d) \in R \\ &\overset{\text{hyp.}}{\Rightarrow} \quad \exists c \in A \ \exists d \in B : X = (c,d) \in R \\ &\Rightarrow \quad X \in A \times B \ . \end{aligned}$$

CQFD

Preuve de [3.9]. Pour la première équivalence on fait le raisonnement

$$\begin{aligned} a < b \text{ ou } a = b \quad &\Leftrightarrow \quad (a \leq b \text{ et } a \neq b) \text{ ou } a = b \\ &\Leftrightarrow \quad (a \leq b \text{ ou } a = b) \text{ et } (a \neq b \text{ ou } a = b) \\ &\Leftrightarrow \quad a \leq b \text{ ou } a = b \quad \Leftrightarrow \quad a \leq b \ , \end{aligned}$$

où la troisième équivalence est vraie car "$a \neq b$ ou $a = b$" est toujours vrai et la quatrième équivalence est vrai car on a l'implication $a = b \ \Rightarrow \ a \leq b$. La deuxième équivalence se montre de la même façon et est laissée aux bons soins du lecteur.

CQFD

Preuve de [3.11]. Par définition de l'inégalité stricte on a aussi l'inégalité large. Donc par transitivité d'une relation d'ordre, on a $a \leq c$. Si on avait $a = c$, alors on aurait en particulier $a \leq b$ et $b \leq a$ (l'inégalité stricte implique l'inégalité large), donc

par anti-symétrie d'une relation d'ordre on aurait $b = a = c$. Mais cela contredit l'inégalité stricte $a < b$ ou $b < c$. On ne peut donc pas avoir $a = c$, d'où l'inégalité stricte $a < c$. CQFD

Preuve de [3.12]. Notons d'abord que, parmi les trois propriétés $a < b$, $a = b$ et $a > b$, il est impossible qu'il y en a deux qui sont vraies. Par définition de $a < b$ et $a > b$ on ne peut pas avoir $a = b$ en même temps que $a < b$ ou $a > b$. Et si on a $a < b$ et $a > b$, alors on aurait en particulier $a \leq b$ et $a \geq b$ et donc par anti-symétrie on aurait $a = b$. Mais cela est exclu par $a < b$. L'équivalence avec la condition (iv) réside donc dans le fait qu'il y a (au moins) une des trois propriétés qui est vraie.

• (i) $\Rightarrow$ (ii). Par hypothèse on a, pour tout $a, b \in A$, $a \leq b$ ou $b \leq a$. Si on a en plus $a \not\leq b$, on a donc $b \leq a$, ce qui est équivalent à $a \geq b$. Ce dernier est équivalent à $a > b$ ou $a = b$. Mais si on avait $a = b$, on aurait en particulier $a \leq b$, ce qui est exclu par hypothèse. On a donc $a > b$. Ainsi on a montré l'implication $a \not\leq b \Rightarrow a > b$.

Pour l'implication réciproque, si on a $a > b$, on a $a \geq b$ et $a \neq b$, ce qui est équivalent à $b \leq a$ et $b \neq a$. Si on avait $a \leq b$, alors par anti-symétrie on aurait $a = b$, ce qui est exclu. Donc on doit avoir $a \not\leq b$.

• (ii) $\Leftrightarrow$ (iii). En prenant la négation dans l'équivalence donné en (ii) on obtient l'équivalence $a \leq b \Leftrightarrow a \not> b$. Par définition ceci est équivalent à l'équivalence $b \geq a \Leftrightarrow b \not< a$. En échangeant les noms a et b on obtient donc (iii).

• (iii) $\Rightarrow$ (iv). Selon (iii), si on n'a pas $a < b$, alors on a $a \geq b$, ce qui est équivalent à $a > b$ ou $a = b$. Ainsi au moins une des trois propriétés est vraie.

• (iv) $\Rightarrow$ (i). Pour tout $a, b \in A$ au moins une des trois propriétés est vraie. On a donc en particulier $a \leq b$ ou $a = b$ ou $a \geq b$, ce qui implique qu'on a (au moins) $a \leq b$ ou $b \geq a$. CQFD

Preuve de [3.13]. Pour tout $X \in \mathcal{P}(A)$ on a $X R X$, car on a l'inclusion $X \subset X$ (valable pour tout ensemble, pas seulement pour les sous-ensembles de A).

Si, pour $X, Y \in \mathcal{P}(A)$ on a $X R Y$ et $Y R X$, alors cela veut dire qu'on a $X \subset Y$ et $Y \subset X$. Par double inclusion on a donc l'égalité $X = Y$ [1.2].

Finalement, si pour $X, Y, Z \in \mathcal{P}(A)$ on a $X R Y$ et $Y R Z$, alors cela veut dire qu'on a les inclusions $X \subset Y$ et $Y \subset Z$. Par transitivité de l'inclusion [1.3] on a donc aussi l'inclusion $X \subset Z$, c'est-à-dire $X R Z$. CQFD

Les preuves de §4

Preuve de [4.3]. Supposons d'abord qu'on a l'égalité $f = g$. Alors on invoque la condition (i) d'une application pour conclure que pour $a \in A$ il existe $b, b' \in B$ tels que $(a, b) \in f$ et $(a, b') \in g$. L'égalité $f = g$ implique donc que (a, b) et (a, b') appartiennent à f, donc par la condition (ii) d'une application on a $b = b'$. Avec l'écriture $b = f(a)$ pour $(a, b) \in f$ et $b' = g(a)$ pour $(a, b') \in g$ on a donc montré l'égalité $f(a) = g(a)$.

Pour l'implication dans l'autre sens, on suppose qu'on a $f(a) = g(a)$ pour tout $a \in A$ et on montre l'égalité $f = g$ par double inclusion. Prenons donc $(a, b) \in f$, ce qu'on note $b = f(a)$. Par hypothèse on a donc $b = g(a)$, ce qui veut dire qu'on a $(a, b) \in g$. Ainsi on a montré l'inclusion $f \subset g$. L'inclusion dans l'autre sens se démontre d'une façon absolument analogue. CQFD

Preuve de [4.6]. Selon la définition, f^{-1} est une application si et seulement si elle vérifie les conditions (i) et (ii) dans [4.1], ce qui se traduit comme

$$\begin{aligned} &\forall x \ : \ x \in A \ \Rightarrow \ \exists y : (x, y) \in f^{-1} \\ &\forall x, y, z \ : \ \big[(x, y) \in f^{-1} \text{ et } (x, z) \in f^{-1} \big] \ \Rightarrow \ y = z \ . \end{aligned}$$

Avec la définition de la relation inverse cela donne les conditions

$$\begin{aligned} &\forall x \ : \ x \in A \ \Rightarrow \ \exists y : (y, x) \in f \\ &\forall x, y, z \ : \ \big[(y, x) \in f \text{ et } (z, x) \in f \big] \ \Rightarrow \ y = z \ , \end{aligned}$$

ce qui sont exactement les conditions (iii) et (iv) d'injectivité et de surjectivité. CQFD

Preuve de [4.8]. Notons d'abord que π_A et π_B sont bien des ensembles : par [2.3] appliqué deux fois $(A \times B) \times A$ et $(A \times B) \times B$ sont des ensembles et donc par l'axiome de séparation π_A et π_B sont des ensembles. Pour montrer que ce sont des applications, on se concentre sur π_A ; le cas de π_B est similaire et laissé au bons soins du lecteur.

Si on sait que π_A est une application, il est immédiat qu'on a $\pi_A((a, b)) = a$, car on a $((a, b), a) \in \pi_A$. Pour montrer que c'est une application, on vérifie les deux conditions, en commençant par la première. Pour cela on prend $C \in A \times B$ et il faut montrer qu'il existe $D \in A$ tel que $(C, D) \in \pi_A$. Mais [2.3] nous dit que prendre $C \in A \times B$ est équivalent à prendre $a \in A$ et $b \in B$ et poser $C = (a, b)$. Mais si on a $a \in A$ et $b \in B$, on peut prendre $D = a$ et on aura $\big((a, b), a\big) \in \pi_A$ par définition de π_A. La première condition est donc vérifiée. Si on veut faire ce raisonnement avec

des équivalences officielles, on pourrait écrire :

$$\begin{aligned}
& \forall C \ : \ C \in A \times B \quad \Longrightarrow \quad \exists D : (C,D) \in \pi_A \\
\overset{[2.3],\,(4.9)}{\Longleftrightarrow} \quad & \forall C \ : \ \exists a \in A \ \exists b \in B : C = (a,b) \\
& \qquad \Longrightarrow \quad \exists D \ \exists a' \in A \ \exists b' \in B : (C,D) = \big((a',b'),a'\big) \\
\overset{[2.2]}{\Longleftrightarrow} \quad & \forall C \ : \ \exists a \in A \ \exists b \in B : C = (a,b) \\
& \qquad \Longrightarrow \quad \exists D \ \exists a' \in A \ \exists b' \in B : C = (a',b') \text{ et } D = a' \\
\Longleftrightarrow \quad & \forall C \ : \ \exists a \in A \ \exists b \in B : C = (a,b) \\
& \qquad \Longrightarrow \quad \exists a' \in A \ \exists b' \in B : C = (a',b') \ .
\end{aligned}$$

La dernière condition est visiblement vraie, donc π_A vérifie bien condition (i) d'une application.

Pour la deuxième condition on prend des ensembles x, y et z et on suppose qu'on a les propriétés $(x,y) \in \pi_A$ et $(x,z) \in \pi_A$. Il faut en déduire qu'on a l'égalité $y = z$. Les deux conditions se traduisent, avec (4.9), par

$$\exists a \in A \ \exists b \in B : (x,y) = \big((a,b),a\big) \qquad \text{et} \tag{33.3}$$

$$\exists a' \in A \ \exists b' \in B : (x,z) = \big((a',b'),a'\big) \ . \tag{33.4}$$

Avec [2.2] on en déduit qu'on doit avoir $x = (a,b)$, $y = a$, $x = (a',b')$ et $z = a'$. Les égalités $(a,b) = x = (a',b')$ impliquent, de nouveau par [2.2], qu'on a $a = a'$ et $b = b'$, donc on a bien $y = a = a' = z$. Ce qui montre que π_A vérifie aussi la condition (ii) et donc que c'est une application de $A \times B$ dans A. CQFD

Preuve de [4.11]. • Une application f de $\emptyset$ dans A est un sous-ensemble du produit cartésien $\emptyset \times A = \emptyset$ vérifiant deux conditions. Mais il n'existe qu'un seul sous-ensemble de l'ensemble vide. Si f existe, cela doit donc être l'ensemble vide : $f = \emptyset$. Reste la question si $f = \emptyset \subset \emptyset \times A$ vérifie ces deux conditions. Mais ces deux conditions contiennent des implications dont les prémisses ne sont jamais vraies car l'ensemble vide ne contient pas d'éléments. Ces implications sont donc trivialement vraies.

La preuve de l'injectivité de ce f utilise le même argument : la condition de l'injectivité contient une implication dont la prémisse n'est jamais vraie car $f = \emptyset$ ne contient aucun élément.

La condition de surjectivité de ce f s'écrit formellement comme

$$\forall x : x \in A \ \Rightarrow \ \exists y : (x,y) \in \emptyset \ .$$

Étant donné que la conclusion de l'implication est toujours fausse, l'implication elle même est fausse dès que la prémisse est vraie. Si A est l'ensemble vide, alors la prémisse n'est jamais vraie, donc l'implication est toujours vraie. Par contre, si A n'est pas vide, il existe $x \in A$ et donc l'implication sera fausse. L'implication n'est donc pas vraie pour tout x et ce f n'est pas surjective.

• Soit $f \subset A \times \emptyset = \emptyset$ une relation entre A et $\emptyset$. Il s'ensuit qu'on a forcément $f = \emptyset$. Si cette relation f serait une application, elle devrait vérifier la condition (i), c'est-à-dire

$$\forall a \ : \ a \in A \ \Rightarrow \ \exists b : (a,b) \in \emptyset \ .$$

Mais A n'est pas vide, il existe donc $a \in A$ et donc il doit exister b tel que $(a,b) \in \emptyset$. Ce qui est en contradiction avec la définition de l'ensemble vide. Il s'ensuit que f ne peut pas être une application. CQFD

Preuve de [4.12]. Pour la condition (i) d'une application, prenons $a \in A$. Alors parce que f est une application, il existe b tel que $(a,b) \in f$. Avec $f \subset A \times B$, il s'ensuit qu'on doit avoir $b \in B$. Et donc, parce que g est une application, il existe c tel que $(b,c) \in g$. Et comme avant, l'inclusion $g \subset B \times C$ nous assure qu'on a $c \in C$. Par définition de $g \circ f$ on a donc $(a,c) \in g \circ f$.

Pour la condition (ii) on suppose qu'on a $(x,y) \in g \circ f$ et $(x,z) \in g \circ f$. Il existe donc b, b' tels que

$$(x,b) \in f \quad , \quad (b,y) \in g \quad , \quad (x,b') \in f \quad \text{et} \quad (b',z) \in g \ .$$

Parce que f est une application, les deux conditions $(x,b) \in f$ et $(x,b') \in f$ impliquent qu'on a $b = b'$. Et donc, parce que g est une application, les deux conditions $(b,y) \in g$ et $(b,z) = (b',z) \in g$ impliquent qu'on a $y = z$. CQFD

Les preuves de §5

Preuve de [5.3]. • (i) : Par définition on a $A \cup B = \cup\{A, B\}$ et $B \cup A = \cup\{B, A\}$. Mais par l'axiome d'extensionnalité on a l'égalité $\{A, B\} = \{B, A\}$.

• (ii) : Selon (1.7) on a les équivalences

$$\begin{aligned} X \in (A \cup B) \cup C &\iff X \in (A \cup B) \text{ ou } X \in C \\ &\iff [\, X \in A \text{ ou } X \in B \,] \text{ ou } X \in C \\ &\iff X \in A \text{ ou } [\, X \in B \text{ ou } X \in C \,] \\ &\iff X \in A \text{ ou } X \in (B \cup C) \\ &\iff X \in A \cup (B \cup C) \ , \end{aligned}$$

ce qui montre la première égalité. Mais on a aussi les équivalences

$$\begin{aligned} X \in \cup\{A, B, C\} &\iff \exists D : D \in \{A, B, C\} \text{ et } X \in D \\ &\iff \exists D : [\, D = A \text{ ou } D = B \text{ ou } D = C \,] \text{ et } X \in D \\ &\iff \exists D : [\, D = A \text{ et } X \in D \,] \text{ ou } [\, D = B \text{ et } X \in D \,] \\ &\qquad\qquad \text{ou } [\, D = C \text{ et } X \in D \,] \\ &\iff \exists D : X \in A \text{ ou } X \in B \text{ ou } X \in C \\ &\iff X \in A \text{ ou } X \in B \text{ ou } X \in C \ , \end{aligned}$$

ce qui montre (avec l'axiome d'extensionnalité) la deuxième égalité. CQFD

Preuve de [5.4]. • Si on décortique la définition de l'intersection pour l'ensemble $D = \{A, B\}$ on trouve :

$$\begin{aligned} X \in \cap\{A, B\} &\Leftrightarrow \forall Y : Y \in \{A, B\} \ \Rightarrow \ X \in Y \\ &\Leftrightarrow \forall Y : [\ Y = A \text{ ou } Y = B\ ] \ \Rightarrow \ X \in Y \\ &\Leftrightarrow X \in A \text{ et } X \in B \ . \end{aligned}$$

• (i) : L'égalité annoncée est une conséquence immédiate de l'équivalence

$$X \in A \text{ et } X \in B \qquad \iff \qquad X \in B \text{ et } X \in A \ .$$

• (ii) : On a les équivalences

$$\begin{aligned} X \in (A \cap B) \cap C &\iff X \in (A \cap B) \text{ et } X \in C \\ &\iff (X \in A \text{ et } X \in B) \text{ et } X \in C \\ &\iff X \in A \text{ et } (X \in B \text{ et } X \in C) \\ &\iff X \in A \cap (B \cap C) \ , \end{aligned}$$

mais aussi

$$\begin{aligned} X \in \cap\{A, B, C\} &\iff \forall Y : Y \in \{A, B, C\} \Rightarrow X \in Y \\ &\iff \forall Y : (Y = A \text{ ou } Y = B \text{ ou } Y = C) \Rightarrow X \in Y \\ &\iff X \in A \text{ et } X \in B \text{ et } X \in C \ . \end{aligned}$$

Avec l'axiome d'extensionnalité on a donc les égalités annoncées. CQFD

Preuve de [5.6]. Vérifions les conditions d'une relation d'ordre, en commençant par le fait qu'on a l'inclusion $R' \subset X \times X$ par [5.2]. Notons ensuite que la définition de R' en termes de la notation avec $\leq'$ s'écrit comme

$$\begin{aligned} x \leq' y &\overset{\text{notat.}}{\iff} (x,y) \in R' \overset{\text{déf. de } R}{\iff} (x,y) \in R \text{ et } (x,y) \in X \times X \\ &\overset{\text{notat.}}{\iff} x \leq y \text{ et } (x,y) \in X \times X \ . \end{aligned}$$

Étant donné que la deuxième condition, $(x,y) \in X \times X$, est automatiquement vérifiée dans les conditions (i)–(iii) pour une relation d'ordre sur X, et que les conditions sur $\leq$ sont vérifiées parce que $\leq$ est une relation d'ordre sur A, il s'ensuit directement que $\leq'$ vérifie les conditions pour une relation d'ordre sur X. CQFD

Preuve de [5.10]. Par définition, l'ensemble f est un sous-ensemble de $A \times B$ vérifiant certaines conditions. Pour montrer que ce f est une application de A dans C, il faut donc montrer que c'est (aussi) un sous-ensemble de $A \times C$ vérifiant ces conditions. Pour cela, prenons $(x,y) \in f \subset A \times B$. Il s'ensuit qu'on a $x \in A$ et $y \in B$. La propriété

$$\exists a \in A : (a,y) \in f$$

est donc vraie, ce qui veut dire (par définition de l'image d'un ensemble par une application) qu'on a $y \in f[A]$. Par hypothèse on a l'inclusion $f[A] \subset C$. Il s'ensuit qu'on a $y \in C$, ce qui montre l'inclusion $f \subset A \times C$. Quant aux conditions que f doit vérifier, elle ne font pas référence à l'ensemble but. Elles sont donc vraies par hypothèse (que f est une application). CQFD

Preuve de [5.12]. Dans la preuve de [5.10] on a montré que l'inclusion $f[A] \subset C$ implique l'inclusion $f \subset A \times C$. Si on définit les ensembles Y et Z par

$$Y = \{\, b \in B \mid \exists a \in X : b = f(a) \,\} \quad \text{et} \quad Z = \{\, c \in C \mid \exists a \in X : c = f(a) \,\} \ ,$$

alors on doit montrer l'égalité $Y = Z$. On le fera par double inclusion. Soit donc $b \in Y$. Alors par définition il existe $a \in X$ tel que $(a,b) \in f$. Par l'inclusion $f \subset A \times C$ on a donc $(a,b) \in A \times C$, donc par définition du produit cartésien on a $a \in A$ et $b \in C$. Il s'ensuit qu'on a $b \in Z$.

Dans l'autre sens, si $c \in Z$, alors il existe $a \in X$ tel que $(a,c) \in f$. Mais alors par l'inclusion $f \subset A \times B$ on a $(a,c) \in A \times B$ et donc en particulier $c \in B$, ce qui prouve que $c \in Y$. CQFD

Preuve de [5.13]. Par [5.2] on a bien l'inclusion $f|_X \subset X \times B$; il suffit donc de vérifier les deux condition pour être une application. Pour la première on prend $x \in X$. L'inclusion $X \subset A$ nous donne $x \in A$ et donc, parce que f est une application de A dans B, il existe b tel que $(x,b) \in f$. Par l'inclusion $f \subset A \times B$ on a $b \in B$ et par hypothèse on a $x \in X$, donc on a aussi $(x,b) \in X \times B$, c'est-à-dire $(x,b) \in f|_X$.

Pour la deuxième condition on suppose qu'on a $(x,y) \in f|_X$ et $(x,z) \in f|_X$. Alors par définition on a en particulier $(x,y) \in f$ et $(x,z) \in f$. Donc, de nouveau parce que f est une application, on a $y = z$. CQFD

Preuve de [5.14]. Par définition de la restriction on a

$$\begin{array}{rcl}(f|_C)|_D & = & (f|_C)\cap(D\times A)=\big(f\cap(C\times A)\big)\cap(D\times A)\\ & \overset{[5.4]}{=} & f\cap\big((C\times A)\cap(D\times A)\big)=f\cap(D\times A)=f|_D\ .\end{array}$$

CQFD

Les preuves de §6

Preuve de [6.3]. Par hypothèse A et B contiennent les successeurs de 0. Si on applique la condition de minimalité de A avec l'ensemble B, on obtient l'inclusion $A \subset B$. Et si on applique la condition de minimalité de B avec l'ensemble A, on obtient l'inclusion $B \subset A$. Par double inclusion on a donc égalité. CQFD

Preuve de [6.4]. Par l'axiome de l'infini il existe un ensemble A contenant les successeurs de 0. En appliquant l'axiome de l'ensemble des parties et l'axiome de séparation on définit l'ensemble $\mathcal{A} \subset \mathcal{P}(A)$ comme les sous-ensembles de A qui contiennent les successeurs de 0 :

$$\mathcal{A} = \{\, B \in \mathcal{P}(A) \mid B \text{ contient les successeurs de } 0 \,\} \ . \tag{33.5}$$

Par hypothèse, l'ensemble A contient les successeurs de 0 et c'est un sous-ensemble de A, c'est-à-dire $A \in \mathcal{P}(A)$. Donc $A \in \mathcal{A}$. L'ensemble $\mathcal{A}$ n'est donc pas l'ensemble vide. En invoquant [1.12] (avec la notation (1.10) et (1.11)) on peut donc définir l'ensemble C par

$$C \ := \ \cap\, \mathcal{A} \ \equiv \ \bigcap_{B \in \mathcal{A}} B \ .$$

Reste à montrer que C est un ensemble minimal contenant les successeurs de 0.

Commençons avec la preuve $\emptyset \in C$. Par [1.12] ou (1.11) on a

$$D \in C \qquad \Longleftrightarrow \qquad \forall B \in \mathcal{A} : D \in B \ . \tag{33.6}$$

Par définition, tout B dans $\mathcal{A}$ contient les successeurs de 0, donc en particulier $\emptyset \in B$ pour tout $B \in \mathcal{A}$. Avec (33.6) il s'ensuit qu'on a $\emptyset \in C$.

Pour montrer la deuxième partie, on suppose qu'on a $c \in C$ et il faut en déduire $S(c) \in C$. Par (33.6) l'hypothèse $c \in C$ se traduit comme $c \in B$ pour tout $B \in \mathcal{A}$. Mais chaque $B \in \mathcal{A}$ contient les successeurs de 0, donc en particulier on a $S(c) \in B$ pour tout $B \in \mathcal{A}$. En invoquant (33.6) dans l'autre sens on en déduit qu'on a bien $S(c) \in C$.

Ainsi on a montré que C contient les successeurs de 0. Pour la minimalité on suppose que X est un ensemble quelconque contenant les successeurs de 0. Comme dans la preuve ci-dessus que C contient les successeurs de 0, on montre que l'intersection $B = A \cap X$ contient les successeurs de 0. Il s'ensuit, avec [5.1.i] et (1.13), qu'on a les inclusions $B \subset A$ et $B \subset X$. Par définition de $\mathcal{A}$ on a donc $B \in \mathcal{A}$. Invoquant [5.1.i] de nouveau, on en déduit qu'on a $C \subset B$. Mais l'inclusion $B \subset X$ combiné avec l'inclusion $C \subset B$ nous donne l'inclusion voulu $C \subset X$. CQFD

Preuve de [6.6]. C'est un simple transcription de la minimalité de $\mathbf{N}$, car l'hypothèse dit exactement que E contient les successeurs de 0, donc par minimalité de $\mathbf{N}$ on a l'inclusion $\mathbf{N} \subset E$. Par double inclusion on a donc l'égalité $E = \mathbf{N}$. CQFD

Preuve de [6.7]. La preuve se fait par récurrence. On définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{n \in \mathbf{N} \mid \forall m \in \mathbf{N} : m \in n \Rightarrow m \subset n\} \ .$$

On a $0 \in E$ si et seulement si on a

$$\forall m \in \mathbf{N} : m \in 0 \Rightarrow m \subset 0 \ .$$

Mais 0 est un autre nom pour l'ensemble vide, donc la prémisse $m \in 0$ est toujours fausse. L'implication est donc toujours vraie, et donc on a $0 \in E$.

Pour montrer l'implication $n \in E \Rightarrow S(n) \in E$ on suppose $n \in E$ et on en déduit $S(n) \in E$. Selon la définition de E, l'hypothèse veut dire

$$\forall m \in \mathbf{N} : m \in n \Rightarrow m \subset n \ . \tag{33.7}$$

Et il faut en déduire

$$\forall m \in \mathbf{N} : m \in S(n) \Rightarrow m \subset S(n) \ . \tag{33.8}$$

Soit donc $m \in \mathbf{N}$ tel que $m \in S(n)$. Par définition du successeur on a

$$m \in n \cup \{n\} \quad \Longleftrightarrow \quad m \in n \text{ ou } m \in \{n\} \quad \Longleftrightarrow \quad m \in n \text{ ou } m = n \ .$$

Selon l'hypothèse de récurrence (33.7) on peut déduire de $m \in n$ qu'on a $m \subset n$. Et si $m = n$ on a aussi $m \subset n$. Mais on a toujours l'inclusion $n \subset n \cup \{n\} = S(n)$. On a donc montré (33.8), ce qui termine la preuve que l'ensemble E vérifie les condition de [6.6]. On a donc $E = \mathbf{N}$. CQFD

Preuve de [6.8]. L'égalité $S(m) = S(n)$ équivaut $m \cup \{m\} = n \cup \{n\}$. À gauche on a l'élément m qui appartient à l'ensemble à droite, ce qui implique qu'on a

$$m \in n \qquad \text{ou} \qquad m = n \ .$$

Mais à droite on a l'élément n qui appartient à l'ensemble à gauche, ce qui implique qu'on a

$$n \in m \qquad \text{ou} \qquad n = m \ .$$

Parmi les quatre possibilités qui en résultent, trois donnent en particulier $n = m$. Dans le quatrième cas on a $m \in n$ et $n \in m$. Selon [6.7] on a donc $m \subset n$ et $n \subset m$, ce qui montre par double inclusion qu'on a aussi dans ce dernier cas l'égalité $m = n$.

Si on regarde maintenant l'application $f : \mathbf{N} \to \mathbf{N}$ définie par

$$f(n) = S(n) \ ,$$

il découle immédiatement du résultat précédent que c'est une application injective. Vu que 0 n'est pas dans l'image de f, elle n'est pas surjective. CQFD

Les preuves de §7

Preuve de [7.1]. Les axiomes (P0) et (P1) sont vrais par définition de $\mathbf{N}$ et $\emptyset = 0$. (P2) est vrai parce que $\mathbf{N}$ contient les successeurs de 0. (P3) est vrai parce que $\mathbf{N}$ est l'ensemble *minimal* contenant les successeurs de 0 (ou par [6.6]). (P4) est vrai à cause de [6.8] et (P5) est vrai car l'ensemble vide ne contient aucun élément et que $S(A)$ contient au moins un élément. CQFD

Preuve de [7.6]. • Commençons par l'unicité et supposons donc qu'il existe deux applications $\varphi, \psi : P \times \mathbf{N} \to A$ vérifiant (7.7). Alors on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, n \in \mathbf{N} \mid \forall p \in P : \varphi(p,n) = \psi(p,n) \,\} \ ,$$

ce qui est bien un ensemble par l'axiome de séparation. Par (7.7) on a $0 \in E$, mais aussi l'implication $n \in E \ \Rightarrow S(n) \in E$. Par récurrence on a l'égalité $E = \mathbf{N}$ et donc $\varphi = \psi$.

• Pour l'existence on définit l'ensemble $\mathcal{F} \subset \mathcal{P}\big((P \times \mathbf{N}) \times A\big)$ par

$$\begin{aligned}(33.9)\quad \mathcal{F} = \big\{ F \in \mathcal{P}((P \times \mathbf{N}) \times A) \mid \forall p \in P : \big((p,0), g(p)\big) \in F \text{ et} \\ \forall p \in P\ \forall n \in \mathbf{N}\ \forall a \in A : \big[\, \big((p,n),a\big) \in F \ \Rightarrow\ \big((p,S(n)), f((p,n),a)\big) \in F \,\big] \big\} \ ,\end{aligned}$$

ce qui est bien un ensemble par l'axiome de l'ensemble des parties et l'axiome de séparation. Il est évident que l'ensemble $(P \times \mathbf{N}) \times A$ appartient à $\mathcal{F}$, donc $\mathcal{F}$ n'est pas l'ensemble vide. On peut donc définir l'ensemble φ comme l'intersection de $\mathcal{F}$:

$$\varphi = \cap\, \mathcal{F} \ .$$

Par [5.1.i] et le fait qu'on a $(P \times \mathbf{N}) \times A \in \mathcal{F}$ on a bien $\varphi \subset \mathbf{N} \times A$. Reste à montrer que cela représente une application de $P \times \mathbf{N}$ dans A selon la définition [4.1] et qu'elle vérifie les conditions (7.7).

Pour la première condition d'une application, on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, n \in \mathbf{N} \mid \forall p \in P\ \exists a \in A : \big((p,n),a\big) \in \varphi \,\} \ .$$

Par définition de $\mathcal{F}$ on a la propriété

$$\forall F \in \mathcal{F}\ \forall p \in P : \big((p,0), g(p)\big) \in F \ .$$

Par (1.11) on a donc aussi $((p,0), g(p)) \in \varphi$. Le choix $a = g(p)$ convient, donc on a $0 \in E$.

Supposons maintenant qu'on a $n \in E$, c'est-à-dire que pour tout $p \in P$ il existe $a \in A$ tel que $\big((p,n),a\big) \in \varphi$. Par (1.11) cela veut dire qu'on a

$$\forall F \in \mathcal{F} : ((p,n),a) \in F \ .$$

Par la définition de $\mathcal{F}$ il s'ensuit qu'on a aussi

$$\forall F \in \mathcal{F} : \big((p,S(n)), f((p,n),a)\big) \in F \ ,$$

ce qui implique (toujours par (1.11)) qu'on a $\big((p,S(n)), f(a)\big) \in \varphi$. Ceci étant vrai pour tout $p \in P$, on a donc $S(n) \in E$. Ainsi on a montré par récurrence qu'on a $E = \mathbf{N}$. Mais la définition de E nous dit alors qu'on a la propriété

$$\forall p \in P\ \forall n \in \mathbf{N}\ \exists a \in A : \big((p,n),a\big) \in \varphi \ ,$$

ce qui veut dire que φ vérifie la première condition d'une application (de $P \times \mathbf{N}$ dans A). Notons en passant qu'on a aussi montré que φ appartient à $\mathcal{F}$, car on a

montré $((p,0),g(p)) \in \varphi$ ainsi que $\big((p,n),a\big) \in \varphi \;\Rightarrow\; \big((p,S(n)),f((p,n),a)\big) \in \varphi$. L'ensemble φ est donc le plus petit (pour l'inclusion) élément de $\mathcal{F}$.

Pour la deuxième condition, on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \big\{\, n \in \mathbf{N} \mid \forall p \in P\ \forall b,c \in A : \big((p,n),b\big) \in \varphi \text{ et } \big((p,n),c\big) \in \varphi \;\Rightarrow\; b = c \,\big\}\ .$$

Si on arrive à montrer l'égalité $E = \mathbf{N}$, on aura montré la deuxième condition d'une application. On le fait encore une fois par récurrence. L'idée qu'on va employer est que φ est le plus petit élément de $\mathcal{F}$, ce qui veut dire que dès qu'on enlève un élément de φ, alors l'ensemble qui reste ne peut plus appartenir à $\mathcal{F}$. La preuve passe donc par l'absurde : on suppose qu'on a deux éléments différents $\big((p,n),x\big)$ et $\big((p,n),y\big)$ dans φ, on enlève un des deux et on montre que ce qu'il reste est encore dans $\mathcal{F}$, ce qui est impossible.

Pour commencer on sait qu'on a $\big((p,0),g(p)\big) \in \varphi$. Supposons qu'on a aussi $\big((p,0),a\big) \in \varphi$ avec $a \neq g(p)$. Alors l'ensemble $\psi \subset (P \times \mathbf{N}) \times A$ définie par

$$\psi = \varphi \setminus \big\{\big((p,0),a\big)\big\} = \big\{c \in \varphi \mid c \neq \big((p,0),a\big)\,\big\}$$

a les propriétés $\psi \subset \varphi$ et $\psi \neq \varphi$. Il est évident qu'on a $\big((p,0),g(p)\big) \in \psi$, car $a \neq g(p)$. En plus, si $\big((p,n),b\big) \in \psi$, alors $\big((p,n),b\big) \in \varphi \in \mathcal{F}$. Donc par la définition de $\mathcal{F}$ on a $\big((p,S(n)),f((p,n),b)\big) \in \varphi$. Mais $\big((p,S(n)),f((p,n),b)\big) \neq \big((p,0),a\big)$ à cause de l'axiome (P5). Donc $\big((p,S(n)),f((p,n),b)\big) \in \psi$, ce qui montre qu'on a $\psi \in \mathcal{F}$. Avec [5.1.i] il s'ensuit qu'on doit avoir $\varphi \subset \psi$, ce qui est impossible. La conclusion est qu'il n'existe pas un élément $\big((p,0),a\big)$ dans φ avec $a \neq g(p)$. Ce qui montre qu'on a $0 \in E$.

Pour montrer l'implication $n \in E \;\Rightarrow\; S(n) \in E$ on procède de la même façon. On suppose que $n \in \mathbf{N}$ appartient à E. Par la propriété (i) d'une application (qu'on a déjà montré), on sait que pour tout $p \in P$ il existe $a \in A$ tel que $((p,n),a) \in \varphi \in \mathcal{F}$. Donc par la définition de $\mathcal{F}$ on a $\big((p,S(n)),f((p,n),a)\big) \in \varphi$. Supposons qu'il existe $b \in A$ tel que $b \neq f\big((p,n),a\big)$ et $\big((p,S(n)),b\big) \in \varphi$. Alors on définit l'ensemble $\psi \subset \mathbf{N} \times A$ par

$$\psi = \varphi \setminus \big\{\big((p,S(n)),b\big)\big\}\ .$$

Par hypothèse on a $\psi \subset \varphi$ et $\psi \neq \varphi$. On a $\big((p,0),g(p)\big) \in \varphi$ et par l'axiome (P5) $\big((p,0),g(p)\big) \neq \big((p,S(n)),b\big)$. Donc $\big((p,0),g(p)\big) \in \psi$. Si $\big((p,m),c\big) \in \psi$, alors $\big((p,m),c\big) \in \varphi \in \mathcal{F}$ et donc $\big((p,S(m)),f((p,m),c)\big) \in \varphi$. Si on a $S(m) \neq S(n)$, alors $\big((p,S(m)),f((p,m),c)\big) \neq \big((p,S(n)),b\big)$ et donc $\big((p,S(m)),f((p,m),c)\big) \in \psi$. Si au contraire on a $S(m) = S((n)$, alors par l'axiome (P4) on a $m = n$. Mais par l'hypothèse que n appartient à E et le fait qu'on a $\big((p,n),a\big) \in \varphi$, on doit avoir $c = a$, donc $f\big((p,n),c\big) = f\big((p,n),a\big)$. Il s'ensuit qu'on a $\big((p,S(m)),f((p,m),c)\big) = \big((p,S(n)),f((p,n),a)\big) \neq \big((p,S(n)),b\big)$. Donc même dans le cas $S(m) = S(n)$ a-t-on $\big((p,S(m)),f((p,m),c)\big) \in \psi$.

On vient donc de montrer que l'ensemble ψ appartient à $\mathcal{F}$ et donc qu'on doit avoir $\varphi \subset \psi$, ce qui est impossible (de nouveau à cause de [5.1.i]). La conclusion est qu'il n'existe pas d'élément $b \in A$ tel que $b \neq f\big((p,n),a\big)$ et $\big((p,S(n)),b\big) \in \varphi$. Donc $S(n)$ appartient aussi à E. Ainsi s'achève la preuve par récurrence qu'on a l'égalité $E = \mathbf{N}$, ce qui voulait dire qu'on a montré la deuxième propriété d'une application.

Une fois qu'on sait que φ est une application, alors la propriété (7.7) devient une simple transcription du fait que φ appartient à $\mathcal{F}$. CQFD

Preuve de [7.8]. Dans les trois cas, l'unicité de l'application φ se démontre comme dans la preuve de [7.6] et est laissée aux bons soins du lecteur.

• (i) : Il suffit d'appliquer [7.6] avec la même application $g : P \to A$ et l'application $f' : (P \times \mathbf{N}) \times A \to A$ définie par

$$f'\big((p,n),a\big) = f(p,a) \ .$$

L'application $\varphi : P \times \mathbf{N} \to A$ donnée par [7.6] vérifie les conditions requises.

• (ii) : On applique [7.6] avec l'ensemble $P = \{0\}$ (qui n'a qu'un seul élément), l'application $g : P \to A$ définie par $g(0) = a_0$ et l'application $f' : (P \times \mathbf{N}) \times A \to A$ définie par

$$f'\big((0,n),a\big) = f(n,a) \ .$$

L'application $\varphi' : P \times \mathbf{N} \to A$ donnée par [7.6] et vérifiant (7.7) nous permet de définir l'application $\varphi : \mathbf{N} \to A$ par

$$\varphi(n) = \varphi'(0,n) \ .$$

Il est alors immédiate que cette application φ vérifie les conditions requises.

• (iii) : Il suffit d'appliquer le résultat précédent avec la fonction $f' : \mathbf{N} \times A \to A$ définie par $f'(n,a) = f(a)$ pour obtenir l'existence requise. CQFD

Preuve de [7.9]. On définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, n \in \mathbf{N} \mid n = 0 \text{ ou } \exists k \in \mathbf{N} : n = S(k) \,\} \ .$$

Il est évident qu'on a $0 \in E$. Si on suppose qu'on a $n \in E$, alors on a $S(n) = S(k)$ pour $k = n$, donc $S(n)$ appartient aussi à E. Donc par récurrence on a l'égalité $E = \mathbf{N}$. CQFD

Preuve de [7.10]. • Si A est un ensemble infini, alors il existe une application $f : A \to A$ qui est injective mais pas surjective. Soit $a_0 \in A$ un élément qui n'est pas dans l'image : $a_0 \notin f[A]$. Avec ces ingrédients on peut appliquer [7.8.iii] et conclure qu'il existe une application $g : \mathbf{N} \to A$ vérifiant

$$g(0) = a_0 \qquad \text{et} \qquad g(S(n)) = f\big((g(n)\big) \ . \tag{33.10}$$

Pour montrer que g est injective, on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, m \in \mathbf{N} \mid \forall n \in \mathbf{N} : g(m) = g(n) \ \Rightarrow \ m = n \,\} \ .$$

Pour montrer qu'on a $0 \in E$ on prend $n \in \mathbf{N}$ et on suppose qu'on a $g(0) = g(n)$. Si $n \neq 0$, alors il existe $k \in \mathbf{N}$ tel que $n = S(k)$ [7.9]. On a donc les égalités

$$a_0 = g(0) = g(n) = g\big(S(k)\big) \overset{(33.10)}{=} f\big(g(k)\big) \ .$$

Mais cela est impossible, car a_0 n'appartient pas à l'image de f. On doit donc avoir $n = 0$ comme voulu.

Supposons maintenant qu'on a $m \in E$ et qu'on a l'égalité $g\big(S(m)\big) = g(n)$. Si on avait $n = 0$, alors on serait dans la situation décrite ci-dessus avec $k = m$, ce qui était impossible. Il s'ensuit qu'il existe $k \in \mathbf{N}$ tel que $n = S(k)$. On peut donc faire le calcul

$$f\big(g(m)\big) \overset{(33.10)}{=} g\big(S(m)\big) = g(n) = g\big(S(k)\big) \overset{(33.10)}{=} f\big(g(k)\big) \ .$$

Par l'injectivité de f on en déduit l'égalité $g(m) = g(k)$ et par l'hypothèse $m \in E$ on en déduit l'égalité $m = k$, donc $S(m) = S(k) = n$. Ainsi on a démontré qu'on a aussi $S(m) \in E$. Par récurrence on a donc $E = \mathbf{N}$, ce qui vaut l'injectivité de g.

• Soit $g : \mathbf{N} \to A$ une application injective et soit $B = g[A] \subset A$ son image. Par définition de l'image et de l'injectivité de g, il existe pour tout $a \in B$ un unique $n \in \mathbf{N}$ tel que $g(n) = a$. On peut donc définir l'application $f : A \to A$ par

$$f(a) = a \quad \text{quand } a \notin B \qquad \text{et} \qquad f(a) = g\big(S(n)\big) \quad \text{quand } a = f(n) \in B = g[A] \ .$$

Pour montrer que cette application est injective, on suppose qu'on a $f(a) = f(a')$. Si on a $a, a' \notin B$, alors il est immédiate qu'on a $a = a'$. Si on a $a \in B$ et $a' \notin B$, alors $f(a') = a' \notin B$ et $f(a) = g\big(S(n)\big) \in g[A] = B$, donc il est impossible qu'on ait $f(a) = f(a')$. Et si $a, a' \in B$, alors il existe $n, n' \in \mathbf{N}$ tels que $a = g(n)$, $a' = g(n')$ et $g\big(S(n)\big) = g\big(S(n')\big)$. L'injectivité de g nous donne alors $S(n) = S(n')$ et l'injectivité de S nous donne $n = n'$. La conclusion est donc que f est bien injective.

Pour montrer qu'elle n'est pas surjective, il suffit de montrer que $g(0)$ n'appartient pas à l'image de f. Supposons donc qu'on a $g(0) = f(a)$. Étant donné qu'on a $g(0) \in B$, il s'ensuit qu'on ne peut pas avoir $a \notin B$, car dans ce cas on aurait $f(a) = a \notin B$. Mais si $a \in B$, alors il existe $n \in \mathbf{N}$ tels que $f(a) = g\big(S(n)\big)$, ce qui nous donne l'égalité $g(0) = g(S(n))$. Par injectivité de g on aura donc $0 = S(n)$, ce qui est exclu par (P5). $\boxed{CQFD}$

Les preuves de §8

Preuve de [8.2]. Si e et e' sont deux éléments neutres, alors par définition d'un élément neutre on a les égalités

$$e' \overset{e \text{ neutre}}{=} e' \star e \overset{e' \text{ neutre}}{=} e \ . \qquad \boxed{CQFD}$$

Preuve de [8.5]. • (i) : On fixe $k, m \in \mathbf{N}$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{n \in \mathbf{N} \mid (k+m)+n = k+(m+n)\} \ .$$

Pour montrer qu'on a $0 \in E$ on constate qu'on a

$$(k+m)+0 \overset{(8.3)}{=} k+m \overset{(8.3)}{=} k+(m+0)$$

et donc $0 \in E$. Pour montrer l'implication $n \in E \Rightarrow S(n) \in E$ on fait le calcul

$$\begin{aligned}(k+m)+S(n) &\overset{(8.3)}{=} S((k+m)+n) \overset{n \in E}{=} S(k+(m+n)) \\ &\overset{(8.3)}{=} k+S(m+n) \overset{(8.3)}{=} k+(m+S(n)) \ .\end{aligned}$$

Ainsi on a montré qu'on a l'implication $n \in E \Rightarrow S(n) \in E$. Donc par récurrence on a l'égalité $E = \mathbf{N}$, ce qui veut dire qu'on a montré (i).

• (ii) : L'égalité $n+0 = n$ est l'initialisation dans (8.3). On définit donc l'ensemble E comme

$$E = \{n \in \mathbf{N} \mid 0+n = n\} \ .$$

On a déjà vu qu'on a $0+0 = 0$, donc $0 \in E$. Si $n \in E$, alors on peut faire le calcul

$$0+S(n) \overset{(8.3)}{=} S(0+n) \overset{n \in E}{=} S(n)$$

et donc on a aussi $S(n) \in E$. Ainsi on a montré par récurrence l'égalité $E = \mathbf{N}$, ce qui veut dire la propriété (ii).

• (iii) : Étant donné qu'on a $1 = S(0)$, on a

$$n+1 \overset{\text{déf}}{=} n+S(0) \overset{(8.3)}{=} S(n+0) \overset{(8.3)}{=} S(n) \ .$$

Pour l'autre égalité on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, n \in \mathbf{N} \mid 1+n = S(n) \,\} \ .$$

Par (ii) ci-dessus on a l'égalité $1+0 = 1$, donc $0 \in E$. Et pour $n \in E$ on peut faire le calcul

$$1+S(n) \overset{(8.3)}{=} S(1+n) \overset{n \in E}{=} S(S(n)) \ ,$$

et donc $S(n) \in E$. Ainsi on a montré par récurrence qu'on a $E = \mathbf{N}$, ce qui termine la preuve de (iii).

• (iv) : On fixe $m \in \mathbf{N}$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{n \in \mathbf{N} \mid n+m = m+n\} \ .$$

Par (ii) ci-dessus on a $0 \in E$. Et si $n \in E$, alors on peut faire le calcul

$$\begin{aligned}S(n)+m &\overset{\text{(iii)}}{=} (n+1)+m \overset{\text{(i)}}{=} n+(1+m) \overset{\text{(ii)}}{=} n+(m+1) \overset{\text{(i)}}{=} (n+m)+1 \\ &\overset{n \in E}{=} (m+n)+1 \overset{\text{(i)}}{=} m+(n+1) \overset{\text{(ii)}}{=} m+S(n) \ ,\end{aligned}$$

ce qui montre qu'on a $S(n) \in E$. Par récurrence on a donc l'égalité $E = \mathbf{N}$, ce qui termine la preuve de (iv). $\boxed{CQFD}$

Preuve de [8.6]. • (i) : On fixe m et n et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, k \in \mathbf{N} \mid m + k = n + k \;\Rightarrow\; m = n \,\} \ .$$

Il est immédiat qu'on a $0 \in E$. Supposons donc qu'on a $k \in E$. Alors on peut faire le raisonnement suivant :

$$\begin{array}{lll} m + S(k) = n + S(k) & \overset{[8.5.\text{iii}]}{\Longleftrightarrow} & m + (k+1) = n + (k+1) \\ & \overset{[8.5.\text{i}]}{\Longleftrightarrow} & (m+k) + 1 = (n+k) + 1 \\ & \overset{[8.5.\text{iii}]}{\Longleftrightarrow} & S(m+k) = S(n+k) \\ & \overset{(\text{P4})}{\Longrightarrow} & m + k = n + k \quad \overset{k \in E}{\Longrightarrow} \quad m = n \ . \end{array}$$

On a donc montré l'implication $k \in E \Rightarrow S(k) \in E$ et donc par récurrence l'égalité $E = \mathbf{N}$, ce qui montre (i).

• (ii) : Si $n \neq 0$, alors par [7.9] il existe $k \in \mathbf{N}$ tel que $n = S(k)$. Et donc

$$m + n = m + S(k) \overset{(8.3)}{=} S(m+k) \overset{(\text{P5})}{\neq} 0 \ ,$$

ce qui contredit l'hypothèse. Le même argument s'applique quand $m \neq 0$, car par [8.5.iv] on a $m + n = n + m$. CQFD

Preuve de [8.7]. Si on avait l'égalité $S(k) = k + 1 = k$, alors par [8.5.ii] et [8.6.i] on aurait $k + 1 = k + 0$ donc $0 = 1 = S(0)$, ce qui est impossible par (P5). CQFD

Preuve de [8.10]. • (i) : L'égalité $n \times 0 = 0$ est l'initialisation dans (8.9). Pour l'égalité $n \times 0 = 0$ on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, n \in \mathbf{N} \mid n \times 0 = 0 \,\}$$

et on constate qu'on a par l'argument précédent $0 \in E$. Et si $n \in E$ on a

$$0 \times S(n) \overset{(8.9)}{=} 0 + 0 \times n \overset{n \in E}{=} 0 + 0 \overset{[8.5.\text{ii}]}{=} 0 \ ,$$

et donc $S(n) \in E$. Ainsi on a montré (i) par récurrence.

• (ii) : Pour l'égalité $n \times 1 = n$ il suffit de remarquer qu'on a $1 = S(0)$ et donc

$$n \times 1 \equiv n \times S(0) \overset{(8.9)}{=} n + n \times 0 \overset{(8.9)}{=} n + 0 \overset{[8.5.\text{ii}]}{=} n \ .$$

Pour l'égalité $1 \times n = n$ on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{n \in \mathbf{N} \mid 1 \times n = n\}$$

et on constate qu'on a $0 \in E$ par (i) ci-dessus. Et si $n \in E$, alors

$$1 \times S(n) \overset{(8.9)}{=} 1 + 1 \times n \overset{n \in E}{=} 1 + n \overset{[8.5.\text{ii}]}{=} S(n) \ ,$$

ce qui montre qu'on a $S(n) \in E$. Donc on a montré (ii) par récurrence.

• (iv) : On fixe $k, m \in \mathbf{N}$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, n \in \mathbf{N} \mid (k+m) \times n = (k \times n) + (m \times n) \,\} \ .$$

Le calcul

$$(k+m) \times 0 \overset{(\text{i})}{=} 0 \overset{[8.5.\text{ii}]}{=} 0 + 0 \overset{(\text{i})}{=} (k \times 0) + (m \times 0)$$

montre qu'on a $0 \in E$. Et si $n \in E$, alors le calcul

$$\begin{array}{rl} (k+m)\times S(n) & \overset{(8.9)}{=} (k+m)+(k+m)\times n \\ & \overset{n\in E}{=} (k+m)+((k\times n)+(m\times n)) \\ & \overset{[8.5.\text{i/iv}]}{=} (k+k\times n)+(m+m\times n) \overset{(8.9)}{=} k\times S(n)+m\times S(n) \end{array}$$

montre qu'on a $S(n) \in E$. Donc par récurrence on a montré (iv).

- (vi) : On fixe $m \in \mathbf{N}$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{n \in \mathbf{N} \mid m \times n = n \times m\} \ .$$

Par (i) ci-dessus on a directement $0 \in E$. Et si $n \in E$, le calcul

$$\begin{array}{rl} m\times S(n) & \overset{(8.9)}{=} m+m\times n \overset{\text{(ii)},\ n\in E}{=} 1\times m+n\times m \overset{\text{(iv)}}{=} (1+n)\times m \\ & \overset{[8.5.\text{iii}]}{=} S(n)\times m \end{array}$$

montre qu'on a aussi $S(n) \in E$. Donc par récurrence $E = \mathbf{N}$, ce qui montre (vi).

- (iii) : En utilisant (iv) et (vi) on calcule :

$$k \times (m+n) \overset{\text{(vi)}}{=} (m+n)\times k \overset{\text{(iv)}}{=} (m\times k)+(n\times k) \overset{\text{(vi)}}{=} (k\times m)+(k\times n) \ ,$$

ce qui montre (iii).

