Théorie des Ensembles et Arithmétique

Florent Michel

,

Résumé

Ce document présente quelques bases de logique mathématique, théorie des ensembles, et arithmétique. Nous nous baserons essentiellement sur la logique du premier ordre et la théorie de Zermelo–Fraenkel avec axiome du choix (ZFC). L'objectif principal est de montrer une construction possible de certains objets mathématiques courants, notamments les nombres entiers, et l'obtention de quelques-unes de leur propriétés, à partir d'idées simples.

Table des matières

Chapitre 1 : Théorie des Ensembles

Cette partie présente quelques bases de logique mathématique et de théorie des ensembles.

1.1 Logique du premier ordre

La *logique du premier ordre*, aussi appelée *logique des prédicats* ou *calcul des prédicats du premier ordre*, est un cadre semi-formel[1] permettant de définir des théories. On peut la voir comme un langage, ou comme un ensemble d'éléments de langage. Elle est utilisée tant en mathématiques qu'en philosophie, linguistique et informatique. Nous l'aborderons ici principalement d'un point de vue mathématique. On considère ici une notion très basique du terme *langage*, que l'on considère formé de deux éléments :

- Un ensemble (au sens intuitif du terme) de *symboles*.

[1] On adopte ici le point de vue que la logique du premier ordre ne repose pas sur une théorie vue comme plus fondamentale. Ses concepts fondamentaux sont ainsi définis intuitivement (puisque nous n'avons aucun concept plus fondamental qui permettrait de les définir formellement), d'où le qualificatif de « semi-formel », et non « formel ».

- Des règles de formations de *phrases* à partir des symboles.

Dans cette vision, les symboles constituent les fondations du langage, premettant de contruire les phrases, porteuses de sens.[2] On sépare parfois les symboles en deux catégories : *fondamentaux* s'ils forment un ensemble unsécable, ou *composites* s'ils sont formés d'autres symboles.

Intuitivement, la logique du premier ordre a pour symboles des variables (décrivant un domaine d'objets non logiques, c'est-à-dire non définis par la logique du premier ordre elle-même) quantifiées (par les quantificateurs « pour tout » et « il existe ») ou non, des symboles non logiques, ainsi que des connecteurs, utilisés pour construire des phrases, appelées *formules*. Ces dernières sont aussi appelées *propositions*, *énoncés* ou *prédicats*.

Elle est une extension de la *logique propositionelle*, qui exprime des énoncés, ou *propositions*, aussi appelés *prédicats*, auxquels on attribue une valeur dite de *vérité* : vrai ou faux. Chaque proposition est soit vraie soit fausse, et ne peut être les deux simultanément. Ces énoncés peuvent être liés par conjonction, disjonction, implication, équivalence, ou modifés par négation. La logique du premier ordre contient, en outre, des variables et quantificateurs, ce qui la rend plus expressive. On peut dire qu'elle contient la logique propositionelle, au sens où cette dernière est équivalente à la logique du premier ordre élaguée des variables et quantificateurs.

Une théorie définie dans le cadre de la logique du premier ordre porte sur un domaine de discours spécifié que les variables quantifiées décrivent, permettant de définir des prédicats sur ce domaine, auxquels un ensemble d'axiomes tenus pour vrais permet d'associer une valeur de vérité. Un prédicat ne peut avoir pour arguments que des variables sur ce domaine, et seules les variables peuvent être quantifiés. Cela distingue la logique du premier ordre des logiques d'ordre supérieur, où un prédicat peut avoir un prédicat plus général comme argument ou des quantificateurs de prédicats peuvent être autorisés.