- (v) : On fixe $k, m \in \mathbf{N}$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{n \in \mathbf{N} \mid k \times (m \times n) = (k \times m) \times n\} \ .$$

Le calcul

$$(k\times m)\times 0 \overset{\text{(i)}}{=} 0 \overset{\text{(i)}}{=} k\times 0 \overset{\text{(i)}}{=} k\times(m\times 0)$$

montre qu'on a $0 \in E$. Et si $n \in E$, le calcul

$$\begin{array}{rl} (k\times m)\times S(n) & \overset{(8.9)}{=} k\times m+(k\times m)\times n \overset{n\in E}{=} k\times m+k\times(m\times n) \\ & \overset{\text{(iii)}}{=} k\times(m+m\times n) \overset{(8.9)}{=} k\times(m\times S(n)) \end{array}$$

montre qu'on a $S(n) \in E$. Ainsi on a montré (v) par récurrence. CQFD

Preuve de [8.12]. On fixe $m \in \mathbf{N}$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{n \in \mathbf{N} \mid \exists k \in \mathbf{N} : (m+k=n) \text{ ou } (n+k=m)\} \ .$$

Il est immédiat qu'on a $0 \in E$ car il suffit de choisir $k = m$ pour obtenir la deuxième clause $0 + k = m$. Supposons donc qu'on a $n \in E$. Alors il existe $k \in \mathbf{N}$ tel que $m + k = n$ ou $n + k = m$. Pour en déduire que $S(n) \in E$, il faut trouver $k' \in \mathbf{N}$ tel que $m + k' = S(n)$ ou $S(n) + k' = m$. L'hypothèse de départ distingue deux cas. Dans le premier cas $m + k = n$ on a

$$S(n) \overset{[8.5.\text{iii}]}{=} n+1 \overset{n=m+k}{=} (m+k)+1 \overset{[8.5.\text{i}]}{=} m+(k+1) \ ,$$

donc en prenant $k' = k+1$ on a $S(n) = m + k'$ et donc $S(n) \in E$. Dans le deuxième cas $n + k = m$ on sépare le cas $k = 0$ et $k \neq 0$. Si $k = 0$ on a $n = m$ et donc

$$S(n) = S(m) \overset{[8.5.\text{iii}]}{=} m+1 \ ,$$

ce qui montre qu'avec $k' = 1$ on a $S(n) = m + k'$, c'est-à-dire $S(n) \in E$. Et pour $k \neq 0$ il existe, par [7.9], $\ell \in \mathbf{N}$ tel que $k = S(\ell)$, donc

$$m = n+k \overset{[8.5.\text{iii}]}{=} n+(\ell+1) \overset{[8.5.\text{i/iv}]}{=} (n+1)+\ell \overset{[8.5.\text{iii}]}{=} S(n)+\ell \ ,$$

ce qui montre qu'avec $k' = \ell$ on a $S(n) \in E$.

On a donc dans tous les cas l'implication $n \in E \Rightarrow S(n) \in E$ et donc on a montré le résultat par récurrence. CQFD

Preuve de [8.13]. • (i) : Si $m = 0$ ou $n = 0$, alors par [8.10.i] on a $m \times n = 0$. Et si ni m ni n est nul, alors par [7.9] il existe $k, \ell \in \mathbf{N}$ tels que $m = S(k)$ et $n = S(\ell)$, ce qui nous permet de faire le calcul

$$m \times n = S(k) \times S(\ell) \overset{[8.5.iii]}{=} (k+1) \times (\ell+1) \overset{[8.10.iii/iv]}{=} (k \times \ell + k \times 1 + 1 \times \ell) + 1 \times 1 \overset{[8.5.iii]}{=} S(k \times \ell + k + \ell) \overset{(P5)}{\neq} 0 \ .$$

Il s'ensuit que $m \times n$ n'est pas nul non plus.

• (ii) : Si $m = n = 1$, alors par [8.10.ii] on a $m \times n = 1$, ce qui montre l'implication inverse. Pour l'implication directe supposons que $m \times n = 1$. Si $m = 0$ ou $n = 0$ on a $m \times n = 0 \neq 1$. Par [7.9] il existe donc $k, \ell \in \mathbf{N}$ tels que $m = S(k) = k + 1$ et $n = S(\ell) = \ell + 1$. Il s'ensuit qu'on a l'égalité

$$m \times n = (k+1) \times (\ell+1) \overset{[8.10.ii–iv]}{=} k \times \ell + k + \ell + 1 = 1 \ .$$

Par [8.6.i] on en déduit l'égalité

$$k \times \ell + k + \ell = 0 \ .$$

Si maintenant on a $\ell \neq 0$, alors de nouveau par [7.9] il existe $j \in \mathbf{N}$ avec $\ell = S(j)$ et donc on a

$$k \times \ell + k + S(j) \overset{(8.3)}{=} S(k \times \ell + k + j) \overset{(P5)}{\neq} 0 \ .$$

Il est donc impossible d'avoir $\ell \neq 0$. Le même argument s'applique pour $k \neq 0$ et on conclut aux égalités $k = \ell = 0$. Et donc $m = n = S(0) = 1$.

• (iii) : Par [8.12] il existe $\ell \in \mathbf{N}$ tel que $m + \ell = n$ ou $n + \ell = m$. Dans le premier cas on fait le raisonnement

$$k \times m = k \times n \iff k \times m = k \times (m + \ell) \overset{[8.10.iii]}{\iff} k \times m = k \times m + k \times \ell \overset{[8.6]}{\iff} 0 = k \times \ell \overset{(i)}{\iff} k = 0 \text{ ou } \ell = 0 \iff k = 0 \text{ ou } m = n \ .$$

Dans l'autre cas le raisonnement est analogue. CQFD

Preuve de [8.14]. Par [8.5.ii] on a $n + 0 = n$, donc $n \leq n$, ce qui montre la réflexivité.

Si on a $m \leq n$ et $n \leq m$, alors il existe $k, \ell \in \mathbf{N}$ tel que

$$m + k = n \qquad \text{et} \qquad n + \ell = m \ .$$

Donc on peut faire le calcul

$$n = m + k = (n + \ell) + k \overset{[8.5.i]}{=} n + (\ell + k) \overset{[8.6.i]}{\Rightarrow} 0 = \ell + k \overset{[8.6.ii]}{\Rightarrow} \ell = k = 0 \ .$$

Il s'ensuit qu'on a $m = n$, ce qui montre l'antisymétrie.

Si $m \leq n$ et $n \leq p$, alors par définition il existe $k, \ell \in \mathbf{N}$ tel que

$$m + k = n \qquad \text{et} \qquad n + \ell = p \ ,$$

donc

$$p = n + \ell = (m + k) + \ell \overset{[8.5.i]}{=} m + (k + \ell) \ ,$$

ce qui montre qu'on a $m \leq p$. Donc $\leq$ est transitive.

Le fait que $\leq$ est total est une conséquence immédiate de [8.12]. CQFD

Preuve de [8.15]. • (i) : Si on a $k \leq \ell$, alors il existe $i \in \mathbf{N}$ tel que $k+i=\ell$. Donc on peut faire le calcul

$$\ell + j = (k+i)+j \overset{[8.5]}{=} (k+j)+i \ ,$$

ce qui montre l'inégalité $\ell + j \geq k + j$. Si au contraire on a $k + j \leq \ell + j$, alors il existe $i \in \mathbf{N}$ tel que $(k + j) + i = \ell + j$. On a donc

$$\ell + j = (k+j)+i \overset{[8.5]}{=} (k+i)+j$$

et par [8.6.i] on en déduit l'égalité $\ell = k + i$, ce qui nous donne l'inégalité $\ell \geq k$.

• (ii) : On commence avec l'implication réciproque $\Leftarrow$. Si $j = 0$, alors $k \times j = 0 = \ell \times j$ et donc en particulier $k \times j \leq \ell \times j$. Si au contraire on a $k \leq \ell$, alors on définit $E \subset \mathbf{N}$ par

$$E = \{\, j \in \mathbf{N} \mid k \times j \leq \ell \times j \,\} \ .$$

Il est évident qu'on a $0 \in E$, car $k \times 0 = 0 = \ell \times 0$. Si $j \in E$, alors on a les inégalités $k \leq \ell$ et $k \times j \leq \ell \times j$. Par (i) ci-dessus on a donc

$$k \times (j+1) = k + k \times j \leq \ell + k \times j \qquad \text{et} \qquad k \times j + \ell \leq \ell \times j + \ell = \ell \times (j+1) \ .$$

Avec $j+1 = S(j)$ on obtient donc $S(j) \in E$. Ainsi on a montré par récurrence qu'on a $E = \mathbf{N}$, ce qui montre l'implication réciproque.

Pour l'implication directe on suppose qu'on a $k \times j \leq \ell \times j$ et $j \neq 0$. Si on avait $\ell < k$, alors en particulier $\ell \leq k$ et donc par l'implication réciproque $\ell \times j \leq k \times j$. Par anti-symétrie d'une relation d'ordre on aurait donc $k \times j = \ell \times j$. Par [8.13.iii] il s'ensuit qu'on a $k = \ell$ (car $j \neq 0$). Mais cela contredit l'inégalité stricte $\ell < k$. Cette contradiction montre qu'on doit avoir $k \leq \ell$. CQFD

Preuve de [8.16]. Par [8.7] on ne peut pas avoir $\ell + 1 = \ell$; on a donc l'inégalité stricte $\ell + 1 > \ell$. L'implication directe s'en déduit avec [3.11] car on a l'implication

$$k \leq \ell \text{ et } \ell < \ell + 1 \quad \Longrightarrow \quad k < \ell + 1 = S(\ell) \ .$$

Pour l'implication réciproque, l'inégalité stricte $k < \ell + 1$ implique l'inégalité large, donc, par définition, l'existence d'un $j \in \mathbf{N}$ tel que $k + j = \ell + 1$. On ne peut pas avoir $j = 0$ car $k \neq \ell + 1$, donc par [7.9] il existe $i \in \mathbf{N}$ tel que $j = S(i)$. On peut donc faire le calcul suivant :

$$S(\ell) = k + S(i) \overset{(8.3)}{=} S(k+i) \quad \overset{(P4)}{\Longrightarrow} \quad \ell = k + i \ .$$

Par définition de la relation d'ordre sur $\mathbf{N}$ on a donc $k \leq \ell$. CQFD

Preuve de [8.17]. On définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, \ell \in \mathbf{N} \mid \forall k \in A : \ell \leq k \,\} \equiv \{\, \ell \in \mathbf{N} \mid \forall k \in A : k \not< \ell \,\} \ ,$$

c'est-à-dire l'ensemble des minorants de A, où pour la deuxième égalité on a utilisé que l'ordre $\leq$ sur $\mathbf{N}$ est total. Si on a $\ell \in A \cap E$, alors ce ℓ sera le plus petit élément de A comme voulu. Supposons donc que $A \cap E = \emptyset$. Pour montrer l'égalité $E = \mathbf{N}$

par récurrence, on invoque d'abord [8.5.ii] et la définition de la relation d'ordre pour conclure qu'on a $0 \leq k$ pour tout $k \in \mathbf{N}$ et donc a fortiori $0 \leq k$ pour tout $k \in A$, ce qui montre qu'on a $0 \in E$.

Supposons maintenant $\ell \in E$. Selon l'hypothèse $A \cap E = \emptyset$ on a $\ell \notin A$ et donc on aura

$$\forall k \in A : \ell < k \qquad \Longleftrightarrow \qquad \forall k \in A : k \not\leq \ell \qquad \overset{[8.16]}{\Longleftrightarrow} \qquad \forall k \in A : k \not< S(\ell) \ ,$$

c'est-à-dire $S(\ell) \in E$. Ainsi on a montré l'implication $\ell \in E \Rightarrow S(\ell) \in E$ et donc par récurrence on a l'égalité $E = \mathbf{N}$. Mais alors $\emptyset = A \cap E = A \cap \mathbf{N}$. Ceci étant contraire à l'hypothèse $A \neq \emptyset$, on ne peut donc pas avoir $A \cap E = \emptyset$ et A admet un plus petit élément. $\boxed{CQFD}$

Les preuves de §9

Preuve de [9.5]. Si on a $C_a = C_b$, alors le fait qu'on a $a \in C_a$ implique qu'on a $C_a \cap C_b \neq \emptyset$, ce qui montre l'implication réciproque.

Pour l'implication directe, si $C_a \cap C_b$ n'est pas vide, il existe $c \in C_a \cap C_b$. On va montrer l'égalité $C_a = C_b$ par double inclusion. On prend donc $d \in C_a$ et $e \in C_b$ et on va montrer $d \in C_b$ et $e \in C_a$. Par définition d'une classe d'équivalence on a

$$d, c \in C_a \;\Leftrightarrow\; a \sim c \text{ et } a \sim d \qquad , \qquad e, c \in C_b \;\Leftrightarrow\; b \sim c \text{ et } b \sim e \;\; .$$

Par symétrie et transitivité d'une relation d'équivalence on en déduit

$$c \sim d \qquad \text{et} \qquad c \sim e \;\; .$$

Mais alors on a $a \sim c$ et $c \sim e$, ce qui implique par transitivité $a \sim e$ et on a aussi $b \sim c$ et $c \sim d$, ce qui donne $b \sim d$. Par définition d'une classe d'équivalence on a donc $d \in C_b$ et $e \in C_a$. Ainsi on a montré les implication $d \in C_a \Rightarrow d \in C_b$ et $e \in C_b \Rightarrow e \in C_a$, ce qui veut dire qu'on a les inclusions $C_a \subset C_b$ et $C_b \subset C_a$ comme voulu.

Pour montrer l'équivalence $C_a = C_b \iff a \sim b$, on constate d'abord que par réflexivité on a $a \in C_a$. Si on a aussi $b \sim a$, alors $a \in C_b$ et donc $C_a \cap C_b$ n'est pas vide. par le résultat précédent on a $C_a = C_b$. D'autre part, si on a $C_a = C_b$ on a en particulier $a \in C_a = C_b$ et donc par définition de C_b on a $a \sim b$. CQFD

Preuve de [9.6]. Notons d'abord que P est bien un ensemble par l'axiome de l'ensemble des parties et l'axiome de séparation.

Pour les deux propriétés d'une partition, commençons par la deuxième. Si X et Y appartiennent à P, alors par définition de P il existe $a, b \in A$ tels que $X = C_a$ et $Y = C_b$. Si on a $X \cap Y \neq \emptyset$, alors par [9.5] on a $X = Y$, ce qui montre l'implication $X \neq Y \Rightarrow X \cap Y = \emptyset$.

On montre l'égalité $\cup P = A$ par double inclusion. On commence à décortiquer l'appartenance à $\cup P$:

$$\begin{aligned} x \in \cup P &\overset{\text{axiome}}{\iff} \exists X : X \in P \text{ et } x \in X \\ &\overset{\text{déf. de } P}{\iff} \exists X \; \exists a \in A : X = C_a \text{ et } x \in X \\ &\iff \exists a \in A : x \in C_a \;\; . \end{aligned} \tag{33.11}$$

La définition d'une classe d'équivalence donne l'inclusion $C_a \subset A$, donc de (33.11) on déduit immédiatement l'implication $x \in \cup P \Rightarrow x \in A$. Pour l'implication inverse il suffit de faire le raisonnement

$$x \in A \implies x \in C_x \implies \exists a \in A : x \in C_a \overset{(33.11)}{\iff} x \in \cup P \;\; . \qquad \text{CQFD}$$

Preuve de [9.9]. • Commençons avec la preuve que si un tel F existe, alors f est compatible avec la relation d'équivalence. Pour cela on prend $a, b \in A$ et on tient le raisonnement suivant :

$$a \sim b \overset{[9.5]}{\iff} C_a = C_b \overset{(9.10)}{\implies} f(a) = F(C_a) = F(C_b) = f(b) \;\; .$$

• Attaquons ensuite la question de l'unicité et supposons qu'on a deux applications $F_1, F_2 : A/\!\sim \to X$ vérifiant $f = F_1 \circ C = F_2 \circ C$. Pour $B \in A/\!\sim$ on peut faire le raisonnement suivant :

$$\begin{aligned} B \in A/\!\sim \quad &\overset{(9.7)}{\Longrightarrow} \quad \exists a \in A : B = C_a \\ &\overset{(9.10)}{\Longrightarrow} \quad F_1(B) = F_1(C_a) = f(a) = F_2(C_a) = F_2(B) \ . \end{aligned}$$

• Et pour terminer on démontre l'existence de F quand f est compatible avec la relation d'équivalence. Pour cela on définit l'ensemble $F \subset (A/\!\sim) \times X$ par

$$F = \{\, t \in (A/\!\sim) \times X \mid \exists a \in A : t = \big(C_a, f(a)\big) \,\} \tag{33.12}$$

et on montre que c'est une application $F : A/\!\sim \to X$ vérifiant $f = F \circ C$. Pour la première condition d'une application on prend $B \in A/\!\sim$ et on raisonne comme suit :

$$B \in A/\!\sim \quad \overset{(9.7)}{\Longrightarrow} \quad \exists a \in A : B = C_a \quad \overset{(33.12)}{\Longrightarrow} \quad \big(B, f(a)\big) \in F \ .$$

Pour la deuxième condition d'une application on suppose qu'on a (B, x) et (B, y) dans F, ce qui veut dire qu'on a

$$\exists a, b \in A : B = C_a \text{ et } x = f(a) \text{ et } B = C_b \text{ et } y = f(b) \ .$$

Mais par [9.5] on a l'équivalence $C_a = C_b \Leftrightarrow a \sim b$. La compatibilité de f avec la relation d'équivalence nous donne alors l'égalité $f(a) = f(b)$. Ce qui démontre l'implication

$$(B, x), (B, y) \in F \quad \Longrightarrow \quad x = y \ .$$

Ainsi on a montré que F est bien une application de $A/\!\sim$ dans X. Pour la condition $f = F \circ C$ on prend $a \in A$ et on constate que par définition de F on a $\big(C_a, f(a)\big) \in F$, ce qui est équivalent à $f(a) = F(C_a) \equiv F(C(a))$. CQFD

Preuve de [9.12]. • Commençons avec la preuve que si R existe, alors r est compatible avec la relation d'équivalence. Pour cela on prend $a, a', b, b' \in A$ et on tient le raisonnement suivant :

$$\begin{aligned} a \sim a' \text{ et } b \sim b' \quad &\overset{[9.5]}{\Longleftrightarrow} \quad C_a = C_{a'} \text{ et } C_b = C_{b'} \\ &\overset{(9.13)}{\Longrightarrow} \quad r(a, b) = R(C_a, C_b) = R(C_{a'}, C_{b'}) = r(a', b') \ . \end{aligned}$$

• Attaquons ensuite la question de l'unicité et supposons qu'on a deux applications $R_1, R_2 : (A/\!\sim) \times (A/\!\sim) \to X$ vérifiant (9.13). Pour $B, B' \in A/\!\sim$ on peut faire le raisonnement suivant :

$$\begin{aligned} B, B' \in A/\!\sim \quad &\overset{(9.7)}{\Longrightarrow} \quad \exists a, a' \in A : B = C_a \text{ et } B' = C_{a'} \\ &\overset{(9.13)}{\Longrightarrow} \quad R_1(B, B') = R_1(C_a, C_{a'}) = r(a, a') \\ &\qquad\qquad = R_2(C_a, C_{a'}) = R_2(B, B') \ . \end{aligned}$$

• Et pour terminer on démontre l'existence de R quand r est compatible avec la relation d'équivalence. Pour cela on définit l'ensemble $R \subset \big((A/\!\sim) \times (A/\!\sim)\big) \times X$ par

$$R = \{\, t \in \big((A/\!\sim) \times (A/\!\sim)\big) \times X \mid \exists a, b \in A : t = \big((C_a, C_b), r(a, b)\big) \,\} \tag{33.13}$$

et on montre que c'est une application $R : (A/\!\sim) \times (A/\!\sim) \to X$ vérifiant (9.13). Pour la première condition d'une application on prend $B, B' \in A/\!\sim$ et on raisonne

comme suit :

$$B, B' \in A/\sim \quad \overset{(9.7)}{\Longrightarrow} \quad \exists a, b \in A : B = C_a \text{ et } B' = C_b \\ \overset{(33.13)}{\Longrightarrow} \quad \big((B, B'), r(a, b)\big) \in R \ .$$

Pour la deuxième condition d'une application on suppose qu'on a $((B, B'), x)$ et $((B, B'), y)$ dans R, ce qui veut dire qu'on a

$$\exists a, a', b, b' \in A : \begin{cases} B = C_a \text{ et } B' = C_{a'} \text{ et } x = r(a, a') \text{ et} \\ B = C_b \text{ et } B' = C_{b'} \text{ et } y = r(b, b') \ . \end{cases}$$

En invoquant [9.5] on obtient $a \sim b$ et $a' \sim b'$. La compatibilité de r avec la relation d'équivalence nous donne alors l'égalité $r(a, a') = r(b, b')$. Ce qui démontre l'implication

$$((B, B'), x), ((B, B'), y) \in R \quad \Longrightarrow \quad x = y \ .$$

Ainsi on a montré que R est bien une application de $(A/\sim) \times (A/\sim)$ dans X. Pour la condition (9.13) on prend $a, b \in A$ et on constate que par définition de R on a $\big((C_a, C_b), r(a, b)\big) \in R$, ce qui est équivalent à $r(a, b) = R(C_a, C_b)$. CQFD

Preuve de [9.15]. • Commençons avec la preuve que si G existe, alors g est compatible avec la relation d'équivalence. Pour cela on prend $a, a', b, b' \in A$ et on tient le raisonnement suivant :

$$a \sim a' \text{ et } b \sim b' \overset{[9.5]}{\Longleftrightarrow} C_a = C_{a'} \text{ et } C_b = C_{b'} \\ \overset{(9.16)}{\Longrightarrow} (a, b) \in g \Leftrightarrow (C_a, C_b) = (C_{a'}, C_{b'}) \in G \Leftrightarrow (a', b') \in g \ .$$

• Attaquons ensuite la question de l'unicité et supposons qu'on a deux sous-ensembles $G_1, G_2 \subset (A/\sim) \times (A/\sim)$ vérifiant (9.16). Pour $B, D \in A/\sim$ on peut faire le raisonnement suivant :

$$B, D \in A/\sim \quad \overset{(9.7)}{\Longrightarrow} \quad \exists a, b \in A : B = C_a \text{ et } D = C_b \\ \overset{(9.13)}{\Longrightarrow} \quad (B, D) \in G_1 \Leftrightarrow (a, b) \in g \Leftrightarrow (B, D) \in G_2 \ .$$

• Et pour terminer on démontre l'existence de $G \subset (A/\sim) \times (A/\sim)$ en posant

$$G = \{\, t \in (A/\sim) \times (A/\sim) \mid \exists a, b \in A : t = (C_a, C_b) \text{ et } (a, b) \in g \,\} \ . \tag{33.14}$$

Pour montrer que ce G vérifie (9.16) on constate d'abord que la définition de G nous donne immédiatement l'implication

$$(a, b) \in g \Longrightarrow (C_a, C_b) \in G \ .$$

Pour l'implication inverse, supposons qu'on a $t = (C_a, C_b) \in G$ et on raisonne comme suit :

$$t = (C_a, C_b) \in G \overset{(33.14)}{\Longleftrightarrow} \exists a', b' \in A : (a', b') \in g \text{ et } t = (C_{a'}, C_{b'}) = (C_a, C_b) \\ \overset{[2.2],\ [9.5]}{\Longrightarrow} (a', b') \in g \text{ et } a \sim a' \text{ et } b \sim b' \\ \overset{\text{compat. } g \text{ avec } \sim}{\Longrightarrow} (a, b) \in g \ .$$ CQFD

Preuve de [9.17]. • Pour montrer que $\sim$ est une relation d'équivalence, on vérifie les trois conditions. La réflexivité exige que pour tout $a \in A$ on a $a \sim a$. Par hypothèse

d'une partition on a $\cup P = A$, donc $a \in \cup P$, ce qui veut dire selon l'axiome de la réunion qu'on a

$$a \in \cup P \quad \overset{\text{axiome}}{\Longleftrightarrow} \quad \exists X \in P : a \in X \ .$$

Et donc a fortiori $a, a \in X$, ce qui implique par définition de $\sim$ qu'on a effectivement $a \sim a$.

Pour la symétrie il suffit de remarquer que $a \sim b$ est équivalent à la condition qu'il existe $X \in P$ tel que a et b appartiennent à X, ce qui est une condition symétrique en a et b, donc aussi $b \sim a$.

Pour la transitivité on suppose $a \sim b$ et $b \sim c$. Selon la définition de $\sim$ il existe donc $X, Y \in P$ tels que $a, b \in X$ et $b, c \in Y$. Mais alors on a $b \in X \cap Y$. Par hypothèse d'une partition on doit donc avoir $X = Y$. Mais alors on a $a, c \in X \in P$ et donc $a \sim c$.

• Pour la deuxième partie on suppose que X est un ensemble non-vide. Si on suppose que X appartient à P, alors par hypothèse d'une partition $A = \cup P$ et [1.9] on a $X \subset A$. X étant non-vide ; il existe $a \in X$ et donc $a \in A$. Maintenant il suffit de montrer l'égalité

$$X = \{b \in A \mid a \sim b\}$$

pour avoir montré l'implication $\Rightarrow$ de l'énoncé. On le fait par double inclusion. Si $c \in X$ est arbitraire, alors par l'inclusion $X \subset A$ on a $c \in A$. On a donc $a, c \in X$, donc par définition de la relation d'équivalence on a $a \sim c$, ce qui donne $c \in \{b \in A \mid a \sim b\}$. Ainsi on a montré l'inclusion $X \subset \{b \in A \mid a \sim b\}$.

Pour l'autre inclusion, prenons $c \in \{b \in A \mid a \sim b\}$. Alors $a \sim c$ et donc par définition de $\sim$ il existe $Y \in P$ tel que $a, c \in Y$. Mais alors $a \in X \cap Y$, donc par définition d'une partition on doit avoir $X = Y$. Il s'ensuit qu'on a $c \in X$, ce qui montre l'inclusion $\{b \in A \mid a \sim b\} \subset X$. On a donc l'égalité $X = \{b \in A \mid a \sim b\}$, ce qui termine la preuve de l'implication directe.

Pour l'implication $\Leftarrow$ on suppose qu'il existe $a \in A$ pour lequel on a l'égalité $X = \{b \in A \mid a \sim b\}$ et il faut en déduire $X \in P$. Par définition d'une relation d'équivalence et en particulier la réflexivité on a $a \in X$. Par définition d'une partition et en particulier $A = \cup P$ il existe donc $Y \in P$ tel que $a \in Y$. Mais dans la preuve de l'implication directe ci-dessus on a montré que si $a \in Y \in P$, alors $Y = \{b \in A \mid a \sim b\}$. Ce qui montre l'égalité $X = Y$ et donc $X \in P$. $\boxed{CQFD}$

Les preuves de §10

Preuve de [10.2]. La réflexivité et la symétrie de $\sim$ sont immédiates à cause de la commutativité de la multiplication dans $\mathbf{N}$ [8.10.vi]. Pour la transitivité il faut travailler un petit peu plus. Supposons qu'on a

$$(a,b) \sim (p,q) \qquad \text{et} \qquad (p,q) \sim (r,s) \ .$$

Par définition on a donc

$$a \times q = b \times p \qquad \text{et} \qquad p \times s = q \times r \ .$$

Si on multiplie (à droite) la première équation par s et la deuxième par b on obtient

$$a \times q \times s = b \times p \times s \qquad \text{et} \qquad p \times s \times b = q \times r \times b \ .$$

En utilisant de nouveau la commutativité de la multiplication dans $\mathbf{N}$ (on a déjà utilisé l'associativité en omettant les parenthèses), on obtient l'équation

$$a \times s \times q = b \times r \times q \ .$$

Par [8.13.iii] on peut en déduire l'égalité $a \times s = b \times r$ (car $q \neq 0$), ce qui est l'équivalence $(a,b) \sim (r,s)$. *CQFD*

Les preuves de §11

Preuve de [11.3]. Il est évident qu'on a $(k,\ell)\sim(k,\ell)$, simplement parce que l'addition dans $\mathbf{N}$ est commutatif. Pour la symétrie on fait le raisonnement (également utilisant la commutativité de l'addition dans $\mathbf{N}$)

$$\begin{aligned}(k,\ell)\sim(i,j) \quad &\iff \quad k+j=\ell+i \quad \iff \quad i+\ell=j+k\\ &\iff \quad (i,j)\sim(k,\ell)\ .\end{aligned}$$

Finalement pour la transitivité on fait le raisonnement

$$\begin{aligned}(i,j)\sim(k,\ell)\text{ et }(k,\ell)\sim(a,b) \quad &\iff \quad i+\ell=k+j\text{ et }k+b=\ell+a\\ &\implies \quad (i+\ell)+b=(k+j)+b \overset{[8.5]}{=} (k+b)+j=(\ell+a)+j\\ &\overset{[8.5]}{\implies} \quad (i+b)+\ell=(j+a)+\ell\\ &\overset{[8.6]}{\implies} \quad i+b=j+a \quad \iff \quad (i,j)\sim(a,b)\ .\end{aligned}$$

CQFD

Preuve de [11.4]. Par définition on a les équivalences

$$\iota(n)=\iota(m) \quad \iff \quad [[\,n,0\,]]_{\mathbf{z}}=[[\,m,0\,]]_{\mathbf{z}} \quad \iff \quad n+0=0+m\ ,$$

ce qui montre directement que ι est injectif. CQFD

Preuve de [11.6]. Pour montrer la compatibilité, on prend $(a,b)\sim(a',b')$ et $(p,q)\sim(p',q')$ et on veut en déduire l'égalité

$$f\big((a,b),(p,q)\big)=f\big((a',b'),(p',q')\big) \quad \text{ou} \quad [[\,a+p,b+q\,]]_{\mathbf{z}}=[[\,a'+p',b'+q'\,]]_{\mathbf{z}}\ .$$

Par hypothèse on a les égalités

$$a+b'=b+a' \qquad \text{et} \qquad p+q'=q+p'\ .$$

En additionnant les membres de gauche et de droite on obtient l'égalité

$$(a+b')+(p+q')=(b+a')+(q+p')\ .$$

En utilisant l'associativité et la commutativité de l'addition dans $\mathbf{N}$ on peut réécrire cela comme

$$(a+p)+(b'+q')=(b+q)+(a'+p') \quad \Leftrightarrow \quad (a+p,b+q)\sim(a'+p',b'+q')\ .$$

La dernière équivalence implique directement l'égalité voulu. CQFD

Preuve de [11.7]. La preuve est un calcul direct :

$$\iota(m)\ +_{\mathbf{z}}\ \iota(n)=[[\,n,0\,]]_{\mathbf{z}}\ +_{\mathbf{z}}\ [[\,m,0\,]]_{\mathbf{z}} \overset{[11.6]}{=} [[\,n+m,0+0\,]]_{\mathbf{z}}=\iota(n+m)\ .$$

CQFD

Preuve de [11.8]. Pour montrer la compatibilité de f avec la relation d'équivalence, il faut montrer l'implication

$$(a,b)\sim(a',b') \quad \text{et} \quad (p,q)\sim(p',q') \qquad \Longrightarrow$$
$$(a\times p+b\times q, a\times q+b\times p)\sim(a'\times p'+b'\times q', a'\times q'+b'\times p') \ .$$

Autrement dit, il faut montrer l'implication

$$a+b'=a'+b \quad \text{et} \quad p+q'=p'+q \qquad \Longrightarrow$$
$$a\times p+b\times q+a'\times q'+b'\times p' = a\times q+b\times p+a'\times p'+b'\times q' \ .$$

Pour le montrer, on multiplie la première équation par p et par q et la deuxième par a' et par b' :

$$\begin{aligned}(a+b')\times p &= (a'+b)\times p\\ (a'+b)\times q &= (a+b')\times q\\ a'\times(p+q') &= a'\times(p'+q)\\ b'\times(p'+q) &= b'\times(p+q')\end{aligned}$$

et on les additionne (en utilisant la distributivité et la commutativité de l'addition dans $\mathbf{N}$) pour obtenir l'égalité

$$\begin{aligned}&(a\times p+b\times q+a'\times q'+b'\times p')+(b'\times p+a'\times q+a'\times p+b'\times q)\\ &\quad=(b\times p+a\times q+a'\times p'+b'\times q')+(a'\times p+b'\times q+a'\times q+b'\times p) \ .\end{aligned}$$

Il suffit maintenant d'invoquer [8.6.i] (et de nouveau la commutativité de l'addition et de la multiplication dans $\mathbf{N}$) pour en déduire l'égalité voulue

$$a\times p+b\times q+a'\times q'+b'\times p' = a\times q+b\times p+a'\times p'+b'\times q' \ . \qquad \boxed{CQFD}$$

Preuve de [11.9]. Il suffit de faire le calcul

$$\begin{aligned}\iota(k)\times_{\mathbf{Z}}\iota(\ell) &= [[\,k,0\,]]_{\mathbf{Z}}\times_{\mathbf{Z}}[[\,\ell,0\,]]_{\mathbf{Z}} \overset{[11.8]}{=} [[\,k\times\ell+0\times 0, k\times 0+0\times\ell\,]]_{\mathbf{Z}}\\ &= [[\,k\times\ell,0\,]]_{\mathbf{Z}} = \iota(k\times\ell) \ .\end{aligned} \qquad \boxed{CQFD}$$

Preuve de [11.23]. • (i) : Pour $a\in A$ on désigne par $b\in A$ l'opposé de $a\times 0_A$ pour l'opération $+$ et on fait le raisonnement

$$\begin{aligned} & 0_A \overset{(G2)}{=} 0_A+0_A\\ \Longrightarrow\quad & a\times 0_A = a\times(0_A+0_A) \overset{(A1\ \text{gauche})}{=} (a\times 0_A)+(a\times 0_A)\\ \Longrightarrow\quad & 0_A \overset{(G3)}{=} (a\times 0_A)+b = (a\times 0_A)+(a\times 0_A)+b = a\times 0_A \ .\end{aligned}$$

L'égalité $0_A\times a=0_A$ se démontre de la même façon en utilisant la distributivité à droite.

• (ii) : En invoquant la propriété de l'unité 1_A on calcule :

$$\begin{aligned}a+\big(\sigma(1_A)\times a\big) &\overset{(A3)}{=} (u\times a)+\big(\sigma(1_A)\times a\big) \overset{(A1)}{=} \big(1_A+\sigma(1_A)\big)\times a\\ &\overset{(G3)}{=} 0_A\times a \overset{(i)}{=} 0_A \ .\end{aligned}$$

Parce que $(A,+)$ est un groupe abélien, on a aussi $\big(\sigma(1_A)\times a\big)+a=0_A$. Avec l'unicité du symétrique pour $+$ il s'ensuit qu'on doit avoir l'égalité $\sigma(a)=\sigma(1_A)\times a$. Un calcul similaire montre qu'on a aussi l'égalité $\sigma(a)=a\times\sigma(1_A)$.

Par l'unicité du symétrique, 1_A est le symétrique de $\sigma(1_A)$ [11.14]. Par le résultat précédent avec $a=\sigma(1_A)$ on a donc $1_A=\sigma(1_A)\times\sigma(1_A)$. CQFD

Preuve de [11.24]. Supposons qu'on a $0_A=1_A$ et prenons $a\in A$ arbitraire. Alors on peut faire le calcul

$$a \overset{\text{(A3)}}{=} 1_A\times a \overset{\text{hyp.}}{=} 0_A\times a \overset{[11.23]}{=} 0_A\ .$$

L'ensemble A ne contient donc que l'élément $0_A=1_A$. CQFD

Preuve de [11.27]. Soit $a,b,c,d\in\mathbf{N}$ tels que $m=[\![a,b]\!]_{\mathbf{Z}}$ et $n=[\![c,d]\!]_{\mathbf{Z}}$. Alors par définition on a l'équivalence

$$m\leq_{\mathbf{Z}} n \qquad\Longleftrightarrow\qquad [\![a,b]\!]_{\mathbf{Z}}\leq_{\mathbf{Z}}[\![c,d]\!]_{\mathbf{Z}} \qquad\Longleftrightarrow\qquad a+d\leq b+c\ .$$

Par [8.14] il existe donc $j\in\mathbf{N}$ tel que $a+d+j=b+c=b+c+0$, ce qui est, par définition de la relation d'équivalence sur $\mathbf{N}\times\mathbf{N}$, équivalent à

$$(b+c,a+d)\sim(j,0) \qquad\Longleftrightarrow\qquad [\![b+c,a+d]\!]_{\mathbf{Z}}=[\![j,0]\!]_{\mathbf{Z}}=\iota(j)\ .$$

D'autre part, on peut faire le calcul

$$\begin{aligned} n-m=[\![c,d]\!]_{\mathbf{Z}}-[\![a,b]\!]_{\mathbf{Z}} &\equiv [\![c,d]\!]_{\mathbf{Z}}+\big(-[\![a,b]\!]_{\mathbf{Z}}\big)\\ &\overset{[11.18]}{=} [\![c,d]\!]_{\mathbf{Z}}+[\![b,a]\!]_{\mathbf{Z}}=[\![b+c,a+d]\!]_{\mathbf{Z}}\ .\end{aligned}$$

On vient donc de montrer l'équivalence

$$m\leq_{\mathbf{Z}} n \qquad\Longleftrightarrow\qquad \exists j\in\mathbf{N}: n-m=\iota(j)\ ,$$

ce qui termine la preuve. CQFD

Preuve de [11.28]. Pour montrer que $\mathbf{Z}$ est un anneau intègre, on prend $m,n\in\mathbf{Z}$ tels que $m\times n=0$. Pour montrer qu'on a $m=0$ ou $n=0$ on va considérer quatre cas selon les signes de m et n. On commence avec le cas $m,n\geq 0$. Alors par [11.27] on a $m,n\in\mathbf{N}$. Mais selon [8.13], si on a $m\times n=0$ avec $m,n\in\mathbf{N}$, alors $m=0$ ou $n=0$. Le lecteur si se sent mal à l'aise avec cet argument devrait revenir à la notation "exacte" selon laquelle notre hypothèse $m,n\geq 0$ (combinée avec [11.27]) est l'existence de $i,j\in\mathbf{N}$ tels que $m=\iota(i)$ est $n=\iota(j)$. On peut donc faire le raisonnement :

$$\begin{aligned} \iota(0)=m\times_{\mathbf{Z}} n \quad&\Longleftrightarrow\quad \iota(0)=\iota(i)\times_{\mathbf{Z}}\iota(j)=\iota(i\times j)\\ &\overset{[11.4]}{\Longrightarrow}\quad 0=i\times j \quad\overset{[8.13]}{\Longrightarrow}\quad i=0 \text{ ou } j=0 \quad\overset{[11.4]}{\Longleftrightarrow}\quad m=\iota(0) \text{ ou } n=\iota(0)\ .\end{aligned}$$

Pour notre deuxième cas on considère la situation $m<0$ et $n\geq 0$. Par [11.16] on a les égalités

$$0-m=0+(-m)=(-m)-(-0)=(-m)-0$$

et donc avec [11.27] on peut faire le raisonnement

$$m < 0 \quad \Rightarrow \quad 0 - m = (-m) - 0 \in \mathbf{N} \quad \Rightarrow \quad -m \geq 0 \ .$$

Mais $m \neq 0$ donc $-m \neq -0 = 0$ [11.16], donc $-m > 0$. Maintenant on peut faire le calcul

$$\begin{aligned} 0 &\overset{[11.16.\text{i}]}{=} -0 \overset{[11.26.\text{ii}]}{=} (-1) \times 0 = (-1) \times (m \times n) \\ &\overset{[11.19.\text{ii}]}{=} \big((-1) \times m\big) \times n \overset{[11.26.\text{ii}]}{=} (-m) \times n \ . \end{aligned}$$

Parce que $-m, n \geq 0$, il s'ensuit (avec l'argument du premier cas ci-dessus) qu'on doit avoir $-m = 0$ ou $n = 0$. Mais $-m \neq 0$, donc on doit avoir $n = 0$, ce qui est de nouveau la conclusion voulue. Les deux cas restants (le cas $m \geq 0$ et $n < 0$ ainsi que le cas $m, n < 0$) se démontrent de la même façon ; les détails sont laissés aux bons soins du lecteur.

Pour en déduire la dernière propriété, on fait le raisonnement suivant :

$$\begin{aligned} p \times m = p \times n \quad &\Leftrightarrow \quad 0 = p \times m - p \times n = p \times (m - n) \\ &\Rightarrow \quad p = 0 \text{ ou } m - n = 0 \quad \Leftrightarrow \quad p = 0 \text{ ou } m = n \ . \end{aligned}$$ CQFD

Preuve de [11.29]. • Pour $m, n, p \in \mathbf{Z}$ on peut faire le calcul :

$$\begin{aligned} n - m = n + (-m) + 0 &= n + (-m) + p + (-p) = n + p + \big((-m) + (-p)\big) \\ &\overset{[11.14.\text{iii}]}{=} n + p + \big(-(p + m)\big) = (n + p) - (m + p) \ . \end{aligned}$$

Selon [11.27] on a donc l'équivalence

$$m \leq n \qquad \Longleftrightarrow \qquad m + p \leq n + p \ .$$

• De nouveau par [11.27], les hypothèses $m, n \geq 0$ sont équivalentes à $m = m - 0 \in \mathbf{N}$ et $n = n - 0 \in \mathbf{N}$. Et parce que $\mathbf{N}$ est stable par multiplication, c'est-à-dire, si n et m sont dans $\mathbf{N}$, alors $n \times m$ appartient à $\mathbf{N}$, on en déduit qu'on a $n \times m \geq 0$. CQFD

Preuve de [11.33]. On commence avec la définition de l'application $\phi_m : \mathbf{Z} \to \mathbf{Z}$ définie par

$$\phi_m(x) = x - m \ .$$

Il est "évident" que ϕ_m est bijective avec application réciproque $\psi_m : \mathbf{Z} \to \mathbf{Z}$ définie par

$$\psi_m(x) = x + m \ .$$

Par [11.29.i] il s'ensuit que ϕ_m et ψ_m préservent la relation d'ordre dans le sens que pour tout $x, y \in \mathbf{Z}$ on a

$$x \leq y \qquad \Longleftrightarrow \qquad \phi_m(x) \leq \phi_m(y) \text{ et } \psi_m(x) \leq \psi_m(y) \ .$$

De plus, par hypothèse sur B on a la propriété

$$\forall n \in B : m \leq n \quad \Leftrightarrow \quad n - m \geq 0 \quad \Leftrightarrow \quad \phi_m(n) \geq 0 \ .$$

Par [11.27] il s'ensuit qu'on a $\phi_m[B] \subset \mathbf{N}$, ce qui nous permet d'appliquer [8.17] (B n'est pas vide, donc $\phi_m[B]$ non plus) pour conclure qu'il existe $k_o \in \phi[B]$ tel que

$$\forall k \in \phi_m[B] : k_o \leq k \ .$$

Maintenant on pose $m_o = \psi_m(k_o)$ et on raisonne :

$$\begin{aligned} n \in B \quad &\Rightarrow \quad \phi_m(n) \in \phi_m[B] \quad \Rightarrow \quad \phi_m(n) \geq k_o \\ &\Rightarrow \quad n = \psi_m\big(\phi_m(n)\big) \geq \psi_m(k_o) = m_o \ , \end{aligned}$$

ce qui termine la preuve. $\boxed{CQFD}$

Les preuves de §12

Preuve de [12.5]. Selon [4.12], si f appartient à $\mathrm{App}(A,B)$ et g à $\mathrm{App}(B,C)$, alors $g\circ f$ appartient à $\mathrm{App}(A,C)$. Ceci montre que la définition de C_{omp} a bien un sens. La vérification que C_{omp} est une application de $\mathrm{App}(B,C)\times\mathrm{App}(A,B)$ dans $\mathrm{App}(A,C)$ [4.1] est immédiate et laissée aux bons soins du lecteur. *CQFD*

Les preuves de §13

Preuve de [13.1]. On fixe l'élément $g \in G$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, k \in \mathbf{N} \mid k \star \sigma(g) = \sigma(k \star g) \,\} \ .$$

Pour montrer qu'on a $0 \in E$ on fait le calcul

$$0 \star \sigma(g) \overset{(12.9)}{=} e \overset{[11.14.\text{i}]}{=} \sigma(e) \overset{(12.9)}{=} \sigma(0 \star g) \ .$$

Supposons maintenant qu'on a $k \in E$, alors on peut faire le calcul

$$S(k) \star \sigma(g) \overset{(12.9)}{=} \big(k \star \sigma(g)\big) \cdot \sigma(g) \overset{k \in E}{=} \sigma(k \star g) \cdot \sigma(g) \overset{[11.14.\text{iii}]}{=} \sigma\big(g \cdot (k \star g)\big)$$

$$\overset{[12.8]}{=} \sigma\big((1+k) \star g\big) \overset{[8.5.\text{iii}]}{=} \sigma\big(S(k) \star g\big) \ ,$$

ce qui montre qu'on a aussi $S(k) \in E$. Par récurrence on a donc $E = \mathbf{N}$, ce qui termine la preuve de la première propriété.

Pour la deuxième propriété on fait le calcul

$$\begin{aligned}(k \star g) \cdot \big(\ell \star \sigma(g)\big) &= \sigma(\ell \star g) \cdot (\ell \star g) \cdot (k \star g) \cdot \sigma(\ell \star g) \\ &\overset{[12.10]}{=} \sigma(\ell \star g) \cdot (k \star g) \cdot (\ell \star g) \cdot \sigma(\ell \star g) \\ &= \big(\ell \star \sigma(g)\big) \cdot (k \star g) \ . \end{aligned}$$

CQFD

Preuve de [13.3]. Soit $F \in \mathrm{App}(P, \mathrm{App}(A, B))$, $p \in P$ et $a \in A$ arbitraire. Alors on peut faire le calcul (en utilisant les définition de Φ et Ψ)

$$((\Psi(\Phi(F)))(p))(a) = (\Phi(F))(p, a) = (F(p))(a) \ .$$

Étant donné que a est arbitraire, l'invocation de [4.3] nous assure qu'on a l'égalité $(\Psi(\Phi(F)))(p) = F(p)$ entre ces deux applications. Mais p était aussi arbitraire, donc le même résultat nous assure l'égalité $\Psi(\Phi(F)) = F$, ce qui veut dire qu'on a l'égalité $(\Psi \circ \Phi)(F) = F$. Le fait que F était arbitraire implique alors qu'on a l'égalité $\Psi \circ \Phi = id_{\mathrm{App}(P,\mathrm{App}(A,B))}$.

Soit maintenant $G \in \mathrm{App}(P \times A, B)$, $p \in P$ et $a \in A$ arbitraire. Alors on peut faire le calcul (en utilisant les définition de Φ et Ψ)

$$(\Phi(\Psi(G)))(p, a) = ((\Psi(G))(p))(a) = G(p, a) \ .$$

Étant donné que p et a sont arbitraires, l'invocation de [4.3] en combinaison avec [2.7] nous assure qu'on a l'égalité $(\Phi \circ \Psi)(G) = \Phi(\Psi(G)) = G$. Le fait que G était arbitraire implique (toujours avec [4.3]) qu'on a l'égalité $\Phi \circ \Psi = id_{\mathrm{App}(P \times A, B)}$. La conclusion de l'énoncé est maintenant une conséquence immédiate de [5.15]. CQFD

Preuve de [13.8]. • Unicité et (13.10). Pour montrer l'unicité, on rappelle d'abord que l'ordre sur $\mathbf{Z}$ est total, ce qui implique que pour $n \in \mathbf{Z}$ on a soit $n \geq \iota(0)$, soit $n \leq \iota(0)$. Dans le premier cas il s'ensuit (avec [11.27]) qu'il existe $k \in \mathbf{N}$ tel que $n = \iota(k)$. Et dans le deuxième cas il existe (par [11.27], et [11.32.iv]) $k \in \mathbf{N}$ tel que $n = -\iota(k)$. Dans les deux cas (13.10) nous donne une expression pour $n \star_{\mathbf{Z}} g$ en termes de l'opération externe de $\mathbf{N}$ sur G. Il s'ensuit que, si (13.10) est juste, alors il ne peuvent pas exister deux opérations externes différentes de $\mathbf{Z}$ sur G.

Mais en mêmê temps cela montre que l'opération $\star_{\mathbf{Z}}$ (si elle existe) est complètement déterminée par l'opération $\star$.

On suppose donc qu'il existe une telle opération $\star_{\mathbf{Z}}$ et on montre (13.10). Pour cela on définit $E_+ \subset \mathbf{N}$ comme

$$E_+ = \{\, k \in \mathbf{N} \mid \forall g \in G : \iota(k) \star_{\mathbf{Z}} g = k \star g \,\} \ .$$

Mais attention, une fois qu'on a décidé d'écrire explicitement l'injection canonique $\iota : \mathbf{N} \to \mathbf{Z}$ pour distinguer les éléments de $\mathbf{N}$ des éléments de $\mathbf{Z}$, il faut écrire les conditions (13.9) comme

$$\iota(0) \star_{\mathbf{Z}} g = e \qquad \text{et} \qquad \forall n \in \mathbf{Z} : (n + \iota(1)) \star_{\mathbf{Z}} g = (n \star_{\mathbf{Z}} g) \cdot g \ . \tag{33.15}$$

La première partie nous dit immédiatement qu'on a $0 \in E_+$ (car $0 \star g = e$) et la deuxième partie, appliquée à $n = \iota(k)$ et en utilisant [11.7], s'écrit comme

$$\iota\big(S(k)\big) \star_{\mathbf{Z}} g = \big(\iota(k) \star_{\mathbf{Z}} g\big) \cdot g \ .$$

Il s'ensuit qu'on a l'implication $k \in E_+ \Rightarrow S(k) \in E_+$. Par récurrence il en découle qu'on a $E_+ = \mathbf{N}$, ce qui montre la première partie de (13.10).

Pour les nombres négatifs, on définit l'ensemble $E_- \subset \mathbf{N}$ comme

$$E_- = \{\, k \in \mathbf{N} \mid \forall g \in G : (-\iota(k)) \star_{\mathbf{Z}} g = k \star \sigma(g) \,\} \ .$$

Parce qu'on a les égalités $-\iota(0) = \iota(0)$ et $\sigma(e) = e$, on a $0 \in E_-$. Supposons donc qu'on a $k \in E_-$. Alors on peut faire le calcul

$$\begin{aligned}\big((-\iota(S(k))) \star_{\mathbf{Z}} g\big) \cdot g &\overset{(33.15)}{=} \big(-\iota(S(k)) + \iota(1)\big) \star_{\mathbf{Z}} g = \big(-\iota(k) - \iota(1) + \iota(1)\big) \star_{\mathbf{Z}} g \\ &= \big(-\iota(k)\big) \star_{\mathbf{Z}} g = k \star \sigma(g) \ .\end{aligned}$$

De cette égalité on déduit l'égalité

$$\Big(\big((-\iota(S(k))) \star_{\mathbf{Z}} g\big) \cdot g\Big) \cdot \sigma(g) = \big(k \star \sigma(g)\big) \cdot \sigma(g) = S(k) \star \sigma(g) \ .$$

Par l'associativité de l'opération $\cdot$, l'égalité $g \cdot \sigma(g) = e$ et la propriété de l'unité e, il s'ensuit qu'on a $S(k) \in E_-$. Par récurrence on a donc $E_- = \mathbf{N}$, ce montre la deuxième partie de (13.10). CQFD

Suite de la preuve de [13.8]. • **Existence de l'opération $\star_{\mathbf{Z}}$.** On définit l'application $\varphi : (\mathbf{N} \times \mathbf{N}) \times G \to G$ par

$$\varphi\big((k, \ell), g\big) = (k \star g) \cdot \big(\ell \star \sigma(g)\big) \ .$$

Ensuite on applique [13.3] avec $P = \mathbf{N} \times \mathbf{N}$ et $A = B = G$ et l'application $\varphi \in \mathrm{App}(P \times A, B)$. Alors $\Psi(\varphi) \in \mathrm{App}(P, \mathrm{App}(A, B))$, c'est-à-dire

$$\Psi(\varphi) : \mathbf{N} \times \mathbf{N} \to \mathrm{App}(G, G) \ .$$

Sur $\mathbf{N} \times \mathbf{N}$ on a une relation d'équivalence et on veut appliquer [9.9]. Pour cela il faut vérifier que $\Psi(\varphi)$ est compatible avec la relation d'équivalence. Plus précisément, il faut montrer l'implication

$$(k, \ell) \sim (m, n) \qquad \Longrightarrow \qquad \big(\Psi(\varphi)\big)\big((k, \ell)\big) = \big(\Psi(\varphi)\big)\big((m, n)\big) \ .$$

On prend donc $(k, \ell) \sim (m, n)$, ce qui veut dire qu'on a $k + n = \ell + m$ [11.2] et on rappelle qu'il existe $j \in \mathbf{N}$ tel qu'on a $k = m + j$ ou $m = k + j$ [8.12]. Dans le premier cas on a donc

$$m + j + n = k + n = m + \ell \quad \overset{[8.6]}{\Longrightarrow} \quad j + n = \ell \ .$$

Et ensuite on fait le calcul

$$\begin{aligned}\Big(\big(\Psi(\varphi)\big)\big((k,\ell)\big)\Big)(g) &= \varphi\big((k,\ell),g\big) = (k\star g)\cdot\big(\ell\star\sigma(g)\big)\\ &= \big((m+j)\star g\big)\cdot\big((j+n)\star\sigma(g)\big)\\ &= (m\star g)\cdot(j\star g)\cdot\big(j\star\sigma(g)\big)\cdot\big(n\star\sigma(g)\big)\\ &= (m\star g)\cdot\big(n\star\sigma(g)\big)\\ &= \varphi\big((m,n),g\big) = \Big(\big(\Psi(\varphi)\big)\big((m,n)\big)\Big)(g)\ .\end{aligned}$$

Ceci étant valable pour tout $g\in G$, on en déduit (avec [4.3]) l'égalité $\big(\Psi(\varphi)\big)\big((k,\ell)\big) = \big(\Psi(\varphi)\big)\big((m,n)\big)$, ce qui est la conclusion voulue. Dans le deuxième cas le raisonnement est analogue et conduit également à cette conclusion.

L'application $\Psi(\varphi):\mathbf{N}\times\mathbf{N}\to \mathrm{App}(G,G)$ est donc compatible avec la relation d'équivalence. Par [9.9] il s'ensuit qu'il existe une application $F:\mathbf{Z}\to\mathrm{App}(G,G)$ vérifiant

$$\forall k,\ell\in\mathbf{N}: F\big([\![k,\ell]\!]_{\mathbf{z}}\big) = \big(\Psi(\varphi)\big)\big((k,\ell)\big)\ .$$

Et finalement on réinvoque [13.3] pour transformer l'application F en une application $\star_{\mathbf{z}} = \Phi(F):\mathbf{Z}\times G\to G$ vérifiant

$$\begin{aligned}[\![k,\ell]\!]_{\mathbf{z}}\star_{\mathbf{z}} g &\equiv \big(\Phi(F)\big)\big([\![k,\ell]\!]_{\mathbf{z}},g\big) = \big(F([\![k,\ell]\!]_{\mathbf{z}})\big)(g)\\ &= \Big(\big(\Psi(\varphi)\big)\big((k,\ell)\big)\Big)(g) = \varphi\big((k,\ell),g\big) = (k\star g)\cdot\big(\ell\star\sigma(g)\big)\ .\end{aligned}\tag{33.16}$$

Maintenant qu'on a l'application, il suffit de vérifier qu'elle a les propriétés requises (13.9)/(33.15). Pour cela on calcule d'abord

$$\iota(0)\star_{\mathbf{z}} g = [\![0,0]\!]_{\mathbf{z}}\star_{\mathbf{z}} g \overset{(33.16)}{=} (0\star g)\cdot\big(0\star\sigma(g)\big) = e\cdot e = e\ .$$

Pour montrer la deuxième propriété on fait le calcul (en utilisant bien l'associativité de l'opération $\cdot$ et les propriétés de l'opération externe $\star$ de $\mathbf{N}$ sur G)

$$\begin{aligned}\big([\![k,\ell]\!]_{\mathbf{z}}+\iota(1)\big)\star_{\mathbf{z}} g &= [\![k+1,\ell]\!]_{\mathbf{z}}\star_{\mathbf{z}} g \overset{(33.16)}{=} \big((k+1)\star g\big)\cdot\big(\ell\star\sigma(g)\big)\\ &\overset{[12.8.ii]}{=} (k\star g)\cdot(1\star g)\cdot\big(\ell\star\sigma(g)\big)\\ &\overset{[13.1]}{=} (k\star g)\cdot\big(\ell\star\sigma(g)\big)\cdot(1\star g)\overset{[12.8.i]}{=}\big([\![k,\ell]\!]_{\mathbf{z}}\star g\big)\cdot g\ .\end{aligned}$$

• **Les propriétés (i) à (v).** Pour la propriété (i) on fait le calcul

$$\iota(1)\star_{\mathbf{z}} g \overset{(13.10)}{=} 1\star g \overset{[12.8.i]}{=} g\ .$$

Pour la propriété (ii) on fait d'abord la remarque qu'il existe $k,\ell,k',\ell'\in\mathbf{N}$ tel qu'on a $m=[\![k,\ell]\!]_{\mathbf{z}}$ et $n=[\![k',\ell']\!]_{\mathbf{z}}$. Ensuite on fait le calcul

$$\begin{aligned}(m+n)\star_{\mathbf{z}} g &= \big([\![k,\ell]\!]_{\mathbf{z}}+[\![k',\ell']\!]_{\mathbf{z}}\big)\star_{\mathbf{z}} g = [\![k+k',\ell+\ell']\!]_{\mathbf{z}}\star_{\mathbf{z}} g\\ &\overset{(33.16)}{=}\big((k+k')\star g\big)\cdot\big((\ell+\ell')\star\sigma(g)\big)\\ &\overset{[12.8.ii]}{=}(k\star_{\mathbf{z}} g)\cdot(k'\star g)\cdot\big(\ell\star\sigma(g)\big)\cdot\big(\ell'\star\sigma(g)\big)\\ &\overset{[13.1]}{=}(k\star_{\mathbf{z}} g)\cdot\big(\ell\star\sigma(g)\big)\cdot(k'\star g)\cdot\big(\ell'\star\sigma(g)\big)\\ &\overset{(33.16)}{=}\big([\![k,\ell]\!]_{\mathbf{z}}\star_{\mathbf{z}} g\big)\cdot\big([\![k',\ell']\!]_{\mathbf{z}}\star_{\mathbf{z}} g\big) = (m\star_{\mathbf{z}} g)\cdot(n\star_{\mathbf{z}} g)\ .\end{aligned}$$

Pour la propriété (iii) on fait le calcul

$$\big((-m)\star_{\mathbf{z}} g\big)\cdot(m\star_{\mathbf{z}} g) = \big(((-m)+m)\star_{\mathbf{z}} g\big) = 0\star_{\mathbf{z}} g = e\ ,$$

ce qui montre qu'on a bien $\sigma(m\star_{\mathbf{z}} g) = (-m)\star_{\mathbf{z}} g$.

Pour la propriété (iv) on fait le calcul (en distinguant la multiplication $\times_{\mathbf{Z}}$ dans $\mathbf{Z}$ de la multiplication $\times$ dans $\mathbf{N}$)

$$\begin{aligned}
(m \times_{\mathbf{Z}} n) \star_{\mathbf{Z}} g &= (\,[\![\, k, \ell \,]\!]_{\mathbf{Z}} \times_{\mathbf{Z}} [\![\, k', \ell' \,]\!]_{\mathbf{Z}}) \star_{\mathbf{Z}} g \\
&\overset{[11.8]}{=} [\![\, k \times k' + \ell \times \ell', k \times \ell' + k' \times \ell \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} g \\
&= \big((k \times k' + \ell \times \ell') \star g\big) \cdot \big((k \times \ell' + k' \times \ell) \star \sigma(g)\big) \\
&\overset{[12.8.\text{ii}]}{=} \big((k \times k') \star g\big) \cdot \big((\ell \times \ell') \star g\big) \cdot \big((k \times \ell') \star \sigma(g)\big) \cdot \big((k' \times \ell) \star \sigma(g)\big) \\
&\overset{[13.1]}{=} \big((k \times k') \star g\big) \cdot \big((k \times \ell') \star \sigma(g)\big) \cdot \big((\ell \times \ell') \star g\big) \cdot \big((k' \times \ell) \star \sigma(g)\big) \\
&\overset{[12.8.\text{iii}]}{=} \big(k \star (k' \star g)\big) \cdot \big(k \star (\ell' \star \sigma(g))\big) \cdot \big(\ell \star (\ell' \star g)\big) \cdot \big(\ell \star (k' \star \sigma(g))\big) \\
&\overset{[12.8.\text{iv}],\ [13.1]}{=} (k \star \big((k' \star g) \cdot (\ell' \star \sigma(g))\big)) \cdot (\ell \star \big((\ell' \star g) \cdot (k' \star \sigma(g))\big)) \\
&\overset{[11.14.\text{ii}],\ [13.1]}{=} \big(k \star \big(\,[\![\, k', \ell' \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} g\big)\big) \cdot (\ell \star \big(\sigma(\ell' \star \sigma(g)) \cdot \sigma(k' \star g)\big)) \\
&\overset{[11.14.\text{iii}]}{=} \big(k \star \big(\,[\![\, k', \ell' \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} g\big)\big) \cdot (\ell \star \sigma\big((k' \star g) \cdot (\ell' \star \sigma(g))\big)) \\
&= \big(k \star (\,[\![\, k', \ell' \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} g)\big) \cdot \big(\ell \star \sigma(\,[\![\, k', \ell' \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} g)\big) \\
&= [\![\, k, \ell \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} (\,[\![\, k', \ell' \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} g) \ .
\end{aligned}$$

Finalement pour la propriété (v) on calcule

$$\begin{aligned}
m \star_{\mathbf{Z}} (g \cdot h) = [\![\, k, \ell \,]\!]_{\mathbf{Z}}(g \cdot h) &= \big(k \star (g \cdot h)\big) \cdot \big(\ell \star \sigma(g \cdot h)\big) \\
&= \big((k \star g) \cdot (k \star h)\big) \cdot \sigma\big((\ell \star g) \cdot (\ell \star h)\big) \\
&= (k \star g) \cdot (k \star h) \cdot \big(\ell \star \sigma(h)\big) \cdot \big(\ell \star \sigma(g)\big) \\
&= (k \star g) \cdot \big(\ell \star \sigma(g)\big) \cdot (k \star h) \cdot \big(\ell \star \sigma(h)\big) \\
&= (\,[\![\, k, \ell \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} g) \cdot (\,[\![\, k, \ell \,]\!]_{\mathbf{Z}} \star_{\mathbf{Z}} h) \\
&= (m \star_{\mathbf{Z}} g) \cdot (m \star_{\mathbf{Z}} h) \ . \qquad \boxed{CQFD}
\end{aligned}$$

Les preuves de §14

Preuve de [14.2]. La réflexivité et la symétrie sont immédiate car ces propriétés sont données par

$$(m,n)\sim(m,n) \quad\Longleftrightarrow\quad m\times n = n\times m \ ,$$

ce qui est vrai par la commutativité de la multiplication dans $\mathbf{Z}$ [11.19.i], et par

$$\big((m,n)\sim(p,q)\ \Rightarrow\ (p,q)\sim(m,n)\big) \quad\Longleftrightarrow\quad \big(m\times q = n\times p\ \Rightarrow\ p\times n = q\times m\big)\ ,$$

ce qui est vrai, de nouveau par la commutativité de la multiplication.

Pour la transitivité on suppose qu'on a $(m,n)\sim(p,q)$ et $(p,q)\sim(a,b)$, ce qui nous donne les égalités

$$m\times q = n\times p \qquad\text{et}\qquad p\times b = q\times a \ .$$

On peut donc faire le raisonnement

$$m\times q\times b = n\times p\times b = n\times q\times a \overset{[11.19.\text{i/ii}],\ [11.28],\ q\neq 0}{\Longrightarrow} m\times b = n\times a \ ,$$

ce qui est équivalent à $(m,n)\sim(a,b)$. CQFD

Preuve de [14.5]. Ce qu'il faut vérifier est l'implication

$$(m,n)\sim(m',n') \text{ et } (p,q)\sim(p',q') \quad\Rightarrow\quad f\big((m,n),(p,q)\big) = f\big((m',n'),(p',q')\big)$$

pour tout $(m,n),(m',n'),(p,q),(p',q')\in\mathbf{Z}\times\mathbf{Z}^*$. Pour cela on part donc de l'hypothèse

$$m\times n' = n\times m' \qquad\text{et}\qquad p\times q' = q\times p' \tag{33.17}$$

et on fait le calcul

$$\begin{aligned}
f\big((m,n),(p,q)\big) &= \frac{m\times q + p\times n}{n\times q} \overset{(14.1)}{=} \frac{(m\times q + p\times n)\times n'\times q'}{n\times q\times n'\times q'} \\
&\overset{[11.19]}{=} \frac{m\times n'\times q\times q' + p\times q'\times n\times n'}{n\times q\times n'\times q'} \\
&\overset{(33.17)}{=} \frac{n\times m'\times q\times q' + q\times p'\times n\times n'}{n\times q\times n'\times q'} \\
&\overset{[11.19]}{=} \frac{(m'\times q' + p'\times n')\times n\times q}{n\times q\times n'\times q'} \overset{(14.1)}{=} \frac{m'\times q' + p'\times n'}{n'\times q'} \\
&= f\big((m',n'),(p',q')\big)\ .
\end{aligned}$$

CQFD

Preuve de [14.10]. • Pour montrer que $\preccurlyeq$ est compatible avec la relation d'équivalence, on prend $(a,b),(a',b'),(p,q),(p',q')\in\mathbf{Z}\times\mathbf{Z}^*$ et on suppose qu'on a

$$(a,b)\sim(a',b') \text{ et } (p,q)\sim(p',q')$$

ce qui est équivalent à

$$a\times b' = a'\times b \text{ et } p\times q' = p'\times q \ . \tag{33.18}$$

Avec cela on fait le calcul suivant :

$$\begin{array}{rc} & (a,b) \preccurlyeq (p,q) \\ \iff & a\times b\times q\times q \leq p\times q\times b\times b \\ \overset{[11.32.i],\,[11.32.v]}{\iff} & a\times b\times q\times q\times b'\times b'\times q'\times q' \leq p\times q\times b\times b\times b'\times b'\times q'\times q' \\ \overset{(33.18)}{\iff} & a'\times b\times q\times q\times b\times b'\times q'\times q' \leq p'\times q\times b\times b\times b'\times b'\times q\times q' \\ \overset{[11.32.iii],\,[11.32.v]}{\implies} & a'\times b'\times q'\times q' \leq p'\times b'\times b'\times q' \\ \iff & (a',b') \preccurlyeq (p',q') \ . \end{array}$$

• Pour la réflexivité de $\leq_{\mathbf{Q}}$ il suffit de faire la remarque qu'on a l'équivalence $\frac{a}{b} \leq_{\mathbf{Q}} \frac{a}{b} \Leftrightarrow a\times b\times b\times b \leq a\times b\times b\times b$, ce qui est vrai car $\leq$ est réflexif.

• Pour l'antisymétrie de $\leq_{\mathbf{Q}}$ on fait le raisonnement suivant :

$$\begin{array}{rc} & \dfrac{a}{b} \leq_{\mathbf{Q}} \dfrac{p}{q} \quad \text{et} \quad \dfrac{p}{q} \leq_{\mathbf{Q}} \dfrac{a}{b} \\ \iff & a\times b\times q\times q \leq p\times q\times b\times b \quad \text{et} \quad p\times q\times b\times b \leq a\times b\times q\times q \\ \overset{\leq \text{ antisym.}}{\implies} & a\times b\times q\times q = p\times q\times b\times b \\ \overset{[11.28]}{\implies} & a\times q = p\times b \quad \iff \quad \dfrac{a}{b} = \dfrac{p}{q} \ . \end{array}$$

• Pour la transitivité de $\leq_{\mathbf{Q}}$ on fait le raisonnement suivant :

$$\begin{array}{rc} & \dfrac{a}{b} \leq_{\mathbf{Q}} \dfrac{p}{q} \quad \text{et} \quad \dfrac{p}{q} \leq_{\mathbf{Q}} \dfrac{r}{s} \\ \iff & a\times b\times q^2 \leq p\times q\times b^2 \quad \text{et} \quad p\times q\times s^2 \leq r\times s\times q^2 \\ \iff & a\times b\times q^2\times s^2 \leq p\times q\times b^2\times s^2 \quad \text{et} \quad p\times q\times s^2\times b^2 \leq r\times s\times q^2\times b^2 \\ \overset{\leq \text{ trans.}}{\implies} & a\times b\times q^2\times s^2 \leq r\times s\times q^2\times b^2 \\ \overset{[11.32.iii],\,[11.32.v]}{\implies} & a\times b\times s^2 \leq r\times s\times b^2 \quad \iff \quad \dfrac{a}{b} \leq_{\mathbf{Q}} \dfrac{r}{s} \ . \end{array}$$

• Finalement, pour montrer que $\leq_{\mathbf{Q}}$ est une relation d'ordre total sur $\mathbf{Q}$ il suffit de remarquer que $\leq$ est une relation d'ordre total sur $\mathbf{Z}$. Pour $(a,b),(p,q) \in \mathbf{Z}\times\mathbf{Z}^*$ on a donc

$$a\times b\times q^2 \leq p\times q\times b^2 \qquad \text{ou} \qquad p\times q\times b^2 \leq a\times b\times q^2 \ ,$$

ce qui est équivalent à $\frac{a}{b} \leq_{\mathbf{Q}} \frac{p}{q}$ ou $\frac{p}{q} \leq_{\mathbf{Q}} \frac{a}{b}$. CQFD

Preuve de [14.27]. Si $r \leq 0$, il suffit de prendre $k = 1$ pour avoir $k > r$. Supposons donc qu'on a $r > 0$. Par définition de $\mathbf{Q}$ il existe $(m,n) \in \mathbf{Z}\times\mathbf{Z}^*$ tel que $r = \frac{m}{n}$. La condition $r > 0$ se traduit par la condition $m\times n > 0$. Si $m \geq 0$ et $n < 0$ ou $m \leq 0$ et $n > 0$, alors par [11.32.i] $m\times n \leq 0$. Il s'ensuit qu'on doit avoir $m,n > 0$ ou $m,n < 0$. Dans le dernier cas on aurait $r = \frac{m}{n} = \frac{-m}{-n}$ avec $-m,-n > 0$ [11.32.iv]. Sans perte de généralité on peut donc supposer qu'on a $m,n > 0$. Autrement dit (avec [11.27] et [11.32.iv]), on peut supposer qu'on a $m,n \in \mathbf{N}$.

Une fois qu'on sait qu'on est dans $\mathbf{N}$, on peut appliquer [8.16] pour déduire de l'inégalité $n > 0$ qu'on a $n \geq 1$. On peut donc faire le raisonnement

$$\begin{array}{ll} & m \times n \geq 0 \text{ et } 1 \leq n \\ \overset{[11.32.i]}{\Longrightarrow} & m \times n \times 1 \leq m \times n \times n \quad \Longleftrightarrow \quad m \times n \times 1 \times 1 \leq m \times n \times n \times 1 \\ \overset{[14.11]}{\Longleftrightarrow} & \dfrac{m}{n} \leq \dfrac{m}{1} = \iota(m) \equiv m \ . \end{array}$$

Si on pose $k = m + 1 \in \mathbf{N}$, on a donc les inégalités (on utilise $1 > 0$)

$$k = m + 1 \overset{[11.29.i]}{>} m \geq \frac{m}{n} = r$$

comme voulu. $\boxed{CQFD}$

Les preuves de §15

Preuve de [15.1]. La condition (C1) est immédiate, car $r+1 \in \,]r,\infty[$ et $r \notin \,]r,\infty[$. La condition (C2) est une conséquence immédiate de la transitivité d'une relation d'ordre. Pour la condition (C3) il suffit de remarquer que si $s \in \,]r,\infty[$, c'est-à-dire $r < s$, alors par [14.26] il existe $t \in \mathbf{Q}$ tel que $r < t < s$. Et donc $t \in \,]r,\infty[$ et $t < s$, ce qui montre que $]r,\infty[$ vérifie (C3).

Pour l'injectivité on prend $r, s \in \mathbf{Q}$ avec $r \neq s$. Parce que $\leq$ est une relation d'ordre total sur $\mathbf{Q}$ on doit avoir $r < s$ ou $s < r$. Dans le cas $r < s$ on a $s \in \,]r,\infty[$ et $s \notin \,]s,\infty[$, donc $]r,\infty[\neq \,]s,\infty[$. Dans le cas $r > s$ l'argument est similaire en échangeant les rôles de r et s, ce qui montre qu'on a bien l'implication $r \neq s \;\Rightarrow\; \iota(r) \neq \iota(s)$. CQFD

Preuve de [15.3]. Le fait que $\leq_{\mathbf{R}}$ est une relation d'ordre sur $\mathbf{R}$ se démontre de plusieurs façons. On peut simplement reprendre les arguments donnés dans la preuve de [3.13] qui dit que l'inclusion est une relation d'ordre sur l'ensembles des parties. On peut aussi invoquer [3.13] et [3.10] pour déduire que la relation $xRy \Leftrightarrow y \subset x$ est une relation d'ordre sur $\mathcal{P}(\mathbf{Q})$ et ensuite [5.6] pour en déduire que la restriction à $\mathbf{R} \subset \mathcal{P}(\mathbf{Q})$ est une relation d'ordre.

Reste donc à montrer que cet ordre est total. Prenons donc x et y deux coupures et supposons qu'on n'a pas l'inclusion $x \subset y$. Il existe donc $r \in x$ tel que $r \notin y$. Si on prend $s \in y$, alors par (C2) (appliqué à y) on doit avoir $r < s$ (car $\leq$ est un ordre total sur $\mathbf{Q}$). Il s'ensuit qu'on a l'implication

$$s \in y \qquad \Longrightarrow \qquad r \leq s \;\;.$$

Par (C2) appliqué à la coupure x on en déduit (avec $r \in x$) qu'on a $s \in x$. Ainsi on a montré l'implication $s \in y \Rightarrow s \in x$, c'est-à-dire l'inclusion $y \subset x$. CQFD

Preuve de [15.4]. Par définition de la relation d'ordre et de l'injection canonique on a l'équivalence

$$\iota(r) \leq_{\mathbf{R}} \iota(s) \qquad \Longleftrightarrow \qquad]s,\infty[\;\subset\;]r,\infty[$$

et par définition d'un intervalle et de l'inclusion on a l'équivalence

$$]s,\infty[\;\subset\;]r,\infty[\qquad \Longleftrightarrow \qquad \forall t \in \mathbf{Q} : t > s \;\Rightarrow\; t > r \;\;. \tag{33.19}$$

Pour montrer l'équivalence avec $r \leq s$, on commence avec l'implication directe en supposant $r \leq s$. Par la transitivité d'une relation d'ordre [3.11] on a l'implication

$$r \leq s \quad \text{et} \quad s < t \qquad \Longrightarrow \qquad r < t \;\;,$$

ce qui montre (avec (33.19)) l'implication $r \leq s \;\Rightarrow\; \iota(r) \leq_{\mathbf{R}} \iota(s)$. Pour l'implication réciproque on suppose $\iota(r) \leq_{\mathbf{R}} \iota(s)$. Si on avait $r > s$, alors en prenant $t = r > s$ dans (33.19) on aurait $r > r$, ce qui est impossible. La condition $\iota(r) \leq_{\mathbf{R}} \iota(s)$ implique donc (par contraposée et le fait que $\leq$ est un ordre total sur $\mathbf{Q}$) la condition $r \leq s$. CQFD

Preuve de [15.5]. Si on a $r \in x$, alors par (C2) on a l'implication $r < s \Rightarrow s \in x$, ce qui s'abrège comme l'inclusion $]r, \infty[\subset x$. On a donc :

$$]r, \infty[\subset x \qquad \Longleftrightarrow \qquad \iota(r) \subset x \qquad \Longleftrightarrow \qquad x \leq_{\mathbf{R}} \iota(r) \ .$$

Mais on a aussi $r \in x$ et $r \notin \ ]r, \infty[\ = \iota(r)$, donc $\iota(r) \neq x$ et donc on a $x <_{\mathbf{R}} \iota(r)$. Ainsi on a montré l'inclusion

$$x \subset \{\, r \in \mathbf{Q} \mid \iota(r) >_{\mathbf{R}} x \,\} \ .$$

Pour montrer l'inclusion dans l'autre sens, on passe par l'absurde et on suppose qu'on a $r \in \mathbf{Q}$, $r \notin x$. Par (C2) on a l'implication

$$s \in x \qquad \Longrightarrow \qquad r < s \ ,$$

ce qui est équivalent à l'inclusion $x \subset \ ]r, \infty[\ = \iota(r)$. On a donc l'inégalité $\iota(r) \leq_{\mathbf{R}} x$, ce qui est la négation de $\iota(r) >_{\mathbf{R}} x$ [3.12.ii] (car $\leq_{\mathbf{R}}$ est une relation d'ordre total). Ainsi on a montré par l'absurde l'inclusion dans l'autre sens. CQFD

Preuve de [15.6]. Soit $m \in \mathbf{R}$ un minorant de A. Par définition de la relation d'ordre sur $\mathbf{R}$ on a donc

$$\forall a \in A : a \subset m \ . \tag{33.20}$$

On définit l'ensemble $z \subset \mathbf{Q}$ par

$$z = \bigcup_{a \in A} a \equiv \cup A$$

et on veut montrer que $z = \inf A$. Pour cela il faut d'abord montrer que z est bien une coupure.

Soit $a \in A$ arbitraire (il en existe car A n'est pas vide), alors par (33.20) et [5.1] on a les inclusions

$$a \subset z \subset m \ . \tag{33.21}$$

Il s'ensuit que z n'est pas vide car a n'est pas vide et que z n'est pas $\mathbf{Q}$ entier car M n'est pas $\mathbf{Q}$ entier. Autrement dit, z vérifie la condition (C1) d'une coupure.

Pour montrer la condition (C2) on prend $r \in z$ et $s > r$. Alors par l'axiome de la réunion (Z4) on a l'équivalence

$$r \in z \quad \Leftrightarrow \quad \exists a \in A : r \in a \ . \tag{33.22}$$

Par la condition (C2) pour la coupure a et le fait qu'on a $s > r$ on a donc

$$\exists a \in A : s \in a \ ,$$

ce qui équivaut (de nouveau par (Z4)) $s \in z$.

Finalement pour montrer la condition (C3) on prend $r \in z$ et on cherche $s \in z$ tel que $s < r$. Selon (33.22) il existe $a \in A$ tel que $r \in a$. Par (C3) pour la coupure a il existe donc $s \in a$ tel que $s < r$. Et donc (toujours par (Z4)) on a $s \in z$.

Une fois qu'on sait que z est une coupure de $\mathbf{Q}$, il nous reste à montrer que ce z vérifie les conditions (BI1) et (BI2). Par (33.21) on sait déjà qu'on a $z \leq_{\mathbf{R}} a$ pour tout $a \in A$ (car le choix de a dans (33.21) était arbitraire), ce qui donne (BI1). Soit donc $x \in \mathbf{R}$ un minorant de A :

$$\forall a \in A : x \leq_{\mathbf{R}} a \qquad \text{ce qui est équivalent à} \qquad \forall a \in A : a \subset x \ .$$

Par [5.1] on en déduit l'inclusion $z \equiv \cup A \subset x$, c'est-à-dire l'inégalité $x \leq_{\mathbf{R}} z$, ce qui montre qu'on a aussi (BI2). CQFD

Preuve de [15.7]. L'inégalité $x <_{\mathbf{R}} y$ se traduit comme la condition $y \subset x$ et $y \neq x$. Il existe donc $s \in x \setminus y$. Mais par (C3) x n'a pas de plus petit élément. Il existe donc $r \in x$ tel que $r < s$. Par [15.5] on a les implications

$$r \in x \;\Rightarrow\; x <_{\mathbf{R}} \iota(r) \qquad \text{et} \qquad s \notin y \;\Rightarrow\; y \geq_{\mathbf{R}} \iota(s) \;.$$

Avec [15.4] et $r < s$ on obtient donc les inégalités $x <_{\mathbf{R}} \iota(r) <_{\mathbf{R}} \iota(s) \leq_{\mathbf{R}} y$. La preuve s'achève avec l'invocation de la transitivité d'une relation d'ordre [3.11]. CQFD

Preuve de [15.8]. Soit $y \in \mathbf{R} \setminus C$ arbitraire (un tel y existe car par (C1') $\mathbf{R} \neq C$). Par (C2') y est un minorant de C qui est lui-même un ensemble non-vide, de nouveau par (C1'). Selon [15.6] on peut donc parler de la borne inférieure de C (vérifiant (BI1) et (BI2')) et de poser $z = \inf C \in \mathbf{R}$.

Pour montrer l'égalité $C = \{\, x \in \mathbf{R} \mid z <_{\mathbf{R}} x \,\}$ par double inclusion on commence avec le raisonnement

$$z <_{\mathbf{R}} x \quad \overset{\text{(BI2')}}{\Longrightarrow} \quad \exists c \in C : c <_{\mathbf{R}} x \quad \overset{\text{(C2')}}{\Longrightarrow} \quad x \in C \;,$$

ce qui montre l'inclusion $\{\, x \in \mathbf{R} \mid z <_{\mathbf{R}} x \,\} \subset C$. Et ensuite on fait le raisonnement

$$d \in C \overset{\text{(C3')}}{\Longrightarrow} \exists c \in C : c <_{\mathbf{R}} d \overset{\text{(BI1)}}{\Longrightarrow} z \leq_{\mathbf{R}} c <_{\mathbf{R}} d \implies d \in \{\, x \in \mathbf{R} \mid z <_{\mathbf{R}} x \,\} \;,$$

ce qui montre l'inclusion dans l'autre sens. CQFD

Preuve de [15.9]. Étant donné que ni x ni y est l'ensemble vide, il existe $r \in x$ et $s \in y$. Il s'ensuit que l'élément $t = r + s$ appartient à z donc z n'est pas vide. D'autre part, il existe $r' \in \mathbf{Q} \setminus x$ et $s' \in \mathbf{Q} \setminus y$. Pour montrer que $r' + s'$ n'appartient pas à z, on raisonne par l'absurde en supposant qu'il existe $r \in x$ et $s \in y$ tels qu'on a l'égalité

$$r' + s' = r + s \;.$$

Mais ceci est impossible, car par (C2) on doit avoir les inégalités strictes $r' < r$ et $s' < s$ ($r \in x$ et $r' \notin x$ et cætera) et donc par [14.25.i] on a aussi l'inégalité stricte $r' + s' < r + s$. Ainsi on a montré que z vérifie la condition (C1) d'une coupure.

Pour la condition (C2), prenons $r \in z$ et $s \in \mathbf{Q}$ tel que $r < s$. Par hypothèse il existe $t \in x$ et $u \in y$ tels que $r = t + u$. Par [14.25.i] on a donc aussi

$$u = r - t < s - t \;.$$

Mais y vérifie (C2), donc $s - t \in y$. Il s'ensuit qu'on a $s = t + (s - t) \in z$.

Finalement pour la condition (C3) prenons $r \in z$. Alors il existe $t \in x$ et $u \in y$ tels que $r = t + u$. Mais x vérifie (C3), donc il existe $t' \in x$ tel que $t' < t$. De nouveau par [14.25.i] on a $t' + u < t + u = r$ et $t' + u \in z$. CQFD

Preuve de [15.10]. Si on décortique les définitions de $+_{\mathbf{R}}$ et de ι, on s'aperçoit qu'il faut montrer l'égalité

$$]r+s,\infty[= \{t+u \mid t\in\,]r,\infty[\text{ et } u\in\,]s,\infty[\}\ ,$$

ce qu'on fera par double inclusion. Les conditions $t\in\,]r,\infty[$ et $u\in\,]s,\infty[$ sont équivalents à $r<t$ et $s<u$. Par [14.25.i] on a donc $r+s<t+u$, ce qui montre qu'on a l'inclusion $\supset$.

Pour l'inclusion dans l'autre sens, on prend $t\in\,]r+s,\infty[$, ce qui veut dire qu'on a $r+s<t$, et on veut montrer qu'il existe $r'\in\,]r,\infty[$ et $s'\in\,]s,\infty[$ tels que $t=r'+s'$. L'inégalité $r+s<t$ nous donne, par [14.25.i], l'inégalité

$$r=r+s-s<t-s\ .$$

Avec [14.26] on en déduit qu'il existe $r'\in\mathbf{Q}$ tel que

$$r<r'<t-s\ .$$

En appliquant [14.25.i] et [14.13] on obtient l'inégalité

$$s=r'+s-r'<t-s+s-r'=t-r'\ .$$

Il s'ensuit que ce r' et $s'=t-r'$ conviennent, ce qui achève la preuve de l'inclusion directe $\subset$. CQFD

Preuve de [15.11]. Par (C1) x n'est pas vide, donc il existe $s=-(-s)\in x$ [14.16], donc $-s$ ne peut pas appartenir à y, donc y n'est pas $\mathbf{Q}$ entier. Mais par (C1) on sait aussi qu'il existe $s\in\mathbf{Q}$ qui n'appartient pas à x : $s=-(-s)\notin x$, donc $-s$ appartient à y, donc y n'est pas vide. La conclusion est que y vérifie bien la condition (C1).

Pour (C2) on prend $r\in y$ et $t\in\mathbf{Q}$ tel que $r<t$. Par [14.25.i] on a donc l'inégalité $-t<-r\notin x$. Par (C2) on en déduit qu'on ne peut pas avoir $-t\in x$, donc $t\in y$.

Pour (C3) on prend $r\in y$ et on cherche $t\in y$ tel que $t<r$. On a donc $-r\notin x$ et on cherche $t\in\mathbf{Q}$ tel que $-t\notin x$ et $t<r$. Par [15.5] on a les équivalences

$$-r\notin x \qquad\Longleftrightarrow\qquad \iota(-r)\leq_{\mathbf{R}} x \qquad\Longleftrightarrow\qquad x\subset\,]-r,\infty[\ .$$

L'hypothèse $x\notin\iota[\mathbf{Q}]$ dit qu'on n'a pas l'égalité $x=\,]-r,\infty[$. Il s'ensuit qu'il existe $u\in\,]-r,\infty[$ tel que $u\notin x$. En posant $t=-u\Leftrightarrow u=-t$ [14.16] on a donc $-t>-r\Leftrightarrow t<r$ et $-t\notin x$ comme voulu. CQFD

Preuve de [15.12]. Par (C1) ni x ni $\mathbf{Q}\setminus x$ est vide, donc il existe $r_o\in x$ et $s_o\notin x$. Par (C2) on a l'inégalité stricte $s_o<r_o$. Mais $\mathbf{Q}$ est archimédien [14.27], donc il existe $n\in\mathbf{N}$ tel que $s_o+n\times t>r_o$. Par (C2) on a donc $s_o+n\times t\in x$. Il s'ensuit que l'ensemble $E\subset\mathbf{N}$ défini par

$$E=\{n\in\mathbf{N}\mid s_o+n\times t\in x\}$$

n'est pas vide. Par [8.17] E a un plus petit élément ; notons le n_o. Mais $0\notin E$ car $s_o+0\times r=s_o\notin x$, donc par [7.9] il existe $k\in\mathbf{N}$ tel que $n_o=S(k)=k+1$. L'élément $k\in\mathbf{N}$ n'appartient pas à E parce que n_o est le plus petit dans E et donc $s_o+k\times t\notin x$. Si on définit $r,s\in\mathbf{Q}$ par

$$r=s_o+n_o\times t=s_o+(k+1)\times t \qquad\text{et}\qquad s=s_o+k\times t\ ,$$

alors $r \in x$, $s \notin x$ et

$$r - s = (s_o + (k+1) \times t) - (s_o + k \times t) = t \ .$$

On a donc trouvé nos r et s voulus CQFD

Preuve de [15.13]. • (i) : Selon la définition les ensembles $x +_{\mathbf{R}} y$ et $y +_{\mathbf{R}} x$ sont donnés par

$$x +_{\mathbf{R}} y = \{\, r + s \mid r \in x, s \in y \,\}$$
$$y +_{\mathbf{R}} x = \{\, s + r \mid s \in y, r \in x \,\} \ .$$

Étant donné que l'addition dans $\mathbf{Q}$ est commutative, l'égalité $x +_{\mathbf{R}} y = y +_{\mathbf{R}} x$ est évidente.

• (ii) : Si on épluche bien la définition, on trouve que les ensembles $(x +_{\mathbf{R}} y) +_{\mathbf{R}} z$ et $x +_{\mathbf{R}} (y +_{\mathbf{R}} z)$ sont donnés par

$$(x +_{\mathbf{R}} y) +_{\mathbf{R}} z = \{\, r + (s + t) \mid r \in x, s \in y, t \in z \,\}$$
$$x +_{\mathbf{R}} (y +_{\mathbf{R}} z) = \{\, (r + s) + t \mid r \in x, s \in y, t \in z \,\} \ .$$

L'addition dans $\mathbf{Q}$ étant associative, l'égalité $(x +_{\mathbf{R}} y) +_{\mathbf{R}} z = x +_{\mathbf{R}} (y +_{\mathbf{R}} z)$ en découle immédiatement.

• (iii) : L'ensemble $x + \iota(0)$ est donné par

$$x + \iota(0) = \{\, r + s \mid r \in x, s \in \,]0, \infty[\, \} = \{\, r + s \mid r \in x, s \in \mathbf{Q}, s > 0 \,\} \ .$$

On montrera l'égalité $x + \iota(0) = x$ par double inclusion et on commence avec l'inclusion directe $\subset$:

$$(33.23) \qquad t \in x + \iota(0) \quad \Rightarrow \quad \exists r \in x \ \ \exists s \in \mathbf{Q} : s > 0 \text{ et } t = r + s \overset{[14.25.i]}{\Rightarrow} \quad r \in x \text{ et } t > r \quad \overset{(C2)}{\Rightarrow} \quad t \in x \ .$$

Pour l'inclusion dans l'autre sens on raisonne comme suit :

$$(33.24) \qquad r \in x \quad \overset{(C3)}{\Rightarrow} \quad \exists s \in x : s < r \quad \overset{[14.25.i]}{\Rightarrow} \quad s \in x \text{ et } 0 < r - s \quad \Rightarrow \quad r = s + (r - s) \in x +_{\mathbf{R}} \iota(0) \ .$$

• (iv) : S'il existe $r \in \mathbf{Q}$ tel que $x = \iota(r)$, alors on pose $y = \iota(-r)$ et on calcule :

$$x +_{\mathbf{R}} y = \iota(r) +_{\mathbf{R}} \iota(-r) \overset{[15.10]}{=} \iota(r + (-r)) \overset{[14.16]}{=} \iota(0) \ .$$

S'il n'existe pas un tel $r \in \mathbf{Q}$, alors on définit y comme

$$y = \{\, r \in \mathbf{Q} \mid -r \notin x \,\} = \{\, -s \mid s \in \mathbf{Q} \setminus x \,\} \ ,$$

ce qui est une coupure par [15.11]. Il s'ensuit que $x +_{\mathbf{R}} y$ est donné par

$$x +_{\mathbf{R}} y = \{\, r - s \mid r \in x, s \in \mathbf{Q} \setminus x \,\} \ .$$

Pour montrer l'égalité $x +_{\mathbf{R}} y = \iota(0) = \,]0, \infty[$ par double inclusion, on commence avec le raisonnement

$$r \in x \text{ et } s \in \mathbf{Q} \setminus x \quad \overset{(C2)}{\Rightarrow} \quad s < r \quad \overset{[14.25.i]}{\Rightarrow} \quad 0 < r - s \ ,$$

ce qui montre l'inclusion $x +_{\mathbf{R}} y \subset \,]0, \infty[$. Pour l'inclusion dans l'autre sens on prend $t \in \mathbf{Q}$ vérifiant $t > 0$. Par [15.12] il existe $r \in x$ et $s \notin x$ tels que $t = r - s \equiv r + (-s)$, ce qui veut dire qu'on a $t \in x +_{\mathbf{R}} y$. CQFD

Preuve de [15.16]. Par définition de $\leq_{\mathbf{R}}$ et $+_{\mathbf{R}}$ il faut montrer l'implication

$$y \subset x \qquad \Longrightarrow \qquad \{\, s+t \mid s \in y \text{ et } t \in z \,\} \subset \{\, r+u \mid r \in x \text{ et } u \in z \,\} \ .$$

Pour cela on prend $s+t \in y +_{\mathbf{R}} z$, c'est-à-dire $s \in y$ et $t \in z$ et on constate que, par l'inclusion $y \subset x$, on a $s \in x$ et donc $s+t \in x +_{\mathbf{R}} z$. CQFD

Preuve de [15.18]. Les conditions $x, y \geq_{\mathbf{R}} \iota(0)$ sont équivalentes aux inclusions

$$x \subset \,]0,\infty[\qquad \text{et} \qquad y \subset \,]0,\infty[\ .$$

Pour $r \in x$ et $s \in y$ on a donc par [14.25.iv] l'inégalité $r \times s > 0$. Ceci implique qu'on a l'inclusion $z \subset \,]0,\infty[$ et donc en particulier $z \neq \mathbf{Q}$ car $0 \in \mathbf{Q} \setminus z$. D'autre part, x et y ne sont pas vides, donc z n'est pas vide non plus. L'ensemble z vérifie donc la condition (C1).

Pour la condition (C2) on prend $t \in z$ et $u \in \mathbf{Q}$ tel que $t < u$. Par définition il existe donc $r \in x$ et $s \in y$ tels que $t = r \times s$. Mais $s \in y$ implique $s > 0$, donc par [14.25.v] $s^{-1} > 0$. Avec [14.25.iv] on en déduit l'inégalité

$$u \times s^{-1} > t \times s^{-1} = r \ .$$

Par (C2) on a donc $u \times s^{-1} \in x$ et donc on a $u = (u \times s^{-1}) \times s \in z$ comme voulu.

Finalement pour a condition (C3) on prend $r \in z$ et on cherche $s \in z$ tel que $s < r$. Par définition il existe $t \in x$ et $u \in y$ tels que $r = t \times u$. Par (C3) il existe donc $t' \in x$ et $u' \in y$ tels que $t' < t$ et $u' < u$. Mais on a aussi $t' > 0$ et $u' > 0$. L'application de [14.25.i/iv] nous donne alors les inégalités

$$0 < t' \times u' < t \times u \ .$$

Il s'ensuit que $s = t' \times u'$ est l'élément recherché.

Une fois qu'on sait que z est une coupure, on constate que l'inclusion $z \subset \,]0,\infty[$ montrée ci-dessus équivaut l'inégalité $z \geq_{\mathbf{R}} \iota(0)$ et donc $z \in \mathbf{R}_+$. CQFD

Preuve de [15.20]. • On considère d'abord la cas $r, s \geq 0$ où il faut (donc) montrer l'égalité

$$\big\{\, u \times v \mid u \in \,]r,\infty[\,, v \in \,]s,\infty[\,\big\} = \,]r \times s,\infty[\ .$$

Pour l'inclusion $\subset$ on constate que $u \in \,]r,\infty[\,, v \in \,]s,\infty[$ et les hypothèses $r, s \geq 0$ nous donnent les inégalités $0 \leq r < u$ et $0 \leq s < v$, et donc par [14.25.iii/iv] on obtient

$$r \times s \leq u \times s < u \times v \ .$$

Ainsi on a montré $u \times v \in \,]r \times s,\infty[$.

Pour l'inclusion réciproque, on prend $t > r \times s$ et on cherche $u > r$ et $v > s$ tels que $t = u \times v$. Si r et s sont nuls, alors $u = t$ et $v = 1$ conviennent. Dans le cas contraire au moins un des deux r ou s est non-nul. Supposons qu'on a $s \neq 0$ et donc $s > 0$. Par [14.25.iv/v] on déduit de $r \times s < t$ l'inégalité

$$r < t \times s^{-1} \ .$$

Avec [14.26] on en déduit qu'il existe $u \in \mathbf{Q}$ tel que

$$0 \leq r < u < t \times s^{-1} \ .$$

En appliquant [14.25.iv] et [14.17] on obtient l'inégalité

$$s = u \times s \times u^{-1} < t \times s^{-1} \times s \times u^{-1} = t \times u^{-1} \ .$$

Il s'ensuit que ce u et $v = t \times u^{-1}$ conviennent. Ainsi on montré l'égalité $\iota(r) \times_{\mathbf{R}} \iota(s) = \iota(r \times s)$ au cas où r et s sont positifs.

• Une fois qu'on a établit le résultat pour r et s positifs, il faut considérer le cas général. Mais le cas général se déduit directement du cas positif en utilisant la compatibilité [15.15]. Prenons par exemple le cas $r = -(-r) < 0$ et $s \geq 0$. Alors $-r > 0$ par [14.25.ii], donc par [15.4] $\iota(-r) >_{\mathbf{R}} \iota(0)$ et $\iota(r) <_{\mathbf{R}} \iota(0)$. On peut donc faire le calcul

$$\begin{array}{rcl} \iota(r) \times_{\mathbf{R}} \iota(s) & \equiv & -_{\mathbf{R}} \big((-_{\mathbf{R}} \iota(r)) \times_{\mathbf{R}} \iota(s) \big) \overset{[15.15]}{=} -_{\mathbf{R}} \big(\iota(-r) \times_{\mathbf{R}} \iota(s) \big) \\ & \overset{-r,\, s \geq 0}{=} & -_{\mathbf{R}} \iota((-r) \times s) \overset{[15.15]}{=} \iota\big(-\big((-r) \times s \big) \big) \overset{[14.16]}{=} \iota(r \times s) \ . \end{array}$$

Les deux autres cas ($r \geq 0$, $s < 0$ et $r, s < 0$) sont similaires et laissés aux bons soins du lecteur. *CQFD*

Preuve de [15.21]. L'hypothèse $x >_{\mathbf{R}} \iota(0) = \ ]0, \infty[$ équivaut $x \subset \ ]0, \infty[\ = \mathbf{Q}_+^*$ et $x \neq \ ]0, \infty[$. Donc il existe $s \in \mathbf{Q}_+^* \setminus x$ et donc y n'est pas vide. Mais la condition $s > 0$ implique aussi $s^{-1} > 0$ [14.25.v], ce qui entraîne l'inclusion $y \subset \ ]0, \infty[$. Il s'ensuit que y n'est pas $\mathbf{Q}$ entier. L'ensemble y vérifie donc la condition (C1).

Pour la condition (C2), prenons $t \in y$ et $u > t$. Il existe donc $s \notin x$ tel que $s > 0$ et $t = s^{-1}$. On peut donc faire le raisonnement

$$0 < s^{-1} = t < u \quad \overset{[14.25.\text{iv/v}]}{\Rightarrow} \quad 0 < u^{-1} < s \ .$$

Par (C2) on doit avoir $u^{-1} \notin x$ (car $s \notin x$). Par définition de y on a donc $u \in y$, ce qui montre que y vérifie (C2).

Pour la condition (C3) on reprend $t \in y$ et on veut montrer l'existence d'un $u \in y$ tel que $u < t$. Par définition de y il existe $s \notin x$ tel que $s > 0$ et $t = s^{-1}$. Par [15.5] et [15.3] on a donc $\iota(s) \leq_{\mathbf{R}} x$, c'est-à-dire l'inclusion $x \subset \ ]s, \infty[$. Mais par hypothèse on ne peut pas avoir égalité car x n'appartient pas à $\iota[\mathbf{Q}]$. Il s'ensuit qu'il existe $v \in \ ]s, \infty[\setminus x$. Autrement dit, v vérifie $0 < s < v$ et $v \notin x$. Par [14.25.iv/v] on a donc $u = v^{-1} \in y$ et $u = v^{-1} < s^{-1} = t$.

Une fois qu'on sait que y est une coupure, on constate que l'inclusion $y \subset \ ]0, \infty[$ vaut l'inégalité $y \geq_{\mathbf{R}} \iota(0)$. *CQFD*

Preuve de [15.22]. • (i) : Pour $x, y \in \mathbf{R}_+$ on peut faire le calcul

$$\begin{array}{rcl} x \times_{\mathbf{R}} y = x \times'_{\mathbf{R}_+} y & = & \{ r \times s \mid r \in x, s \in y \} \\ & \overset{[14.17.\text{i}]}{=} & \{ s \times r \mid s \in y, r \in x \} = y \times_{\mathbf{R}} x \ . \end{array} \tag{33.25}$$

Les trois autres cas s'en déduisent facilement. Par exemple pour $x \in \mathbf{R}_+$ et $y <_{\mathbf{R}} \iota(0)$ on a

$$x \times_{\mathbf{R}} y \overset{(15.19)}{=} -_{\mathbf{R}} (x \times_{\mathbf{R}} (-_{\mathbf{R}} y)) \overset{(33.25)}{=} -_{\mathbf{R}} \big((-_{\mathbf{R}} y) \times_{\mathbf{R}} x \big) \overset{(15.19)}{=} y \times_{\mathbf{R}} x \ .$$

• (ii) : Pour $x,y,z\in\mathbf{R}_+$ on peut faire le calcul

$$\begin{aligned} x\times_{\mathbf{R}}(y\times_{\mathbf{R}}z) &= x\times'_{\mathbf{R}_+}(y\times'_{\mathbf{R}_+}z)=x\times'_{\mathbf{R}_+}\big(\{s\times t\mid s\in y,t\in z\}\big)\\ &= \{r\times(s\times t)\mid r\in x,s\in y,t\in z\}\\ &\overset{[14.17.\text{ii}]}{=} \{(r\times s)\times t\mid r\in x,s\in y,t\in z\}=(x\times_{\mathbf{R}}y)\times_{\mathbf{R}}z\ , \end{aligned}\tag{33.26}$$

où on utilise le fait que la multiplication de deux réels positifs donne un réel positif [15.18].