Plus formellement, une théorie définie dans le cadre de la logique du premier ordre se compose des éléments suivants :

- Un *alphabet*, c'est-à-dire un ensemble (au sens intuitif du terme) de symboles, dont certaines chaînes forment des *termes*. On divise généralement les symboles et deux catégories : les *symboles logiques*, dont la signification est fixée, et les *symboles non logiques*, dont le sens n'est pas univoquement défini par la théorie et doit être défini au cas par cas. Certains de ces symboles sont définis par la logique du premier ordre ; d'autres peuvent être propres à la théorie.
- Un *domaine de discours* non vide que les variables décrivent (si x désigne une variable, la formule $\exists x \mathsf{V}$ est toujours vraie (voir ci-dessous pour la signification de cette formule)).
- Des *règles de formation*, exprimant comment construire les termes et formules. Là encore, certaines sont définies par la logique du premier ordre et d'autres peuvent être propres à la théorie.
- Des *formules* (aussi appelées *propositions*) obtenues à partir de ces règles, exprimant des prédicats. (Le terme *prédicat* est aussi utilisé pour désigner une formule elle-même.) Une proposition est toujours vraie ou fausse[3], et ne peut être simultanément vraie et fausse. Deux formules seront dites *équivalentes* si elles prennent toujours la même valeur de vérité.
  - Si f et g sont deux formules équivalentes, g et f sont équivalentes.
  - Si f et g sont trois formules telles que f et g sont équivalentes et g et h sont équivalentes, alors f et h sont équivalentes.
- Un ensemble d'*axiomes*, ou propositions tenues pour vraies. Ces axiomes permettent en général de déterminer la valeur de vérité d'autres prédicats.

1.1.1 Symboles logiques

Les symboles logiques incluent :

- Le symbole de quantification universelle $\forall$ (« pour tout »).
- Le symbole de quantification existentielle $\exists$ (« il existe »).
- Le connecteur de conjonction $\wedge$ (« et ») : si P et Q sont deux formules, $P \wedge Q$ est vraie si P et Q sont vraies et fausse sinon.
- Le connecteur de disjonction $\vee$ (« ou ») : si P et Q sont deux formules, $P \vee Q$ est vraie si P est vraie ou si Q est vraie et fausse sinon.
- Le connecteur de négation $\neg$ (« non ») : si P est une formule, $\neg P$ est vraie si P est fausse et fausse si P est vraie.

[2] Ce sens étant défini, *in fine*, par un élément extérieur au langage, par exemple l'intuition de qui l'utilise.
[3] À moins d'inclure la valeur de vérité indéfinie, voir section ??.

- Le connecteur d'implication $\Rightarrow$ (« implique ») : si P et Q sont deux formules, $P \Rightarrow Q$ est fausse si P est vraie et Q est fausse et vraie sinon. La formule $P \Rightarrow Q$ est ainsi équivalente à $Q \vee \neg P$ (voir ci-dessous pour la signification des parenthèses et les règles d'évaluation).
- Le connecteur $\Leftarrow$: si P et Q sont deux formules, $P \Leftarrow Q$ est fausse si P est fausse et Q est vraie et vraie sinon. La formule $P \Leftarrow Q$ est ainsi équivalente à $P \vee \neg Q$.
- Le connecteur biconditionnel $\Leftrightarrow$ (« est équivalent à ») : si P et Q sont deux formules, $P \Leftrightarrow Q$ est vraie si P et Q sont soit toutes deux vraies soit toutes deux fausses, et fausse sinon. La formule $P \Leftrightarrow Q$ est ainsi équivalente à $(P \wedge Q) \vee (\neg P \wedge \neg Q)$. Notons que, si P et Q sont deux prédicats, si $P \Leftrightarrow Q$ est vrai, alors $(\neg P) \Leftrightarrow (\neg Q)$ est vrai aussi.
- Un ensemble infini de *variables*, souvent notées par des lettres grecques ou latines, éventuellement avec des indices ou exposants. Les variables sont interprétées comme décrivant un domaine d'objets de base, qui ne peut être vide. Elles sont aussi parfois appelées *paramètres*.

On définit également les constantes de vérité V pour « vraie » et F pour « fausse ». Elles sont deux formules, et F est équivalente à $\neg \mathsf{V}$.` Si f est une formule, ces deux constantes de vérité sont équivalentes, respectivements, aux formules $f \vee (\neg f)$ et $f \wedge (\neg f)$.