Les sept autres cas s'en déduisent facilement en utilisant [15.18], [15.17.ii] et (15.19). Par exemple pour $x,z\in\mathbf{R}_+$ et $y<_{\mathbf{R}}\iota(0)$ on a

$$\begin{aligned} x\times_{\mathbf{R}}(y\times_{\mathbf{R}}z) &= x\times_{\mathbf{R}}\big(-_{\mathbf{R}}\big((-_{\mathbf{R}}y)\times_{\mathbf{R}}z\big)\big)=-_{\mathbf{R}}\big(x\times_{\mathbf{R}}\big((-_{\mathbf{R}}y)\times_{\mathbf{R}}z\big)\big)\\ &\overset{(33.26)}{=} -_{\mathbf{R}}\big(\big(x\times_{\mathbf{R}}(-_{\mathbf{R}}y)\big)\times_{\mathbf{R}}z\big)\\ &= \big(-_{\mathbf{R}}\big(x\times_{\mathbf{R}}(-_{\mathbf{R}}y)\big)\big)\times_{\mathbf{R}}z=(x\times_{\mathbf{R}}y)\times_{\mathbf{R}}z \end{aligned}$$

et pour $x,z<_{\mathbf{R}}\iota(0)$ et $y\in\mathbf{R}_+$ on a, avec les mêmes arguments

$$\begin{aligned} x\times_{\mathbf{R}}(y\times_{\mathbf{R}}z) &= x\times_{\mathbf{R}}\big(-_{\mathbf{R}}\big(y\times_{\mathbf{R}}(-_{\mathbf{R}}z)\big)\big)=(-_{\mathbf{R}}x)\times_{\mathbf{R}}\big(y\times_{\mathbf{R}}(-_{\mathbf{R}}z)\big)\\ &\overset{(33.26)}{=} \big((-_{\mathbf{R}}x)\times_{\mathbf{R}}y\big)\times_{\mathbf{R}}(-_{\mathbf{R}}z)\\ &= \big(-_{\mathbf{R}}\big((-_{\mathbf{R}}x)\times_{\mathbf{R}}y\big)\big)\times_{\mathbf{R}}z=(x\times_{\mathbf{R}}y)\times_{\mathbf{R}}z\ . \end{aligned}$$

• (iii) : On commence à considérer le cas où x, y et z sont positifs, au quel cas $y+_{\mathbf{R}}z$ est aussi positif [15.16] :

$$\iota(0)\le_{\mathbf{R}}y,z\qquad\Longrightarrow\qquad \iota(0)\le_{\mathbf{R}}z=\iota(0)+_{\mathbf{R}}z\le_{\mathbf{R}}y+_{\mathbf{R}}z\ .$$

La définition de la multiplication [15.18] nous donne alors les égalités

$$\begin{aligned} x\times_{\mathbf{R}}(y+_{\mathbf{R}}z)&=x\times_{\mathbf{R}}\{t+u\mid t\in y,u\in z\}\\ &=\{r\times(t+u)\mid r\in x,t\in y,u\in z\} \end{aligned}$$

et

$$\begin{aligned} x\times_{\mathbf{R}}y+_{\mathbf{R}}x\times_{\mathbf{R}}z&=\{r\times t\mid r\in x,t\in y\}+_{\mathbf{R}}\{s\times u\mid s\in x,u\in z\}\\ &=\{r\times t+s\times u\mid r,s\in x,t\in y,u\in z\}\ . \end{aligned}$$

L'égalité de ces deux ensembles se montre par double inclusion. L'inclusion dans un sens est quasi-immédiate :

$$\begin{array}{c} r\times(t+u)\in x\times_{\mathbf{R}}(y+_{\mathbf{R}}z)\\ \Downarrow\\ r\times(t+u)=r\times t+r\times u\in x\times_{\mathbf{R}}y+_{\mathbf{R}}x\times_{\mathbf{R}}z\ . \end{array}$$

Pour l'inclusion dans l'autre sens on note d'abord que la positivité des réels x, y et z entraîne la positivité des éléments de ces ensembles :

$$x\ge_{\mathbf{R}}\iota(0)\qquad\Longleftrightarrow\qquad x\subset\,]0,\infty[\ .$$

Ensuite on prend $r\times t+s\times u\in x\times_{\mathbf{R}}y+_{\mathbf{R}}x\times_{\mathbf{R}}z$. Pour monter que ce rationnel appartient à $x\times_{\mathbf{R}}(y+_{\mathbf{R}}z)$ on distingue deux cas : $r\ge s$ et $r<s$. Dans le premier cas on raisonne comme suit :

$$\begin{array}{c} r,s,t>0\text{ et }r\ge s\overset{[14.25.\text{iii}]}{\Longrightarrow} r\times t\ge s\times t\\ \overset{[14.23.\text{i}]}{\Longrightarrow} r\times t+s\times u\ge s\times t+s\times u=s\times(t+u)\in x\times_{\mathbf{R}}(y+_{\mathbf{R}}z)\ . \end{array}$$

Par (C2) on a donc aussi $r \times t + s \times u \in x \times_{\mathbf{R}} (y +_{\mathbf{R}} z)$. Pour le deuxième cas on échange les rôles de r et s :

$$\begin{array}{l} r, s, u > 0 \text{ et } s > r \quad \overset{[14.25.\text{iv}]}{\Longrightarrow} \quad s \times u > r \times u \\ \overset{[14.25.\text{i}]}{\Longrightarrow} \quad r \times t + s \times u > r \times t + r \times u = r \times (t + u) \in x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) \ . \end{array}$$

Et de nouveau par (C2) on en déduit $r \times t + s \times u \in x \times_{\mathbf{R}} (y +_{\mathbf{R}} z)$.

Après le cas où tous les trois réels sont positifs on considère le cas $x <_{\mathbf{R}} \iota(0)$ et $y, z \geq_{\mathbf{R}} \iota(0)$ (et donc $y +_{\mathbf{R}} z \geq_{\mathbf{R}} \iota(0)$). Dans ce cas $-_{\mathbf{R}} x$ est positif et selon le premier cas on a donc l'égalité

$$(-_{\mathbf{R}} x) \times_{\mathbf{R}} (y +_{\mathbf{R}} z) = (-_{\mathbf{R}} x) \times_{\mathbf{R}} y +_{\mathbf{R}} (-_{\mathbf{R}} x) \times_{\mathbf{R}} z \ .$$

La définition (15.19.ii) et (??) impliquent qu'on peut ré-écrire cette égalité comme

$$-_{\mathbf{R}} (x \times_{\mathbf{R}} (y +_{\mathbf{R}} z)) = -_{\mathbf{R}} (x \times_{\mathbf{R}} y) +_{\mathbf{R}} (-_{\mathbf{R}} (x \times_{\mathbf{R}} z)) \ .$$

En ajoutant des deux côtés la quantité $x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) +_{\mathbf{R}} x \times_{\mathbf{R}} y +_{\mathbf{R}} x \times_{\mathbf{R}} z$ et en utilisant les propriétés de l'addition $+_{\mathbf{R}}$ [15.13], on obtient l'égalité recherchée

$$x \times_{\mathbf{R}} y +_{\mathbf{R}} x \times_{\mathbf{R}} z = x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) \ .$$

Une fois qu'on sait que l'égalité est vraie pour tout x et pour y et z positifs, on considère les autres cas possibles selon les signes de y, z *et* $y +_{\mathbf{R}} z$. Le premier cas qu'on peut considérer est le cas $y <_{\mathbf{R}} \iota(0)$, $z \geq_{\mathbf{R}} \iota(0)$ et $y +_{\mathbf{R}} z \geq_{\mathbf{R}} \iota(0)$. Dans ce cas les deux réels $y' = y +_{\mathbf{R}} z$ et $z' = -_{\mathbf{R}} y$ sont positifs et donc, comme on vient de montrer, on a l'égalité

$$x \times_{\mathbf{R}} y' +_{\mathbf{R}} x \times_{\mathbf{R}} y' = x \times_{\mathbf{R}} (y' +_{\mathbf{R}} z') \ ,$$

ce qui se traduit comme

$$x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) +_{\mathbf{R}} x \times_{\mathbf{R}} (-_{\mathbf{R}} y) = x \times_{\mathbf{R}} ((y +_{\mathbf{R}} z) +_{\mathbf{R}} (-_{\mathbf{R}} y)) \overset{[15.13]}{=} x \times_{\mathbf{R}} z \ .$$

En ajoutant $x \times_{\mathbf{R}} y$ des deux côtés on obtient

$$\begin{array}{rl} x \times_{\mathbf{R}} z +_{\mathbf{R}} x \times_{\mathbf{R}} y & = \quad x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) +_{\mathbf{R}} x \times_{\mathbf{R}} (-_{\mathbf{R}} y) +_{\mathbf{R}} x \times_{\mathbf{R}} y \\ & \overset{(15.19.\text{iii/iv})}{=} \quad x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) +_{\mathbf{R}} \iota(0) \\ & \overset{[15.13]}{=} \quad x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) \ , \end{array}$$

ce qui est l'égalité voulue.

Les quatre autres cas se démontrent de la même façon. Par exemple, dans le cas $y, z <_{\mathbf{R}} \iota(0)$ on constate que $-_{\mathbf{R}} y$ et $-_{\mathbf{R}} z$ sont positifs et qu'on a donc l'égalité

$$x \times_{\mathbf{R}} ((-_{\mathbf{R}} y) +_{\mathbf{R}} (-_{\mathbf{R}} z)) = x \times_{\mathbf{R}} (-_{\mathbf{R}} y) +_{\mathbf{R}} x \times_{\mathbf{R}} (-_{\mathbf{R}} z) \ .$$

Par [15.13] on a l'égalité $(-_{\mathbf{R}} y) +_{\mathbf{R}} (-_{\mathbf{R}} z) = -_{\mathbf{R}} (y +_{\mathbf{R}} z)$ et ensuite on ajoute $x \times_{\mathbf{R}} (y +_{\mathbf{R}} z) +_{\mathbf{R}} x \times_{\mathbf{R}} y +_{\mathbf{R}} x \times_{\mathbf{R}} z$ des deux côtés et on invoque (15.19) pour obtenir l'égalité voulue. Les trois cas restants sont laissés aux bons soins du lecteur.

• (iv) : Pour $x \geq_{\mathbf{R}} \iota(0)$ on a l'inclusion $x \subset \ ]0, \infty[$ et l'égalité

$$x \times_{\mathbf{R}} \iota(1) = \{\, r \times s \mid r \in x, s > 1 \,\} \ .$$

On raisonne alors comme suit

$$r \in x \text{ et } s > 1 \quad \Rightarrow \quad r > 0 \text{ et } s > 1 \quad \overset{[14.25.\text{iv}]}{\Rightarrow} \quad r \times s > r \times 1 = r \quad \overset{(\text{C2})}{\Rightarrow} \quad r \times s \in x \ ,$$

ce qui nous donne l'inclusion

$$x \times_{\mathbf{R}} \iota(1) \subset x \ .$$

Pour montrer l'inclusions dans l'autre sens, on prend $t \in x$ et on cherche $r \in x$ et $s > 1$ tel que $r \times s = t$. Par (C3) il existe $r \in x$ tel que $r < t$. Par l'inclusion

$x \subset \,]0,\infty[$ on a $r > 0$ et par [14.25.iv/v] on a donc l'inégalité $1 = r^{-1} \times r < r^{-1} \times t$. Le rationnel $s = r^{-1} \times t$ vérifie donc $s > 1$ et $r \times s = t$, ce qui termine la preuve de l'inclusion dans l'autre sens. Pour $x \geq_{\mathbf{R}} \iota(0)$ on a donc montré l'égalité voulue.

Pour $x <_{\mathbf{R}} \iota(0)$ on fait le calcul

$$x \times_{\mathbf{R}} \iota(1) = -_{\mathbf{R}} \big((-_{\mathbf{R}}\, x) \times_{\mathbf{R}} \iota(1) \big) \overset{\text{cas préc.}}{=} -_{\mathbf{R}} (-_{\mathbf{R}}\, x) \overset{(??)}{=} x \ .$$

• (v) : Pour $x = \iota(r) \in \iota[\mathbf{Q}^*]$ on pose $y = \iota(r^{-1})$ et on vérifie la propriété :

$$x \times_{\mathbf{R}} y = \iota(r) \times_{\mathbf{R}} \iota(r^{-1}) \overset{[15.20]}{=} \iota(r \times r^{-1}) \overset{[14.21]}{=} \iota(1) \ .$$

Pour $x >_{\mathbf{R}} \iota(0)$ et $x \notin \iota[\mathbf{Q}]$ on définit y comme

$$y = \{\, s^{-1} \mid s \in \mathbf{Q}_+^* \setminus x \,\} \ ,$$

ce qui est une coupure vérifiant $y \geq_{\mathbf{R}} \iota(0)$ selon [15.21]. On a donc

$$x \times_{\mathbf{R}} y = \{\, r \times s^{-1} \mid r \in x \,,\ s \in \mathbf{Q}_+^* \setminus x \,\} \overset{[15.18]}{\geq_{\mathbf{R}}} \iota(0) \ .$$

La preuve que ce produit est égal à $\iota(1) = \,]1,\infty[$ se fait par double inclusion. D'abord, si on avait $r \times s^{-1} \leq 1$ avec $r \in x$, $s \in \mathbf{Q} \setminus x$ et $s > 0$, alors par [14.25.iii] on aurait $r \leq s$. Mais $r \in x$ et $s \notin x$, ce qui donne une contradiction avec (C2). Donc on doit avoir l'inclusion

$$\{\, r \times s^{-1} \mid r \in x \,,\ s \notin x \,,\ s > 0 \,\} \subset \,]1,\infty[\ .$$

Pour l'inclusions dans l'autre sens, on prend un $t > 1$ et on veut montrer $t \in x \times_{\mathbf{R}} y$. L'inégalité stricte $x >_{\mathbf{R}} \iota(0)$ équivaut l'inclusion $x \subset \,]0,\infty[= \mathbf{Q}_+^*$ et $x \neq \,]0,\infty[$. Il existe donc $s_o > 0$ tel que $s_o \notin x$. Par [14.25.i] on a $t - 1 > 0$ et ensuite par [14.25.iv] $(t-1) \times s_o > 0$. Avec [15.12] il s'ensuit qu'il existe $r' \in x$ et $s' \in \mathbf{Q} \setminus x$ tel que

$$r' - s' = (t-1) \times s_o \ .$$

On définit maintenant $r, s \in \mathbf{Q}$ par

$$s = \max(s_o, s') = \begin{cases} s_o & s' < s_o \\ s' & s' \geq s_o \end{cases} \qquad \text{et} \qquad r = r' - s' + s \ .$$

Alors $s \notin x$ car ni s_o ni s' appartient à x, et, par (C2), $r \in x$ car $s - s' \geq 0$ et $r' \in x$. En plus on a l'inégalité $s \geq s_o > 0$ et donc par [14.25.iii/iv/v] on a $0 < s_o \times s^{-1} < 1$. Maintenant on fait le raisonnement

$$\begin{aligned} & r - s = r' - s' = (t-1) \times s_o \\ \Longrightarrow \qquad & s^{-1} \times r - 1 = (t-1) \times s_o \times s^{-1} \leq t - 1 \\ \Longrightarrow \qquad & s^{-1} \times r \leq t \end{aligned}$$

Par définition on a $r \times s^{-1} \in x \times_{\mathbf{R}} y$ et donc par (C2) on a $t \in x \times_{\mathbf{R}} y$. On a donc montré l'inclusion dans l'autre sens, ce qui termine la preuve de l'égalité $x \times_{\mathbf{R}} y = \iota(1)$ dans le cas $x >_{\mathbf{R}} \iota(0)$.

Pour le cas $x <_{\mathbf{R}} \iota(0)$ on sait que $-_{\mathbf{R}}\, x >_{\mathbf{R}} \iota(0)$ et on définit $y \in \mathbf{R}$ comme $y = -_{\mathbf{R}}\, z$ avec

$$z = \{\, s^{-1} \mid s \in \mathbf{Q}_+^* \setminus (-_{\mathbf{R}}\, x) \,\} \ .$$

Selon l'argument précédent, z est une réel vérifiant $z \geq_{\mathbf{R}} \iota(0)$ et $(-_{\mathbf{R}}\, x) \times_{\mathbf{R}} z = \iota(1)$. Par définition de la multiplication on a donc

$$x \times_{\mathbf{R}} y \overset{(15.19.\text{iv})}{=} (-_{\mathbf{R}}\, x) \times_{\mathbf{R}} (-_{\mathbf{R}}\, y) = (-_{\mathbf{R}}\, x) \times_{\mathbf{R}} z = \iota(1) \ . \qquad \boxed{CQFD}$$

Preuve de [15.28]. L'inégalité stricte $x >_{\mathbf{R}} \iota(0)$ équivaut $x \subset \,]0,\infty[$ et $x \neq \,]0,\infty[$. Donc il existe $r \in \mathbf{Q}_+^* \setminus x$. L'ensemble y n'étant pas vide, il existe $s \in y$. Par [15.5] on a donc les inégalités

$$\iota(0) <_{\mathbf{R}} \iota(r) \leq_{\mathbf{R}} x \qquad \text{et} \qquad \iota(0) \leq_{\mathbf{R}} y <_{\mathbf{R}} \iota(s) \ . \tag{33.27}$$

Il s'ensuit (avec [15.4], mais on peut aussi le monter autrement) qu'on doit avoir $s > 0$. Par [14.27] il existe $k \in \mathbf{N}$ tel que $k \times r > s$. Par [15.4], [15.27.v] et (33.27) on a donc

$$\iota(k) \ \times_{\mathbf{R}} \ x \geq_{\mathbf{R}} \iota(k) \ \times_{\mathbf{R}} \ \iota(r) = \iota(k \times r) >_{\mathbf{R}} \iota(s) >_{\mathbf{R}} y \ . \qquad \boxed{CQFD}$$

Les preuves de §16

Preuve de [16.4]. On définit $n = m-k$, on fixe k et on fait la preuve par récurrence sur n. Pour $n = 0$ il faut montrer l'implication

$$t(k) \leq u(k) \quad \Longrightarrow \quad \sum_{i=k}^{k} t(i) \leq \sum_{i=k}^{k} u(i) \ .$$

Mais par la définition (16.3) on a $\sum_{i=k}^{k} t(i) = t(k)$ et $\sum_{i=k}^{k} u(i) = u(k)$. L'implication est donc vraie pour $n = 0$.

Supposons donc qu'elle soit vraie pour n et regardons l'implication pour $n+1$:

$$\Big(\ \forall i \in \mathbf{N} : k \leq i \leq k+n+1 \Rightarrow t(i) \leq u(i) \ \Big) \quad \Longrightarrow \quad \sum_{i=k}^{k+n+1} t(i) \leq \sum_{i=k}^{k+n+1} u(i) \ .$$

Mais si on a

$$\forall i \in \mathbf{N} : k \leq i \leq k+n+1 \Rightarrow t(i) \leq u(i) \ , \tag{33.28}$$

on a en particulier

$$\forall i \in \mathbf{N} : k \leq i \leq k+n \Rightarrow t(i) \leq u(i) \ .$$

Par hypothèse de récurrence on a donc l'inégalité $\sum_{i=k}^{k+n} t(i) \leq \sum_{i=k}^{k+n} u(i)$. Par la définition (16.3) on a les égalités

$$\sum_{i=k}^{k+n+1} t(i) = \left(\sum_{i=k}^{k+n} t(i) \right) + t(k+n+1) \quad \text{et} \tag{33.29}$$

$$\sum_{i=k}^{k+n+1} u(i) = \left(\sum_{i=k}^{k+n} u(i) \right) + u(k+n+1) \ .$$

Mais dans l'hypothèse (33.28) on a aussi l'inégalité $t(k+n+1) \leq u(k+n+1)$. Par [15.16] on obtient l'inégalité voulue. Ainsi on a démontré que si l'implication est vraie pour n, elle est vraie aussi pour $n+1$, ce qui termine la preuve par récurrence. CQFD

Preuve de [16.7]. On réécrit la formule comme

$$\left(\sum_{i=k}^{k+j} t(i) \right) + \left(\sum_{i=k+j+1}^{k+j+1+\ell} t(i) \right) = \sum_{i=k}^{k+j+1+\ell} t(i)$$

avec $j = m - k \in \mathbf{N}$ et $\ell = n - m - 1 \in \mathbf{N}$ et on la démontre par récurrence sur ℓ en fixant $k, j \in \mathbf{N}$. Pour $\ell = 0$ la formule à montrer se réduit à

$$\left(\sum_{i=k}^{k+j} t(i) \right) + \left(\sum_{i=k+j+1}^{k+j+1} t(i) \right) = \sum_{i=k}^{k+j+1} t(i) \ .$$

Mais par définition on a $\sum_{i=k+j+1}^{k+j+1} t(i) = t(k+j+1)$ et on retrouve la formule de récurrence pour $\sum_{i=k}^{k+j+1} t(i)$. Pour $\ell = 0$ la formule est donc vraie.

Supposons qu'elle est vraie pour ℓ et faisons le calcul

$$\begin{aligned}
&\left(\sum_{i=k}^{k+j} t(i)\right) + \left(\sum_{i=k+j+1}^{k+j+1+\ell+1} t(i)\right) \\
&\overset{(16.3)}{=} \left(\sum_{i=k}^{k+j} t(i)\right) + \left(\left(\sum_{i=k+j+1}^{k+j+1+\ell} t(i)\right) + t(k+j+1+\ell+1)\right) \\
&\overset{\text{ass. de } +}{=} \left(\left(\sum_{i=k}^{k+j} t(i)\right) + \left(\sum_{i=k+j+1}^{k+j+1+\ell} t(i)\right)\right) + t(k+j+1+\ell+1) \\
&\overset{\text{hyp. de réc.}}{=} \left(\sum_{i=k}^{k+j+1+\ell} t(i)\right) + t(k+j+1+\ell+1) \\
&\overset{(16.3)}{=} \sum_{i=k}^{k+j+1+\ell+1} t(i) \ .
\end{aligned}$$

Ce calcul montre que la formule est vrai aussi pour $\ell+1$, ce qui termine la preuve par récurrence. CQFD

Preuve de [16.8]. On réécrit la formule avec $n = m - k$ sous la forme

$$\sum_{i=k}^{k+n} \frac{b-1}{b^i} = \frac{b^{n+1}-1}{b^{k+n}} \ ,$$

qu'on démontre par récurrence sur n. Pour $n = 0$ on a par définition

$$\sum_{i=k}^{k+0} \frac{b-1}{b^i} = \frac{b-1}{b^k} = \frac{b^{0+1}-1}{b^k} \ ,$$

ce qui montre que la formule est vraie pour $n = 0$. Et si elle est vraie pour n, alors on fait le calcul

$$\begin{aligned}
\sum_{i=k}^{k+n+1} \frac{b-1}{b^i} &= \sum_{i=k}^{k+n} \frac{b-1}{b^i} + \frac{b-1}{b^{k+n+1}} = \frac{b^{n+1}-1}{b^{k+n}} + \frac{b-1}{b^{k+n+1}} \\
&= \frac{(b^{n+1}-1)\times b}{b^{k+n}\times b} + \frac{b-1}{b^{k+n+1}} = \frac{b^{n+1+1}-b}{b^{k+n+1}} + \frac{b-1}{b^{k+n+1}} \\
&= \frac{b^{(n+1)+1}-1}{b^{k+n+1}} \ ,
\end{aligned}$$

ce qui montre qu'elle est vraie aussi pour $n+1$. CQFD

Les preuves de §17

Preuve de [17.1]. Selon la définition d'une application, il faut montrer que pour tout $x \in \mathbf{R}$ il existe un et un seul entier $n \in \mathbf{Z}$ vérifiant $(x, n) \in \mathrm{Ent}$, c'est-à-dire $n \leq x < n+1$. Commençons avec l'existence.

Pour $x \in \mathbf{R}$ il existe, selon [15.28], $m_+ \in \mathbf{N} \subset \mathbf{Z}$ tel que $m_+ = m_+ \times 1 > x$. Mais on a aussi $-x \in \mathbf{R}$, donc par le même argument il existe $m_- \in \mathbf{N} \subset \mathbf{Z}$ tel que $m_- = m_- \times 1 > -x$, ce qu'on peut écrire comme $-m_- < x$ [15.27.vi]. On définit maintenant l'ensemble $E \subset \mathbf{Z}$ par

$$E \stackrel{\text{déf}}{=} \{ m \in \mathbf{Z} \mid x < m \} \ .$$

L'inégalité $x < m_+$ montre que E n'est pas vide et l'inégalité $-m_- < x$ (avec la transitivité d'une relation 'ordre) montre que E est minoré par $-m_- \in \mathbf{Z}$. Par [11.33] E admet donc un plus petit élément $m_o \in E$. Si on pose $n = m_o - 1$, on aura donc $x < m_o = n+1$ car $m_o \in E$ et $x \geq n = m_o - 1$ car par minimalité $m_o - 1 \notin E$.

Pour l'unicité de ce n, supposons qu'on a $m \leq x < m+1$ et $n \leq x < n+1$. Si on a $m < n$, alors $n - m > 0$, donc $n - m \in \mathbf{N}$ [11.27] et donc $n - m \geq 1$ [8.16], c'est-à-dire $m + 1 \leq n$. Mais alors on a

$$x < m + 1 \leq n \leq x \ ,$$

et donc (par la transitivité d'une relation d'ordre) $x < x$, ce qui est impossible. Le cas $n < m$ est similaire et conduit aussi à une contradiction. Étant donné que la relation d'ordre sur $\mathbf{Z}$ est totale, la seule possibilité qui reste est donc $m = n$, ce qui montre l'unicité. CQFD

Preuve de [17.2]. Il est "évident" que l'ensemble $A \subset \mathbf{R}$ défini par

$$A = \{ b^{-n} \mid n \in \mathbf{N} \} \equiv \{ x \in \mathbf{R} \mid \exists n \in \mathbf{N} : x = b^{-n} \}$$

est minoré par 0 : on montre facilement par récurrence qu'on a $b^n > 0$ pour tout $n \in \mathbf{N}$, et donc $b^{-n} = 1/b^n > 0$ par [15.27.ix]. Il s'ensuit que $\inf A$ existe [15.6] et vérifie $\inf A \geq 0$. Pour montrer l'égalité, on commence à montrer par récurrence l'inégalité

$$\forall n \in \mathbf{N} : b^n \geq 1 + n \times (b-1) \ .$$

Pour $n = 0$ on a $b^0 = 1 \geq 1 = 1 + 0 \times (b-1)$ et si c'est vrai pour n, alors on calcule

$$\begin{aligned} b^{n+1} &= b \times b^n \geq b \times \big(1 + n \times (b-1)\big) = b + b \times n \times (b-1) \\ &\overset{b>1 \text{ et } [15.27.\text{v}]}{\geq} 1 + (b-1) + n \times (b-1) = 1 + (n+1) \times (b-1) \ . \end{aligned}$$

Pour montrer l'égalité $\inf A = 0$, on montre la propriété (BI2'). On prend donc $e \in \mathbf{R}$, $e > 0$. Par [15.27.ix] il s'ensuit qu'on a $e^{-1} > 0$. La condition $b > 1$ se traduit comme $b - 1 > 0$ et donc par [15.28] il existe $n \in \mathbf{N}$ tel que $n \times (b-1) > e^{-1}$. Pour ce n on a donc

$$b^n \geq 1 + n \times (b-1) > n \times (b-1) > e^{-1} \ .$$

Par [15.27.v,ix] on a donc $1/b^n < e$, ce qui montre que la condition (BI2') est satisfaite. CQFD

Preuve de [17.6]. On commence avec la remarque que $\sum_{j=1}^{n} \frac{d(j)}{b^j}$ est une application de [16.2] avec la suite $t : \mathbf{N} \to \mathbf{R}$ définie par

$$t(0) = 0 \qquad \text{et} \qquad \forall n \in \mathbf{N}^* : t(n) = \frac{d(n)}{b^n} \ .$$

Pour simplifier les notations, on introduit l'ensemble $A \subset \mathbf{R}$ comme

$$A = \left\{ \sum_{j=1}^{n} \frac{d(j)}{b^j} \;\middle|\; n \in \mathbf{N} \right\} \ .$$

Si on trouvait $x \in \mathbf{R}$, $x > 0$ tel que A_x [17.4] est majoré par 1, alors par définition du sup on aurait $\sup A_x \leq 1$ et par [17.4] on aurait $x + \sup A \leq 1$, c'est-à-dire $\sup A \leq 1 - x < 1$ comme voulu.

Pour trouver un tel x, on rappelle que d est une suite réduite. Il existe donc $m \in \mathbf{N}^*$ tel que $m \geq 2$ et $d(m) \neq b - 1$. Associé à ce m on pose $x = 1/b^m > 0$. On définit aussi les suites $c, u : \mathbf{N} \to \mathbf{R}$ par

$$\forall n \in \mathbf{N} : c(n) = \frac{b-1}{b^n}$$

et

$$u(m) = t(m) + \frac{1}{b^m} \qquad \text{et} \qquad \forall n \in \mathbf{N} : n \neq m \Rightarrow u(n) = t(n) \ .$$

Par le choix de m on a $u(n) \leq c(n)$ pour tout $n \in \mathbf{N}$. Pour un $n > m$ on peut donc faire le calcul

$$\begin{aligned} x + \sum_{j=1}^{n} t(j) &\overset{[16.7]}{=} \frac{1}{b^m} + \sum_{j=1}^{m-1} \frac{d(j)}{b^j} + \sum_{j=m}^{m} \frac{d(j)}{b^j} + \sum_{j=m+1}^{n} \frac{d(j)}{b^j} \\ &= \sum_{j=1}^{m-1} \frac{d(j)}{b^j} + \frac{d(m)+1}{b^m} + \sum_{j=m+1}^{n} \frac{d(j)}{b^j} \\ &\overset{[16.7]}{=} \sum_{j=1}^{n} u(j) \overset{[16.4]}{\leq} \sum_{j=1}^{n} c(j) \overset{[16.8]}{=} \frac{b^n - 1}{b^n} < \frac{b^n}{b^n} = 1 \ . \end{aligned}$$

D'autre part, pour $n \leq m$ on applique [**??**] pour obtenir la majoration

$$x + \sum_{j=1}^{n} t(j) \leq x + \sum_{j=1}^{m+1} t(j) \overset{\text{calcul préc.}}{<} 1 \ .$$

Ainsi on a montré que chaque élément de A_x est majoré par 1 et on conclut qu'on a $\sup A < 1$.

Pour la minoration on constate qu'on a $\sum_{j=1}^{1} \frac{d(j)}{b^j} = \frac{d(1)}{b} \geq 0$ et donc il y a un élément dans A qui est positif. Il s'ensuit qu'on doit avoir $\sup A \geq 0$ [**??**]. CQFD

Preuve de [17.7]. • Pour l'injectivité, prenons $d, d' \in \mathcal{DR}_b$ tels que $d \neq d'$. Par [4.3] l'ensemble $E \subset \mathbf{N}$ défini comme

$$E = \{\, n \in \mathbf{N} \mid d(n) \neq d'(n) \,\}$$

n'est pas vide. Il admet donc un plus petit élément $k \in E$ [8.17]. On a donc

$$d(k) \neq d'(k) \qquad \text{et} \qquad \forall n \in \mathbf{N} : n < k \Rightarrow d(n) = d'(n) \ .$$

Sans perte de généralité on peut supposer qu'on a $d(k) < d'(k)$. Et parce que d est une suite réduite, il existe $m > k+1$ tel que $d(m) \neq b-1$. Associé à ce m on pose $x = \frac{1}{b^m}$. Avec ces ingrédients on fait, pour $n > m$ et en supposant $k > 1$, le calcul

$$\begin{aligned} x + \sum_{i=1}^{n} \frac{d(i)}{b^i} &= \frac{1}{b^m} + \sum_{i=1}^{k-1} \frac{d(i)}{b^i} + \frac{d(k)}{b^k} + \sum_{i=k+1}^{m-1} \frac{d(i)}{b^i} + \sum_{i=m+1}^{n} \frac{d(i)}{b^i} \\ &= \sum_{i=1}^{k-1} \frac{d(i)}{b^i} + \frac{d(k)}{b^k} + \sum_{i=k+1}^{m-1} \frac{d(i)}{b^i} + \frac{d(m)+1}{b^m} + \sum_{i=m+1}^{n} \frac{d(i)}{b^i} \end{aligned}$$

$\forall i \in \mathbf{N} : d(i) \leq b-1$ et en plus $d(m) < b-1$ donc $b(m)+1 \leq b-1$

$$\begin{aligned} &= \sum_{i=1}^{k-1} \frac{d(i)}{b^i} + \frac{d(k)}{b^k} + \sum_{i=k+1}^{n} \frac{b-1}{b^i} \\ &= \sum_{i=1}^{k-1} \frac{d(i)}{b^i} + \frac{d(k)}{b^k} + \frac{b^{n-k}-1}{b^n} = \sum_{i=1}^{k-1} \frac{d(i)}{b^i} + \frac{d(k)}{b^k} + \frac{1}{b^k} - \frac{1}{b^n} \\ &< \sum_{i=1}^{k-1} \frac{d(i)}{b^i} + \frac{d(k)}{b^k} + \frac{1}{b^k} = \sum_{i=1}^{k-1} \frac{d(i)}{b^i} + \frac{d(k)+1}{b^k} \end{aligned}$$

$\forall i \in \mathbf{N} : i < k \Rightarrow d(i) = d'(i)$ et $d(k) < d'(k)$ donc $d(k)+1 \leq d'(k)$

$$\leq \sum_{i=1}^{k-1} \frac{d'(i)}{b^i} + \frac{d'(k)}{b^k} = \sum_{i=1}^{k} \frac{d'(i)}{b^i} \quad .$$

En résumé, on a montré, pour tout $n > m$ et sous l'hypothèse $k > 1$, l'inégalité

$$x + \sum_{i=1}^{n} \frac{d(i)}{b^i} < \sum_{i=1}^{k} \frac{d'(i)}{b^i} \quad . \tag{33.30}$$

Si $k = 1$, la conclusion reste inchangée, seulement le terme $\sum_{i=1}^{k-1}$ disparaît du calcul. D'autre part, pour $n \leq m$ on peut invoquer [**??**] pour obtenir la conclusion

$$x + \sum_{i=1}^{n} \frac{d(i)}{b^i} \leq x + \sum_{i=1}^{m+1} \frac{d(i)}{b^i} \quad ,$$

ce qui montre que (33.30) est vrai pour tout $n \in \mathbf{N}$. Si on définit les ensembles $A, A' \subset \mathbf{R}$ par

$$A = \left\{ \sum_{j=1}^{n} \frac{d(j)}{b^j} \mid n \in \mathbf{N} \right\} \qquad \text{et} \qquad A' = \left\{ \sum_{j=1}^{n} \frac{d(j)}{b^j} \mid n \in \mathbf{N} \right\} ,$$

alors on a montré (en utilisant [17.4] et [**??**]) les inégalités

$$x + \sup A = \sup A_x \leq \sum_{i=1}^{k} \frac{d'(i)}{b^i} \leq \sup A' \quad ,$$

d'où la conclusion $\sup A < \sup A'$. En supposant $d \neq d'$ on a donc montré $f_b(d) \neq f_b(d')$, ce qui veut dire que f_b est injective.

• Pour montrer que f_b est surjective, on prend $x \in \mathbf{R}$ tel que $0 \leq x < 1$ et on cherche $d \in \mathcal{DR}_b$ tel que $f_b(d) = x$. On va construire d (en tant que suite) par

récurrence, ou plutôt on va construire deux suites $d, s : \mathbf{N}^* \to \mathbf{R}$ vérifiant pour tout $n \in \mathbf{N}$ les conditions

$$0 \leq x - s(n) < \frac{1}{b^n} \quad , \quad d(n) \in B_b \quad , \quad s(n) = \sum_{i=1}^{n} \frac{d(i)}{b^i} \ . \tag{33.31}$$

Formellement on va construire une suite $D : \mathbf{N}^* \to \mathbf{R} \times \mathbf{R}$ et on posera $d = \pi_1 \circ D$ et $s = \pi_2 \circ D$, où $\pi_i : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$, $i = 1, 2$ est la projection sur la i-ième composante. Ainsi on aura pour tout $n \in \mathbf{N}^*$ l'égalité $D(n) = \big(d(n), s(n)\big)$.

Quand on regarde les conditions (33.31), on a, à première vu, l'impression que l'introduction de la deuxième suite s est superflue, car cette suite est complètement déterminé par la suite d par la troisième condition. Mais on en a besoin pour rentrer dans le cadre de la construction par récurrence, car si on enlève cette suite, la définition/construction de l'élément $d(n+1)$ dépendra non seulement de l'élément $d(n)$, mais de *tous* les éléments précédents $d(1)$ jusqu'à $d(n)$.

La construction de la suite D commence avec la définition

$$D(1) = \Big(\operatorname{Ent}(b \times x) \, , \, \frac{\operatorname{Ent}(b \times x)}{b} \Big) \quad \Longleftrightarrow \quad d(1) = \operatorname{Ent}(b \times x) \quad , \quad s(1) = \frac{d(1)}{b} \ .$$

Et si on connaît $D(n) = \big(d(n), s(n)\big)$, on définit $D(n+1) = \big(d(n+1), s(n+1)\big)$ par

$$d(n+1) = \operatorname{Ent}\big(\, b^{n+1} \times \big(x - s(n)\big) \, \big) \quad , \quad s(n+1) = s(n) + \frac{d(n+1)}{b^{n+1}} \ . \tag{33.32}$$

C'est une application de [7.8.ii] avec l'application $f : \mathbf{N} \times (\mathbf{R} \times \mathbf{R}) \to \mathbf{R} \times \mathbf{R}$ définie par

$$f\big(n, (d, s)\big) = \Big(\operatorname{Ent}\big(b^{n+1} \times (x - s)\big) \ , \ s + \frac{\operatorname{Ent}\big(b^{n+1} \times (x - s)\big)}{b^{n+1}} \Big) \ .$$

La vérification de (33.31) pour tout $n \in \mathbf{N}^*$ se fait (peut-on faire autrement) par récurrence en commençant le cas $n = 1$. Par définition on a $s(1) = d(1)/b$, ce qui donne la troisième partie de (33.31). La définition de la partie entière nous donne l'encadrement

$$d(1) \leq b \times x < d(1) + 1 \qquad \Longleftrightarrow \qquad 0 \leq x - \frac{d(1)}{b} < \frac{1}{b} \ ,$$

ce qui est la première partie de (33.31). D'autre part, l'encadrement $0 \leq x < 1$ implique (par [15.27.v/vii]) l'encadrement

$$0 \leq b \times x < b \ .$$

Si on avait $d(1) < 0$, alors on aurait $d(1) + 1 \leq 0$ [**??**], ce qui donnerait les inégalités $0 \leq b \times x < d(1) + 1 \leq 0$, ce qui est impossible. De la même façon, si on avait $b \leq d(1)$, alors on aurait $b \times x < b \leq d(1) < b \times x$, ce qui est impossible. On conclut que $d(1)$ est un entier vérifiant $0 \leq d(1) < b$, c'est-à-dire $d(1) \in B_b$ comme voulu. Ainsi on a montré (33.31) pour $n = 1$.

Supposons maintenant que (33.31) soit vérifié au rang n. Si on combine l'hypothèse de récurrence avec la définition de $s(n+1)$ (33.32) et la définition d'une somme (16.3), on obtient

$$s(n+1) \overset{(33.32)}{=} s(n) + \frac{d(n+1)}{b^{n+1}} \overset{\text{hyp. de réc.}}{=} \sum_{i=1}^{n} \frac{d(i)}{b^i} + \frac{d(n+1)}{b^{n+1}} \overset{(16.3)}{=} \sum_{i=1}^{n+1} \frac{d(i)}{b^i} \ ,$$

ce qui est la troisième partie de (33.31) au rang $n+1$.

Par (33.32) et la définition de la partie entière on a l'encadrement

$$d(n+1) \leq b^{n+1} \times \big(x - s(n)\big) < d(n+1) + 1 \qquad \Longleftrightarrow$$

$$0 \leq x - s(n) - \frac{d(n+1)}{b^{n+1}} < \frac{1}{b^{n+1}} \qquad \overset{\text{arg. préc.}}{\Longleftrightarrow}$$

$$0 \leq x - s(n+1) < \frac{1}{b^{n+1}} \quad , \tag{33.33}$$

ce qui montre la première partie de (33.31) au rang $n+1$.

D'autre part, en multipliant l'encadrement dans l'hypothèse de récurrence par b^{n+1} on obtient l'encadrement

$$0 \leq b^{n+1} \times \big(x - s(n)\big) < b \quad .$$

En comparant ceci avec l'encadrement

$$d(n+1) \leq b^{n+1} \times \big(x - s(n)\big) < d(n+1) + 1$$

donné précédemment, on obtient, comme pour $d(1)$, les inégalités $d(n+1) \geq 0$ et $d(n+1) < b$. Il s'ensuit, comme pour $d(1)$, qu'on a $d(n+1) \in B_b$, ce qui termine la preuve qu'on a (33.31) au rang $n+1$.

Selon les définitions de A et s on a l'égalités

$$A = \{\, s(n) \mid n \in \mathbf{N}^* \,\} \quad .$$

Mais l'encadrement dans (33.31) peut être réécrit comme les inégalités

$$x - b^{-n} < s(n) \qquad \text{et} \qquad s(n) \leq x \quad ,$$

ce qui nous donne immédiatement les inégalités

$$x - b^{-n} < \sup A \qquad \text{et} \qquad \sup A \leq x \quad ,$$

valable pour tout $n \in \mathbf{N}^*$. La première inégalité peut être réécrit comme

$$x - \sup A < b^{-n} \quad ,$$

ce qui montre que $x - \sup A$ est un minorant pour l'ensemble $\{\, b^{-n} \mid n \in \mathbf{N}^* \,\}$. Par [17.2] on a donc $x - \sup A \leq 0$, c'est-à-dire $\sup A \geq x$. Avec l'inégalité dans l'autre sens on a donc l'égalité

$$\sup A = x \quad .$$

Sans argument supplémentaire on ne peut pas conclure qu'on a $f_b(d) = x$, car on ne sait pas encore que d est une suite réduite ! Par contre, dès qu'on sait cela on aura $d \in \mathcal{DR}_b$ et donc $f_b(d) = \sup A = x$, ce qui terminera la preuve que f_b est surjective.

Pour montrer que d est une suite réduite, on passe par l'absurde. Supposons donc qu'il existe $m \in \mathbf{N}^*$ tel qu'on a

$$\forall i \in \mathbf{N}^* : i \geq m \Rightarrow d(i) = b - 1 \quad .$$

Alors on a, pour tout $n \geq m$ et en supposant $m > 1$, l'égalité

$$s(n) = s(m-1) + \sum_{i=m}^{n} \frac{d(i)}{b^i} = s(m-1) + \sum_{i=m}^{n} \frac{b-1}{b^i}$$

$$= s(m-1) + \frac{b^{n-m+1} - 1}{b^n} = s(m-1) + \frac{1}{b^{m-1}} - \frac{1}{b^n} \quad .$$

On a donc l'inégalité

$$\sup A \geq s(m-1) + \frac{1}{b^{m-1}} - \frac{1}{b^n} \quad ,$$

valable pour tout $n \geq m$. En réécrivant ceci comme

$$s(m-1) + \frac{1}{b^{m-1}} - \sup\, A \leq \frac{1}{b^n}$$

on en déduit, avec [17.2], l'inégalité

$$s(m-1) + \frac{1}{b^{m-1}} - \sup\, A \leq \inf\,\{\, b^{-n} \mid n \in \mathbf{N}\,\} = 0 \ .$$

Mais on a déjà montré l'égalité $\sup\, A = x$, donc on a obtenu l'inégalité

$$x - s(m-1) \geq \frac{1}{b^{m-1}} \ ,$$

ce qui est en contradiction avec (33.31) au rang $m-1$.

Tout ceci était sous l'hypothèse qu'on a $m > 1$. Dans le cas $m = 1$ l'argument ne change pas, mais le terme $s(m-1)$ disparaît des calculs. Et au lieu d'obtenir l'inégalité $x - s(m-1) \geq b^{1-m}$, on obtient l'inégalité $x \geq 1$, ce qui est en contradiction avec l'hypothèse $x < 1$. Dans tous les cas on obtient donc une contradiction, ce qui montre (par l'absurde) que la suite d doit être réduite, c'est-à-dire, appartenir à $\mathcal{DR}_b$. CQFD

Preuve de [17.8]. Supposons le contraire, c'est-à-dire, que $g : \mathbf{N}^* \to [0,1[$ est une surjection. En composant avec la réciproque de la bijection $f_{10} : \mathcal{DR}_{10} \to [0,1[$ donnée dans [17.7] on obtient une surjection

$$F : \mathbf{N}^* \to \mathcal{DR}_{10} \quad , \quad F = f_{10}^{-1} \circ g \ .$$

Pour tout $k \in \mathbf{N}^*$ l'image $F(k)$ est donc une suite à valeurs dans $\{0,1,\ldots,9\}$. En particulier on a $\big(F(k)\big)(n) \in \{0,1,\ldots,9\}$ pour tout $n \in \mathbf{N}^*$. Si on écrit ces suites dans une liste, on obtient un tableau de chiffres décimaux comme suit.

$$\begin{aligned}
F(1) &= 0\,,\, \textcircled{a_1}\ a_2\ a_3\ a_4\ a_5\ldots \\
F(2) &= 0\,,\, b_1\ \textcircled{b_2}\ b_3\ b_4\ b_5\ldots \\
F(3) &= 0\,,\, c_1\ c_2\ \textcircled{c_3}\ c_4\ c_5\ldots \\
&\vdots \\
F(n) &= 0\,,\, x_1\ x_2\ldots\ x_{n-1}\textcircled{x_n}\ x_{n+1}\ldots \\
F(n+1) &= 0\,,\, y_1\ y_2\ldots\ y_{n-1}\ y_n\ \textcircled{y_{n+1}}\ldots \\
&\vdots
\end{aligned}$$

Si on ne regarde que les éléments (décimaux) sur le diagonale, on obtient une nouvelle suite $z = 0, a_1 b_2 c_3 \ldots x_n y_{n+1} \ldots$ à valeurs dans $\{0,1,\ldots,9\}$. La surjectivité de F implique que cette nouvelle suite est dans notre liste, c'est-à-dire qu'il existe $k \in \mathbf{N}^*$ (pas forcément unique) tel que $F(k) = z$. Par exemple il est possible qu'on a $k = 2$, à condition qu'on a $c_1 = a_1$, $c_2 = b_2$, …, $c_n = x_n$ et cætera.

Mais il est plus intéressant de changer ces éléments sur le diagonale, car la suite qu'on obtient ainsi ne peut plus être dans la liste : le n-ième élément de la liste aura son n-ième décimale différent. On aura donc une contradiction avec la surjectivité de F. Formellement on définit par exemple la suite $d \in \mathcal{DR}_{10}$ par

$$\forall n \in \mathbf{N}^* \quad : \quad d(n) = 0 \quad \text{si } \big(F(n)\big)(n) > 5 \quad , \quad d(n) = 8 \quad \text{si } \big(F(n)\big)(n) \leq 5 \ .$$

La construction est telle que pour tout $n \in \mathbf{N}^*$ on a $d(n) \neq \big(F(n)\big)(n)$. La surjectivité de F implique qu'il existe $k \in \mathbf{N}^*$ tel que $F(k) = d$. En particulier on doit avoir $\big(F(k)\big)(k) = d(k)$. Mais cela est impossible selon la construction de la suite d. Cette contradiction montre qu'une telle surjection ne peut pas exister. $\boxed{CQFD}$

Les preuves de §18

Preuve de [18.1]. • ($\Rightarrow$) : Supposons qu'on a un ensemble A vérifiant les hypothèses, c'est-à-dire que ces éléments ne sont pas vides et 2 à 2 disjoints. Pour trouver un ensemble C qui contient un et un seul élément de chaque élément de A, on constate d'abord qu'on a la propriété [1.9]

$$\forall a \in A : a \subset \cup A \ .$$

On peut donc définir l'application $g : A \to \mathcal{P}(\cup A)$ par $g(a) = a$. Le fait que les éléments de A ne sont pas vides nous garantit que g prend ses valeurs dans $\mathcal{P}(\cup A) \setminus \{\emptyset\}$. On peut donc invoquer l'axiome du choix pour obtenir une fonction $f : A \to \cup A$ vérifiant $f(a) \in g(a) = a$ pour tout $a \in A$. On définit l'ensemble C comme l'image de f :

$$C \stackrel{\text{déf}}{=} f[A] \equiv \{\, f(a) \mid a \in A \,\} \equiv \{\, c \in \cup A \mid \exists a \in A : c = f(a) \,\} \subset \cup A \ .$$

Pour montrer que ce C a la propriété voulue, on prend $a \in A$. Alors on a $f(a) \in a$ par l'axiome du choix et $f(a) \in C$ par définition de C. On a donc $\{f(a)\} \subset a \cap C$. D'autre part, si on a $c \in a \cap C$, alors par définition de C il existe $a' \in A$ tel que $c = f(a')$. On a donc $f(a') = c \in a \cap C$, donc en particulier $f(a') \in a$. Mais par l'axiome du choix on a aussi $f(a') \in a'$, donc $a \cap a' \neq \emptyset$. Par l'hypothèse sur A, on doit donc avoir $a' = a$ et donc $c = f(a)$. Ainsi on a bien montré l'égalité $a \cap C = \{f(a)\}$.

• ($\Leftarrow$) : Supposons qu'on a une fonction $g : I \to \mathcal{P}(B) \setminus \{\emptyset\}$. Alors il faut construire une fonction $f : I \to B$ vérifiant $f(i) \in g(i)$ pour tout $i \in I$. Le problème principal est que les ensembles $g(i) \subset B$ ne sont pas forcément disjoints, ni différents. Pour les rendre disjoints on considère l'ensemble $A \subset \mathcal{P}(I \times B)$ défini comme

$$A = \{\, a \subset I \times B \mid \exists i \in I : a = \{i\} \times g(i) \,\} = \{\, \{i\} \times g(i) \subset I \times B \mid i \in I \,\} \ .$$

Si on a $a, b \in A$ tel que $a \cap b \neq \emptyset$, alors par définition de A il existe $i, j \in I$ tels que $a = \{i\} \times g(i)$ et $b = \{j\} \times g(j)$. Si on a $x \in a \cap b$, on doit avoir $x = (i, y)$ avec $y \in g(i)$ car $x \in a$ et $x = (j, z)$ avec $z \in g(j)$ car $x \in b$. Donc $i = j$ [**??**] et $a = b$. Ainsi on a montré que les éléments de A sont 2 à 2 disjoints. Qu'ils ne sont pas vides est une conséquence immédiate du fait que les ensembles $g(i)$ ne sont pas vides. On peut donc invoquer la propriété qui dit qu'il existe un ensemble $f \subset \cup A$ tel que $\forall a \in A \ \exists c : a \cap f = \{c\}$. On prétend que ce f est une application de I dans B vérifiant $f(i) \in g(i)$ pour tout $i \in I$.

Pour le montrer, commençons avec l'observation qu'on a l'inclusion $\cup A \subset I \times B$, car pour $c \in \cup A$ il existe $a \in A$ tel que $c \in a$. Mais $a \subset I \times B$, donc $c \in I \times B$ comme annoncé. On a donc bien $f \subset I \times B$. Ensuite on constate que si $(i, b) \in f$, alors par l'inclusion $f \subset \cup A$, il existe $a \in A$ tel que $(i, b) \in a$. Mais par définition de A il existe $j \in I$ tel que $a = \{j\} \times g(j)$. Il s'ensuit qu'on doit avoir $j = i$ et (donc) $b \in g(i)$. Autrement dit, on a l'implication

$$(i, b) \in f \qquad \Longrightarrow \qquad b \in g(i) \ , \tag{33.34}$$

ce qui dit déjà qu'on a $f(i) \in g(i)$, à condition d'avoir montré que f est une application.

Pour la première condition d'une application, prenons $i \in I$ et regardons l'élément $a = \{i\} \times g(i) \in A$. Par hypothèse il existe $(j, b) \in f$ tel que

$$\{(j, b)\} = a \cap f \equiv \big(\{i\} \times g(i)\big) \cap f \ .$$

Il s'ensuit qu'on a $j = i$, donc, pour notre $i \in I$ donné, il existe bien $b \in B$ tel que $(i, b) \in f$. Pour la deuxième condition, suppposons qu'on a $(i, b), (i, b') \in f$. Alors

par (33.34) on a $b, b' \in g(i)$, donc

$$(i,b),(i,b') \in \big(\{i\} \times g(i)\big) \cap f \ .$$

Le fait que cette intersection ne contient qu'un seul élément implique qu'on doit avoir $b = b'$. Ainsi on a montré que f est bien une application de I dans B vérifiant $f(i) \in g(i)$ pour tout $i \in I$. $\boxed{CQFD}$

Les preuves de §19

Preuve de [19.8]. Si l'application min existe, alors l'unicité est garantit par [19.2.i] (version pour élément minimal) : il n'existe qu'un seul élément minimal dans chaque sous-ensemble non-vide. Pour l'existence, on définit $\min \subset (\mathcal{P}(E) \setminus \{\emptyset\}) \times E$ par

$$\min = \{\, (A,m) \in (\mathcal{P}(E) \setminus \{\emptyset\}) \times E \mid m \in A \text{ et } \forall a \in A : m \leq a \,\}$$

et on montre que c'est bien une application. Pour la première condition, prenons $A \in \mathcal{P}(E) \setminus \{\emptyset\}$, c'est-à-dire $A \subset E$ et $A \neq \emptyset$. Par hypothèse d'un bon ordre, il existe un élément minimal $m \in A$, c'est-à-dire qu'on a $m \in A$ et $\forall a \in A : m \leq a$. Il s'ensuit qu'on a $(A,m) \in \min$, ce qui montre que min remplit la première condition d'une application. Pour la deuxième, on suppose qu'on a $(A,m), (A,m') \in \min$. Alors par définition on a les propriétés

$$m, m' \in A \quad , \quad \forall a \in A : m \leq a \quad \text{et} \quad \forall a \in A : m' \leq a \ .$$

Il s'ensuit qu'on a $m' \leq m$ et $m \leq m'$, c'est-à-dire $m = m'$ comme voulu pour la deuxième propriété d'une application. Une fois qu'on sait que min est une application, la définition nous donne immédiatement les équivalences

$$m = \min(A) \iff (A,m) \in \min \iff m \in A \text{ et } \forall a \in A : m \leq a$$

comme voulu. CQFD

Preuve de [19.11]. Pour un sous-ensemble $A \subset E$ on définit le sous-ensemble $B \subset E$ par $B = E \setminus A$, ce qui veut dire que si on connaît B, A est donné par $A = E \setminus B$. On a donc les équivalences (pour $x \in E$)

$$x \notin A \ \Leftrightarrow \ x \in B \qquad \text{et} \qquad A = \emptyset \ \Leftrightarrow \ B = E \ .$$

Avec ces observations on constate qu'on a les équivalences logiques

$$\begin{aligned}
& A \neq \emptyset \ \Rightarrow \ \Big[\ \exists a \in A \ \forall x \in A : x \not< a \ \Big] \\
\Leftrightarrow \quad & \neg \Big[\ \exists a \in A \ \forall x \in A : x \not< a \ \Big] \ \Rightarrow \ A = \emptyset \\
\Leftrightarrow \quad & \Big[\ \forall a \in A \ \exists x \in A : x < a \ \Big] \ \Rightarrow \ A = \emptyset \\
\Leftrightarrow \quad & \Big[\ \forall a \in E : a \in A \Rightarrow \ \big(\ \exists x \in A : x < a \ \big) \ \Big] \ \Rightarrow \ A = \emptyset \\
\Leftrightarrow \quad & \Big[\ \forall a \in E : \neg \ \big(\ \exists x \in A : x < a \ \big) \ \Rightarrow \ a \notin A \ \Big] \ \Rightarrow \ A = \emptyset \\
\Leftrightarrow \quad & \Big[\ \forall a \in E : \ \big(\ \forall x \in A : x \not< a \ \big) \ \Rightarrow \ a \notin A \ \Big] \ \Rightarrow \ A = \emptyset \\
\Leftrightarrow \quad & \Big[\ \forall a \in E : \ \big(\ \forall x \in E : x \in A \ \Rightarrow \ x \not< a \ \big) \ \Rightarrow \ a \notin A \ \Big] \ \Rightarrow \ A = \emptyset \\
\Leftrightarrow \quad & \Big[\ \forall a \in E : \ \big(\ \forall x \in E : x < a \ \Rightarrow \ x \notin A \ \big) \ \Rightarrow \ a \notin A \ \Big] \ \Rightarrow \ A = \emptyset \\
\Leftrightarrow \quad & \Big[\ \forall a \in E : \ \big(\ \forall x \in E : x < a \ \Rightarrow \ x \in B \ \big) \ \Rightarrow \ a \in B \ \Big] \ \Rightarrow \ B = E \ .
\end{aligned}$$

Pour l'implication (i) $\Rightarrow$ (ii) il suffit donc de prendre un sous-ensemble $B \subset E$ et d'invoquer (i) avec $A = E \setminus B$ et pour l'implication (ii) $\Rightarrow$ (i) il suffit de prendre un sous-ensemble $A \subset E$ et d'invoquer (ii) avec $B = E \setminus A$. CQFD

Preuve de [19.17]. • On commence avec une définition qui facilite le discours qui suit. On dit qu'une application $\varphi : I \to A$ sur un idéal $I \subset E$ *vérifie la condition de récurrence* si elle vérifie la condition

$$\forall x \in I : \varphi(x) = F(\varphi|_{E_{<x}}) \ .$$

• La première étape consiste à montrer qu'il existe au plus une application sur un idéal I vérifiant la condition de récurrence. Pour cela on suppose qu'on en a deux : $\varphi, \psi : I \to A$ et on considère le sous-ensemble $D \subset I$ défini comme

$$D = \{\, x \in I \mid \varphi(x) = \psi(x) \,\} \ .$$

On va démontrer par récurrence transfinie qu'on a $D = I$. Pour cela on prend $x \in I$ et on suppose qu'on a $E_{<x} \subset D$. Par définition de D on a donc l'égalité $\varphi|_{E_{<x}} = \psi|_{E_{<x}}$ et parce que φ et ψ vérifient la condition de récurrence on a

$$\varphi(x) = F(\varphi|_{E_{<x}}) = F(\psi|_{E_{<x}}) = \psi(x) \ ,$$

ce qui montre qu'on a aussi $x \in D$ et donc par récurrence transfinie on a $D = I$, c'est-à-dire, $\varphi = \psi$.

• La deuxième étape consiste à montrer que **si** pour tout x dans un idéal I il existe une application $\varphi_x : E_{\leq x} \to A$ vérifiant la condition de récurrence (et par la première étape une telle application est unique car $E_{\leq x}$ est un idéal), **alors** il existe une application $\varphi : I \to A$ vérifiant la condition de récurrence. Pour cela on pose

$$\varphi = \{\, (x, \varphi_x(x)) \mid x \in I \,\} \equiv \{\, c \in I \times A \mid \exists x \in I : c = (x, \varphi_x(x)) \,\}$$

et il faut montrer (dans l'ordre) que c'est une application de I dans A et qu'elle vérifie la condition de récurrence. Par définition de φ, on a

$$\forall x \in I : (x, \varphi_x(x)) \in \varphi \ ,$$

donc la première condition d'une application est vérifiée. Mais si on a $(x, a) \in \varphi$, alors par définition on a $a = \varphi_x(x)$, ce qui montre la deuxième condition d'une application. Reste à montrer qu'elle vérifie la condition de récurrence. Pour cela on montre qu'on a l'égalité

$$\varphi|_{E_{\leq x}} = \varphi_x$$

pour tout $x \in I$, car si on a cela, on aura

$$\varphi(x) \overset{[5.13]}{=} \varphi|_{E_{\leq x}}(x) = \varphi_x(x) \overset{\text{cond. réc.}}{=} F(\varphi_x|_{E_{<x}}) = F((\varphi|_{E_{\leq x}})|_{E_{<x}}) \overset{[5.14]}{=} F(\varphi|_{E_{<x}}) \ .$$

Prenons donc $y \in E_{\leq x}$, alors $\varphi_x|_{E_{\leq y}}$ est une application de $E_{\leq y} \subset E_{\leq x}$ dans A vérifiant la condition de récurrence : pour tout $z \in E_{\leq y}$ on a les égalités

$$(\varphi_x|_{E_{\leq y}})(z) \overset{[5.13]}{=} \varphi_x(z) \overset{\text{cond. réc.}}{=} F(\varphi_x|_{E_{<z}}) \overset{[5.14]}{=} F((\varphi_x|_{E_{\leq y}})|_{E_{<z}}) \ .$$

Par la première étape on doit avoir $\varphi_x|_{E_{\leq y}} = \varphi_y$ et donc en particulier

$$\varphi(y) \overset{\text{déf. } \varphi}{=} \varphi_y(y) = (\varphi_x|_{E_{\leq y}})(y) \overset{[5.13]}{=} \varphi_x(y) \ .$$

Ainsi on a montré l'égalité $\varphi|_{E_{\leq x}} = \varphi_x$, ce qui termine la deuxième étape.

• Dans la troisième étape on définit l'ensemble $D \subset E$ comme

$$D = \{\, x \in E \mid \exists \varphi_x : E_{\leq x} \to A \text{ vérifiant la condition de récurrence} \,\}$$

et on montre par récurrence transfinie qu'on a l'égalité $D = E$. On suppose donc qu'on a $E_{<x} \subset D$ et on essaie d'en déduire $x \in D$. Par hypothèse il existe $\varphi_y : E_{\leq y} \to A$ vérifiant la condition de récurrence pour tout $y < x$ et en plus $E_{<x}$ est

un idéal. Par la deuxième étape il existe une application $\varphi : E_{<x} \to A$ vérifiant la condition de récurrence. Avec ce φ on définit la relation $\varphi_x \subset E_{\leq x} \times A$ comme

$$\varphi_x = \varphi \cup \left\{ \big(x, F(\varphi)\big) \right\}$$

et on montre que φ_x est une application de $E_{\leq x}$ dans A vérifiant la condition de récurrence. Si $y < x$, alors il existe $a \in A$ tel que $(y, a) \in \varphi \subset \varphi_x$, car φ est une application ; et par définition on a $(x, F(\varphi)) \in \varphi_x$. La première condition d'une application est donc vérifiée. Pour la deuxième, si on a $(y, a), (y, b) \in \varphi_x$, alors si $y < x$ on doit avoir $(y, a), (y, b) \in \varphi$, donc $a = b$ parce que φ est une application ; et si $y = x$ on a $a = F(\varphi) = b$. La conclusion est que φ_x est bien une application de $E_{\leq x}$ dans A.

Pour la condition de récurrence, on a pour tout $y \in E_{\leq x}$ la propriété $x \notin E_{<y}$, donc on a l'égalité

$$\varphi_x|_{E_{<y}} = \varphi_x \cap (E_{<y} \times A) = \varphi \cap (E_{<y} \times A) = \varphi|_{E_{<y}} \ .$$

Il s'ensuit qu'on a

$$\varphi_x(x) \overset{\text{déf. } \varphi_x}{=} F(\varphi) = F(\varphi_x|_{E_{<x}})$$

et si $y < x$ on a

$$\varphi_x(y) \overset{\text{déf. } \varphi_x}{=} \varphi(y) = F(\varphi|_{E_{<y}}) = F(\varphi_x|_{E_{<y}}) \ .$$

La conclusion est qu'on a $x \in D$.

• Pour la quatrième étape on invoque la deuxième étape avec l'idéal $I = E$ et le résultat de la troisième étape. Il s'ensuit qu'il existe une application sur E dans A vérifiant la condition de récurrence ; elle est unique par la première étape. CQFD

Les preuves de §20

Preuve de [20.2]. Preuve du lemme de Zorn renforcé [20.1] avec l'axiome du choix.

Commençons avec l'invocation de l'axiome du choix avec $B = X$, $I = \mathcal{P}(X)\setminus\{\emptyset\}$ et $g = id : \mathcal{P}(X)\setminus\{\emptyset\} \to \mathcal{P}(X)\setminus\{\emptyset\}$ (remarquons en passant que $\mathcal{P}(X)\setminus\{\emptyset\}$ n'est pas vide, car X n'est pas vide). Alors on obtient une fonction de choix $f : \mathcal{P}(X)\setminus\{\emptyset\} \to X$ telle que $f(A) \in A$ pour tout $A \subset X$, $A \neq \emptyset$. Pour tout sous-ensemble $A \subset X$ on introduit aussi l'ensemble $\mathrm{MajStr}(A)$ de tous les majorants stricts de A défini comme

$$\mathrm{MajStr}(A) = \{x \in X \mid \forall a \in A : a < x\} \ .$$

À noter qu'on a l'égalité $\mathrm{MajStr}(\emptyset) = X$, car la condition $\forall a \in \emptyset : a < x$ est toujours vraie : il n'y a rien à vérifier.

On définit la notion d'une f-chaîne comme un sous-ensemble B de X vérifiant les conditions suivantes :

(i) $(B, \leq)$ est bien ordonné ;

(ii) $\forall x \in B : x = f\big(\mathrm{MajStr}(B_{<x})\big)$.

On remarque que la condition (ii) traduit l'idée qu'un élément dans une f-chaîne est l'élément choisi parmi les majorants stricts de ses prédécesseurs. Avec la notion de f-chaîne on définit $\mathcal{F}$ comme l'ensemble de toutes les f-chaînes :

$$\mathcal{F} = \{B \in \mathcal{P}(X) \mid B \text{ est une } f\text{-chaîne}\} \ .$$

Pour montrer que les éléments de $\mathcal{F}$ sont tous le début d'une même f-chaîne "maximal," on commence à montrer que si $A, B \in \mathcal{F}$ sont tels que $A \setminus B$ n'est pas vide, alors il existe $a \in A$ tel que

$$B = A_{<a} \equiv \{\, y \in A \mid y < a \,\} \ . \tag{33.35}$$

Pour cela on définit l'ensemble $\mathcal{J} \subset \mathcal{P}(X)$ comme l'ensemble des idéaux inclus dans A et dans B :

$$\mathcal{J} = \{I \subset X \mid \ I \text{ est un idéal de } A \text{ et de } B\} \ .$$

Associé à $\mathcal{J}$ on définit l'ensemble $J = \cup\mathcal{J} \subset X$ comme la réunion de $\mathcal{J}$. Étant donné que les éléments de $\mathcal{J}$ sont en particulier des idéaux de A, J est un idéal de A [20.2]. De même, car les éléments de $\mathcal{J}$ sont des idéaux de B, J est aussi un idéal de B. On ne peut pas avoir $J = A$, car dans ce cas on aurait $A = J \subset B$, ce qui contredit l'hypothèse $A \setminus B \neq \emptyset$. Par [19.13] il existe donc $a \in A$ tel que $J = A_{<a}$. Supposons qu'on n'a pas non plus $J = B$. Alors de nouveau par [19.13] il existe $b \in B$ tel que $J = B_{<b}$. Mais alors par définition d'une f-chaîne on peut faire le calcul

$$a = f\big(\mathrm{MajStr}(A_{<a})\big) = f\big(\mathrm{MajStr}(J)\big) = f\big(\mathrm{MajStr}(B_{<b})\big) = b \ .$$

Il s'ensuit qu'on a l'égalité $A_{\leq a} = A_{<a} \cup \{a\} = B_{<b} \cup \{b\} = B_{\leq b}$. Mais ces ensembles sont des idéaux de A et de B [19.12]. Ils appartiennent donc à $\mathcal{J}$ et par définition de J on doit avoir $A_{\leq a} \subset J$. Mais par définition de a on a $a \notin A_{<a} = J$. Cette contradiction montre qu'on doit avoir $A_{<a} = J = B$, ce qui montre l'égalité (33.35).

Pour "trouver" la f-chaîne maximal C on la définit comme la réunion de $\mathcal{F}$:

$$C \stackrel{\text{déf}}{=} \cup\,\mathcal{F} \ .$$

Pour montrer que ce C est bien une f-chaîne (c'est-à-dire, appartient à $\mathcal{F}$), on vérifie les propriétés. On commence avec l'observation que $(C, \leq)$ est totalement ordonné, car si x, y appartiennent à $C = \cup\mathcal{F}$, il existe, par l'axiome de la réunion (Z4),

$A, B \in \mathcal{F}$ tels que $x \in A$ et $y \in B$. Si on a $x \in B$, alors on peut comparer x et y car B est bien ordonné et en particulier totalement ordonné. Si on n'a pas $x \in B$, alors par le résultat précédent on doit avoir $B = A_{<a}$ pour un $a \leq x$ et donc $y < a \leq x$, ce qui implique (par transitivité d'une relation d'ordre) qu'on peut comparer x et y.

Soit maintenant $D \subset C$ un sous-ensemble non-vide et soit $x \in D$. Alors par définition de C il existe $A \in \mathcal{F}$ tel que $x \in A$. A étant bien ordonné, il existe un plus petit élément y dans $D \cap A$. Pour un élément $z \in D$ quelconque, si $z \in A$, alors forcément $y \leq z$. Si $z \notin A$, alors il existe $B \in \mathcal{F}$ tel que $z \in B$. Mais par le résultat précédent on doit avoir $A = B_{<b}$ pour un $b \leq z$. Donc dans ce cas on a $y < b \leq z$, donc en particulier $y \leq z$. Par conséquent l'ensemble D admet un plus petit élément et C est bien ordonné.

Reste à montrer que C vérifie la condition (ii) d'une f-chaîne. Pour cela on prend $x \in C$ et on considère l'ensemble $\{y \in C \mid y < x\}$. Par définition de C il existe $B \in \mathcal{F}$ tel que $x \in B$. Pour tout $y \in C$ il existe $B' \in \mathcal{F}$ tel que $y \in B'$. On déduit du résultat précédent que si $y \leq x$, alors forcément $B' \subset B$ et donc $y \in B$. Il s'ensuit qu'on a l'égalité

$$\{y \in C \mid y < x\} = \{y \in B \mid y < x\} \ .$$

Mais B est une f-chaîne, donc $x = f\big(\mathrm{MajStr}(\{y \in B \mid y < x\})\big)$, ce qui termine la preuve que C est une f-chaîne.

Par hypothèse du lemme, la chaîne bien ordonné C admet un majorant $m \in X$. Si ce m est un majorant strict, alors l'ensemble $\mathrm{MajStr}(C)$ n'est pas vide et on peut définir l'ensemble C' comme

$$C' = C \cup \{\, f\big(\mathrm{MajStr}(C)\big) \,\} \ .$$

Il est presque immédiat que C' est une f-chaîne strictement plus grand que C. Mais cela est impossible car C est la réunion de toutes les f-chaînes, y compris C'. Il s'ensuit que m appartient à C. Si $m' \in X$ est un majorant strict de m, c'est-à-dire $m' > m$, alors m' est un majorant strict de C, car m est un majorant de C. Mais C n'a pas de majorant strict, donc il n'existe pas d'élément $m' \in X$ vérifiant $m' > m$, c'est-à-dire que m est un élément maximal dans X. CQFD

Preuve de [20.2]. Preuve du lemme de Zorn avec [20.1]

Si tout sous-ensemble totalement ordonné $C \subset X$ admet un majorant, alors en particulier tout sous-ensemble bien ordonné. Par [20.1] il existe donc un élément maximal. CQFD

Preuve de [20.2]. Preuve du théorème du bon ordre avec le lemme de Zorn

On commence avec la définition de l'application "domaine d'une relation" qui à un sous-ensemble d'un produit associe les éléments du premier facteur qui interviennent dans la relation. Plus précisément, pour un ensemble E on définit l'application Dom :

$\mathcal{P}(E \times E) \to \mathcal{P}(E)$ par

$$\mathrm{Dom}(R) = \{\, x \in E \mid \exists y \in E : (x,y) \in R \,\} \ .$$

Il est immédiate, à partir de la définition, qu'on a la propriété

$$\forall R, S \subset E \times E \quad : \quad R \subset S \qquad \Rightarrow \qquad \mathrm{Dom}(R) \subset \mathrm{Dom}(S) \ . \tag{33.36}$$

À l'aide de cette application on définit la collection $\mathcal{B}$ de sous-ensembles bien ordonnés par

$$\mathcal{B} = \{\, R \subset E \times E \mid R \subset \mathrm{Dom}(R) \times \mathrm{Dom}(R) \text{ et } R \text{ est un bon ordre sur } \mathrm{Dom}(R) \,\} \ . \tag{33.37}$$

Sur $\mathcal{B}$ on définit une relation d'ordre $\preccurlyeq$ par

$$R \preccurlyeq S \qquad \Longleftrightarrow \qquad R \subset S \text{ et } \forall x \in \mathrm{Dom}(R)\ \forall y \in \mathrm{Dom}(S) \setminus \mathrm{Dom}(R) : (x,y) \in S \ ,$$

où la dernière condition dit que les éléments dans $\mathrm{Dom}(S) \setminus \mathrm{Dom}(R)$ sont tous plus grand que tous les éléments de $\mathrm{Dom}(R)$.

• La première chose à faire est de montrer que cette relation sur $\mathcal{B}$ est bien une relation d'ordre. Pour cela on commence avec la réflexivité en prenant $R \in \mathcal{B}$. Pour montrer $R \preccurlyeq R$, il faut montrer

$$R \subset R \text{ et } \forall x \in \mathrm{Dom}(R)\ \forall y \in \mathrm{Dom}(R) \setminus \mathrm{Dom}(R) : (x,y) \in R \ .$$

Mais la première condition est évidente, ainsi que la deuxième car $\mathrm{Dom}(R) \setminus \mathrm{Dom}(R)$ est vide.

Pour l'antisymétrie on suppose qu'on a $R \preccurlyeq S$ et $S \preccurlyeq R$, ce qui veut dire qu'on a en particulier $R \subset S$, $S \subset R$, donc $R = S$ comme voulu.

Finalement pour la transitivité on suppose $R \preccurlyeq S$ et $S \preccurlyeq T$ et on veut en déduire $R \preccurlyeq T$. L'hypothèse nous donne en particulier les inclusions $R \subset S$ et $S \subset T$, donc on a bien $R \subset T$. Prenons donc $x \in \mathrm{Dom}(R)$ et $y \in \mathrm{Dom}(T) \setminus \mathrm{Dom}(R)$. Par (33.36) on a les inclusions $\mathrm{Dom}(R) \subset \mathrm{Dom}(S) \subset \mathrm{Dom}(T)$, d'où on déduit l'égalité

$$\mathrm{Dom}(T) \setminus \mathrm{Dom}(R) = \mathrm{Dom}(T) \setminus \mathrm{Dom}(S) \cup \mathrm{Dom}(S) \setminus \mathrm{Dom}(R) \ .$$

Pour y il y a donc deux possibilités : $y \in \mathrm{Dom}(S) \setminus \mathrm{Dom}(R)$ ou $y \in \mathrm{Dom}(T) \setminus \mathrm{Dom}(S)$. Dans le premier cas on a, par $R \preccurlyeq S$, $(x,y) \in S \subset T$ et dans le deuxième cas on a $x \in \mathrm{Dom}(R) \subset \mathrm{Dom}(S)$ et, par $S \preccurlyeq T$, $(x,y) \in S$. Ainsi on a montré la transitivité et donc que $\preccurlyeq$ est bien une relation d'ordre sur $\mathcal{B}$.

• La deuxième chose à montrer est que $(\mathcal{B}, \preccurlyeq)$ vérifie l'hypothèse du lemme de Zorn : tout sous-ensemble totalement ordonné (de $\mathcal{B}$) admet un majorant. Soit donc $\mathcal{C} \subset \mathcal{B}$ un sous-ensemble totalement ordonné. Pour trouver un majorant de $\mathcal{C}$, on définit M comme la réunion de $\mathcal{C}$:

$$M = \cup \mathcal{C}$$

et on tente de montrer que M est un élément de $\mathcal{B}$ et un majorant de $\mathcal{C}$. Pour cela on commence avec la remarque qu'on a (par définition de $\mathcal{B}$)

$$\forall R \in \mathcal{C} : R \subset E \times E \ .$$

Par [5.1] on a donc les inclusions

$$\forall R \in \mathcal{C} \quad : \quad R \subset M \equiv \cup \mathcal{C} \subset E \times E$$

et par l'axiome de la réunion (Z4) on a la propriété

$$\forall (x,y) \in E \times E \quad : \quad (x,y) \in M \quad \Leftrightarrow \quad \exists R \in \mathcal{C} : (x,y) \in R \ . \tag{33.38}$$

Pour montrer qu'on a l'inclusion $M \subset \mathrm{Dom}(M) \times \mathrm{Dom}(M)$, on prend $(x, y) \in M$. Par définition de $\mathrm{Dom}(M)$ on a d'office $x \in \mathrm{Dom}(M)$. Par (33.38) il existe $R \in \mathcal{C}$ tel que $(x, y) \in R$. Mais R est une relation d'ordre sur $\mathrm{Dom}(R)$ et en particulier réflexif, donc on a aussi $(y, y) \in R \subset M$. Il s'ensuit qu'on a $y \in \mathrm{Dom}(M)$, ce qui termine la preuve de l'inclusion $M \subset \mathrm{Dom}(M) \times \mathrm{Dom}(M)$.

Pour montrer que M est un bon ordre sur $\mathrm{Dom}(M)$, il faut montrer les propriétés, en commençant avec la réflexivité. Pour $x \in \mathrm{Dom}(M)$, il existe y tel que $(x, y) \in M$. Par (33.38) il existe donc $R \in \mathcal{C}$ tel que $(x, y) \in R$. Mais R est une relation d'ordre, donc en particulier $(x, x) \in R \subset M$, ce qui montre que M est réflexif.

Pour l'antisymétrie on suppose qu'on a $(x, y) \in M$ et $(y, x) \in M$. Par (33.38) il existe donc $R, S \in \mathcal{C}$ tels que $(x, y) \in R$ et $(y, x) \in S$. Mais $\mathcal{C}$ est totalement ordonné ; on a donc $R \preccurlyeq S$ ou $S \preccurlyeq R$ et en particulier $R \subset S$ ou $S \subset R$. Dans le premier cas on a (x, y) et (y, x) dans S. Mais S est une relation d'ordre, donc on en déduit qu'on doit avoir $x = y$. Dans le deuxième cas les deux éléments sont dans R, mais la conclusion reste le même : $x = y$.

Pour la transitivité on suppose qu'on a $(x, y) \in M$ et $(y, z) \in M$ et on veut en déduire $(x, z) \in M$. Par (33.38) il existe $R, S \in \mathcal{C}$ tels que $(x, y) \in R$ et $(y, z) \in S$. Mais $\mathcal{C}$ est totalement ordonné, donc on a, comme pour l'antisymétrie, $R \preccurlyeq S$ ou $S \preccurlyeq R$ et en particulier $R \subset S$ ou $S \subset R$. Dans le premier cas on a (x, y) et (y, z) dans S, qui est une relation d'ordre, et il s'ensuit qu'on a $(x, z) \in S \subset M$. Dans le deuxième cas on est dans R, mais la conclusion est la même : $(x, z) \in M$.

Pour la propriété d'un bon ordre, prenons $A \subset \mathrm{Dom}(M)$ un sous-ensemble non-vide. Il existe donc $a \in A \subset \mathrm{Dom}(M)$. Par définition de $\mathrm{Dom}(M)$, il existe b tel que $(a, b) \in M$. Par (33.38) il existe $R \in \mathcal{C}$ tel que $(a, b) \in R$. Mais R est un bon ordre sur $\mathrm{Dom}(R)$ et l'ensemble $B = A \cap \mathrm{Dom}(R) \subset \mathrm{Dom}(R)$ n'est pas vide. Il existe donc un élément minimal $m \in B \subset A$:

$$\forall x \in B : (m, x) \in R \ .$$

Pour montrer que m est l'élément minimal dans A on prend $x \in A$ arbitraire. Si on a $x \in \mathrm{Dom}(R)$, alors on a $x \in B$ et donc $(m, x) \in R \subset M$, ce qui est la conclusion souhaitée. Si on n'a pas $x \in \mathrm{Dom}(R)$, il faut utiliser la deuxième propriété de la relation d'ordre $\preccurlyeq$. Comme pour $a \in A$, il existe y tel que $(x, y) \in M$ et (ensuite) $S \in \mathcal{C}$ tel que $(x, y) \in S$. Il s'ensuit qu'on a $x \in \mathrm{Dom}(S)$. Mais $\mathcal{C}$ est totalement ordonné, donc on a $R \preccurlyeq S$ ou $S \preccurlyeq R$. Si on avait $S \preccurlyeq R$, alors on aurait $S \subset R$ et donc $\mathrm{Dom}(S) \subset \mathrm{Dom}(R)$, ce qui est exclu par l'hypothèse $x \notin \mathrm{Dom}(R)$. On a donc $R \subset S$ et la propriété

$$\forall x' \in \mathrm{Dom}(R)\ \forall y' \in \mathrm{Dom}(S) \setminus \mathrm{Dom}(R) : (x', y') \in S \ .$$

Mais on a $m \in \mathrm{Dom}(R)$ et $x \in \mathrm{Dom}(S) \setminus \mathrm{Dom}(R)$, donc $(m, x) \in S \subset M$, ce qui termine la preuve que $A \subset \mathrm{Dom}(M)$ contient un plus petit élément (pour la relation d'ordre M).

• Une fois qu'on sait que M appartient à $\mathcal{B}$, il faut montrer que c'est bien un majorant du sous-ensemble totalement ordonné $\mathcal{C}$. Soit donc $R \in \mathcal{C}$ arbitraire. La définition de M nous donne immédiatement l'inclusion $R \subset M$. Pour l'autre condition dans la définition de la relation d'ordre $\preccurlyeq$, prenons $x \in \mathrm{Dom}(R)$ et $y \in \mathrm{Dom}(M)$. Par définition de $\mathrm{Dom}(M)$, il existe z tel que $(y, z) \in M$, donc (par (33.38)) il existe $S \in \mathcal{C}$ tel que $(y, z) \in S$. Le fait que $\mathcal{C}$ est totalement ordonné implique qu'on a $R \preccurlyeq S$ ou $S \preccurlyeq R$. Si on a $S \preccurlyeq R$, alors on a $S \subset R$, donc $\mathrm{Dom}(S) \subset \mathrm{Dom}(R)$ (33.36), ce qui est exclu par l'hypothèse $y \notin \mathrm{Dom}(R)$. On a

donc $R \preccurlyeq S$ et en particulier la propriété

$$\forall x' \in \mathrm{Dom}(R)\ \forall y' \in \mathrm{Dom}(S) \setminus \mathrm{Dom}(R) : (x', y') \in S \ .$$

Le fait qu'on a $x \in \mathrm{Dom}(R)$ et $y \in \mathrm{Dom}(S) \setminus \mathrm{Dom}(R)$ implique donc $(x, y) \in S \subset M$. Ainsi on a montré que M est un majorant de $\mathcal{C}$ dans $\mathcal{B}$.

• On vient de montrer que tout sous-ensemble totalement ordonné de l'ensemble partiellement ordonné $\mathcal{B}$ admet un majorant. Par le lemme de Zorn il existe donc un élément maximal $P \in \mathcal{B}$. Si on a $\mathrm{Dom}(P) = E$, alors P est un bon ordre sur E comme voulu. Supposons donc qu'on n'a pas $\mathrm{Dom}(P) = E$. Il existe donc $e \in E \setminus \mathrm{Dom}(P)$ et on peut définir $Q \subset E \times E$ par

$$Q = P \ \cup \ (\mathrm{Dom}(P) \cup \{e\}) \times \{e\} \ .$$

Il est immédiat qu'on a $\mathrm{Dom}(Q) = \mathrm{Dom}(P) \cup \{e\}$ et $P \neq Q$. On laisse au lecteur la vérification élémentaire que Q est une relation d'ordre sur $\mathrm{Dom}(Q)$ (il suffit de séparer les cas où un élément de $\mathrm{Dom}(Q)$ appartient à $\mathrm{Dom}(P)$ ou est égal à e). Pour montrer que c'est un bon ordre sur $\mathrm{Dom}(Q)$ on prend $A \subset \mathrm{Dom}(Q)$ non-vide. Si $A \cap \mathrm{Dom}(P) = \emptyset$, alors A ne contient que l'élément e, qui est donc a fortiori le plus petit. Dans le cas contraire, l'ensemble $A \cap \mathrm{Dom}(P)$ contient un plus petit élément $m \in A \cap \mathrm{Dom}(P)$ pour la relation d'ordre P :

$$\forall x \in A \cap \mathrm{Dom}(P) : (m, x) \in P \subset Q \ .$$

Mais si on a $x \in A \setminus \mathrm{Dom}(P)$, alors forcément $x = e$, donc $(m, e) \in Q$ par définition de Q. On a donc pour tous les éléments $x \in A$ l'appartenance $(m, x) \in Q$, ce qui veut dire que $m \in A$ est le plus petit élément de A pour la relation d'ordre Q.

La conclusion est que Q appartient à $\mathcal{B}$ et qu'on a $\mathrm{Dom}(Q) \setminus \mathrm{Dom}(P) = \{e\}$. Il s'ensuit immédiatement qu'on a la propriété

$$\forall x \in \mathrm{Dom}(P)\ \forall y \in \mathrm{Dom}(Q) \setminus \mathrm{Dom}(P) : (x, y) \in Q \ ,$$

simplement parce que $y \in \mathrm{Dom}(Q) \setminus \mathrm{Dom}(P)$ implique $y = e$ et qu'on a $(x, e) \in Q$ pour tout $x \in \mathrm{Dom}(P) \subset \mathrm{Dom}(Q)$. On a donc $P \preccurlyeq Q$ et $P \neq Q$, ce qui est en contradiction avec la maximalité de P. L'hypothèse $\mathrm{Dom}(P) \neq E$ est donc fausse et P est un bon ordre sur E. CQFD

Preuve de [20.2]. Preuve de l'axiome du choix avec le théorème du bon ordre

Soit $g : I \to \mathcal{P}(B) \setminus \{\emptyset\}$ une application d'un ensemble I dans l'ensemble de tous les sous-ensembles non-vides d'un ensemble B. Pour construire une fonction de choix pour g, on invoque le théorème du bon ordre pour obtenir un bon ordre $\leq$ sur B. L'application f est alors définie comme donnant le plus petit élément dans chaque $g(i)$. Plus précisément, on définit f comme la composée de g avec l'application $\min : \mathcal{P}(B) \setminus \{\emptyset\} \to B$ [19.8] :

$$f = \min \circ g : I \to B \ .$$

Par définition de l'application min on a, pour tout $i \in I$, la propriété

$$f(i) = (\min \circ g)(i) = \min(g(i)) \in g(i)$$

comme voulu pour l'axiome du choix. CQFD

Les preuves de §21

Les preuves de §22

Preuve de [22.1]. Si $X \subset A$ et $Y \subset B$ sont deux ensembles tels qu'on a les égalités

$$f[X] = B \setminus Y \qquad \text{et} \qquad g[Y] = X \setminus A \ , \tag{33.39}$$

alors par [??] les applications $f|_X : X \to f[X] = B \setminus Y$ et $g|_Y : Y \to g[Y] = A \setminus X$ sont bijectives. Si on définit l'application $h : A \to B$ par

$$h(a) = f(a) \quad \text{si } a \in X \qquad \text{et} \qquad h(a) = (g|_Y)^{-1}(a) \quad \text{si } a \in A \setminus X,$$

alors h est une bijection comme voulu. Pour trouver de tels ensembles X et Y on présente deux constructions différentes. La différence entre ces deux constructions est que la première utilise la récurrence, et donc implicitement l'axiome de l'infini, ce qui n'est pas le cas pour la deuxième.

Dans la première construction on définit par récurrence une suite décroissante $(C_n)_{n\in\mathbf{N}}$ de sous-ensembles de A et une suite croissante $(D_n)_{n\in\mathbf{N}}$ de sous-ensembles de B. On commence avec $C_0 = A$ et $D_0 = B \setminus f[C_0] = B \setminus f[A]$. Si on a construit C_n et D_n, on pose

$$C_{n+1} = A \setminus g[D_n] \qquad \text{et} \qquad D_{n+1} = B \setminus f[C_{n+1}] \ . \tag{33.40}$$

Cette façon de présenter les choses est la façon habituelle, mais il faut bien vérifier que cela rentre dans le cadre d'une définition par récurrence [7.6] ou [7.8]. Pour le faire, on considère l'ensemble $\mathbf{A}$ défini comme

$$\mathbf{A} = \mathcal{P}(A) \times \mathcal{P}(B) \ ,$$

ainsi que l'élément $(A, B \setminus f[A]) \in \mathbf{A}$ et l'application $F : \mathbf{A} \to \mathbf{A}$ définie par

$$F\big((P,Q)\big) = \big(\,(\,A \setminus g[Q]\ ,\ B \setminus f\big[A \setminus g[Q]\big]\,)\,\big) \ .$$

Avec ces ingrédients on invoque [7.8.iii] pour conclure qu'il existe une application $\varphi : \mathbf{N} \to \mathbf{A}$ vérifiant

$$\varphi(0) = (A, B \setminus f[A]) \equiv (C_0, D_0) \qquad \text{et} \qquad \varphi(n+1) = F\big(\varphi(n)\big) \ .$$

On introduit maintenant les applications $\varphi_A : \mathbf{N} \to \mathcal{P}(A)$ et $\varphi_B : \mathbf{N} \to \mathcal{P}(B)$ par

$$\varphi_A = \pi_A \circ \varphi \qquad \text{et} \qquad \varphi_B = \pi_B \circ \varphi \ ,$$

où π_A et π_B sont les projections canonique $\pi_A : \mathbf{A} \to \mathcal{P}(A)$ et $\pi_B : \mathbf{A} \to \mathcal{P}(B)$ sur les deux facteurs constituants de $\mathbf{A} = \mathcal{P}(A) \times \mathcal{P}(B)$. Si, avec ces définitions, on écrit $C_n = \varphi_A(n)$ et $D_n = \varphi_B(n)$, on obtient l'égalité

$$\varphi(n) = (C_n, D_n)$$

et la condition de récurrence s'écrit comme

$$\begin{aligned}(C_{n+1}, D_{n+1}) = F\big((C_n, D_n)\big) &= \big(\,(\,A \setminus g[D_n]\ ,\ B \setminus f\big[A \setminus g[D_n]\,\big]\,)\,\big) \\ &= \big(\,(\,A \setminus g[D_n]\ ,\ B \setminus f[C_{n+1}]\,)\,\big) \ ,\end{aligned}$$

ce qui est exactement la définition donnée dans (33.40). Notre construction par récurrence rentre donc bien dans le cadre des constructions par récurrence, ce qui veut dire que les suites $(C_n)_{n\in\mathbf{N}}$ et $(D_n)_{n\in\mathbf{N}}$, représentées par les applications φ_A et φ_B, sont bien définies.

Pour montrer que ces deux suites sont bien (dé)croissantes, on note d'abord qu'on a $C_1 \subset A = C_0$. Mais par définition des C_n et D_n on a pour tout $n \in \mathbf{N}$ les implications

$$\begin{aligned} C_{n+1} \subset C_n \quad &\Longrightarrow \quad f(C_{n+1}) \subset f(C_n) \quad \Longrightarrow \quad D_{n+1} \supset D_n \\ &\Longrightarrow \quad g(D_{n+1}) \supset g(D_n) \quad \Longrightarrow \quad C_{n+2} \subset C_{n+1} \ , \end{aligned}$$

ce qui montre par récurrence que ces suites sont (dé)croissantes.

On pose maintenant $X = \cap_{n\in\mathbf{N}} C_n$ et $Y = \cup_{n\in\mathbf{N}} D_n$. Et de nouveau, c'est la définition habituelle ; pour bien rentrer dans le cadre de l'axiome de la réunion on devrait les définir comme

$$X = \cap\, \varphi_A[\mathbf{N}] \qquad \text{et} \qquad Y = \cup\, \varphi_B[\mathbf{N}] \ ,$$

où $\varphi_A[\mathbf{N}] = \{\, C_n \mid n \in \mathbf{N} \,\}$ est l'image de $\mathbf{N}$ par l'application φ_A (et l'analogue pour φ_B).

Pour montrer les égalités (33.39) on fait les calculs

$$f[X] = f\Big[\bigcap_{n\in\mathbf{N}} C_n\Big] \overset{???}{=} \bigcap_{n\in\mathbf{N}} f[C_n] = \bigcap_{n\in\mathbf{N}} (B \setminus D_n) \overset{???}{=} B \setminus \bigcup_{n\in\mathbf{N}} D_n = B \setminus Y$$

et

$$g[Y] = g\Big(\bigcup_{n\in\mathbf{N}} D_n\Big) \overset{???}{=} \bigcup_{n\in\mathbf{N}} g[D_n] = \bigcup_{n\in\mathbf{N}} (A \setminus C_{n+1}) \overset{???}{=} A \setminus \bigcap_{n\in\mathbf{N}} C_{n+1} = A \setminus X \ ,$$

où pour la dernière égalité on a utilisé l'égalité $\bigcap_{n\in\mathbf{N}} C_{n+1} = \bigcap_{n\in\mathbf{N}} C_n$, ce qui est justifié par la décroissance de la suite $(C_n)_{n\in\mathbf{N}}$.

La deuxième construction commence avec la définition de l'ensemble $\mathcal{Z} \subset \mathcal{P}(B)$ par

$$\mathcal{Z} = \{D \subset B \mid f\big[g[D]\big] \subset D \text{ et } B \setminus f[A] \subset D \,\} \ . \tag{33.41}$$

Il est évident que B appartient à $\mathcal{Z}$, donc $\mathcal{Z}$ n'est pas vide. On peut donc invoquer [**??**] et définir Y comme

$$Y = \cap\, \mathcal{Z} \ .$$

Avec ce Y on pose $X = A \setminus g[Y]$. Pour vérifier (33.39) il suffit donc de montrer l'égalité $f[X] = B \setminus Y$. Pour cela on démontre d'abord que Y appartient à $\mathcal{Z}$. Pour l'inclusion $f\big[g[Y]\big] \subset Y$ on fait le raisonnement :

$$\begin{aligned} ???, (33.41) \quad &\Longrightarrow \quad \forall D \in \mathcal{Z} : Y \subset D \text{ et } f\big[g[D]\big] \subset D \\ &\Longrightarrow \quad \forall D \in \mathcal{Z} : f\big[g[Y]\big] \overset{???}{\subset} f\big[g[D]\big] \subset D \\ &\overset{???}{\Longrightarrow} \quad f\big[g[Y]\big] \subset \cap\, \mathcal{Z} = Y \ . \end{aligned}$$

Et pour l'inclusion $B \setminus f[A] \subset Y$ on fait le raisonnement :

$$\forall D \in \mathcal{Z} : B \setminus f[A] \subset D \qquad \overset{???}{\Longrightarrow} \qquad B \setminus f[A] \subset \cap\, \mathcal{Z} = Y \ .$$

Ensuite on montre l'inclusion $B \setminus Y \subset f[X]$ (ce qui équivaut $B \setminus f[X] \subset Y$) :

$$\left.\begin{aligned} f[A] \setminus f[X] = f[A \setminus X] = f\big[g[Y]\big] \subset Y \\ B \setminus f[A] \subset Y \end{aligned}\right\} \quad \Longrightarrow \quad B \setminus f[X] \subset Y \ .$$

En dernier on montre l'inclusion $f[X] \subset B \setminus Y$ et pour cela on montre que $Y \setminus f[X]$ appartient à $\mathcal{Z}$. Si on a réussi cela, on aura, par définition de Y, l'inclusion $Y \subset Y \setminus f[X]$, ce qui implique directement l'inclusion voulue.

On commence avec l'inclusion $B \setminus f[A] \subset Y \setminus f[X]$:

$$B \setminus f[A] \subset Y \text{ et } f[X] \subset f[A] \implies B \setminus f[A] \stackrel{???}{=} \big(B \setminus f[A]\big) \setminus f[X] \subset Y \setminus f[X] \ . \tag{33.42}$$

Et on termine avec l'inclusion $f\big[g[Y \setminus f[X]]\big] \subset Y \setminus f[X]$:

$$g[Y] \subset A \setminus X \implies f\big[g[Y]\big] \subset f[A \setminus X] = f[A] \subset f[X] \subset B \setminus f[X] \ ,$$

mais aussi (parce que $Y \in \mathcal{Z}$)

$$f\big[g[Y]\big] \subset Y$$

et donc

$$f\big[g[Y]\big] \subset Y \setminus f[X] \ .$$

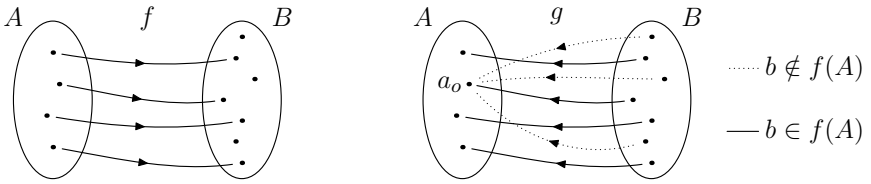
Il s'ensuit qu'on a l'inclusion

$$f\big[g[Y \setminus f[X]]\big] \subset f\big[g[Y]\big] \subset Y \setminus f[X] \ .$$

On a donc montré que $Y \setminus f[X]$ appartient à $\mathcal{Z}$ et comme dit ci-dessus, on en déduit l'inclusion $f[X] \subset B \setminus Y$. Par double inclusion on a donc l'égalité $f[X] = B \setminus Y$.
CQFD

Preuve de [22.3]. Soit $f : A \to B$ une injection et soit $a_o \in A$ un élément arbitraire (qui existe car A n'est pas vide). L'injectivité de f veut dire que pour un $b \in B$ on n'a que deux possibilités : ou bien b n'appartient pas à l'image $f(A)$, ou bien, si b appartient à $f(A)$, il existe un seul $a \in A$ tel que $f(a) = b$. On peut donc définir l'application $g : B \to A$ par

$$g(b) = a \quad \text{si } b \in f(A) \text{ avec } f(a) = b \qquad \text{et} \qquad g(b) = a_o \quad \text{si } b \notin f(A).$$



Vu que chaque $a \in A$ a une image dans B, il est immédiat que g est surjective. Cette application g est un inverse à gauche de f : $g \circ f = id_A$; ce n'est un inverse à droite que si f est une bijection.
CQFD

Preuve de [22.4]. • Si $g : B \to A$ est une surjection, alors pour tout $a \in A$ l'image réciproque $g^{-1}[\{a\}]$ n'est pas vide. On peut donc définir une application $G : A \to \mathcal{P}(B) \setminus \{\emptyset\}$ par

$$G(a) = g^{-1}[\{a\}] \ .$$

Par l'axiome du choix il existe alors une application $f : A \to B$ vérifiant $f(a) \in G(a) = g^{-1}[\{a\}]$ pour tout $a \in A$, et donc $g(f(a)) = a$ pour tout $a \in A$. Autrement dit, on a $g \circ f = id_A$.

DESSIN

Pour montrer que f est injective, on suppose qu'on a $f(a) = f(a')$. Alors on a $a = g(f(a)) = g(f(a')) = a'$, ce qui montre que f est injective.

• Pour déduire l'axiome du choix de la propriété donnée, prenons une application $g : I \to \mathcal{P}(B) \setminus \{\emptyset\}$. L'idée de la preuve est de voir les ensembles $g(i) \subset B$ comme des images réciproques d'une application surjective. Mais les images réciproques d'une surjection sont 2 à 2 disjoints et de réunion l'ensemble source. Par contre, les ensembles $g(i) \subset B$ de l'axiome du choix ne sont ni (forcément) 2 à 2 disjoints, ni (forcément) de réunion B. Pour rentrer dans les conditions de la propriété, il faut donc se ramener à ce cas. Pour cela on définit l'ensemble $C \subset I \times B$ comme

$$C = \{\, (i,b) \in I \times B \mid b \in g(i) \,\} \ .$$

Ensuite on considère l'application $\pi_I : D \to I$ (la projection sur la deuxième composante du produit cartésien) et on constate que c'est une surjection : pour $i \in I$ l'ensemble $g(i)$ n'est pas vide. Il existe donc $b \in g(i)$, donc $(i,b) \in C$ et donc $i = \pi_I\big((i,b)\big)$.

DESSIN

Quand on sait que $\pi_I : C \to I$ est une surjection, on invoque la propriété donnée pour obtenir une injection $F : I \to C$ vérifiant $\pi_I \circ F = id_I$. Cela veut dire que, si on a $F(i) = (j,b) \in C \subset I \times B$, alors $j = \pi_I\big((j,b)\big) = \pi_I(F(i)) = i$. Autrement dit, pour tout $i \in I$ il existe $b \in B$ tel que $F(i) = (i,b)$. Si on pose $f = \pi_B \circ F : I \to B$, la composée de F avec la projection sur la première composante du produit cartésien, alors on peut faire le raisonnement

$$F(i) = (i,b) \in C \qquad \Longrightarrow \qquad f(i) = \pi_B(F(i)) = \pi_B\big((i,b)\big) = b \in g(i) \ ,$$

ce qui montre que f est une fonction de choix. CQFD

Preuve de [22.5]. La preuve utilise l'axiome du choix dans la forme du lemme de Zorn, qu'on applique à un sous-ensemble de $\mathcal{P}(A \times B)$ muni de la relation d'ordre donnée par l'inclusion. Si l'élément maximal n'est pas une injection de A dans B, alors on montre que la relation réciproque est une injection de B dans A. Pour réaliser ce projet on définit $\mathcal{B} \subset \mathcal{P}(A \times B)$ comme

$$\mathcal{B} = \Big\{\, f \subset A \times B \mid \forall a,b,c : \ \big[\ (a,b),(a,c) \in f \ \Rightarrow\ b = c \ \big] \text{ et } \big[\ (a,c),(b,c) \in f \ \Rightarrow\ a = b \ \big] \,\Big\} \ . \tag{33.43}$$

Il y a deux façons d'interpréter cette définition. On peut voir $\mathcal{B}$ comme les relations entre A et B qui sur chaque ligne verticale $\{a\} \times B$ ont au plus un élément (l'intersection $f \cap \{a\} \times B$ ne contient pas deux éléments distincts) et qui sur chaque ligne horizontale $A \times \{c\}$ ont au plus un élément (l'intersection $f \cap A \times \{c\}$ ne contient pas deux éléments distincts). Mais on peut aussi le voir comme les relations qui vérifient la deuxième condition d'une application et la condition d'injectivité d'une application.

On muni l'ensemble $\mathcal{B}$ de la relation d'ordre induite pas l'inclusion. Pour montrer que $\mathcal{B}$ muni de cet ordre vérifie l'hypothèse du lemme de Zorn, on prend un sous-ensemble totalement ordonné $\mathcal{C} \subset \mathcal{B}$ et on définit l'ensemble r comme la réunion de $\mathcal{C}$:

$$r \ \stackrel{\text{déf}}{=} \ \cup\, \mathcal{C} \ .$$

Par définition on a $f \subset A \times B$ pour tout $f \in \mathcal{B}$. Par [5.1] on a donc les inclusions

$$\forall f \in \mathcal{C} \quad : \quad f \subset r \subset A \times B \ .$$

L'ensemble $r \subset A \times B$ est donc un majorant de $\mathcal{C}$ dès qu'on a montré qu'il appartient bien à $\mathcal{B}$. Pour cela on suppose d'abord q'on a $(a,b),(a,c) \in r$. Par l'axiome de la réunion il existe $f,g \in \mathcal{C}$ tels que $(a,b) \in f$ et $(a,c) \in g$. Mais $\mathcal{C}$ est totalement ordonné. On a donc $f \subset g$ ou $g \subset f$. Dans le premier cas on a $(a,b),(a,c) \in g \in \mathcal{B}$ et donc $b = c$ et dans le deuxième cas on a $(a,b),(a,c) \in f \in \mathcal{B}$, donc de nouveau $b = c$. Et pour la deuxième condition le raisonnement est analogue. On suppose qu'on a $(a,c),(b,c) \in r$, donc il existe $f,g \in \mathcal{C}$ tels que $(a,c) \in f$ et $(b,c) \in g$. Mais $\mathcal{C}$ est totalement ordonné, donc on a $f \subset g$ ou $g \subset f$. Dans le premier cas on a $(a,c),(b,c) \in g \in \mathcal{B}$ donc $a = b$ et dans le deuxième cas la conclusion reste inchangé.

L'ensemble $\mathcal{B}$ muni de sa relation d'ordre vérifie donc l'hypothèse du lemme de Zorn. Il existe donc un élément maximal $m \in \mathcal{B}$. Si m vérifie la première condition d'une application, à savoir que pour tout $a \in A$ il existe b tel que $(a,b) \in m$, alors l'appartenance de m à $\mathcal{B}$ nous dit que c'est une injection de A dans B. Supposons donc que m ne vérifie pas cette condition, c'est-à-dire qu'on a la propriété

$$\exists a_o \in A \ \forall b : (a_o,b) \notin m \ . \tag{33.44}$$

Alors on regarde la relation réciproque m^{-1} entre B et A. Par définition de $\mathcal{B}$ cette relation vérifie les deux conditions

$$\forall a,b,c : \ \big[\ (b,a),(c,a) \in m^{-1} \Rightarrow b = c\ \big] \text{ et } \big[\ (c,a),(c,b) \in m^{-1} \Rightarrow a = b\ \big] \ .$$

Autrement dit, cette relation vérifie la deuxième condition d'une application et la condition d'injectivité. Si m^{-1} vérifie aussi la première conditin d'une application, à savoir que pour tout $b \in B$ il existe a tel que $(b,a) \in m^{-1}$, alors m^{-1} est une application injective de B dans A comme voulu.

Pour montrer que cette condition doit être vérifiée, on procède par l'absurde en supposant que cette condition n'est pas vérifiée, c'est-à-dire qu'on a

$$\exists b_o \in B \ \forall a : (b_o,a) \notin m^{-1} \qquad (\text{ce qui est équivalent à } (a,b_o) \notin m) \ . \tag{33.45}$$

On a donc en particulier $(a_o,b_o) \notin m$; l'ensemble $m' = m \cup \{(a_o,b_o\}$ vérifie donc $m \subset m'$ et $m \neq m'$. Pour arriver à une contradiction, il suffit de montrer que m' appartient à $\mathcal{B}$, car ces deux propriétés contredisent la maximalité de m. Pour le faire, prenons donc a,b,c arbitraire et supposons qu'on a $(a,b),(a,c) \in m'$. La définition de m' nous donne $2 \times 2 = 4$ cas à considérer :

$$\begin{aligned}
(a,b),(a,c) \in m \quad &\overset{m \in \mathcal{B}}{\Longrightarrow} \quad b = c \\
(a,b) \in m \text{ et } (a,c) \in \{(a_o,b_o)\} \quad &\Longrightarrow \quad (a,b) \in m \text{ et } a = a_o \quad \text{exclu par (33.44)} \\
(a,b) \in \{(a_o,b_o)\} \text{ et } (a,c) \in m \quad &\Longrightarrow \quad a = a_o \text{ et } (a,c) \in m \quad \text{exclu par (33.44)} \\
(a,b),(a,c) \in \{(a_o,b_o)\} \quad &\Longrightarrow \quad b = c = b_o \ .
\end{aligned}$$

Il s'ensuit que m' vérifie la première condition pour appartenir à $\mathcal{B}$. La vérification de la deuxième condition est similaire et laissée aux bons soins du lecteur (il faut utiliser (33.45) à la place de (33.44)). La conclusion est donc que m' appartient à $\mathcal{B}$ et qu'il est strictement plus grand que m, ce qui contredit la maximalité de m. L'hypothèse que m^{-1} n'est pas une application injective est donc intenable. Ainsi on a montré que si m n'est pas une application injective de A dans B, alors m^{-1} est une application injective de B dans A. CQFD

Les preuves de §23

Les preuves de §24

Preuve de [24.1]. Un élément $f \in A^{B\cup C}$ est une application $f : B \cup C \to A$ et donc en particulier un sous-ensemble du produit $f \subset (B \cup C) \times A$. La définition de la restriction nous donne

$$f|_B = f \cap (B \times A) \qquad \text{et} \qquad f|_C = f \cap (C \times A) \ .$$

Par [5.13] on sait que ces restrictions sont des applications et donc l'application Φ est bien définie. Mais on a plus :

$$\begin{aligned} f &= f \cap \big((B \cup C) \times A\big) = f \cap \big((B \times A) \cup (C \times A)\big) \\ &= \big(f \cap (B \times A)\big) \cup \big(f \cap (C \times A)\big) = f|_B \cup f|_C \ . \end{aligned}$$

Il s'ensuit qu'on a $\Psi \circ \Phi = id$.

Dans l'autre sens, on commence avec la remarque qu'on a les inclusions

$$g \subset B \times A \subset (B \cup C) \times A \qquad \text{et} \qquad h \subset C \times A \subset (B \cup C) \times A \ ,$$

et donc on a bien $g \cup h \subset (B \cup C) \times A$. Pour montrer que cette réunion représente/est une application, on vérifie les conditions. Pour $x \in B \cup C$ on a $x \in B$ ou $x \in C$. Dans le premier cas on invoque le fait que g est une application pour pouvoir conclure qu'il existe $a \in A$ tel que $(x, a) \in g \subset g \cup h$, et dans le deuxième cas on invoque le fait que h est une application pour obtenir l'existence d'un $a \in A$ tel que $(x, a) \in h \subset g \cup h$. Dans les deux cas il existe donc $a \in A$ tel que $(x, a) \in g \cup h$.

Pour la deuxième condition d'une application on suppose qu'on a $(x, a), (x, a') \in g \cup h \subset (B \cup C) \times A$. En particulier on a $x \in B \cup C$ et donc $x \in B$ ou $x \in C$. Si on a $x \in B$, on n'a pas $x \in C$ parce que $B \cap C = \emptyset$. On ne peut donc pas avoir $(x, a) \in h$, ni $(x, a') \in h$. On doit donc avoir $(x, a) \in g$ et $(x, a') \in g$. Mais g est une application, donc on peut en déduire qu'on a $a = a'$. Dans le cas $x \in C$ l'argument est similaire et aboutit à la même conclusion : $a = a'$.

Ainsi on a montré que l'application Ψ est bien une application à valeurs dans $A^{B\cup C}$. Sachant cela, on peut faire le raisonnement

$$h \subset C \times A) \quad \text{et} \quad B \cap C = \emptyset \qquad \Longrightarrow \qquad h \cap (B \times C) = \emptyset \ .$$

Et ensuite on peut faire le calcul

$$\begin{aligned} (g \cup h)|_B &= (g \cup h) \cap (B \times A) = \big(g \cap (B \times A)\big) \cup \big(h \cap (B \times A)\big) \\ &= \big(g \cap (B \times A)\big) = g \ . \end{aligned}$$

Un raisonnement analogue montre qu'on a l'égalité

$$(g \cup h)|_C = h \ ,$$

ce qui montre qu'on a l'égalité $\Psi \circ \Phi = id$. CQFD

Preuve de [24.5]. • (iii) B étant non-vide, il existe $b \in B$. Si on part de $1 \precsim B$, il existe une injection $g : 1 \equiv \{0\} \to B$ et on peut poser $b = g(0)$. Avec ce b on définit l'ensemble $f \subset A \times B$ par

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

Il est immédiat que ce f est une application de A dans B : c'est une application constante. En définissant $G : 1 \to B^A$ par $G(0) = f$, on obtient une injection de 1 dans B^A, c'est-à-dire $1 \precsim B^A$. CQFD

Preuve de [24.8]. On fait le calcul de $\Phi\circ\Psi$ et $\Psi\circ\Phi$, ce qui donne

$$(\Phi\circ\Psi)(B) = \Phi\big(\Psi(B)\big) = \{\, a\in A \mid \mathbf{1}_B(a) = 1 \,\} = B$$
$$(\Psi\circ\Phi)(f) = \Psi\big(\Phi(f)\big) = \mathbf{1}_{\{a\in A|f(a)=1\}} \ .$$

La première ligne nous donne immédiatement l'égalité $\Phi\circ\Psi = id$; pour élucider la deuxième ligne, on applique ces fonctions à un élément $\hat{a}\in A$, ce qui donne

$$\big((\Psi\circ\Phi)(f)\big)(\hat{a}) = \mathbf{1}_{\{a\in A|f(a)=1\}}(\hat{a}) = \begin{cases} 1 & \text{si } \hat{a}\in\{a\in A \mid f(a)=1\} \\ 0 & \text{si } \hat{a}\notin\{a\in A \mid f(a)=1\} \end{cases}$$

$$= \begin{cases} 1 & \text{si } f(\hat{a})=1 \\ 0 & \text{si } f(\hat{a})\neq 1 \end{cases} = \begin{cases} 1 & \text{si } f(\hat{a})=1 \\ 0 & \text{si } f(\hat{a})=0 \end{cases} = f(\hat{a}) \ .$$

Ceci étant vrai pour tout $\hat{a}\in A$, il s'ensuit qu'on a l'égalité $(\Psi\circ\Phi)(f) = f$ et donc, parce que ceci est vrai pour tout $f\in 2^A$, on a l'égalité $\Psi\circ\Phi = id$. Par [**??**] on en déduit que Ψ et Φ sont des bijections vérifiant $\Psi^{-1} = \Phi$ comme annoncé. CQFD

Preuve de [24.9]. Pour une application $f : A\to\mathcal{P}(A)$ définissons le sous-ensemble $B\subset A$ par

$$B = \{a\in A \mid a\notin f(a)\} \ ,$$

ce qui a un sens, car $f(a)$ est un sous-ensemble de A. S'il existe $b\in A$ tel que $f(b) = B$, alors on a deux possibilités :

$$b\in B = f(b) \qquad \text{ou} \qquad b\notin B = f(b) \ .$$

Dans le premier cas, selon la définition de B, on ne pourrait pas avoir $b\in B$, ce qui donne une contradiction. Mais dans le deuxième cas on a aussi une contradiction, car, de nouveau selon la définition de B, on devrait avoir $b\in B$. La conclusion est donc que B n'appartient pas à l'image $f(A)$, ce qui implique que f n'est pas surjective. Il n'existe donc pas de surjection $f : A\to\mathcal{P}(A)$.

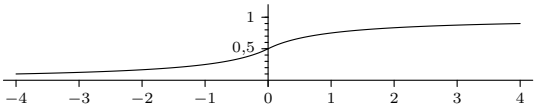
D'autre part, l'application $f : A\to\mathcal{P}(A)$ définie par

$$f(a) = \{a\}$$

est clairement injective, ce qui montre $A\precsim\mathcal{P}(A)$. Si on avait $\mathcal{P}(A)\precsim A$, alors on aurait $A\approx\mathcal{P}(A)$ par [22.1]. Et si on avait $A\approx\mathcal{P}(A)$, on aurait une bijection de A dans $\mathcal{P}(A)$, ce qui est en particulier surjective. Ceci contredit la non-existence d'une surjection. CQFD

Preuve de [24.10]. Il n'est pas difficile de montrer que l'application $f_{a,b} : \mathbf{R}\to\,]a,b[$ définie par

$$f_{a,b}(x) = \frac{a\,(\,|x| - x + 1) + b\,(\,|x| + x + 1)}{2(\,|x|+1)} = \frac{a+b}{2} + \frac{b-a}{2}\cdot\frac{x}{|x|+1}$$



$y = f_{0,0}(x)$

est une bijection, donc en particulier une injection. Avec cette application $f_{a,b}$ on regarde maintenant la suite d'injections

$$]a,b[\xrightarrow{id} [a,b[\xrightarrow{id} [a,b] \xrightarrow{id} \mathbf{R} \xrightarrow{f_{a,b}}]a,b[\ ,$$

où les trois premières applications sont l'identité (qui envoie un élément vers lui-même). En prenant des composées (en boucle) on obtient facilement des injections dans les deux sens entre chaque paire d'ensembles parmi ces quatre. Par [22.1] il existe donc aussi des bijections entre chaque paire.

Pour montrer que ces quatre ensembles sont aussi en bijection avec $\{0,1\}^{\mathbf{N}^*}$, on commence avec la remarque qu'on vient de montrer qu'il y a une bijection entre $\mathbf{R}$ et $[0,1[$. Étant donné que la composée de deux bijections est encore une bijection, il suffit donc de montrer qu'il y a une bijection entre $[0,1[$ et $\{0,1\}^{\mathbf{N}^*}$. Pour faire cela, on considère la suite d'injections

$$[0,1[\xrightarrow{(f_2)^{-1}} \mathcal{DR}_2 \xrightarrow{id} \{0,1\}^{\mathbf{N}^*} \xrightarrow{g} \mathcal{DR}_3 \xrightarrow{f_3} [0,1[\ .$$

Dans cette suite, les applications $f_{2/3} : \mathcal{DR}_{2/3} \to [0,1[$ sont les bijections définies dans [17.7] pour le développement en base 2 (respectivement 3) d'un réel dans $[0,1[$ et l'application g est l'application qui envoie un élément $f \in \{0,1\}^{\mathbf{N}^*}$ (c'est-à-dire une application $f : \mathbf{N}^* \to \{0,1\}$) vers elle-même, mais vue comme application sur $\mathbf{N}^*$ à valeurs dans $\{0,1,2\} \supset \{0,1\}$. Vu que $g(f)$ ne prend jamais la valeur 2, c'est une suite réduite en base 3, donc appartient bien à $\mathcal{DR}_3$. En prenant comme avant des composées et en invoquant [22.1], on obtient des bijections entre chaque paire d'ensembles parmi ces quatre. $\boxed{CQFD}$

Les preuves de §25

Preuve de [25.1]. Si A n'est pas fini, alors il existe une application injective $g : \mathbf{N} \to A$ [??]. Alors l'application $h = f \circ g : \mathbf{N} \to B$ est aussi injective [??], ce qui veut dire que B est aussi un ensemble infini. Cette contradiction montre que A doit être fini. $\boxed{CQFD}$

Preuve de [25.2]. • Pour l'implication directe on fixe n et on définit

$$E = \{\, k \in \mathbf{N} \mid \text{ il existe une injection } f : n \to n+k \,\} \ .$$

Pour $k = 0$ l'application identité $id : n \to n$ est une application bijective (donc injective) de n dans $n = n + 0$. Ce qui veut dire qu'on a $0 \in E$. Supposons maintenant qu'on a $k \in E$. Il existe donc une application injective $f : n \to n + k$. Mais l'application $g : n + k \to S(n + k) = (n + k) \cup \{n + k\}$ définie par $g(j) = j$ est aussi injective. Par [5.7], l'application composée $g \circ f : n \to S(n + k)$ est injective. Mais, par définition de l'addition dans $\mathbf{N}$, on a l'égalité $S(n + k) = n + S(k)$. Il s'ensuit qu'on a $S(k) \in E$ et donc, par récurrence, $E = \mathbf{N}$. Par définition de la relation d'ordre sur $\mathbf{N}$, si $n \leq m$, il existe $k \in \mathbf{N}$ tel que $m = n + k$. Le résultat $E = \mathbf{N}$ nous assure alors qu'il existe une injection de n dans m.

• Pour l'implication réciproque on définit l'ensemble $E \subset \mathbf{N}$ comme

$$E = \{\, n \in \mathbf{N} \mid \forall m \in \mathbf{N} : \big[\text{ il existe } f : n \to m \text{ injective }\big] \ \Rightarrow \ n \leq m \,\} \ ,$$

et on va montrer par récurrence qu'on a l'égalité $E = \mathbf{N}$.

Il est évident qu'on a $0 \in E$, car pour tout $m \in \mathbf{N}$ on a $0 \leq m$. Supposons donc qu'on a $n \in E$. Pour en déduire $S(n) \in E$ on prend $m \in \mathbf{N}$ et on suppose q'il existe une application injective $f : S(n) \to m$. On aura montré l'appartenance $S(n) \in E$ quand on aura montré l'inégalité $S(n) \leq m$. Pour cela on commence avec l'observation qu'on ne peut pas avoir $m = 0 \equiv \emptyset$ car $S(n) \neq \emptyset$ (P5) et il n'existe pas d'application (donc en particulier pas une qui est injective) de $S(n)$ dans $\emptyset$ [4.11]. Par [7.9] il existe donc $k \in \mathbf{N}$ tel que $m = S(k)$. On dispose donc d'une application injective

$$f : n \cup \{n\} \to k \cup \{k\} \ .$$

Danc cette situation il faut bien distinguer *l'élément* $n \in S(n)$ du *sous-ensemble* $n \subset S(n)$ (et de même pour l'élément $k \in S(k)$ et le sous-ensemble $k \subset S(k)$). Pour mieux distinguer ces deux aspects de l'ensemble n (et k), on mettra $_o$ en indice quand on le considère comme *élément* : n_o est *l'élément* $n \in S(n)$ et n (sans l'indice) désigne le sous-ensemble $n \subset S(n)$. Avec cette convention, on a donc une application injective

$$f : n \cup \{n_o\} \to k \cup \{k_o\} \ .$$

Si on considère l'image $f[n]$ par f du sous-ensemble $n \subset S(n)$, il y a deux possibilités : $k_o \notin f[n]$ et $k_o \in f[n]$. Dans le premier cas on aura $f[n] \subset k$, ce qui veut dire que la restriction de f au sous-ensemble $n \subset S(n)$ est une application de n dans k : $f|_n : n \to k$. Par l'hypothèse de récurrence on a donc $n \leq k$, et donc par [8.15] $S(n) \leq S(k) = m$. Ce qui montre qu'on a bien $S(n) \in E$.

Dans le deuxième cas $k_o \in f[n]$ il existe $j \in n$ tel que $f(j) = k_o$. Par l'injectivité de f on ne peut pas avoir $f(n_o) = k_o$, car par [8.8] on a $n_o \equiv n \notin n$, donc $n_o \neq j$.

On a donc $f(n_o) \in k$. Avec ces ingrédients on définit l'application $g : n \to k$ par

$$g(j) = f(n_o) \qquad \text{et} \qquad \forall i \in n \setminus \{j\} : g(i) = f(i) \ .$$

Une fois qu'on a montré que ce g est injective, le même argument que ci-dessus s'applique : par l'hypothèse de récurrence on aura $n \leq k$, donc $S(n) \leq S(k) = m$, donc $S(n) \in E$. Pour montrer l'injectivité de g, prenons $i, i' \in n$ tels que $i \neq i'$. Si ni i ni i' est égale à j, on a $g(i) = f(i)$ et $g(i') = f(i')$. L'injectivité de f garantit alors qu'on a $g(i) \neq g(i')$. Si l'un des deux est égale à j, disons $i' = j$, alors on a $g(i') = f(n_o)$ et $i \neq j$, donc $g(i) = f(i)$. De nouveau par l'injectivité de f on en déduit qu'on a $g(i) \neq g(i')$. Ainsi on a montré l'injectivité de g, ce qui termine la preuve que $S(n)$ appartient à E (sous l'hypothèse que n y appartient). Par récurrence on a donc $E = \mathbf{N}$. CQFD

Preuve de [25.4]. Soit $f : n \to n$ une application injective. Si f n'est pas surjective, il existe $k \in n$ tel que $k \notin f[n]$. Dans ce cas on définit l'application $g : S(n) \to n$ par

$$g(n) = k \qquad \text{et} \qquad \forall j \in n : g(j) = f(j) \ .$$

Comme dans la preuve de [25.2], il faut distinguer *l'élément* $n \in S(n)$ du *sous-ensemble* $n \subset S(n)$. Si de nouveau on fait la distinction en ajoutant l'indice $_o$ à l'élément, on écrit la définition de l'application g comme

$$g(n_o) = k \qquad \text{et} \qquad \forall j \in n : g(j) = f(j) \ .$$

À noter que ceci est bien une application, car on n'a pas $n_o \in n$ [8.8], donc on n'est pas en train de définir l'image $f(n_o)$ de deux façons. Cette application g est injective, car supposons qu'on a $i, i' \in S(n)$ tels que $i \neq i'$. Si ni i ni i' est égale à n_o, on a $g(i) = f(i)$ et $g(i') = f(i')$, donc $g(i) \neq g(i')$ par l'injectivité de f. Si l'un des deux est égale à n_o, disons $i' = n_o$, alors on a $g(i') = k$ et $i \neq n_o$, donc $i \in n$ et $g(i) = f(i)$. Par définition de k on a $f(i) \neq k$, c'est-à-dire $g(i') \neq g(i)$.

Mais si $g : S(n) \to n$ est injective, alors on a $n + 1 = S(n) \leq n$ par [25.2]. La définition de la relation d'ordre sur $\mathbf{N}$ nous donne aussi $n \leq n + 1$, donc (par antisymétrie) $n + 1 = n$, ce qui est impossible [8.7]. Donc l'hypothèse que f n'est pas surjective est intenable et n est un ensemble fini. CQFD

Preuve de [25.8]. • (i) ⇒ (ii) : On prend $m = n$ et on suppose qu'on a une application $g : m \to A$ qui est injective mais pas surjective. Alors la composée avec la bijection f nous donne une application $h = f \circ g : n \to n$ qui est injective mais pas surjective. Ceci contredit le fait que n est un ensemble fini [25.4]. Il s'ensuit que g doit être soit surjective, soit non-injective.

• (ii) ⇒ (i) : On définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, m \in \mathbf{N} \mid \forall g : m \to A : g \text{ surjective ou non-jective} \,\} \ .$$

Par hypothèse E n'est pas vide et contient donc un plus petit élément n [8.17]. Si $n = 0 \equiv \emptyset$, alors il existe une (et une seule) application $g : n \equiv 0 \to A$ qui est injective [4.11]. Mais n est dans E, donc ce g doit être surjective. Il s'ensuit que $g : 0 \to A$ est une bijection et donc que A est un ensemble à $n = 0$ éléments.

Si on a $n \neq 0$, alors il existe $k \in \mathbf{N}$ tel que $n = S(k)$ [7.9]. On ne peut pas avoir $k \in E$, car n est le plus petit élément de E et $k < S(k) = n$ [8.16]. On a donc $k \notin E$, ce qui implique qu'il existe $f : k \to A$ injective mais pas surjective. Il existe donc $a \in A$ tel que $a \notin f[k]$. On peut donc définir l'application $g : n = S(k) \equiv k \cup \{k\} \to A$ par

$$\forall i \in k : g(i) = f(i) \qquad \text{et} \qquad g(k) = a \ .$$

Cette application est injective, car si on a $g(i) = g(j)$ pour $i, j \in n$, on a trois cas possible : (i) $i, j \in k$, ce qui donne l'égalité $f(i) = f(j)$ et donc par l'injectivité de f on a $i = j$, (ii) $i, j \in \{k\}$, ce qui veut dire $i = j$, et (iii) $i \in k$ et $j \in \{k\}$, ce qui donne l'égalité $f(i) = a$, ce qui est impossible car $a \notin f[k]$. Ainsi on a bien montré que $g : n \to A$ est injective. Le fait qu'on a $n \in E$ implique que ce g doit être surjective, donc bijective. Il s'ensuit que A est un ensemble à n éléments. CQFD

Preuve de [25.9]. B étant un ensemble fini à n éléments, il existe une bijection $j : B \to n$. Soit maintenant $g : n \to A$ une application injective, alors la composition $h = j \circ f \circ g : n \to n$ est aussi injective [5.7.i]. Mais n est un ensemble fini, donc h doit être bijective. Il s'ensuit que $j^{-1} \circ h = f \circ g$ est aussi bijective et donc en particulier surjective. Par [5.7.iv] il s'ensuit que f doit être surjective. Mais f est supposée être injective, donc elle est bijective. On en déduit que $f^{-1} \circ h = g$ est bijective et donc en particulier surjective. Au final on a donc montré que si l'application g est injective, elle est aussi surjective. Il s'ensuit que toute application $g : n \to A$ est soit surjective, soit non-injective. Par [25.8] on en déduit qu'il existe $k \in \mathbf{N}$ tel que A est un ensemble fini à k éléments.

Une fois qu'on sait que A est un ensemble fini à k éléments, il existe une bijection $i : A \to k$. La composée $j \circ f \circ i^{-1} : k \to n$ est donc en particulier injective. Par [25.2] il s'ensuit qu'on a $k \leq n$. Si on a $k = n$, alors par le fait que n est un ensemble fini, cette application $j \circ f \circ i^{-1}$ doit être bijective. Il s'ensuit avec [**??**] que $f = j^{-1} \circ (j \circ f \circ i^{-1}) \circ i$ est aussi bijective. CQFD

Preuve de [25.10]. • (i) : On commence avec la preuve que si $A \cap B = \emptyset$, alors on a $\text{card}(A \cup B) = n + m$. Pour cela on fixe l'ensemble A et on fait une récurrence sur m, en définissant l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, m \in \mathbf{N} \mid \forall B : \text{card}(B) = m \text{ et } A \cap B = \emptyset \Rightarrow \text{card}(A \cup B) = n + m \,\} \ .$$

Si $m = 0 \equiv \emptyset$, alors forcément $B = \emptyset$, car si B n'est pas vide, il n'existe pas d'application de B dans $\emptyset$ (et il existe une seule application $f : \emptyset \to \emptyset$ qui en plus est bijective). Donc il existe une bijection de $A \cup B = A$ dans $n = n + 0$. Ce qui montre qu'on a bien $0 \in E$.

Supposons maintenant qu'on a $m \in E$ et qu'on a $\text{card}(B) = S(m)$. Comme dans les preuves de [25.2] et [25.4] on doit bien distinguer *l'élément* $m \in S(m)$ et le *sous-ensemble* $m \subset S(m)$. Comme avant, on le fait en ajoutant l'indice $_o$ pour l'élément. Soit $g : B \to S(m) = m \cup \{m_o\}$ une bijection et soit $b_o \in B$ l'unique élément tel que $g(m_o) = b_o$. Alors on pose $B' = B \setminus \{b_o\}$ et on considère l'application $g|_{B'} : B' \to S(m)$, la restriction de g à B'. Étant donné que $g : B \to S(m)$ est une bijection, il est facile de vérifier que $g|_{B'}$ établit une bijection entre B' et m. L'hypothèse $A \cap B = \emptyset$ implique directement que $A \cap B' = \emptyset$. On peut donc invoquer

l'hypothèse de récurrence et dire qu'il existe une bijection

$$h : A \cup B' \to n + m \ .$$

Mais l'hypothèse $A \cap B = \emptyset$ implique aussi $(A \cup B') \cap \{b_o\} = \emptyset$. On peut donc invoquer [24.1] avec les ensembles $A \cup B'$, $\{b_o\}$ et $S(n+m)$ ainsi que les applications $h : A \cup B' \to n + m \subset S(n + m)$ et $g' : \{b_o\} \to S(n + m)$ définie par

$$g'(b_o) = (n + m)_o \in S(n + m) \equiv (n + m) \cup \{(n + m)_o\} \ .$$

On obtient alors une application $h' = \Psi(h, g') : (A \cup B') \cup \{b_o\} = A \cup B \to S(n+m)$. Étant donné que h est une bijection, il est facile à vérifier que h' est aussi une bijection. Par définition on a donc l'égalité

$$\mathrm{card}(A \cup B) = S(n + m) = n + S(m) \ ,$$

ce qui montre qu'on a $S(m) \in E$. Par récurrence on a donc montré l'égalité $E = \mathbf{N}$ et donc la propriété annoncée.

Supposons maintenant qu'on est dans le cas arbitraire. Alors on a les égalités

$$A \cup B = A \cup (B \setminus A) \qquad \text{et} \qquad A \cap (B \setminus A) = \emptyset \ .$$

Si on considère l'injection canonique (l'inclusion) $i : B \setminus A \to B$, alors selon [25.9] $B \setminus A$ est un ensemble fini à $\ell \leq m = \mathrm{card}(B)$ éléments et on a égalité si et seulement si cette injection est bijective, c'est-à-dire, si $B \setminus A = B$, ce qui est le cas si et seulement si $A \cap B = \emptyset$. Maintenant on invoque la première partie pour conclure qu'on a

$$\mathrm{card}(A \cup B) = \mathrm{card}(A) + \mathrm{card}(B \setminus A) = n + \ell \leq n + m \ ,$$

avec égalité si et seulement si $A \cap B = \emptyset$ comme annoncé.

• (ii) : Comme dans la première partie, on fixe A et on fait une récurrence sur m en posant

$$E = \{\, m \in \mathbf{N} \mid \forall B : \mathrm{card}(B) = m \Rightarrow \mathrm{card}(A \times B) = n \times m \,\} \ .$$

Si $m = 0$, alors on a forcément $B = \emptyset$ et donc $A \times B = \emptyset$ [2.8]. Il s'ensuit qu'on a $\mathrm{card}(A \times B) = 0$. Mais $n \times 0 = 0$ et donc on peut conclure qu'on a $0 \in E$.

Supposons maintenant qu'on a $m \in E$ et qu'on a $\mathrm{card}(B) = S(m)$. Soit donc $g : B \to S(m)$ une bijection, soit $b_o \in B$ l'unique élément vérifiant $g(b_o) = m_o$ et posons $B' : B \setminus \{b_o\}$. Alors $g|_{B'} : B' \to S(m)$ fournit une bijection entre B' et $m \subset S(m)$. On peut donc invoquer l'hypothèse de récurrence qui dit qu'on a $\mathrm{card}(A \times B') = n \times m$. Autrement dit, il existe une bijection $h : A \times B' \to n \times m$.

Il est immédiate qu'on a $A \times B' \cap A \times \{b_o\} = \emptyset$ et $A \times B' \cup A \times \{b_o\} = A \times B$. En plus, si $f : A \to n$ est une bijection, alors l'application $f' : A \times \{b_o\} \to n$ définie par $f'(a, b_o) = f(a)$ l'est aussi, ce qui veut dire qu'on a $\mathrm{card}(A \times \{b_o\}) = n$. On peut donc invoquer la première partie et conclure qu'on a

$$\begin{aligned} \mathrm{card}(A \times B) &= \mathrm{card}(A \times B' \cup A \times \{b_o\}) = \mathrm{card}(A \times B') + \mathrm{card}(A \times \{b_o\}) \\ &= n \times m + n = n \times (m + 1) = n \times S(m) \ . \end{aligned}$$

Ainsi on a montré $S(m) \in E$ et donc par récurrence $E = \mathbf{N}$, ce qui montre la propriété annoncée.

• (iii) : Comme dans les deux premières parties on fixe A et on fait une récurrence sur m en posant

$$E = \{\, m \in \mathbf{N} \mid \forall B : \mathrm{card}(B) = m \Rightarrow \mathrm{card}(A^B) = n^m \,\} \ .$$

Si $m = 0$, alors on doit avoir $B = \emptyset$ et donc A^B ne contient qu'un seul élément [4.11]. Étant donné qu'on a aussi $n^0 = 1$ pour tout $n \in \mathbf{N}$, on vient de montrer qu'on a bien $0 \in E$.

Supposons maintenant $m \in E$ et qu'on a $\mathrm{card}(B) = S(m)$. Comme avant il existe donc une bijection $g : B \to S(m)$ et on définit $b_o \in B$ comme l'unique élément vérifiant $g(b_o) = m_o \in S(m)$ ainsi que $B' = B \setminus \{b_o\}$. Et comme avant l'application $g|_{B'}$ fournit une bijection entre B' et m. Par hypothèse de récurrence il existe donc une bijection $h : A^{B'} \to n^m$. On vérifie aussi facilement que l'application $k : A^{\{b_o\}} \to A$ définie comme $k(\varphi) = \phi(b_o)$ est une bijection. On a donc $\mathrm{card}(A^{B'}) = n^m$ et $\mathrm{card}(A^{\{b_o\}}) = n$. Par l'étape précédente on peut donc conclure qu'on a

$$\mathrm{card}(A^{B'} \times A^{\{b_o\}}) = n^m \times n = n^{m+1} = n^{S(m)} \ .$$

Mais il est évident qu'on a $B' \cap \{b_o\} = \emptyset$, ce qui nous permet d'appliquer [24.1] pour obtenir une bijection

$$A^B = A^{B' \cup \{b_o\}} \to A^{B'} \times A^{\{b_o\}} \ .$$

Avec [25.5] et [25.6] on peut donc conclure qu'on a l'égalité

$$\mathrm{card}(A^B) = n^{S(m)} \ ,$$

ce qui montre qu'on a $S(m) \in E$. Ainsi s'achève la preuve par récurrence qu'on a $E = \mathbf{N}$ et donc la preuive de la dernière propriété. CQFD

Preuve de [25.11]. On fixe $m \in \mathbf{N}$ et on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, k \in \mathbf{N} \mid f(m) \leq_A f(m+k) \,\} \ .$$

Si on a $m \leq n$, alors par [8.14] il existe $k \in \mathbf{N}$ tel que $n = m + k$. Donc si $A = \mathbf{N}$ on peut conclure qu'on a $f(m) \leq_A f(n)$. La preuve de l'égalité $E = \mathbf{N}$ se fait par récurrence.

Il est évident qu'on a $0 \in E$, car $m + 0 = m$ et donc $f(m) = f(m + 0)$ et a fortiori $f(m) \leq f(m + 0)$. Supposons donc qu'on a $k \in E$. Alors par définition de l'addition (8.3) on a

$$f(m) \overset{\text{hyp. réc.}}{\leq_A} f(m+k) \overset{\text{hyp. gén.}}{\leq_A} f\big(S(m+k)\big) \overset{(8.3)}{=} f\big(m + S(k)\big) \ .$$

Par la transitivité d'une relation d'ordre il s'ensuit qu'on a $S(k) \in E$. CQFD

Preuve de [25.12]. Selon [25.8] il suffit de montrer qu'il existe $m \in \mathbf{N}$ tel que toute application $f : m \to A$ est soit surjective, soit non-injective. On le fait par l'absurde en supposant qu'il n'existe pas un tel m et on tente d'en déduire l'existence d'une application injective $f : \mathbf{N} \to A$. Par [7.10] l'ensemble A serait infini, en contradiction avec le fait que A est un ensemble fini.

On suppose donc que pour tout $n \in \mathbf{N}$ il existe une application $f_n : m \to A$ qui est injective mais pas surjective. Pour respecter les règles de l'art, il faut invoquer l'axiome du choix dénombrable. Pour cela on considère l'ensemble $I \subset \mathcal{P}(\mathbf{N} \times A)$ défini par

$$I = \{\, g \in \mathcal{P}(\mathbf{N} \times A) \mid \exists n \in \mathbf{N} : g \subset n \times A \text{ et } g \text{ est une application de } n \text{ dans } A \text{ injective mais pas surjective} \,\} \ , \tag{33.46}$$

et dans I on considère les sous-ensembles $I_n \subset I$ définis par

$$I_n = \{\, g \in I \mid g : n \to A \,\} \ .$$

On a donc une application $\Phi : \mathbf{N} \to \mathcal{P}(I)$, $\Phi(n) = I_n$ et notre hypothèse dit que chaque I_n n'est pas vide. Dans ce cas l'axiome du choix dénombrable nous donne une application $\phi : \mathbf{N} \to I$ vérifiant $\phi(n) \in I_n$. Par définition de I et de I_n l'élément $f_n \equiv \phi(n)$ est une application de n dans A, injective mais pas surjective.

Si on définit l'ensemble $A_n = f_n[n] \subset A$ comme l'image de n sous l'application injective f_n, alors $f_n : n \to A_n$ est une bijection [5.11], donc A_n est un ensemble fini à n éléments. On a donc des ensembles avec de plus en plus d'éléments. L'idée intuitive est de construire par récurrence une application injective $f : \mathbf{N} \to A$ par la procédure suivante. Si on connaît $f(0), \ldots, f(n-1)$, qui constituent n éléments distincts de A, alors l'ensemble A_{n+1} contient $n+1$ éléments, donc au moins un élément distinct des $f(0), \ldots, f(n-1)$. On choisit un tel élément dans A_{n+1} comme image $f(n)$ et on aura trouvé $n+1$ éléments distincts $f(0), \ldots, f(n)$ dans A. Le problème avec cette approche est qu'on fait un nombre dénombrable de fois un choix (celui de l'élément dans A_{n+1} qui n'était pas encore dans la liste) et que ce choix dépend des choix qu'on a fait avant. Ne connaissant rien sur les application f_n, choisir d'avance un élément $a_n \in A_{n+1}$ pour tout $n \in \mathbf{N}$ ne garantit pas que ces éléments sont tous distincts. Par exemple, $f(1)$ contient un seul élément, $f(2)$ en contient deux et $f(3)$ en contient trois. Mais rien ne nous garantit que les trois éléments de $f(3)$ sont distincts des trois éléments qu'on trouve dans $f(1)$ et $f(2)$ ensemble. Pour pouvoir appliquer l'axiome du choix dénombrable, il faut donc ruser pour être sûr qu'on obtient des éléments distincts.

L'idée est de sauter des ensembles dans la liste des A_n. A_1 contient un élément et A_2 en contient deux. Donc il y a un élément dans A_2 différent de l'élément dans A_1. A_3 contient 3 éléments et on ne peut pas affirmer directement qu'il y a un élément différent des éléments dans A_1 et A_2 réuni. Bien sûr, une fois qu'on a choisi un élément dans A_2, on est sûr qu'il y a dans A_3 un élément différent des deux éléments choisis dans A_1 et A_2. Mais cela nous ne permet pas d'appliquer l'axiome du choix (dénombrable). Par contre, dans A_4 il y a 4 éléments, donc forcément un élément différent des trois éléments dans A_1 et A_2 réuni. On peut donc choisir cet élément (le troisième), indépendamment des deux éléments choisis préalablement dans A_1 et A_2. Ensuite, il faut trouver un quatrième élément distinct des trois éléments choisis dans, successivement, A_1, A_2 et A_4. Ne sachant pas quels éléments on a choisi, ces trois ensembles contiennent (au plus) $1+2+4=7$ éléments. Pour être sûr de trouver un élément distinct, on passe donc à A_8. Et là on est sûr qu'il y a un (quatrième) élément distinct des trois éléments choisi préalablement dans $A_1 \cup A_2 \cup A_4$, indépendamment de ce choix. Pour l'élément suivant, il faut éviter les éléments de A_1, A_2, A_4 et A_8, ce qui représente (au plus) $1+2+4+8=15$ éléments. On passe donc à A_{16} pour être sûr de trouver un élément distinct. Ce qui suit est la mise en forme de cette procédure, en respectant les règles de la construction par récurrence et de l'axiome du choix dénombrable.

On commence avec la définition par récurrence des ensembles $B_n \subset A$ comme

$$B_0 = A_1 \qquad \text{et} \qquad B_{S(n)} = B_n \cup A_{2^{S(n)}} \ .$$

Formellement on invoque [7.8.ii] avec l'élément $A_1 \in \mathcal{P}(A)$ et l'application $\mathbf{N} \times \mathcal{P}(A) \to \mathcal{P}(A)$ définie comme

$$(n, X) \mapsto X \cup A_{2^{S(n)}} \ .$$

Ensuite on définit les ensembles $C_n \subset A$ par

$$C_0 = B_0 \qquad \text{et} \qquad \forall n \in \mathbf{N} : C_{S(n)} = B_{S(n)} \setminus B_n = A_{2^{n+1}} \setminus B_n \ . \tag{33.47}$$

Par [7.8.iii] ceci définit C_n pour tout $n \in \mathbf{N}$. Le but est de montrer que les ensembles C_n sont 2 à 2 disjoints et non-vides. L'invocation de l'axiome du choix dénombrable à l'application $n \mapsto C_n$ nous fournit alors l'application injective $f : \mathbf{N} \to A$ recherchée.

Commençons avec la preuve par récurrence qu'on a $\forall n \in \mathbf{N} : B_n \subset B_{S(n)}$, ce qui est une trivialité, car on a par définition

$$B_n \subset B_n \cup A_{2^{S(n)}} = B_{S(n)} \ .$$

Par [25.11] on en déduit l'implication

$$\forall m, n \in \mathbf{N} : m \leq n \ \Rightarrow \ B_m \subset B_n \ . \tag{33.48}$$

Soit maintenant $m, n \in \mathbf{N}$ deux entier naturels distincts. Sans perte de généralité on peut supposer qu'on a $m < n$ et donc en particulier $n \neq 0$. Il existe donc $k \in \mathbf{N}$ tel que $n = S(k)$ [7.9] et, par [8.16], on a l'inégalité $m \leq k$. On a donc les relations

$$C_m \overset{(33.47)}{\subset} B_m \overset{(33.48)}{\subset} B_k \qquad \text{et} \qquad C_n = C_{S(k)} \overset{(33.47)}{=} A_{2^{k+1}} \setminus B_k \ .$$

Il s'ensuit qu'on a $C_m \cap C_n = \emptyset$, c'est-à-dire que les ensembles C_n sont 2 à 2 disjoints. Pour montrer que les C_n ne sont pas vides, on montre d'abord par récurrence que chaque B_n contient strictement moins d'éléments que $A_{2^{n+1}}$. Plus précisément : on montre que chaque B_n est un ensemble fini à $k_n \in \mathbf{N}$ éléments avec $k_n < 2^{n+1}$.

Si on commence avec $B_0 = A_1 = f_1[1]$, on constate que $f_1 : 1 \to B_0$ est une bijection, donc B_0 est un ensemble fini à 1 élément et $1 < 2 = 2^{0+1}$. Supposons maintenant (hypothèse de récurrence) que B_n est un ensemble fini à k éléments avec $k < 2^{n+1}$. On sait aussi que $f_{2^{n+1}} : 2^{n+1} \to A_{2^{n+1}} = f_{2^{n+1}}[2^{n+1}]$ est une bijection et donc que $A_{2^{n+1}}$ est un ensemble fini à 2^{n+1} éléments. Par [**??**] on en déduit que $B_{S(n)} = B_n \cup A_{2^{n+1}}$ est un ensemble fini à k' éléments avec

$$k' \leq k + 2^{n+1} < 2^{n+1} + 2^{n+1} = 2 \times 2^{n+1} = 2^{S(n)+1} \ .$$

Ainsi on a montré par récurrence que chaque B_n est fini avec un nombre d'éléments strictement inférieur à 2^{n+1}. Par [**??**] il s'ensuit qu'on ne peut pas avoir $A_{2^{n+1}} \subset B_n$, ce qui veut dire que l'ensemble C_n n'est pas vide.

Une fois qu'on sait que les ensembles C_n ne sont pas vides, on peut invoquer l'axiome du choix dénombrable une deuxième fois pour obtenir des éléments $a_n \in C_n$. Le fait que les C_n sont 2 à 2 disjoints implique que ces a_n sont tous distincts. L'application $f : \mathbf{N} \to A$, $f(n) = a_n$ est donc injective. Par [7.10] ceci implique que l'ensemble A est infini, contraire au fait que A est un ensemble fini. L'hypothèse du départ est donc fausse, ce qui veut dire qu'il existe $n \in \mathbf{N}$ tel que A est un ensemble fini à n éléments. *CQFD*

Les preuves de §26

Preuve de [26.3]. On donnera deux preuves, une rapide et une directe. La preuve rapide utilise la dichotomie ensemble fini-infini : si A est fini il existe $n \in \mathbf{N}$ tel que A est un ensemble fini à n éléments [25.12]. Et si A est un ensemble infini, il existe une application injective $\psi : \mathbf{N} \to A$ [7.10]. Mais par hypothèse il existe aussi une application injective $g : A \to \mathbf{N}$, donc il existe une bijection $h : A \to \mathbf{N}$ [22.1].

Le fait qu'on invoque [25.12] dans cette preuve implique qu'on a besoin de l'axiome du choix dénombrable. Mais une preuve qui part directement de la définition d'un ensemble dénombrable a aussi besoin de cet axiome, comme on peut le voir dans la deuxième preuve qu'on donne ici.

On part donc de l'hypothèse qu'il existe une injection $g : A \to \mathbf{N}$. S'il existe $\ell \in \mathbf{N}$ tel que pour tout $a \in A$ on a $g(a) < \ell$, alors on définit l'ensemble $E \subset \mathbf{N}$ par

$$E = \{\, m \in \mathbf{N} \mid \exists f : A \to \mathbf{N} \text{ injective } f[A] \subset m \,\} \ .$$

Par hypothèse E n'est pas vide, car $g[A] \subset \ell$ [26.2]. Il existe donc un plus petit élément $n \in E$ [8.17]. Par définition de E il existe donc une application injective $f : A \to n$ et il suffit de montrer que ce f est bijective pour montrer que A est un ensemble fini à n éléments.

Supposons que f n'est pas bijective. Étant injective, elle n'est donc pas surjective. Il existe donc $k \in n$ tel que $k \notin f[A]$. Ceci implique en particulier qu'on a $n \neq \emptyset \equiv 0$, donc il existe $m \in \mathbf{N}$ tel que $n = S(m)$ [7.9]. Comme dans les preuves de [25.2] et [25.4] il faut maintenant bien distinguer *l'élément* $m \in S(m)$ du *sous-ensemble* $m \subset S(m)$, qu'on fait de nouveau en ajoutant l'indice $_o$ quand on le considère comme élément. On a donc une application injective

$$f : A \to m \cup \{m_o\} = n \ .$$

Si $m_o \in S(m)$ n'est pas dans l'image de f, alors $f[A] \subset m$. Il s'ensuit qu'on a $m \in E$ et $m < n$, ce qui contredit l'hypothèse de minimalité de n. Par contre, si $m_o \in f[A]$, il existe, par la non-surjectivité de f, $k \in m \subset S(m)$ tel que $k \notin f[A]$ et il existe $a \in A$ tel que $f(a) = m_o$. L'injectivité de f implique qu'on a la propriété

$$\forall b \in A : b \neq a \ \Rightarrow \ f(b) \neq m_o \ .$$

On peut donc définir l'application $f' : A \to m$ par

$$f'(a) = k \qquad \text{et} \qquad \forall b \in A : b \neq a \ \Rightarrow \ f'(b) = f(b) \ .$$

Cette application est injective, car si $b \neq b'$ avec $b, b' \in A \setminus \{a\}$, alors $f'(b) = f(b) \neq f(b') = f'(b')$ par l'injectivité de f, et si $b \in A \setminus \{a\}$, alors $f'(b) \neq m_o = f'(a)$. Il s'ensuit, comme avant, qu'on a $m \in E$ et $m < n$ en contradiction avec la minimalité de n. La conclusion inévitable est que l'application f est aussi surjective. Ainsi on a trouvé une application bijective $f : A \to n$, ce qui montre que A est un ensemble fini à n éléments [25.7].

Reste donc la cas où il n'existe pas $\ell \in \mathbf{N}$ tel que pour tout $a \in A$ on a $g(a) < \ell$. Par contraposée on a donc la condition

$$\forall m \in \mathbf{N} \ \exists a \in A \ : \ f(a) \geq m \ . \tag{33.49}$$

Si on définit l'application $F : \mathbf{N} \to \mathcal{P}(A)$ par

$$F(n) = \{\, a \in A \mid f(a) \geq n \,\} \ ,$$

alors par hypothèse on a $F(n) \neq \emptyset$. On peut donc invoquer l'axiome du choix dénombrable pour obtenir une application $\phi : \mathbf{N} \to A$ vérifiant

$$\forall n \in \mathbf{N} : \phi(n) \in F(n) \ ,$$

ce qui est équivalent à $f(\phi(n)) \geq n$. Pour en déduire l'existence d'une application injective $\mathbf{N} \to A$, on invoque la construction par récurrence [7.8.iii] pour obtenir une application $\psi : \mathbf{N} \to A$ vérifiant

$$\psi(0) = \phi(0) \qquad \text{et} \qquad \psi(S(n)) = \phi(f(\psi(n)) + 1) \ .$$

Pour montrer l'injectivité de ψ, on constate d'abord que l'application $\mathbf{N} \to \mathbf{N}$, $n \mapsto f(\psi(n))$ est strictement croissante :

$$\forall n \in \mathbf{N} : f(\psi(S(n))) = f(\phi(f(\psi(n)) + 1)) \geq f(\psi(n)) + 1 > f(\psi(n)) \ .$$

On en déduit facilement par récurrence (sur $k \in \mathbf{N}$) la propriété

$$\forall k, n \in \mathbf{N} : f(\psi(S(n) + k)) > f(\psi(n)) \ . \tag{33.50}$$

Mais l'ensemble $\{m \in \mathbf{N} \mid \exists k \in \mathbf{N} : m = S(n) + k\}$ est, par définition de la relation d'ordre, égale à l'ensemble $\{m \in \mathbf{N} \mid m \geq S(n)\}$, ce qui est égale à l'ensemble $\{m \in \mathbf{N} \mid m > n\}$ par [8.16]. La propriété (33.50) peut donc s'écrire comme

$$\forall m, n \in \mathbf{N} : m > n \ \Rightarrow \ f(\psi(m)) > f(\psi(n)) \ . \tag{33.51}$$

Supposons maintenant qu'on a $\psi(m) = \psi(n)$. Il s'ensuit qu'on a l'égalité

$$f(\psi(m)) = f(\psi(n)) \ ,$$

ce qui n'est possible que si $m = n$, car sinon on aurait $m < n$ ou $m > n$ et par [33.51] on aurait $f(\psi(m)) \neq f(\psi(n))$.

La conclusion est donc que $\psi : \mathbf{N} \to A$ est injective. Avec l'application injective $g : A \to \mathbf{N}$ et [22.1] on en déduit l'existence d'une bijection entre $\mathbf{N}$ et A. CQFD

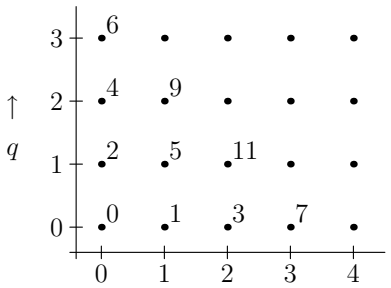
Preuve de [26.4]. L'énoncé dit qu'il existe une bijection entre $\mathbf{N}^2$ et $\mathbf{N}$; on va en donner deux. La première est facile à comprendre et repose sur la théorie (très élémentaire) des nombres. Chaque entier non-nul s'écrit d'une façon unique comme un produit d'une puissance de 2 et un nombre impair (il suffit de diviser par 2 jusqu'à ce qu'on obtienne un nombre impair). On a donc

$$\forall n \in \mathbf{N}^* \ \exists p, q \in \mathbf{N} \ : \ n = 2^p \cdot (2q + 1) \ .$$

L'existence et unicité de cette écriture montre que l'application $n \mapsto (p, q)$ est une bijection entre $\mathbf{N}^*$ et $\mathbf{N} \times \mathbf{N}$. En décalant d'un cran en posant

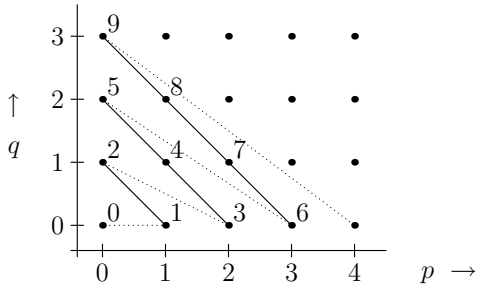
$$f : \mathbf{N} \times \mathbf{N} \to \mathbf{N} \qquad , \qquad f(p, q) = 2^p \cdot (2q + 1) - 1$$

on obtient une bijection entre $\mathbf{N} \times \mathbf{N}$ et $\mathbf{N}$ comme voulu.



la fonction $f(p, q) = 2^p \cdot (2q + 1) - 1$

La deuxième bijection est plus compliquée à établir, bien que visuellement plus claire : on compte les points dans le produit $\mathbf{N} \times \mathbf{N}$ vu comme sous-ensemble du premier quadrant du plan $\mathbf{R}^2$ en passant par les anti-diagonales successives (qui contiennent successivement 1, 2, 3, ...éléments).



La formule explicite qui donne cette bijection $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ est donnée par

$$f(p,q) = \tfrac{1}{2}(p+q)(p+q+1) + q \ .$$

En inspectant le dessin on vérifie aisément que cette formule correspond au comptage donné. Mais la preuve que c'est bien une bijection est un peu plus longue. On commence avec l'observation que la suite $(a_n)_{n\in\mathbf{N}}$ définie par $a_n = \frac{1}{2}n(n+1)$ est une suite strictement croissante d'entiers vérifiant $a_0 = 0$ et $a_{n+1} = a_n + (n+1)$ (c'est la suite donnée par $a_n = \sum_{i=0}^{n} i$). Cette suite a donc la propriété suivante :

(33.52) pour tout $m \in \mathbf{N}$ il existe un unique $n \in \mathbf{N}$ tel que $a_n \leq m < a_{n+1}$.

Pour ce n on a donc $0 \leq m - a_n < a_{n+1} - a_n = n+1$. Si on pose $q = m - a_n$ et $p = n - q$ on aura donc $f(p,q) = m$, ce qui montre la surjectivité de f. Pour l'injectivité on note d'abord qu'on a les inégalités

$$c_{p+q} \leq f(p,q) = c_{p+q} + q < c_{p+q} + (p+q+1) = c_{p+q+1} \ .$$

Donc si on a l'égalité $f(p,q) = f(a,b)$, on a les inégalités $c_{p+q} \leq f(a,b) < c_{p+q+1}$ et $c_{p+q} \leq f(a,b) < c_{p+q+1}$. L'unicité de n dans (33.52) implique alors qu'on a l'égalité $p+q = a+b$. Mais alors on a l'égalité

$$q = f(p,q) - c_{p+q} = f(a,b) - c_{a+b} = b$$

et donc aussi $p = a$. Ainsi on a montré que f est injective. CQFD

Preuve de [26.6]. Par hypothèse il existe une application injective $f : I \to \mathbf{N}$ et pour chaque $i \in I$ il existe une application injective $g_i : f(i) \to \mathbf{N}$. Par définition de la réunion, on a la propriété

$$a \in R \qquad \Longleftrightarrow \qquad \exists A \in \phi[I] : a \in A \qquad \Longleftrightarrow \qquad \exists i \in I : a \in A_i \ .$$

L'idée de la preuve est de définir une application injective $\psi : R \to \mathbf{N} \times \mathbf{N}$ par

$$\psi(a) = \big(f(i), g_i(a)\big) \qquad \text{quand } a \in A_i \equiv \phi(i) \ .$$

Si on compose ce ψ avec une bijection $F : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ [26.4], on obtient une application injective de R dans $\mathbf{N}$ comme voulue [5.7]. Le problème avec cette définition de ψ est que l'indice $i \in I$ n'est pas (forcément) unique, car les ensembles A_i ne sont pas (forcément) disjoints ; un élément $a \in R$ peut appartenir à plusieurs de ces ensembles. Pour en faire une définition correcte, on utilise la dénombrabilité de I pour choisir "le premier" $i \in I$ tel que $a \in A_i \equiv \phi(i)$. Voici les détails.

On définit, pour chaque $a \in R$, l'ensemble $I_a \subset I$ par

$$I_a = \{\, i \in I \mid a \in A_i \,\} \ .$$

Si on veut être très précis, on définit une application $\Phi : R \equiv \cup\phi[I] \to \mathcal{P}(I)$ par

$$\forall a \in R : \Phi(a) = I_a \equiv \{\, i \in I \mid a \in A_i \,\} \ .$$

Par définition de la réunion $R \equiv \cup\phi[I]$, aucun des I_a n'est vide, donc l'image $f[I_a]$ n'est pas vide non plus. Par [8.17] il existe donc un (unique) élément minimal n_a dans chaque $f[I_a]$:

$$\forall i \in I_a : f(i) \geq n_a \ .$$

Par définition de l'image $f[I_a]$, il existe $i_a \in I_a$ tel que $f(i_a) = n_a$ et par l'injectivité de f cet i_a est unique. Maintenant qu'on a trouvé notre (unique) $i_a \in I_a$, on peut définir correctement l'application $\psi : R \to \mathbf{N} \times \mathbf{N}$ par

$$\psi(a) = \big(n_a, g_{i_a}(a)\big) \ .$$

On peut aussi, en vue de la discussion précédente, caractériser ψ par

$$\psi(a) = (n,m) \qquad \Longleftrightarrow \qquad \exists i \in I : \Big(\, n = f(i) \text{ et } m = g_i(a) \text{ et } a \in A_i \text{ et } \big(\, \forall j \in I : a \in A_j \ \Rightarrow \ f(j) \geq f(i) \, \big) \Big) \ . \tag{33.53}$$

Pour montrer que ce ψ est injective, on suppose qu'on a $\psi(a) = \psi(b) = (n,m)$. Par définition ceci implique en particulier qu'il existe $i, j \in I$ tels que

$$a \in A_i \quad , \quad b \in A_j \quad , \quad f(i) = f(j) = n \quad \text{et} \quad g_i(a) = g_j(b) = m \ .$$

Par l'injectivité de f on a $i = j$, ce qui nous donne l'égalité $g_i(a) = g_i(b)$. Mais chaque g_i est injective, donc ceci implique $a = b$.

Pour terminer, soit $F : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ une bijection (il en existe par [26.4]). F étant en particulier injective, on peut invoquer [5.7] pour déduire que la composée $F \circ \psi : R \to \mathbf{N}$ est une application injective. CQFD

Preuve de [26.7]. • La définition de $\mathbf{Z}$ comme ensemble des classes d'équivalences nous donne l'équivalence

$$m \in \mathbf{Z} \qquad \Longleftrightarrow \qquad \exists k, \ell \in \mathbf{N} : m = [[\, k, \ell \,]]_{\mathbf{Z}} \ .$$

On a donc l'égalité (informelle)

$$\mathbf{Z} = \bigcup_{\ell \in \mathbf{N}} \{\, m \in \mathbf{Z} \mid \exists k \in \mathbf{N} : m = [[\, k, \ell \,]]_{\mathbf{Z}} \,\} \ ,$$

qui est une réunion dénombrable d'ensembles dénombrables, car chaque ensemble $\{\, [[\, k, \ell \,]]_{\mathbf{Z}} \mid k \in \mathbf{N} \,\}$ est en bijection avec $\mathbf{N}$ donc dénombrable. Pour bien rentrer dans la forme officielle de [26.6], on définit l'application $\phi : \mathbf{N} \to \mathcal{P}(\mathbf{Z})$ par

$$\phi(\ell) = \{\, m \in \mathbf{Z} \mid \exists k \in \mathbf{N} : m = [[\, k, \ell \,]]_{\mathbf{Z}} \,\} \ .$$

Ensuite on définit, pour chaque $\ell \in \mathbf{N}$, l'application $g_\ell : \mathbf{N} \to \phi(\ell)$ par

$$g_\ell(k) = [[\, k, \ell \,]]_{\mathbf{Z}} \ .$$

Par définition de l'ensemble $\phi(\ell)$, l'application g_ℓ est surjective. Mais elle est aussi injective car

$$g_\ell(k) = g(k') \quad \Leftrightarrow \quad [[\, k, \ell \,]]_{\mathbf{Z}} = [[\, k', \ell \,]]_{\mathbf{Z}} \quad \Leftrightarrow \quad k + \ell = k' + \ell \quad \overset{[8.6]}{\Rightarrow} \quad k = k' \ .$$

C'est donc une application bijective ; l'application réciproque $g_\ell^{-1} : \phi(\ell) \to \mathbf{N}$ est donc aussi bijective et en particulier injective. Il s'ensuit que $\phi(\ell)$ est un ensemble dénombrable pour chaque $\ell \in \mathbf{N}$. L'ensemble $\mathbf{N}$ étant lui même aussi dénombrable, on peut invoquer [26.6] et conclure que la réunion $R \equiv \cup\phi[\mathbf{N}]$ est dénombrable. Mais on a les équivalences

$$\begin{aligned} m \in R \quad &\iff \quad \exists A \in \phi[\mathbf{N}] : m \in A \quad \iff \quad \exists \ell \in \mathbf{N} : m \in \phi(\ell) \\ &\iff \quad \exists \ell \in \mathbf{N}\ \exists k \in \mathbf{N} : m = [[\, k, \ell \,]]_{\mathbf{Z}} \quad \iff \quad m \in \mathbf{Z} \ , \end{aligned}$$

ce qui montre qu'on a l'égalité $\mathbf{Z} = \cup\phi[\mathbf{N}] \equiv \cup_{\ell\in\mathbf{N}}\phi(\ell)$.

• Une autre façon de montrer que $\mathbf{Z}$ est dénombrable est d'établir directement une injection $f : \mathbf{Z} \to \mathbf{N}$. Une application possible est donnée par la formule

$$f(m) = 2 \times m \quad \text{quand } m \geq 0 \qquad \text{et} \qquad f(m) = 1 + 2 \times (-m) \quad \text{quand } m < 0.$$

Par [11.27], [11.32.iv] et [11.29] cette application prend bien ses valeurs dans $\mathbf{N} \subset \mathbf{Z}$. Pour montrer rigoureusement que ce f est injective, on suppose qu'on a $f(m) = f(n)$. Si $m, n \geq 0$ on en déduit l'égalité

$$2 \times m = 2 \times n$$

et donc $m = n$ [11.28]. Si on a $m, n < 0$, alors on a l'égalité

$$1 - 2 \times m = 1 - 2 \times n \qquad \iff \qquad 2 \times m = 2 \times n$$

et donc de nouveau par [11.28] $m = n$. Finalement si $m \geq 0$ et $n < 0$, alors on a l'égalité

$$2 \times m = 1 - 2 \times n \qquad \iff \qquad 2 \times (m + n) = 1 \ .$$

Si $m+n \leq 0$, alors par [11.32.i] on a $2 \times (m+n) \leq 0$, ce qui est impossible car $1 > 0$. Et si $m + n > 0$, alors par [11.27] on a $m + n \in \mathbf{N}$ et $m + n > 0$. Par [8.16] on a donc $m + n \geq 1$ et donc par [11.32.i] $2 \times (m + n) \geq 2$, ce qui est aussi impossible car $1 < 2$. La conclusion est que cette application f est bien injective.

• Pour montrer que $\mathbf{Q}$ est dénombrable on utilise [26.6], comme dans la première preuve pour la dénombrabilité de $\mathbf{Z}$. La définition de $\mathbf{Q}$ nous donne l'équivalence

$$r \in \mathbf{Q} \qquad \iff \qquad \exists m, n \in \mathbf{Z} : n \neq 0 \text{ et } r = \frac{m}{n} \ .$$

Informellement on peut donc écrire

$$\mathbf{Q} = \bigcup_{n\in\mathbf{Z}^*} \{\, r \in \mathbf{Q} \mid \exists m \in \mathbf{Z} : r = \frac{m}{n} \,\} \ ,$$

qui est une réunion dénombrable d'ensembles dénombrables, car chaque ensemble $\{\, \frac{m}{n} \mid m \in \mathbf{Z} \,\}$ est en bijection avec $\mathbf{Z}$, donc dénombrable.

La preuve formelle passe par la définition de l'application $\phi : \mathbf{Z}^* \to \mathcal{P}(\mathbf{Q})$ définie par

$$\phi(n) = \{\, r \in \mathbf{Q} \mid \exists m \in \mathbf{Z} : r = \frac{m}{n} \,\}$$

et les application $g_n : \mathbf{N} \to \phi(n)$ (une pour chaque $n \in \mathbf{Z}^*$) définies par

$$g_n(m) = \frac{m}{n} \ .$$

Par définition de l'ensemble $\phi(n)$, l'application g_n est surjective, mais elle est aussi injective car on a les équivalences

$$g_n(m) = g_m(n') \quad \Leftrightarrow \quad \frac{m}{n} = \frac{m}{n'} \quad \Leftrightarrow \quad m \times n' = m \times n \quad \overset{[11.28]}{\Leftrightarrow} \quad n' = n \ .$$

Comme pour $\mathbf{Z}$, l'application g_n est donc bijective, ce qui implique que l'application réciproque $g_n^{-1} : \phi(n) \to \mathbf{N}$ est en particulier injective. Il s'ensuit que $\phi(n)$ est un

ensemble dénombrable. L'ensemble $\mathbf{Z}^*$ est aussi dénombrable comme sous-ensemble de l'ensemble dénombrable $\mathbf{Z}$ [26.1]. On peut donc conclure avec [26.6] que la réunion $\cup\phi[\mathbf{Z}^*]$ est dénombrable. Mais on a les équivalences

$$\begin{aligned} r \in \cup\phi[\mathbf{Z}^*] \quad &\Longleftrightarrow \quad \exists A \in \phi[\mathbf{Z}^*] : r \in A \quad \Longleftrightarrow \quad \exists n \in \mathbf{Z}^* : r \in \phi(n) \\ &\Longleftrightarrow \quad \exists n \in \mathbf{Z}^*\ \exists m \in \mathbf{Z} : r = \frac{m}{n} \quad \Longleftrightarrow \quad r \in \mathbf{Q}\ , \end{aligned}$$

ce qui montre l'égalité $\mathbf{Q} = \cup\phi[\mathbf{Z}^*] = \cup_{n\in\mathbf{Z}^*}\phi(n)$. *CQFD*

Les preuves de §27

Preuve de [27.4]. La preuve ressemble, mais en plus facile, à la preuve que le lemme de Zorn implique le théorème du bon ordre. L'idée est une application assez simple du lemme de Zorn : on considère la collection $\mathcal{B}$ de tous les sous-ensembles B de A pour lesquels il existe une bijection $B \to B \times B$. Cet ensemble est partiellement ordonné par l'inclusion et on montre que tout sous-ensemble totalement ordonné de $\mathcal{B}$ admet un majorant. Selon le lemme de Zorn il exist donc un élément maximal M. Si $M \neq A$, alors on construit un sous-ensemble plus grand appartenant à $\mathcal{B}$, ce qui contredit la maximalité de M. Et donc on doit avoir $M = A$ et donc il existe une bijection $A \to A \times A$.

Comme (presque) toujours, les choses ne sont pas aussi simple que l'idée de base. Pour pouvoir montrer que tout sous-ensemble totalement ordonné de $\mathcal{B}$ admet un majorant, il faut inclure la bijection $B \to B \times B$ dans la description des éléments de $\mathcal{B}$ et de la relation d'ordre. Mais cette modification nous empêche de déduire une contradiction si l'élément maximal M n'est pas l'espace total A. Par contre, on peut déduire une contradiction s'il n'existe pas une bijection entre l'élément maximal M et l'espace total A. Et c'est ici qu'on a besoin du fait que l'ensemble M (et donc A) est un ensemble infini. Il faut donc inclure dans la définition de $\mathcal{B}$ la condition que B doit être un ensemble infini. La définition officielle de $\mathcal{B}$ devient donc

$$\mathcal{B} = \{\, (B, f) \mid B \subset A \text{ et } f : B \to B \times B \text{ une bijection et } \mathbf{N} \precsim B \,\} \ .$$

Pour se convaincre que c'est bien un ensemble (par l'axiome de séparation (Z5)), il suffit de remarquer qu'on a $B \in \mathcal{P}(A)$, que $f \subset B \times (B \times B) \subset A \times (A \times A)$ et donc $f \in \mathcal{P}\big(A \times (A \times A)\big)$ et donc au final

$$(B, f) \in \mathcal{P}(A) \times \mathcal{P}\big(A \times (A \times A)\big) \ .$$

La première chose à faire est de montrer que $\mathcal{B}$ n'est pas vide. Pour cela on invoque l'hypothèse $\mathbf{N} \precsim A$, ce qui veut dire qu'il existe une injection $g : \mathbf{N} \to A$. Si on définit $B = g[\mathbf{N}] \subset A$, l'image de $\mathbf{N}$ sous l'application g, alors $g : \mathbf{N} \to B$ est une bijection et donc en particulier $\mathbf{N} \precsim B$. En utilisant la bijection $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ définie en [26.4] on définit l'application $h : B \times B \to B$ par

$$h(b, c) = g\big(\quad f\big(\, g^{-1}(b)\,,\, g^{-1}(c)\,\big)\quad\big) \ .$$

Il est immédiat que h est bijective (car f et g le sont) et donc le couple (B, h^{-1}) appartient à $\mathcal{B}$, montrant que $\mathcal{B}$ n'est pas vide.

Sur ce $\mathcal{B}$ on définit la relation d'ordre partiel $\preccurlyeq$ par

$$(B, f) \preccurlyeq (C, g) \qquad \Longleftrightarrow \qquad B \subset C \text{ et } f = g|_B \ .$$

Il est immédiat que cette relation est reflexive et anti-symétrique. Pour la transitivité il suffit de remarquer que prendre une restriction est transitive. C'est donc bien une relation d'ordre partiel. (Dans [27.5] on trouve une autre description de l'ensemble $\mathcal{B}$ et sa relation d'ordre.)

Vérifions maintenant que $(\mathcal{B}, \preccurlyeq)$ vérifie la condition du lemme de Zorn [19.4]. Pour cela on considère une collection totalement ordonné $\mathcal{C} \subset \mathcal{B}$. Pour trouver un majorant de $\mathcal{C}$, on définit l'ensemble $M \subset A$ par

$$M = \cup\{\, B \in \mathcal{P}(A) \mid \exists X \in \mathcal{C}\ \exists f : X = (B, f) \,\} \equiv \bigcup_{(B,f)\in\mathcal{C}} B \ .$$

En mots : on extrait la première composante B des couples (B, f) dans $\mathcal{C}$ et on prend la réunion de tous ces ensembles. Par définition de la réunion on a $B \subset M$

pour tout $(B, f) \in \mathcal{C}$. Mais il faut aussi fournir une bijection $F : M \to M \times M$ pour qu'on a un majorant dans $\mathcal{C}$. Commençons avec la remarque que si $m \in M$, alors par l'axiome de la réunion (Z4) et la définition de M il existe $(B, f) \in \mathcal{C}$ tel que $m \in B \subset M$. Il s'ensuit qu'on a $f(m) \in B \times B \subset M \times M$. On définit "donc" F par

$$F(m) = f(m) \quad \text{si } (B, f) \in \mathcal{C} \text{ et } m \in B.$$

Mais pour que cette définition a un sens, il faut montrer que l'image ne dépend pas du choix du couple (B, f) avec $m \in B$. On suppose donc qu'on a $(B, f), (C, g) \in \mathcal{C}$ avec $m \in B \cap C$. Et il faut montrer qu'on a $f(m) = g(m)$. Pour cela on invoque que $\mathcal{C}$ est totalement ordonné, donc on a $(B, f) \preccurlyeq (C, g)$ ou $(C, g) \preccurlyeq (B, f)$. Dans le premier cas on a $f = g|_B$ et donc $f(m) = g|_B(m) = g(m)$ et pareille dans le deuxième cas. La définition de $F(m)$ ne dépend donc pas du choix de B qui contient m.

Une fois qu'on a défini l'application F, on peut retourner la définition dans l'autre sens et l'écrire comme

$$(B, f) \in \mathcal{C} \text{ et } m \in B \subset M \qquad \Longrightarrow \qquad f(m) = F(m) \ ,$$

ce qui montre qu'on a $(B, f) \preccurlyeq (M, F)$. Autrement dit, le couple (M, F) est un majorant pour $\mathcal{C}$, à condition d'avoir montré que (M, F) appartient à $\mathcal{B}$.

Pour montrer que (M, F) appartient à $\mathcal{B}$ il faut montrer trois choses. La première, $M \subset A$, est automatiquement remplie. La troisième, $\mathbf{N} \precsim M$, est aussi facile à montrer, car on sait qu'il existe $(B, f) \in \mathcal{C} \subset \mathcal{B}$ avec $B \subset M$ et donc $\mathbf{N} \precsim B \precsim M$. La transitivité de $\precsim$ [23.4.iii] nous donne $\mathbf{N} \precsim M$ comme souhaité. Reste la preuve que $F : M \to M \times M$ est une bijection. Commençons avec l'injectivité en supposant qu'on a $F(m) = F(n)$. Il existe donc $(B, f), (C, g) \in \mathcal{C}$ tels que $m \in B$ et $n \in C$ avec

$$f(m) = F(m) = F(n) = g(n) \ .$$

Mais $\mathcal{C}$ est totalement ordonné. Si on a $(B, f) \preccurlyeq (C, g)$, alors on a $f = g|_B$ et donc $g(n) = f(m) = g|_B(m) = g(m)$. Mais g est bijective donc en particulier injective. Il s'ensuit qu'on a $m = n$. Dans le cas contraire $(C, g) \preccurlyeq (B, f)$ on a la même conclusion en passant par $f(m) = f(n)$ et l'injectivité de f.

Pour la surjectivité on prend $(m, n) \in M \times M$ et on cherche $k \in M$ tel que $F(k) = (m, n)$. Par définition de M il existe $(B, f), (C, g) \in \mathcal{C}$ tels que $m \in B$ et $n \in C$. Mais $\mathcal{C}$ est totalement ordonné. Si on a $(B, f) \preccurlyeq (C, g)$, alors on a $B \subset C$ et donc $(m, n) \in B \times C \subset C \times C$. Étant donné que $g : C \to C \times C$ est une bijection, il existe $k \in C \subset M$ tel que $g(k) = (m, n)$. La définition de F nous dit qu'on a $F(k) = g(k) = (m, n)$. Et si $(C, g) \preccurlyeq (B, f)$ on a $(m, n) \in B \times C \subset B \times B$ et donc il existe $k \in B$ tel que $f(k) = (m, n)$ et donc, par définition de F, $F(k) = f(k) = (m, n)$. Ce qui termine la preuve que F est aussi surjective.

Ainsi on a montré que $\mathcal{C}$ admet un majorant dans $\mathcal{B}$. La condition du lemme de Zorn [19.4] est donc remplie, ce qui permet de conclure qu'il existe un élément maximal $(M, F) \in \mathcal{B}$. Comme annoncé, on ne peut pas montrer qu'on a $M = A$. La raison est une particularité de la relation d'ordre qu'on a mis sur $\mathcal{B}$. Pour bien comprendre cette particularité, on commence avec un cas iréel. Supposons qu'on a $(B, f) \preccurlyeq (C, g)$ et qu'on a $C \setminus B = \{a\}$: C ne contient qu'un seul élément de plus que B. On a donc l'égalité

$$\begin{aligned} C \times C &= (\, B \cup \{a\}\,) \times (\, B \cup \{a\}\,) \\ &= (\, B \times B\,) \cup (\, B \times \{a\}\,) \cup (\, \{a\} \times B\,) \cup (\, \{a\} \times \{a\}\,) \ . \end{aligned}$$

DESSIN

La restriction de la bijection $g : C \to C \times C$ à B est, par définition de la relation d'ordre, la bijection $f : B \to B \times B$. Il s'ensuit que la restriction de g à $\{a\}$ doit fournir une bijection

$$g|_{\{a\}} : \{a\} \to (\, B \times \{a\}\,) \cup (\, \{a\} \times B\,) \cup (\, \{a\} \times \{a\}\,) \ . \tag{33.54}$$

Mais cela est absurde, car B est un ensemble infini, donc $\{a\} \times B$ aussi et l'image d'un ensemble avec un seul élément n'est pas plus grand qu'un seul élément, pas une infinité. La morale de cet exemple est que même si M est presque l'espace total A, il ne sera pas facile (voire impossible) d'obtenir une contradiction avec la maximalité de (M, F) dans $(\mathcal{B}, \preccurlyeq)$.

Heureusement on n'a pas besoin de montrer l'égalité $M = A$ pour pouvoir conclure $A \approx A \times A$. Il suffit de montrer qu'on a $M \approx A$ pour le faire. Car si on a cela, c'est-à-dire qu'on a une bijection $G : M \to A$, alors, comme dans la preuve que $\mathcal{B}$ n'est pas vide, on définit l'application $H : A \times A \to A$ par

$$H(a, b) = G\big(\ F(\, G^{-1}(a)\,,\, G^{-1}(b)\,)\ \big) \ .$$

Le fait que G et F sont des bijections implique directement que H l'est aussi, donc qu'on a $A \times A \approx A$ comme voulu.

Pour montrer que la maximalité de (M, F) dans $(\mathcal{B}, \preccurlyeq)$ implique qu'on a $M \approx A$, on va jongler avec les relations $\approx$ et $\precsim$. On commence avec un petit calcul dont on aura besoin plusieurs fois. La définition de $\mathcal{B}$ nous dit qu'on a $\mathbf{N} \precsim M$ et $M \times M \approx M$, ce qui nous permet de faire le raisonnement

$$2 \precsim \mathbf{N} \precsim M \qquad \overset{[23.4]}{\Longrightarrow} \qquad 1 \precsim 2 \precsim M$$

et donc, avec [23.8] et [23.5]

$$M \approx 1 \times M \precsim 2 \times M \precsim M \times M \approx M \ .$$

En particulier on a donc

$$M \precsim 2 \times M \precsim M \qquad \overset{[22.1]}{\Longrightarrow} \qquad 2 \times M \approx M \ . \tag{33.55}$$

À noter que c'est ici qu'on utilise le fait que M est un ensemble infini, ou plutôt que M contient au moins deux éléments, pour obtenir "l'inégalité" $2 \times M \precsim M \times M$.

Selon [22.5] on a $A \setminus M \precsim M$ ou $M \precsim A \setminus M$ (on a déjà utilisé l'axiome du choix sous la forme du lemme de Zorn, donc on peut l'invoquer ici une deuxième fois). Dans le premier cas $A \setminus M \precsim M$ on peut faire le "calcul" suivant :

$$A = M \cup A \setminus M \approx M \sqcup A \setminus M \precsim M \sqcup M \overset{[23.12]}{\approx} 2 \times M \overset{[33.55]}{\approx} M \ .$$

Avec [23.4] on en déduit $A \precsim M$. Mais l'inclusion $M \subset A$ implique directement $M \precsim A$ et donc par [22.1] on a $M \approx A$.

Dans le deuxième cas on va déduire une contradiction avec la maximalité de (M, F). Pour cela il faut donc trouver un élément strictement plus grand dans $(\mathcal{B}, \preccurlyeq)$. Par l'hypothèse $M \precsim A \setminus M$ il existe une injection $f : M \to A \setminus M$, ce qui nous permet de définir l'ensemble $B = f[M]$, l'image de M sous f. Et parce que f est injective, on a $M \approx B$. Le fait qu'on a $B \subset A \setminus M$ implique en particulier qu'on a $B \cap M = \emptyset$ et donc $M' = M \cup B$ est strictement plus grand que M. Pour que M' soit strictement plus grand que (M, F) dans $(\mathcal{B}, \preccurlyeq)$, il faut trouver une bijection

$F' : M' \to M' \times M'$ qui prolonge la bijection F. Comme dans l'exemple autour (33.54) on remarque d'abord que la réunion du membre de droite dans l'égalité

$$\begin{aligned} M' \times M' &= (M \cup B) \times M \cup B) \\ &= (M \times M) \cup (M \times B) \cup (B \times M) \cup (B \times B) \end{aligned}$$

est une réunion disjointe. Le fait que F' doit prolonger F implique que F' doit établir une bijection

$$F' : B \to (M \times B) \cup (B \times M) \cup (B \times B) \ .$$

Pour trouver une telle bijection, on fait le "calcul" suivant.

$$\begin{aligned} B &\overset{\text{déf. de } B}{\approx} M \overset{(33.55)}{\approx} 2 \times M \overset{[23.12]}{\approx} M \sqcup M \overset{(33.55),\,[23.11]}{\approx} (\,2 \times M\,) \sqcup M \\ &\overset{[23.11],\,[23.12]}{\approx} (\,M \sqcup M\,) \sqcup M \\ &\overset{[23.11],\ M \approx M \times M}{\approx} \big((M \times M) \sqcup (M \times M)\big) \sqcup (M \times M) \\ &\overset{[23.11],\,[23.6],\ M \approx B}{\approx} \big((M \times B) \sqcup (B \times M)\big) \sqcup (B \times B) \\ &\overset{[23.12]}{\approx} \big((M \times B) \cup (B \times M)\big) \cup (B \times B) \\ &= (M \times B) \cup (B \times M) \cup (B \times B) \ . \end{aligned}$$

Par [23.2] il s'ensuit qu'il existe une bijection

$$g : B \to (M \times B) \cup (B \times M) \cup (B \times B) \ .$$

Avec cette bijection on définit l'application $F' : M' \to M' \times M'$ par

$$F'(m) = \begin{cases} F(m) & \text{si } m \in M \\ g(m) & \text{si } m \in B \ . \end{cases}$$

La preuve que ce F' est une bijection est élémentaire et laissée comme exercice au lecteur (et on n'a pas besoin de courage pour le faire).

Ainsi on a $(M', F') \in \mathcal{B}$ (car on a aussi $\mathbf{N} \precsim M \precsim M'$) et $(M, F) \preccurlyeq (M', F')$ et (cérise sur le gateau) $M \neq M'$. Ceci contredit la maximalité de (M, F), ce qui montre que la possibilité $M \precsim A \setminus M$ est exclue. On doit donc avoir $A \setminus M \precsim M$, ce qui entraînait $M \approx A$ et donc $A \approx A \times A$ comme voulu. CQFD

Preuve de [27.6]. • (i) Comme dans la preuve de [27.4], on jongle avec les opérations $\approx$ et $\precsim$ en faisant le "calcul"

$$A \overset{[23.12]}{\approx} A \sqcup 0 \overset{[23.10]}{\precsim} A \sqcup B \overset{[23.10] \text{ et hyp.}}{\precsim} A \sqcup A \overset{[23.12]}{\approx} 2 \times A \overset{[23.5],\,[27.2]}{\precsim} A \times A \overset{[27.4]}{\approx} A \ .$$

En utilisant [23.4] on en déduit en particulier

$$A \precsim A \sqcup A \precsim A \quad \overset{[23.4] \text{ ou } [22.1]}{\Longrightarrow} \quad A \sqcup B \approx A \ .$$

• (ii) : On a les "inégalités" et "égalités"

$$A \overset{[23.8]}{\approx} 1 \times A \overset{[23.5]}{\precsim} B \times A \overset{[23.5]}{\precsim} A \times A \overset{[27.4]}{\approx} A \ .$$

Il suffit maintenant, comme dans la preuve de la première partie, d'invoquer [23.4] pour conclure qu'on a bien $B \times A \approx A$.

• (iii) On fait le "calcul"

$$2^A \overset{[24.6],\ 2 \precsim B}{\precsim} B^A \overset{[24.9]}{\precsim} (2^B)^A \overset{[13.3]}{\approx} 2^{A\times B} \overset{[24.7],\ \text{(i)}}{\approx} 2^A \ ,$$

et donc comme avant avec [23.4] on en déduit $2^A \approx B^A$.

• (iv) C'est une simple preuve par récurrence. Pour $n = 1$ c'est [24.5]. Et si c'est vrai pour n, on peut faire pour $n + 1 = S(n)$ le calcul

$$A^{n+1} = A^{n\cup\{n\}} \overset{[24.1]}{\approx} A^n \times A^{\{n\}} \overset{[23.6],\ [24.7],\ \{n\}\approx 1}{\approx} A^n \times A^1$$
$$\overset{[24.5],\ \text{hyp. de réc.}}{\approx} A \times A \overset{[27.4]}{\approx} A \ .$$

CQFD

Les preuves de §28

Preuve de [28.1]. Si on a $a < b$ et $b < a$, on a en particulier $a \leq b$ et $b \leq a$. Par antisymétrie d'une relation d'ordre on a donc $a = b$. Mais ceci est en contradiction avec (par exemple) $a < b$. On a donc la propriété (i). La propriété (ii) est une conséquence immédiate de [3.11]. CQFD

Preuve de [28.2]. Il est immédiat que la relation $\leq$ est réflexive (à cause de la clause $a = b$). Pour la transitivité de $\leq$ il suffit d'invoquer les équivalences et les implications suivantes :

$$\begin{array}{c} a \leq b \text{ et } b \leq c \\ \Updownarrow \\ (a < b \text{ ou } a = b) \text{ et } (b < c \text{ ou } b = c) \\ \Updownarrow \\ (a < b \text{ et } b < c) \text{ ou } (a < b \text{ et } b = c) \text{ ou } (a = b \text{ et } b < c) \text{ ou } (a = b \text{ et } b = c) \\ \Downarrow \\ (a < b \text{ et } b < c) \text{ ou } (a < c) \text{ ou } (a < c) \text{ ou } (a = c) \\ \Downarrow \text{ (ii)} \\ (a < c) \text{ ou } (a = c) \ . \end{array}$$

Pour l'antisymétrie on suppose qu'on a $a \leq b$ et $b \leq a$. Les mêmes équivalences logiques que données pour la transitivité nous donnent l'équivalence

$$\begin{array}{c} a \leq b \text{ et } b \leq a \\ \Updownarrow \\ (a < b \text{ et } b < a) \text{ ou } (a < b \text{ et } b = a) \text{ ou } (a = b \text{ et } b < a) \text{ ou } (a = b \text{ et } b = a) \ . \end{array}$$

La première clause est explicitement exclu par la propriété (i). Mais les deux clauses suivantes le sont aussi, car la propriété (i) appliquée au cas $a = b$ dit qu'on a $a \not< a$. Il nous reste donc la dernière clause, c'est-à-dire $a = b$, ce qui montre l'antisymétrie.

Pour montrer que la relation d'ordre stricte associée est la relation $<$, on fait le raisonnement

$$\begin{array}{c} a \leq b \text{ et } a \neq b \quad \Longleftrightarrow \quad (a < b \text{ ou } a = b) \text{ et } a \neq b \quad \Longleftrightarrow \\ (a < b \text{ et } a \neq b) \text{ ou } (a = b \text{ et } a \neq b) \quad \Longleftrightarrow \quad a < b \text{ et } a \neq b \ . \end{array}$$

Mais on a vu ci-dessus qu'on ne peut pas avoir $a < a$ (en prenant $a = b$ dans la propriété (i)), donc $a < b$ implique automatiquement $a \neq b$. On a donc l'équivalence

$$a \leq b \text{ et } a \neq b \quad \Longleftrightarrow \quad a < b \ ,$$

ce qui montre bien que la relation d'ordre stricte associée est la relation $<$. CQFD

Preuve de [28.2]. Preuve des implications mentionnées ci-dessus

• Pour montrer l'implication (O4) $\Rightarrow$ (O1) on prend l'ensemble $A = \{x, y\} \subset \alpha$ (c'est bien un ensemble par l'axiome de la paire (Z3)). Par (04) il existe $z \in A$ tel

que $\forall t \in A : t \notin z$. Mais pour z il n'y a que deux possibilités : $z = x$ ou $z = y$. Dans le premier cas il suffit de prendre $t = y$ et dans le deuxième cas $t = x$ pour obtenir $y \notin x$ ou $x \notin y$.

• Pour l'implication (O4') $\Rightarrow$ (O3) on prend $A = \{x, y\}$ dans (O4'). Il existe donc $z \in A$ tel que $\forall t \in A : z \in t$ ou $z = t$. Mais (de nouveau) il n'y a que deux possibilités : $z = x$ ou $z = y$. Dans le premier cas on prend $t = y$ pour obtenir $x \in y$ ou $x = y$ et dans le deuxième cas on prend $t = x$ pour obtenir $y \in x$ ou $y = x$. Dans les deux cas on obtient donc en particulier (O3).

• Pour l'implication (O3) et (O4) $\Rightarrow$ (O4') il suffit de remarquer que la condition $y \notin x$ qui figure dans (O4) en combinaison avec (O3) implique la condition $x \in y$ ou $x = y$.

• Pour l'implication (O1) et (O4') $\Rightarrow$ (O4) on remarque d'abord que (O1) implique qu'on ne peut pas avoir $z \in z$ pour aucun $z \in \alpha$. Si on combine maintenant la condition $x \in y$ ou $x = y$ figurant dans (O4') avec la condition $x \notin y$ ou $y \notin x$ de (O1), on constate d'abord que $x \in y$ est contradictoire avec $x \notin y$ et après que la condition $x = y$ aussi est contradictoire avec $x \notin y$, car on aurait $x \in x$ ce qui est exclu. On doit donc avoir $y \notin x$ comme voulu dans la condition (O4).

• Pour l'implication (O3), (04) et (O5) $\Rightarrow$ (O2) on prend $x, y, z \in \alpha$ vérifiant $x \in y$ et $y \in z$. Selon (O3) on a $x \in z$ ou $x = z$ ou $z \in x$. Si on avait $x = z$, on aurait $x \in y$ et $y \in z = x$, ce qui contredit (O1) qui est une conséquence de (O4) comme on a déjà vu ci-dessus. On regarde maintenant l'ensemble $A = \{x, y, z\} \subset \alpha$ et on applique (O4). Il existe donc $t \in A$ tel que $\forall u \in A : u \notin t$. Mais il n'y a que trois possibilités pour t. Si on a $t = y$, alors en prenant $u = x$ on aurait $x \notin y$, ce qui contredit l'hypothèse $x \in y$. Et si on a $t = z$, alors en prenant $u = y$ on aurait $y \notin z$, ce qui contredit l'hypothèse $y \in z$. On doit donc avoir $t = x$ et en prenant $u = z$ on en déduit qu'on a $z \notin x$. Il nous reste donc que $x \in z$, ce qui montre qu'on a bien (O2).

• Pour montrer que les conditions (O2), (O4) et (O5) impliquent (O3), on introduit la propriété $C(x, y)$ de deux ensembles comme

$$C(x, y) \stackrel{\text{déf}}{=} \big(\, x \in y \text{ ou } x = y \text{ ou } y \in x \, \big) \ .$$

On introduit aussi l'ensemble $A \subset \alpha$ comme

$$A = \{ \, x \in \alpha \mid \exists y \in \alpha : \neg C(x, y) \, \}$$

et le but est de montrer que A est l'ensemble vide.

On le fait par l'absurde en supposant que A ne l'est pas. Par (O4) il existe donc $x_1 \in A$ tel qu'on a $\forall y \in A : y \notin x_1$. En prenant la contraposée, on obtient l'implication

$$t \in x_1 \quad \Longrightarrow \quad t \notin A \quad \Longleftrightarrow \quad \forall y \in \alpha : C(t, y) \ . \tag{33.56}$$

Avec ce x_1 on définit l'ensemble $B \subset \alpha$ comme

$$B = \{ \, y \in \alpha \mid \neg C(y, x_1) \, \} \ .$$

Le fait qu'on a $x_1 \in A$ implique que B n'est pas vide. On peut donc de nouveau invoquer (O4) et déduire qu'il existe $y_1 \in B$ tel que $\forall y \in B : y \notin y_1$. Par (O5) on a l'implication $t \in y_1 \ \Rightarrow t \in \alpha$ et donc avec la définition de B et de y_1 on a les implications

$$t \in y_1 \quad \Longrightarrow \quad t \in \alpha \text{ et } t \notin B \quad \Longrightarrow \quad C(t, x_1) \ .$$

Autrement dit, on a l'implication

$$t \in y_1 \quad \Longrightarrow \quad t \in x_1 \quad \text{ou} \quad t = x_1 \quad \text{ou} \quad x_1 \in t \ .$$

Mais si $t = x_1$, on aurait $x_1 \in y_1$ et en particulier $C(x_1, y_1)$, ce qui est impossible car $y_1 \in B$. Et si $x_1 \in t$, alors on, aurait $x_1 \in t$ et $t \in y_1$, donc par (O2) de nouveau $x_1 \in y_1$, ce qui est impossible. La conclusion est qu'on doit avoir l'implication $t \in y_1 \Rightarrow t \in x_1$, c'est-à-dire $y_1 \subset x_1$.

Si on avait $x_1 = y_1$, on aurait a fortiori $C(x_1, y_1)$, ce qui est impossible car $y_1 \in B$. Il s'ensuit qu'il existe $t \in x_1 \setminus y_1$, donc en particulier $t \in x_1$. Par (33.56) on a donc en particulier $C(t, y_1)$. Cela veut dire qu'on a $t \in y_1$ ou $t = y_1$ ou $y_1 \in t$. Mais $t \in y_1$ est impossible car par définition $t \notin y_1$. Si on avait $t = y_1$, alors on aurait $y_1 \in x_1$, qui est aussi impossible car $y_1 \in B$. Et finalement, si on avait $y_1 \in t$ (et $t \in x_1$), on invoque (O5) pour déduire qu'on a $t \in \alpha$ et (O2) pour en déduire qu'on a $y_1 \in x_1$, ce qui était impossible. On arrive donc à une contradiction, ce qui montre que notre hypothèse que A n'est pas vide doit être fausse, ce qui termine la preuve qu'on a bien (O3). CQFD

Preuve de [28.3]. Si on avait $\alpha \in \alpha$, alors on pourrait appliquer (O1) avec $x = y = \alpha$ pour en déduire $\alpha \notin \alpha$. Cette contradiction montre qu'on doit avoir $\alpha \notin \alpha$ dès le début. CQFD

Preuve de [28.4]. Si on a $\alpha \in \beta$, alors par $(O5)_\beta$ on a $\alpha \subset \beta$, ce qui montre l'implication réciproque. Supposons donc qu'on a $\alpha \subset \beta$ et $\alpha \neq \beta$. Alors l'ensemble $A = \beta \setminus \alpha$ n'est pas vide, ce qui entraîne qu'il existe, par $(O4)_\beta$, $a \in A$ tel que

$$\forall y \in A : y \notin a \ . \tag{33.57}$$

Le but est de montrer l'égalité $a = \alpha$, ce qui montrerait qu'on a $\alpha \in \beta$. On le fait par double inclusion. En prenant la contraposée de (33.57) on obtient l'implication $t \in a \Rightarrow t \notin A$. Mais par $(O5)_\beta$ on a $a \subset \beta$, donc $t \notin A$ veut dire qu'on a $t \in \alpha$. Ainsi on a montré l'inclusion $a \subset \alpha$.

Pour l'inclusion dans l'autre sens, prenons $y \in \alpha$. Par l'hypothèse $\alpha \subset \beta$ on a donc $y \in \beta$, et donc par $(O3)_\beta$ on a $y \in a$ ou $a = y$ ou $a \in y$. Si on a $a \in y$, alors par $(O5)_\alpha$ on a $a \in \alpha$, ce qui contredit $a \in A = \beta \setminus \alpha$. Et si on a $y = a$, on aura de nouveau $a \in \alpha$, ce qui était impossible. On doit donc avoir $y \in a$, ce qui montre l'inclusion $\alpha \subset a$. CQFD

Preuve de [28.5]. Par $(O5)_\alpha$ on a $\beta \subset \alpha$. Étant donné que $\in$ est la version stricte d'une relation d'ordre total sur α, elle l'est aussi sur le sous-ensemble $\beta \subset \alpha$. Autrement dit, β vérifie les conditions (O1) à (O4). Pour montrer que β vérifie aussi (O5), on prend $x \in \beta$ et $y \in x$. Alors on peut faire le raisonnement

$$y \in x \text{ et } x \in \beta \text{ et } \beta \in \alpha \quad \overset{(O5)_\alpha}{\Longrightarrow} \quad y \in x \text{ et } x \in \beta \text{ et } x, \beta \in \alpha$$

$$\overset{(O5)_\alpha}{\Longrightarrow} \quad y \in x \text{ et } x \in \beta \text{ et } y, x, \beta \in \alpha \quad \overset{(O2)_\alpha}{\Longrightarrow} \quad y \in \beta \ .$$

Ainsi on a montré l'implication $y \in x \Rightarrow y \in \beta$, c'est-à-dire l'inclusion $x \subset \beta$. Étant donné que $x \in \beta$ était arbitraire, on a montré $(O5)_\beta$. CQFD

Preuve de [28.6]. Pour montrer que m est un ordinal, il faut vérifier les propriétés. Les propriétés $(\mathrm{O1})_m$ à $(\mathrm{O3})_m$ concernent seulement les éléments de m, qui sont d'office des éléments de chaque $x \in X$. Les éléments de X étant des ordinaux, ces propriétés sont donc vraies pour ces éléments. Prenons par exemple la propriété $(\mathrm{O3})_m$. Pour le montrer on prend $s, t \in m$ et il faut en déduire qu'on a $s \in t$ ou $s = t$ ou $t \in s$. L'ensemble X n'étant pas vide, il existe $x \in X$. Et donc par [5.1.i] on a $m \subset x$. Donc par $(\mathrm{O3})_x$ et le fait qu'on a $s, t \in x$ on peut déduire qu'on a la conclusion souhaitée. Le même raisonnement s'applique aux propriétés $(\mathrm{O1})_m$ et $(\mathrm{O2})_m$.

Pour montrer $(\mathrm{O4})_m$ on prend $A \subset m$, $A \neq \emptyset$. Comme avant, il existe $x \in X$ tel que $m \subset x$. On a donc $A \subset x$. En invoquant $(\mathrm{O4})_x$ on obtient $s \in A$ tel que pour tout $t \in A$ on a $t \notin s$. Autrement dit, on a montré $(\mathrm{O4})_m$.

Pour $(\mathrm{O5})_m$ on prend $s \in t$ et $t \in m$ et on veut en déduire qu'on a $s \in m$. Soit maintenant $x \in X$, alors par définition de l'intersection, on a $m \subset x$. On a donc $s \in t$ et $t \in x$, donc par $(\mathrm{O5})_x$ on a $s \in x$. Ceci étant vrai pour tout $x \in X$, il s'ensuit, avec (1.11) et [1.12], qu'on a $s \in \cap X \equiv m$.

Pour montrer qu'on a $m \in X$ on raisonne comme suit. Par [5.1.i] on a

$$\forall x \in X : m \subset x \ .$$

Mais on vient de voir que m aussi est un ordinal. On peut donc invoquer [28.4] pour obtenir la propriété

$$\forall x \in X : m \in x \text{ ou } m = x \ .$$

Supposons maintenant qu'on a $m \in x$ pour tout $x \in X$. Alors par (1.11) et [1.12] on aurait $m \in \cap X \equiv m$, ce qui est exclu par [28.3]. Il s'ensuit qu'il existe $x \in X$ tel qu'on ait $m = x$. CQFD

Preuve de [28.7]. La réflexivité de l'inclusion est dans sa définition et l'antisymétrie et la transitivité sont montré dans [1.2] et [1.3]. C'est donc une relation d'ordre sur X (on pourrait déduire cela aussi de [3.13] avec l'ensemble $A = \cup X$). Pour montrer que c'est un bon ordre, il suffit, selon [19.6], de montrer que tout sous-ensemble non-vide possède un plus petit élément (pour l'inclusion !). Soit donc $A \subset X$ un sous-ensemble non-vide (si X est vide, un tel A n'existe pas et il n'y a rien à montrer). Alors par [28.6] on a $m = \cap A \in A$. Par [5.1.i] on a donc l'inclusion $m \subset a$ pour tout $a \in A$, ce qui montre que m est le plus petit élément de A (pour la relation donnée par l'inclusion). Par [19.6] il s'ensuit donc que l'inclusion est un bon ordre sur X. Que l'appartenance est la relation d'ordre stricte associée est une conséquence immédiate de [28.4] et [28.3] (on a besoin de [28.3] pour pouvoir réduire la propriété "$\alpha \neq \beta$ et $\alpha \in \beta$" à la seule condition $\alpha \in \beta$). CQFD

Preuve de [28.8]. Par l'axiome de la paire, l'ensemble $\{\alpha, \beta\}$ est un ensemble dont tous les éléments sont des ordinaux. Selon [28.7] c'est donc en particulier un ensemble totalement ordonné et la version stricte de la relation d'ordre est l'appartenance. Si on n'a pas $\alpha = \beta$, on doit donc avoir $\alpha \in \beta$ ou $\beta \in \alpha$, c'est-à-dire, α strictement plus petit que β ou β strictement plus petit que α. Et parce que c'est un ordre total, ces trois possibilités sont mutuellement exclusives. CQFD

Preuve de [28.9]. Supposons que Y est un ensemble qui contient tous les ordinaux. En définissant l'ensemble X (avec l'axiome de séparation) comme

$$X = \{\, \alpha \in Y \mid \alpha \text{ est un ordinal} \,\}$$

on aurait un ensemble qui contient tous les ordinaux et que des ordinaux. Alors selon [28.7] l'appartenance est la version stricte d'un bon ordre sur X. Les propriétés (O1) à (O4) sont donc vraies. Et si on a $\alpha \in X$, c'est-à-dire que α est un ordinal, et si on a $\beta \in \alpha$, alors par [28.5] β est un ordinal. Et donc par définition de X on a $\beta \in X$. Ce qui montre qu'on a $\alpha \subset X$ et donc (O5) est aussi vrai. Il s'ensuit que X est un ordinal, donc par définition de X on doit avoir $X \in X$, ce qui est exclu par [28.3]. CQFD

Preuve de [28.10]. • Pour montrer que M est un ordinal, on commence avec la remarque que pour $x \in M$ il existe, par définition de la réunion, $\alpha \in X$ tel que $x \in \alpha$. Par hypothèse α est un ordinal, donc par [28.5] x l'est aussi. Donc par [28.7] M est bien ordonné par l'inclusion et la version stricte de ce bon-ordre est l'appartenance. Il s'ensuit que M vérifie les conditions $(\mathrm{O1})_M$ à $(\mathrm{O4})_M$.

Pour montrer $(\mathrm{O5})_M$ on prend x, y vérifiant $x \in y$ et $y \in M$ et on veut en déduire $x \in M$. Comme avant, il existe $\alpha \in X$ tel que $y \in \alpha$. Par $(\mathrm{O5})_\alpha$ on a $x \in \alpha$. Et donc par défnition de la réunion on a $x \in M$.

• Si β vérifie $x \subset \beta$ pour tout $x \in X$, alors par [5.1.ii] (ce qui est valable aussi quand $X = \emptyset$) on a directement $M = \cup X \subset \beta$. CQFD

Preuve de [28.11]. Il est trivial de vérifier directement que l'ensemble vide est un ordinal, car tous les conditions d'un ordinal demandent une propriété d'éléments de l'ensemble. Étant donné que l'ensemble vide ne contient pas d'éléments, ces conditions sont donc trivialement vérifiées. Mais on le déduit aussi de [28.10] avec la remarque que tous les éléments du vide sont des ordinaux, et donc $\cup\emptyset = \emptyset$ est un ordinal. CQFD

Preuve de [28.12]. Par $(\mathrm{O5})_\alpha$ on a l'implication $\gamma \in \alpha \Rightarrow \gamma \subset \alpha$. Par [5.1.ii] on a donc l'inclusion $\beta \equiv \cup\alpha \subset \alpha$. Selon [28.4] on a donc $\beta = \alpha$ ou $\beta \in \alpha$. Il nous reste donc à montrer que la possibilité $\beta \in \alpha$ implique l'égalité $\alpha = \beta \cup \{\beta\}$, ce qu'on fera par double inclusion.

Pour $x \in \beta \cup \{\beta\}$ on a deux possibilités : $x \in \beta$ ou $x = \beta$. Dans le deuxième cas on a bien $x \in \alpha$ par hypothèse. Dans le premier cas il existe (par définition de la réunion) $\gamma \in \alpha$ tel que $x \in \gamma$. Alors par $(\mathrm{O5})_\alpha$ il s'ensuit qu'on a aussi $x \in \alpha$. Ainsi on a montré l'inclusion $\beta \cup \{\beta\} \subset \alpha$.

Pour l'inclusion dans l'autre sens, prenons $\gamma \in \alpha$. Alors par [5.1.i] on a $\gamma \subset \beta$ et donc par [28.4] on a $\gamma \in \beta$ ou $\gamma = \beta$. Dans les deux cas on a $\gamma \in \beta \cup \{\beta\}$. CQFD

Preuve de [28.13]. • Si A est un ensemble, alors $A \in S(A)$. Il s'ensuit que, si $S(A)$ est un ordinal, alors par [28.5] A l'est aussi. Dans l'autre sens, supposons que A est un ordinal. Alors par hypothèse et par [28.5] il s'ensuit que tous les éléments de $S(A) = A \cup \{A\}$ sont des ordinaux. Par [28.7] on en déduit que $S(A)$ est bien ordonné par la relation d'ordre stricte d'appartenance. Pour que $S(A)$ soit un ordinal, il suffit donc de montrer la condition $(\mathrm{O5})_{S(A)}$. Soit donc $x \in S(A)$, alors on a $x \in A$ ou $x = A$. Par $(\mathrm{O5})_A$ on a l'implication $x \in A \Rightarrow x \subset A \subset S(A)$ et dans le deuxième cas on a directement $x = A \subset S(A)$. Ainsi on a montré que $S(A)$ vérifie la condition (O5), donc que $S(A)$ est bien un ordinal.

• Quand on sait que A et $S(A)$ sont des ordinaux, le fait qu'on a $A \in S(A)$ implique (avec [28.3]) qu'on ne peut pas avoir $A = S(A)$.

• L'appartenance $A \in S(A)$ implique (avec [5.1.i]) qu'on a l'inclusion $A \subset \cup S(A)$. Pour l'inclusion dans l'autre sens, prenons $x \in \cup S(A)$. Par définition de la réunion il existe donc $y \in S(A) = A \cup \{A\}$ tel que $x \in y$. Mais pour y on a deux possibilités : $y = A$ ou $y \in A$. Si on a $y = A$, alors on a $x \in y = A$ comme souhaité. Et si on a $y \in A$, on invoque $(\mathrm{O5})_A$ pour en déduire qu'on a (de nouveau) $x \in A$.

CQFD

Preuve de [28.14]. • (i) $\Rightarrow$ (ii) : Soit $\beta \in \alpha$. $S(\beta)$ étant un ordinal, il n'y a que trois possibilités selon [28.8] : $S(\beta) = \alpha$, $\alpha \in S(\beta)$ ou $S(\beta) \in \alpha$. Si on avait $S(\beta) = \alpha$, on aurait

$$\beta \overset{[28.13]}{=} \cup S(\beta) = \cup \alpha \overset{\text{(i)}}{=} \alpha \ ,$$

ce qui est exclu par [28.3]. Et si on avait $\alpha \in S(\beta) \equiv \beta \cup \{\beta\}$, on aurait $\alpha \in \beta$ ou $\alpha = \beta$. Mais ceci est exclu par [28.8] car on a déjà $\beta \in \alpha$. Il nous reste donc la troisième possibilité $S(\beta) \in \alpha$.

• (ii) $\Rightarrow$ (iii) : Supposons qu'on a $\alpha = S(A) = A \cup \{A\}$. Alors on a $A \in \alpha$, donc par (ii) $S(A) \in \alpha$ et donc par hypothèse $\alpha \in \alpha$. Ceci est exclu par [28.3]. Un tel ensemble A ne peut donc pas exister.

• (iii) $\Rightarrow$ (i) : On pose $\beta = \cup\alpha$ et on invoque [28.12]. L'égalité $\alpha = S(\beta)$ est exclu par (iii), donc on doit avoir $\alpha = \beta \equiv \cup\alpha$. *CQFD*

Preuve de [28.15]. Pour montrer que $\mathbf{N}$ est un ordinal, on commence à montrer par récurrence que les éléments de $\mathbf{N}$ sont des ordinaux. Pour cela on introduit l'ensemble $E \subset \mathbf{N}$ comme

$$E = \{\, n \in \mathbf{N} \mid n \text{ est un ordinal} \,\} \ .$$

Par [28.11] on a $\emptyset \in E$ ainsi que l'implication $n \in E \Rightarrow S(n) \in E$. On a donc bien $E = \mathbf{N}$ par récurrence.

Ensuite on invoque [28.7] pour déduire que la relation d'appartenance est un bon ordre sur $\mathbf{N}$. Autrement dit, $\mathbf{N}$ vérifie les conditions (O1) à (O4) d'un ordinal. Pour montrer que $\mathbf{N}$ est un ensemble transitif (condition (O5)), on utilise de nouveau la récurrence. Cette fois on définit l'ensemble $E \subset \mathbf{N}$ comme

$$E = \{\, n \in \mathbf{N} \mid \forall m \in n : m \in \mathbf{N} \,\} \ .$$

Parce que l'ensemble vide ne contient pas d'éléments, il est immédiat qu'on a $\emptyset \in E$. Supposons donc qu'on a $n \in E$. Pour $m \in S(n) = n \cup \{n\}$ on a donc $m \in n$ ou

$m = n$. Dans le premier cas on a $m \in \mathbf{N}$ car $n \in E$ et dans le deuxième cas on a $m \in \mathbf{N}$ car $n \in \mathbf{N}$. Il s'ensuit (par récurrence) qu'on a $E = \mathbf{N}$ et donc que $\mathbf{N}$ est un ordinal.

La définition de $\mathbf{N}$ nous donne l'implication $n \in \mathbf{N} \Rightarrow S(n) \in \mathbf{N}$, donc l'ordinal $\mathbf{N}$ vérifie la condition (ii) de [28.14]. C'est donc un ordinal limite. CQFD

Preuve de [28.16]. Que l'ensemble vide est un ordinal fini est immédiat. Soit donc α un ordinal fini. Alors $S(\alpha)$ est un ordinal par [28.13]. Il est immédiat que $S(\alpha)$ vérifie la condition (N1), car c'est le successeur de α. Et pour la condition (N2), si $\gamma \in S(\alpha) = \alpha \cup \{\alpha\}$, alors $\gamma \in \alpha$ ou $\gamma = \alpha$. Dans le premier cas on invoque $(\mathrm{N2})_\alpha$ et dans le deuxième cas on invoque $(\mathrm{N1})_\alpha$ pour conclure qu'on a $\gamma = \emptyset$ ou $\exists \beta : \gamma = S(\beta)$. Ce qui termine la preuve que $S(\alpha)$ est un ordinale fini.

Soit maintenant $\delta \in \alpha$. Par [28.5] δ est un ordinal. La condition $(\mathrm{N2})_\alpha$ nous donne immédiatement la condition $(\mathrm{N1})_\delta$. Soit donc $\gamma \in \delta$. Mais α est un ordinal, donc on a la propriété $(\mathrm{O5})_\alpha$, ce qui implique qu'on a $\gamma \in \alpha$. Avec $(\mathrm{N2})_\alpha$ on en déduit qu'on a $\gamma = \emptyset$ ou $\exists \beta : \gamma = S(\beta)$. Ce qui termine la preuve que δ est un ordinal fini. CQFD

Preuve de [28.17]. • $\Rightarrow$: On définit l'ensemble $E \subset \mathbf{N}$ comme

$$E = \{\, n \in \mathbf{N} \mid n \text{ est un ordinal fini} \,\} \ .$$

Par [28.16] on a $\emptyset \in E$ et l'implication $n \in E \Rightarrow S(n) \in E$. Par récurrence on a donc $E = \mathbf{N}$, ce qui montre l'implication directe.

• $\Leftarrow$: Soit α un ordinal fini. Si on a $\alpha = \emptyset$, alors on a $\alpha \in \mathbf{N}$. Sinon, il existe β tel que $\alpha = S(\beta)$. On définit l'ensemble $A \subset \alpha$ comme

$$A = \{\, \gamma \in \alpha \mid \gamma \notin \mathbf{N} \,\} \ .$$

Si $A = \emptyset$, alors on doit avoir $\beta \in \mathbf{N}$, car $\beta \in S(\beta) = \alpha$ et $\beta \notin A$. Et donc $\alpha = S(\beta) \in \mathbf{N}$.

Supposons donc que A n'est pas vide. Alors par $(\mathrm{O4})_\alpha$ il existe $a \in A \subset \alpha$ tel que $\forall y \in A : y \notin a$. (Autrement dit, a est le plus petit élément de A pour la relation d'ordre donnée par l'appartenance/inclusion, ce qui est un bon ordre.) On ne peut pas avoir $a = \emptyset$, car on a $a \notin \mathbf{N}$ et $\emptyset \in \mathbf{N}$. Par $(\mathrm{N2})_\alpha$ il existe donc γ tel que $a = S(\gamma)$. Par $(\mathrm{O5})_\alpha$ on a donc $\gamma \in \alpha$. Par définition de a on ne peut pas avoir $\gamma \in A$, car dans ce cas on devrait avoir $\gamma \notin a$. (En termes de la relation d'ordre : $\gamma \in S(\gamma) = a$ veut dire que γ est plus petit que a. Mais a est le plus petit élément de A, donc on ne peut pas avoir $\gamma \in A$.) Donc $\gamma \in \mathbf{N}$, donc $a = S(\gamma) \in \mathbf{N}$. Ce qui contredit le fait qu'on a $a \in A$. Il s'ensuit que A doit être vide et donc $\alpha \in \mathbf{N}$ comme voulu. CQFD

Preuve de [28.18]. • $\Rightarrow$: Soit α un ordinal fini. Selon [28.17] c'est donc un entier naturel et donc par [25.4] c'est un ensemble fini.

• $\Leftarrow$: Supposons que α soit un ensemble fini et considérons les deux ordinaux α et $\mathbf{N}$. Selon [28.8] il n'y a que trois possibilités : $\alpha \in \mathbf{N}$, $\alpha = \mathbf{N}$ ou $\mathbf{N} \in \alpha$. Et selon

[28.4] on peut résumer les deux derniers comme $\mathbf{N} \subset \alpha$. Si on avait $\mathbf{N} \subset \alpha$, alors l'application identité $g : \mathbf{N} \to \alpha$ définie par $g(x) = x$ est une application injective. Donc par [7.10] α serait un ensemble infini, ce qui n'est pas le cas. On doit donc avoir $\alpha \in \mathbf{N}$, c'est-à-dire que α est un entier naturel. Avec [28.17] il s'ensuit que α est un ordinal fini. *CQFD*

Preuve de [28.19]. La relation d'ordre définie à l'aide des axiomes de Peano est notée $\leq$ et celle des ordinaux est l'inclusion $\subset$. Il faut donc montrer, pour tout $m, n \in \mathbf{N}$, l'équivalence $m \leq n \Leftrightarrow m \subset n$. Si on part de l'hypothèse $m \subset n$, alors l'application identité $id|_m : m \to n$ est une application injective de m dans n. Par [25.2] il s'ensuit qu'on a $m \leq n$.

Dans l'autre sens, supposons qu'on a $m \leq n$. Parce que l'ordre sur les ordinaux est total, on a $m \subset n$ ou $n \subset m$. Dans le deuxième cas on a, selon l'argument précédent, $n \leq m$. Avec l'hypothèse $m \leq n$ il s'ensuit qu'on a $m = n$ et donc en particulier $m \subset n$. Dans les deux cas on a donc $m \subset n$. *CQFD*

Les preuves de §29

Preuve de [29.3]. Soit A un ensemble et $p(x)$ une formule. Alors il faut montrer qu'il existe un *ensemble* B tel que

$$C \in B \quad \Longleftrightarrow \quad C \in A \text{ et } p(C) \ . \tag{33.58}$$

L'idée de l'utilisation de l'axiome de remplacement est qu'on remplace un élément $x \in A$ par lui même si $p(x)$ est vrai et qu'on le remplace par un x_o quand $p(x)$ est faux, où x_o est un élément de A pour lequel $p(x_o)$ est vrai. Pour que cela marche, il faut donc qu'il existe au moins un élément $x_o \in A$ pour lequel $p(x_o)$ est vrai. On distingue donc deux cas :

$$\text{(i)} \quad \forall C \ : \ C \notin A \text{ ou } \neg p(C) \qquad \text{et (ii)} \quad \exists x_o \ : \ x_o \in A \text{ et } p(x_o) \ .$$

Dans le premier cas la condition à droite dans (33.58) est toujours fausse. Pour que la condition à gauche soit toujours fausse, il faut que B soit l'ensemble vide, qui est bien un ensemble selon l'axiome de l'ensemble vide. Dans le premier cas, (33.58) définit donc bien un ensemble.

Dans le deuxième cas on définit la formule $q(x,y)$ par

$$q(x,y) \quad \stackrel{\text{déf}}{=} \quad \big(\ y = x \text{ et } p(x) \ \big) \text{ ou } \big(\ y = x_o \text{ et } \neg p(x) \ \big) \ .$$

Il est immédiat que pour tout $x \in A$ il existe un unique y tel que $q(x,y)$ soit vrai. Par l'axiome de remplacement on obtient donc un ensemble B défini par

$$\begin{aligned} C \in B \quad &\Longleftrightarrow \quad \exists x \ : \ x \in A \text{ et } q(x,C) \\ &\Longleftrightarrow \quad \exists x \ : \ x \in A \text{ et } \big(\ C = x \text{ et } p(x) \ \big) \text{ ou } \big(\ C = x_o \text{ et } \neg p(x) \ \big) \\ &\Longleftrightarrow \quad \exists x \ : \ \big(\ C \in A \text{ et } p(C) \ \big) \text{ ou } \big(\ x \in A \text{ et } C = x_o \text{ et } \neg p(x) \ \big) \\ &\Longleftrightarrow \quad \big[\ C \in A \text{ et } p(C) \ \big] \text{ ou } \big(\ \big[\ \exists x \ : \ x \in A \text{ et } \neg p(x) \ \big] \text{ et } C = x_o \ \big) \ . \end{aligned}$$

Mais la condition $\exists x \ : \ x \in A$ et $\neg p(x)$ ne dépend pas de C. Si c'est faux, alors on obtient l'équivalence

$$C \in B \quad \Longleftrightarrow \quad C \in A \text{ et } p(C) \ ,$$

ce qui montre que (33.58) définit bien un ensemble dans ce cas. Et si la condition $\exists x \ : \ x \in A$ et $\neg p(x)$ est vraie, on obtient l'équivalence

$$C \in B \quad \Longleftrightarrow \quad \big[\ C \in A \text{ et } p(C) \ \big] \text{ ou } C = x_o \ .$$

Mais par définition de x_o on a l'implication

$$C = x_o \quad \Longrightarrow \quad C \in A \text{ et } p(C) \ ,$$

ce qui donne immédiatement l'équivalence

$$\big[\ C \in A \text{ et } p(C) \ \big] \text{ ou } C = x_o \quad \Longleftrightarrow \quad C \in A \text{ et } p(C) \ .$$

Il s'ensuit que même dans ce dernier cas on a l'équivalence

$$C \in B \quad \Longleftrightarrow \quad C \in A \text{ et } p(C)$$

et donc même dans ce dernier cas (33.58) définit un ensemble. CQFD

Les preuves de §30

Preuve de [30.3]. En utilisant la définition de l'idéal, le fait qu'on a $\beta \in \alpha$ et la propriété $(\mathrm{O5})_\alpha$ d'un ordinal, on peut faire le raisonnement

$$\gamma \in \alpha_{\prec\beta} \overset{\text{déf. idéal}}{\Longleftrightarrow} \gamma \in \alpha \text{ et } \gamma \prec \beta \overset{\text{déf. } \prec}{\Longleftrightarrow} \gamma \in \alpha \text{ et } \gamma \in \beta \overset{(\mathrm{O5})_\alpha}{\Longleftrightarrow} \gamma \in \beta \ .$$

CQFD

Preuve de [30.4]. • (i) : La preuve se fait par récurrence transfinie sur γ. On suppose donc que c'est vrai pour tout $\gamma \prec \gamma_o$ et on en déduit que c'est vrai pour γ_o. Pour cela on pose $\delta = f(\gamma_o)$. Mais γ_o et δ sont deux ordinaux, donc comparable [28.4], [28.8]. On a donc soit $\delta \prec \gamma_o$, soit $\gamma_o \preccurlyeq \delta$. Si on a $\delta \prec \gamma_o$, alors parce que f est strictement croissante on a $f(\delta) \prec f(\gamma_o)$. Par l'hypothèse de récurrence transfinie on en déduit

$$\delta \preccurlyeq f(\delta) \prec f(\gamma_o) = \delta \ .$$

Cette contradiction montre qu'on doit avoir $\gamma_o \preccurlyeq \delta \equiv f(\gamma_o)$. Ainsi on a vérifié les conditions du principe de récurrence transfinie et donc la propriété est vraie pour tout $\gamma \in \alpha$.

• (ii) : On vient de montrer l'implication $\gamma \in \alpha \Rightarrow \gamma \in f(\gamma) \in \beta$. Par $(\mathrm{O5})_\beta$ (la transitivité de l'ordinal β) on a donc $\gamma \in \beta$. Autrement dit on a l'inclusion $\alpha \subset \beta$, ce qui est la même chose que $\alpha \preccurlyeq \beta$.

• (iii) : Si f est bijective, la réciproque $f^{-1} : \beta \to \alpha$ est aussi strictement croissante [30.1.iii]. Par (ii) ci-dessus on a donc aussi $\beta \preccurlyeq \alpha$ et donc $\alpha = \beta$. Mais par (i) ci-dessus on a aussi

$$\forall \delta \in \beta : \delta \preccurlyeq f^{-1}(\delta) \ .$$

En prenant $\delta = f(\gamma)$ on obtient (en combinaison avec (i) ci-dessus) :

$$\forall \gamma \in \alpha : \gamma \preccurlyeq f(\gamma) \preccurlyeq f^{-1}(f(\gamma)) = \gamma \ .$$

On a donc $f(\gamma) = \gamma$ pour tout $\gamma \in \alpha$, ce qui implique qu'on doit avoir $f = id$.

CQFD

Preuve de [30.6]. Si $f : W \to \alpha$ est un isomorphisme, alors $f^{-1} : \alpha \to W$ l'est aussi. Donc la composée $g \circ f^{-1} : \alpha \to \beta$ est un isomorphisme. Par [30.4] on a donc $\alpha = \beta$ et $g \circ f^{-1} = id$. CQFD

Preuve de [30.7]. On définit la formule $q(x, y)$ comme

$$q(x,y) \quad \overset{\text{déf.}}{\Longleftrightarrow} \quad \begin{cases} y \text{ est un ordinal, } x \in W \text{ et} \\ \exists f : W_{<x} \to y \text{ un isomorphisme.} \end{cases}$$

Selon [30.6] on a l'implication

$$q(x,y) \text{ et } q(x,z) \quad \Longrightarrow \quad y = z$$

et par hypothèse il existe, pour tout $x \in W$ un ordinal α tel qu'on a $q(x,\alpha)$. La formule q remplit donc les conditions de l'axiome de remplacement, ce qui nous permet d'affirmer que la collection β définie par

$$\beta = \{\, \alpha \mid \exists x \in W : q(x,\alpha) \,\}$$

est bien un ensemble. Une fois qu'on sait que β est un ensemble, on peut définir l'ensemble $g \subset W \times \beta$ par

$$g = \{\, (x,\alpha) \in W \times \beta \mid q(x,\alpha) \,\}$$

et il est immédiat de ce qui précède que g est une application surjective de W dans β. En plus, avec [30.6] on peut dire que pour tout $x \in W$ l'ordinal $g(x)$ est l'unique ordinal qui est isomorphe à $W_{<x}$.

Avant de montrer que β est un ordinal et qu'il est isomorphe à W, on prépare le terrain. Pour cela on prend $x \in W$ et on note $f : W_{<x} \to g(x)$ l'unique isomorphisme entre $W_{<x}$ et $g(x)$. Alors selon [30.1.iv] l'application f fournit, pour tout $y \in W_{<x}$, un isomorphisme entre $(W_{<x})_{<y}$ et $g(x)_{\prec f(x)}$. Mais il est immédiat qu'on a l'égalité $(W_{<x})_{<y} = W_{<y}$ et par [30.3] on a l'égalité $g(x)_{\prec f(y)} = f(y)$. Il s'ensuit qu'on a un isomorphisme entre $W_{<y}$ et $f(y)$. Mais $g(y)$ est l'unique ordinal isomorphe à $W_{<y}$, ce qui implique qu'on a $f(y) = g(y)$. On a donc montré la propriété

$$\forall y \in W_{<x} : f(y) = g(y) \quad . \tag{33.59}$$

Avec cette préparation on va montrer que β est un ordinal équivalent à W. Par [28.7] l'ensemble β, qui ne contient que des ordinaux, est bien ordonné par l'appartenance/inclusion. Autrement dit, β vérifie les conditions (O1–4) d'un ordinal. Pour montrer que c'est un ordinal, il suffit donc de montrer qu'il vérifie la condition (O5). Pour le montrer, on prend $\alpha \in \beta$ et $\gamma \in \alpha$ et on tente d'en déduire qu'on a $\gamma \in \beta$. Par définition de β il existe $x \in W$ et un isomorphisme $f : W_{<x} \to \alpha = g(x)$. Selon (33.59) appliqué à l'élément $y = f^{-1}(\gamma)$ on a $\gamma = f(y) = g(y) \in \beta$. Ainsi on a montré l'implication $\gamma \in \alpha \in \beta \Rightarrow \gamma \in \beta$. Cela montre que β vérifie (O5) ; c'est donc bien un ordinal.

On sait déjà que l'application $g : W \to \beta$ est surjective. Pour montrer que c'est un isomorphisme, il suffit donc de montrer qu'il est strictement croissante [30.1.iii]. Pour le faire, on prend $x, y \in W$ avec $y < x$. Par hypothèse il existe un isomorphisme $f : W_{<x} \to g(x)$. Selon (33.59) on a donc l'égalité $g(y) = f(y) \in g(x)$. Par définition de la relation d'ordre $\preccurlyeq$ on a donc $g(y) \prec g(x)$, ce qui montré l'implication $y < x \Rightarrow \alpha_y \prec \alpha_x$. CQFD

Preuve de [30.5]. L'idée de la preuve est de montrer par récurrence transfinie que $(W, \leq)$ vérifie les conditions de [30.7]. Ainsi on aurait l'existence ; l'unicité étant assurée par [30.6] on aurait montré le résultat.

L'hypothèse qu'on veut montrer par récurrence transfinie est l'affirmation que pour tout $x \in W$ il existe un ordinal α et un isomorphisme $f : W_{<x} \to \alpha$. On suppose donc qu'on le sait pour tout $x < x_o$ et on tente d'en déduire que c'est vrai pour x_o. Pour cela on remarque que l'ensemble $W_{<x_o}$ avec la relation d'ordre induite est un ensemble bien ordonné. Et on remarque aussi qu'on a l'égalité $(W_{<x_o})_{<x} = W_{<x}$ pour tout $x \in W_{<x_o}$. Ainsi l'hypothèse de récurrence nous dit que l'ensemble bien ordonné $(W_{<x_o}, \leq)$ vérifie les conditions de [30.7]. Il existe donc un ordinal β et un isomorphisme $g : W_{<x_o} \to \beta$. Ainsi on a vérifié la condition pour la récurrence

transfinie. La propriété est donc vraie pour tout $x \in W$ et on a terminé la preuve.
$\boxed{CQFD}$

Les preuves de §31

Preuve de [31.2]. • (i) : Soit $\beta = \min\{\,\gamma \in S(\aleph) \mid \gamma \approx \aleph\,\}$. Pour montrer qu'on a $\beta = \aleph$ on constate qu'on a par définition de $\aleph$ et de β

$$\beta \in S(\aleph) \quad , \quad \aleph \approx \alpha \quad , \quad \beta \approx \aleph \quad \text{et} \quad \aleph \in S(\alpha) \ .$$

Avec [31.1] les deux premiers se traduisent comme $\beta \subset \aleph$ et $\aleph \subset \alpha$, donc $\beta \subset \alpha$ et de nouveau avec [31.1] $\beta \in S(\alpha)$. Et avec [23.2.iii] les deux derniers impliquent $\beta \approx \alpha$. Par définition de $\aleph$ comme le minimum, on doit donc avoir

$$\aleph \preccurlyeq \beta \ .$$

Avec $\beta \in S(\aleph)$ et [31.1] il s'ensuit immédiatement qu'on a $\beta = \aleph$, ce qui termine la preuve que $\aleph$ est bien un cardinal. Et la définition même de $\aleph$ implique qu'on a $\aleph \approx \alpha$.

• (ii) : Soit α un cardinal et $\beta \prec \alpha$. Alors par définition d'un ordinal on a $\beta \subset \alpha$ et donc il existe une injection $g : \beta \to \alpha$. S'il existe aussi une injection $f : \alpha \to \beta$, alors par [22.1] il existe une bijection $h : \beta \to \alpha$, c'est-à-dire $\beta \approx \alpha$. Mais ceci contredit la définition d'un cardinal, car on aura trouvé un ordinal strictement plus petit que α qui a la même taille que α. Une telle injection $f : \alpha \to \beta$ ne peut donc pas exister.

Dans l'autre sens, on peut d'abord invoquer (i) pour conclure que

$$\aleph = \min\{\,\gamma \in S(\alpha) \mid \gamma \approx \alpha\,\}$$

est un cardinal vérifiant $\aleph \approx \alpha$, c'est-à-dire qu'il existe une bijection $f : \aleph \to \alpha$ qui est en particulier une injection. Si on avait $\aleph \prec \alpha$, alors l'existence de ce f serait en contradiction avec l'hypothèse. On doit donc avoir $\aleph = \alpha$, ce qui veut dire que α est un cardinal.

• (iii) : Supposons qu'on a $\aleph \approx \aleph'$. parce qu ce sont des ordinaux, on a l'une des trois possibilités $\aleph \prec \aleph'$, $\aleph = \aleph'$ ou $\aleph' \prec \aleph$ [28.8]. Dans le premier cas on invoque (ii) avec le cardinal $\alpha = \aleph'$ et l'ordinal $\beta = \aleph$. Et dans ce cas on obtient une contradiction avec l'existence d'une bijection $f : \aleph \to \aleph'$ qui est en particulier injective. Le troisième cas est exclu de la même manière, ce qui montre qu'on doit avoir $\aleph = \aleph'$. Et pour l'implication réciproque, il suffit de prendre l'identité comme bijection.

• (iv) : Si n est un ordinal fini, $S(n)$ l'est aussi, ainsi que tout élément de $S(n)$ [28.16]. Mais un ordinal fini n'est rien d'autre qu'un entier naturel [28.17]. Si pour $m \in S(n)$ on a $m \approx n$, on a donc des injections $n \to m$ et $m \to n$. Selon [25.2] on a donc $n \leq m$ et $m \leq n$, c'est-à-dire $m = n$. Il s'ensuit que le seul élément $m \in S(n)$ vérifiant $m \approx n$ est donc n lui même, et donc n est un cardinal.

• (v) : Par définition on a l'équivalence $\beta \in S(\mathbf{N}) \Leftrightarrow \beta = \mathbf{N}$ ou $\beta \in \mathbf{N}$. Si on a $\beta \in \mathbf{N}$, alors β est un entier naturel, donc un ensemble fini. Il ne peut donc pas exister une bijection $\beta \to \mathbf{N}$. Le seul élément $\beta \in S(\mathbf{N})$ vérifiant $\beta \approx \mathbf{N}$ est donc $\mathbf{N}$ lui même, ce qui montre que $\mathbf{N}$ est bien un cardinal. *CQFD*

Preuve de [31.3]. L'unicité du cardinal est une conséquence immédiate de [31.2.iii] (et le fait que la composée de deux bijection est une bijection).

Pour l'existence, on invoque le théorème du bon-ordre [19.10] (ce qui équivaut à invoquer l'axiome du choix) selon lequel il existe un bon ordre $\leq$ sur A. Avec l'axiome de remplacement on peut invoquer [30.5] pour en déduire qu'il existe un ordinal α tel que l'ensemble bien ordonné $(A, \leq)$ est isomorphe à $(\alpha, \preccurlyeq)$. En particulier on a donc $A \approx \alpha$. Selon [31.2.i] l'ensemble $\aleph$ défini par

$$\aleph = \min\{\, \gamma \in S(\alpha) \mid \gamma \approx \alpha \,\}$$

est un cardinal vérifiant $\aleph \approx \alpha$ et donc $\aleph \approx A$. CQFD

Preuve de [31.5]. Si on a $\mathrm{card}(A) = \mathrm{card}(B)$, on a par définition

$$A \approx \mathrm{card}(A) = \mathrm{card}(B) \approx B$$

et donc par [23.2.iii] on a $A \approx B$. Et si on a $A \approx B$, on a

$$\mathrm{card}(A) \approx A \approx B \approx \mathrm{card}(B)$$

et donc, de nouveau par [23.2.iii], on a $\mathrm{card}(A) \approx \mathrm{card}(B)$. Avec [31.2.iii] il s'ensuit qu'on a $\mathrm{card}(A) = \mathrm{card}(B)$.

Si on a $\mathrm{card}(A) \preccurlyeq \mathrm{card}(B)$, alors par définition cela veut dire qu'on a $\mathrm{card}(A) \subset \mathrm{card}(B)$. Il existe donc une injection $f : \mathrm{card}(A) \to \mathrm{card}(B)$ (l'application identité suffit), autrement dit, on a $\mathrm{card}(A) \precsim \mathrm{card}(B)$. On a donc

$$A \approx \mathrm{card}(A) \precsim \mathrm{card}(B) \approx B$$

et donc par [23.3] on a $A \precsim B$ comme voulu.

Et si on a $A \precsim B$, on peut de toute façon comparer les ordinaux $\mathrm{card}(A)$ et $\mathrm{card}(B)$. Si on n'a pas $\mathrm{card}(A) \preccurlyeq \mathrm{card}(B)$, on doit avoir $\mathrm{card}(B) \prec \mathrm{card}(A)$. Dans ce cas on aurait en particulier $\mathrm{card}(B) \subset \mathrm{card}(A)$ et donc, par l'argument précédent, on aurait $B \precsim A$. Par [22.1] on aurait $A \approx B$ et donc, par la première équivalence, $\mathrm{card}(A) = \mathrm{card}(B)$, ce qui contredit l'hypothèse $\mathrm{card}(B) \prec \mathrm{card}(A)$. On doit donc avoir $\mathrm{card}(A) \preccurlyeq \mathrm{card}(B)$. CQFD

Preuve de [31.12]. Supposons que B est un ensemble contenant tous les cardinaux. Alors l'ensemble A défini comme

$$A = \cup B$$

a la propriété (par définition de la réunion) qu'on a $\aleph \subset A$ pour tout cardinal $\aleph$. On a donc en particulier

$$\mathrm{card}(2^A) \subset A \ .$$

(C'est ici qu'on a besoin des axiomes de remplacement et du choix, car on atttribue un cardinal à l'ensemble 2^A.) Avec [31.6.ii], on en déduit l'inégalité $2^{\mathrm{card}(A)} \preccurlyeq \mathrm{card}(A)$, ce qui est en contradiction avec [31.10]. CQFD

Preuve de [31.13]. • (i) : Si on a $\aleph' \in I(\aleph)$, alors en particulier $\aleph' \in \aleph$, donc $\aleph' \subset \aleph$ (des cardinaux sont en particulier des ordinaux). Et parce que $\aleph'$ est aussi

un cardinal infini, on peut faire le raisonnement

$$\begin{array}{rcl} \aleph'' \in I(\aleph') & \iff & \aleph'' \in \aleph' \ , \ \aleph'' \text{ un cardinal infini} \\ & \overset{\aleph' \subset \aleph}{\iff} & \aleph'' \in \aleph \ , \ \aleph'' \in \aleph' \ , \ \aleph'' \text{ un cardinal infini} \\ & \iff & \aleph'' \in I(\aleph) \text{ et } \aleph'' \prec \aleph' \ , \end{array}$$

ce qui veut dire qu'on a l'égalité $I(\aleph') = \big(I(\aleph)\big)_{\prec \aleph'}$. Si $f : I(\aleph') \to \mathcal{R}(\aleph')$ est l'unique isomorphisme d'ensembles bien ordonnés, on peut invoquer [30.1] et [30.3] pour en déduire qu'on a un isomorphisme

$$f|_{\big(I(\aleph)\big)_{\prec \aleph'}} : \big(I(\aleph)\big)_{\prec \aleph'} = I(\aleph') \to \big(\mathcal{R}(\aleph)\big)_{f(\aleph')} = f(\aleph') \ .$$

Mais par définition de $\mathcal{R}(\aleph')$, c'est l'unique ordinal pour lequel il y a un isomorphisme avec $I(\aleph')$. On doit donc avoir

$$\mathcal{R}(\aleph') = f(\aleph') \in \mathcal{R}(\aleph) \ .$$

• (ii) : Pour $\beta \in \mathcal{R}(\aleph)$ on note $\aleph' = f^{-1}(\beta)$. Le résultat est maintenant une conséquence immédiate de (i). CQFD

Preuve de [31.14]. L'inégalité $\aleph \prec \aleph'$ ne veut rien dire d'autre que l'appartenance $\aleph \in I(\aleph')$. Donc par [31.13.i] on a $\mathcal{R}(\aleph) \prec \mathcal{R}(\aleph')$. D'autre part, si on a l'égalité $\mathcal{R}(\aleph) = \mathcal{R}(\aleph')$, alors par le résultat précédent on ne peut avoir ni $\aleph \prec \aleph'$ ni $\aleph' \prec \aleph$. On doit donc avoir $\aleph = \aleph'$. CQFD

Preuve de [31.15]. Remarquons d'abord que l'unicité est donné par [31.14]. Ensuite, pour l'existence, on suppose dans un premier temps que pour tout $\beta \in \alpha$ il existe un cardinal infini $\aleph$ tel qu'on a $\beta = \mathcal{R}(\aleph)$. On invoque maintenant l'axiome de remplacement avec la formule

$$q(x,y) \qquad \overset{\text{déf}}{=} \qquad y \text{ un cardinal infini et } \mathcal{R}(y) = x \ .$$

À cause de l'unicité [31.14] on a bien $q(x,y)$ et $q(x,z) \Rightarrow y = z$. Et l'hypothèse dit que pour tout $x \in \alpha$ il existe y tel que $q(x,y)$. Par l'axiome de remplacement on obtient donc l'ensemble B défini comme

$$B = \{\, \aleph \mid \exists \beta \in \alpha : \aleph \text{ un cardinal infini et } \mathcal{R}(\aleph) = \beta \,\} \ .$$

Ce B a donc la propriété

$$\aleph \text{ un cardinal infini et } \mathcal{R}(\aleph) \in \alpha \qquad \iff \qquad \aleph \in B \ .$$

On définit maintenant $C = \cup B$, la réunion de tous ces cardinaux et on définit l'ordinal γ comme

$$\gamma = \mathcal{R}\big(2^{\text{card}(C)}\big) \ .$$

Maintenant on prend un ordinal β et on raisonne :

$$\beta \in \alpha \overset{\text{hyp.}}{\Rightarrow} \exists \aleph \text{ un cardinal infini et } \mathcal{R}(\aleph) = \beta \overset{\text{déf. de } B}{\Rightarrow} \aleph \in B$$

$$\overset{\text{déf. de } C}{\Rightarrow} \aleph \subset C \Rightarrow \aleph \overset{[31.6.i]}{=} \operatorname{card}(\aleph) \overset{[31.6.ii]}{\preccurlyeq} \operatorname{card}(C) \overset{[31.10]}{\prec} 2^{\operatorname{card}(C)}$$

$$\overset{[31.14]}{\Rightarrow} \beta = \mathcal{R}(\aleph) \prec \gamma \ .$$

En résumé, on a montré l'implication

$$\beta \in \alpha \implies \beta \in \gamma \qquad \text{c'est-à-dire :} \qquad \alpha \subset \gamma \overset{\text{déf}}{\equiv} \alpha \preccurlyeq \gamma \ .$$

Avec [31.13] on en déduit qu'il existe un cardinal infini $\aleph$ tel que $\alpha = \mathcal{R}(\aleph)$: si $\alpha = \gamma$ on a $\alpha = \mathcal{R}\big(2^{\operatorname{card}(C)}\big)$ et si $\alpha \in \gamma$, alors par [31.13.ii] α sera le rang d'un cardinal infini.

On a donc montré que, si pour tout ordinal β strictement plus petit que α il existe un cardinal infini dont le rang est β, alors il existe un cardinal infini dont le rang est α. On pourrait dire qu'ainsi on a montré par récurrence transfinie (sur les ordinaux) que pour tout ordinal α il existe un cardinal infini dont le rang est α. Mais la collection de tous les ordinaux n'est pas un ensemble. Pour rester dans le cadre de l'axiomatique (ZFC), il faut donc rajouter un petit raisonnement.

On suppose qu'il existe un ordinal α pour lequel il n'existe pas un cardinal infini avec rang α. Dans ce cas il y a deux possibilités : ou bien pour tout β strictement plus petit que α, c'est-à-dire $\beta \in \alpha$, il existe un tel cardinal. Mais par notre raisonnement ci-dessus il existe alors aussi un tel cardinal pour α. Cette contradiction montre qu'il doit y avoir un ordinal $\beta \in \alpha$ pour lequel il n'existe pas un tel cardinal. L'ensemble A défini par

$$A = \{\, \beta \in \alpha \mid \text{ il n'existe pas un cardinal infini } \aleph \text{ tel que } \mathcal{R}(\aleph) = \beta \,\}$$

n'est donc pas vide. En tant qu'ensemble ne contenant que des ordinaux, il existe donc un plus petit élément $\alpha' \in A$ [28.7]. Par définition du plus petit élément, on a donc la propriété que pour tout $\beta \in \alpha'$ il existe un tel cardinal. Mais de nouveau par notre raisonnement ci-dessus, cela implique qu'il existe aussi un tel cardinal pour α', en contradiction avec la définition de A. L'hypothèse qu'il n'existe pas un cardinal infini dont le rang est α nous amène à une contradiction, et donc par l'absurde il s'ensuit que pour tout ordinal α il existe un cardinal infini dont le rang est α.

CQFD

Les preuves de §32

Preuve de [32.1]. • (i) ⇒ (ii) : On suppose qu'il existe $f : \mathbf{N} \to E$ vérifiant $f(n+1) < f(n)$ pour tout $n \in \mathbf{N}$. Alors on définit l'ensemble $A = f[\mathbf{N}] \subset E$, l'image de $\mathbf{N}$ par f. Par (i) il existe $a \in A$ tel que pour tout $x \in A$ on a $x \not< a$. Par définition de A ceci veut dire qu'il existe $n_o \in \mathbf{N}$ tel que $a = f(n_o)$ et que pour tout $n \in \mathbf{N}$ on a $f(n) \not< f(n_o)$. Pour $n = n_o + 1$ ceci est clairement en contradiction avec l'hypothèse sur f. Cette contradiction montre qu'un tel f ne peut pas exister.

• (ii) ⇒ (i) : Par négation de (i) on suppose qu'il existe $A \subset E$, $A \neq \emptyset$ tel que pour tout $a \in A$ il existe $x \in A$ vérifiant $x < a$. Si on définit, pour chaque $a \in A$, l'ensemble $A_a \subset A$ par

$$A_a = \{\, x \in A \mid x < a \,\} \ ,$$

alors l'hypothèse nous dit que les ensembles A_a ne sont pas vides. Par l'axiome du choix il existe donc une fonction $F : A \to A$ vérifiant $F(a) \in A_a$ pour tout $a \in A$ (on choisit dans chaque A_a un élément particulier $F(a)$). L'ensemble A lui-même n'étant pas vide, il existe $a_o \in A$. Avec ces données on invoque [7.8.iii] pour obtenir une suite (définie par récurrence) $f : \mathbf{N} \to A \subset E$ vérifiant

$$f(0) = a_o \qquad \text{et} \qquad \forall n \in \mathbf{N} : f(n+1) = F\big(f(n)\big) \ .$$

Mais par définition de F et les ensembles A_a, cette définition par récurrence se traduit comme

$$f(0) = a_o \qquad \text{et} \qquad \forall n \in \mathbf{N} : f(n+1) < f(n) \ .$$

Autrement dit, f est une fonction vérifiant $f(n+1) < f(n)$ pour tout $n \in \mathbf{N}$. Mais une telle application n'existe pas par (ii). Donc notre hypothèse que la négation de (i) est vrai doit être fausse. CQFD

Preuve de [32.2]. S'il existe un ensemble A vérifiant $A \in A$, alors l'application $f : \mathbf{N} \to A$ définie par

$$\forall n \in \mathbf{N} : f(n) = A$$

sera une application vérifiant $f(n+1) \in f(n)$ pour tout $n \in \mathbf{N}$, et cela est exclu par l'axiome de fondation et l'implication (i) ⇒ (ii) de [32.1].

Et s'il existe deux ensembles A et B vérifiant $A \in B$ et $B \in A$, alors l'application $f : \mathbf{N} \to A \cup B$ définie par

$$\forall n \in \mathbf{N} \qquad : \qquad f(2n) = A \qquad \text{et} \qquad f(2n+1) = B$$

sera une application vérifiant $f(n+1) \in f(n)$ pour tout $n \in \mathbf{N}$, ce qui est comme avant exclu par l'axiome de fondation. CQFD

La liste des axiomes

(Z1) Axiome d'extensionnalité, §1.

$$\forall A, B \ : \ \big[\ \forall C \ : \ C \in A \Longleftrightarrow C \in B \ \big] \implies \big[\ A = B \ \big] \ .$$

(Z2) Axiome de l'ensemble vide, §1.

$$\exists A \ \forall B \ : \ B \notin A \ .$$

Notation : $A \overset{\text{not}}{=} \emptyset$.

(Z3) Axiome de la paire, §1.

$$\forall A, B \ \exists C \ \forall D \ : \ D \in C \iff \big[\ D = A \text{ ou } D = B \ \big] \ .$$

Notation : $C \overset{\text{not}}{=} \{A, B\}$.

(Z4) Axiome de la réunion, §1.

$$\forall A \ \exists B \ \forall C \ : \ C \in B \iff \big[\ \exists D \ : \ D \in A \text{ et } C \in D \ \big] \ .$$

Notation : $B \overset{\text{not}}{=} \cup A$ ou $B \overset{\text{not}}{=} \underset{D \in A}{\cup} D$.

(Z5) Axiome de séparation, §1.

$$\forall A \ \exists B \ \forall C \ : \ C \in B \iff \big[\ C \in A \text{ et } p(C) \ \big] \ .$$

Notation : $B \overset{\text{not}}{=} \{C \in A \mid p(C)\}$.

(Z6) Axiome de l'ensemble des parties, §2.

$$\forall A \ \exists B \ \forall C \ : \ C \in B \iff C \subset A \ .$$

Notation : $B \overset{\text{not}}{=} \mathcal{P}(A)$.

(Z7) Axiome de l'infini, §6.

$$\exists \, A \ : \ \emptyset \in A \text{ et } \forall a \in A : a \cup \{a\} \in A \ .$$

(Z8)=(C) Axiome du choix, §18.

$$\forall B, I, g \ : \ g : I \to \mathcal{P}(B) \setminus \{\emptyset\} \implies \Big[\ \exists f \ : \ f : I \to B \text{ et } \big[\ \forall i \in I : f(i) \in g(i) \ \big] \ \Big] \ .$$

L'application f est appelée une fonction de choix.

(F) Axiome de remplacement, deuxième version, §29.

$$\forall A \ : \ \Big[\ \forall x \in A \ \forall y, z \ : \ \big[\ q(x,y) \text{ et } q(x,z) \ \big] \implies y = z \ \Big] \quad \implies$$
$$\Big[\ \exists B \ \forall C \ : \ C \in B \iff \big[\ \exists x \ : \ x \in A \text{ et } q(x,C) \ \big] \ \Big] \ .$$

Notation : $B \overset{\text{not}}{=} \{C \mid \exists x \in A : q(x,C)\}$.

(Z10) Axiome de fondation, §32.

$$\forall A \ : \ A \neq \emptyset \implies \big[\ \exists a \in A \ \forall x \in A : x \notin a \ \big] \ .$$

Bibliographie

Pour écrire ce texte, j'ai consulté plusieurs ouvrages pour en copier ce qui me convenait. Je me suis inspiré en particulier du livre de James Dugundji [**Dug66**], mais le lecteur trouvera certainement des traces d'autres ouvrages. La liste complète se trouve ci-dessous.

[AZ98] Martin Aigner and Günter M. Ziegler, *Proofs from the book*, Springer, Berlin, 1998.

[AZ06] ———, *Raisonnements divins*, Springer, Berlin, 2006, Traduction en français de [**AZ98**].

[Bou07] Nicolas Bourbaki, *Éléments d'histoire des mathématiques*, Springer-Verlag, Berlin, 1984, 2007.

[Cam78] Paul J. Campbell, *The origin of "Zorn's lemma"*, Historia Mathematica **5** (1978), 77–89.

[Ded72] Richard Dedekind, *Stetigkeit und irrationale Zahlen*, Braunschweig, 1872.

[Ded87] ———, *Was sind und was sollen die Zahlen*, 1887.

[Ded63] ———, *Essays on the theory of numbers*, Dover Publications, Inc., New York, NY, 1963, Translation into english of [**Ded72**] and [**Ded87**].

[Dra74] Frank R. Drake, *Set theory : an introduction to large cardinals*, Studies in Logic and the Foundations of Mathematics 76, North-Holland Publishing Company, Amsterdam, 1974.

[Dug66] James Dugundji, *Topology*, Allyn and Bacon, Inc., Boston, MA, 1966.

[Ebb07] H.-D. Ebbinghaus, *Ernst Zermelo, an approach to his life and work*, Springer, Berlin, 2007.

[EHH98] H.-D. Ebbinghaus, H. Hermes, and F. Hirzebruch, *Les nombres*, Vuibert, Paris, 1983, 1998.

[GS65] Carl Friedrich Gauß and Heinrich Christian Schumacher, *Briefwechsel zwischen C.F. Gauß und H.C. Schumacher*, vol. 3, C.A.F. Peters, Altona, 1860/65, Scan sur `gauss.adw-goe.de`, le site de l'Akademie der Wissenschaften zu Göttingen.

[Her06] Horst Herrlich, *Axiom of choice*, Springer-Verlag, Berlin, 2006.

[JW96] Winfried Just and Martin Weese, *Discovering modern set theory I. The basics*, AMS, Providence, RI, 1996.

[Kel55] John L. Kelley, *General topology*, D. Van Nostrand Company, Inc, Princeton, NJ, 1955.

[Kor11] A. Korselt, *Über einen Beweis des Äquivalenzsatzes*, Math. Annalen **70** (1911), 294–296.

[Kri07] Jean-Louis Krivine, *Théorie des ensembles*, 2^e ed., Cassini, Paris, 2007.

[Kur22] Casimir Kuratowski, *Une méthode d'élimination des nombres transfinis des raisonnements mathématiques*, Fundamenta Mathematicae **3** (1922), 76–108.

[Lan51] Edmund Landau, *Foundations of analysis : the arithmetic of whole, rational, irrational and complex numbers*, Chelsea Publishing Company, 1951.

[Moo82] Gregory H. Moore, *Zermelo's axiom of choice. its origins, development & influence*, Dover Publications, Inc., Mineola, New York, 1982.

[Pea91] Giuseppe Peano, *Sul concetto di numero*, Rivista di matematica **1** (1891), 87–102, 256–267.

[Pea08] ———, *Formulario mathematico editio V*, Fratres Bocca Editores, Torino, 1908.

[Pea60] ———, *Formulario mathematico editio V*, Edizioni Cremonese, Roma, 1960, Riproduzione in fac-simile dell'edizione originale [**Pea08**], Ugo Cassina ed.

[Pot04] Michael Potter, *Set theory and its philosophy*, Oxford University Press, Oxford, 2004.

[RR63] Herman Rubin and Jean E. Rubin, *Equivalents of the axiom of choice*, North-Holland Publishing Company, Amsterdam, 1963.

[Szp09] Aviva Szpirglas (ed.), *Mathématiques Algèbre L3 : Cours complet avec 400 tests et exercices corrigés*, Collection SCIENCES, Pearson Education, 2009.

[Wol05] Robert S. Wolf, *A tour through mathematical logic*, The Mathematical Association of America, Washington DC, 2005.

[Zor35] Max Zorn, *A remark on method in transfinite algebra*, Bulletin of the AMS **41** (1935), 667–670.