Enfin, on peut définir le connecteur (non standard) de vérité $\sharp$: si f est une formule, $\sharp f$ est vraie si f est vraie et fausse sinon. (Avec ces notations, $\sharp f$ a toujours la même valeur de vérité que f. On introduit ce nouveau connecteur uniquement pour pouvoir exprimer la véracité d'une formule dans le cadre de la théorie ; il sera très peu employé dans la suite.) Ce dernier connecteur ne rendant pas la théorie plus expressive, on l'omettra dans la suite sauf mention contraire.

Pour être plus formel, on peut ne définir dans un premiers temps que les variables et constantes de vérité, puis les symboles non logiques, les termes, et enfin les autres symboles logiques avec les formules qu'ils permettent de construire et l'égalité (voir ci-dessous). On adoptera ce point de vue dans la suite. Pour le moment, les symboles logiques (y compris l'égalité définie ci-dessous) ne sont donnés que comme une liste de symboles utilisés, qui prendront leur sens lorsque les formules et la sémantique seront définies.

Si P est un prédicat à un ou plusieurs paramètres libres $a_1 a_2 \ldots$ et si $b_1 b_2 \ldots$ sont un même nombre de variables, on notera $P b_1 b_2 \ldots$, ou $P(b_1, b_2, \ldots)$ la formule obtenue en remplaçant dans P les paramètres $a_1 a_2 \ldots$ par $b_1 b_2 \ldots$.

1.1.2 Égalité

La *logique du premier ordre avec égalité* inclut un autre symbole logique, $=$, définissant une relation binaire, dite *égalité*, satisfaisant les axiomes suivants :

- Axiome de réciprocité : $\forall x\,(x = x)$.
- Réflexivité : $\forall x\,\forall y\,[(x = y) \Rightarrow (y = x)]$.
- Transitivité : $\forall x\,\forall y\,\forall z\,[((x = y) \wedge (y = z)) \Rightarrow (x = z)]$.
- Schéma d'axiomes de Leibniz : Soit P un prédicat à une variable. On a : $\forall x\,\forall y\,[(x = y) \Rightarrow (P(x) \Leftrightarrow P(y))]$.

Deux objets x et y définis par une théorie sont dits *égaux* si $x = y$. On considèrera alors qu'il s'agit du même objet. En particulier, changer l'un pour l'autre dans une formule ne modifie pas sa valeur de vérité.

Si x, y et z sont trois objets, on notera parfois par $x = y = z$ la formule $(x = y) \wedge (y = z)$.

En présence de l'égalité, on définit aussi le symbole d'*inégalité* $\neq$ définissant une relation binaire comme suit : la formule $x \neq y$ est équivalente à $\neg(x = y)$.

1.1.3 Symboles non logiques

Un symbole non logique est un symbole n'ayant pas de signification donnée par la logique du premier ordre. Il représentent généralement un prédicat, pouvant dépendre de variables placées à sa droite, éventuellement entre parenthèses.

1.1.4 Parenthèses, symboles (,), [,]

Si f est une formule, alors (f) et $[f]$ sont deux formule équivalentes à f. Nous omettrons parfois les parenthèses lorsque qu'il n'y a pas d'ambiguité sur la manière dont elles peuvent être incluses, ou lorsque les différentes manières de les inclure donnent des formules équivalentes.

L'écriture d'une formule en terme de sous-formules contient toujours des arenthèses implicites. Ainsi, si les symboles f et g désignent deux formules, si $\mathrm{C_u}$ est un connecteur unaire et $\mathrm{C_b}$ un connecteur binaire, alors la notation $\mathrm{C_u}\, f$ désigne $\mathrm{C_u}(f)$ et $f\, \mathrm{C_b}\, g$ désigne $(f)\, \mathrm{C_b}(g)$.

1.1.5 Termes

Les termes sont définis comme suit :

- Si P est un prédicat ne dépendant d'aucune variable, alors P est un terme.
- Si P est un prédicat dépendant des variables $a_1 \dots a_N$, alors $Pa_1 \dots a_N$, aussi noté $P(a_1 \dots a_N)$, est un terme.
- En présence de l'égalité, si x et y sont deux variables, alors $x = y$ est un terme.

Une théorie formulée dans le cadre de la logique du premier ordre peut définir de règles spécifiques de construction de prédicats, par exemple *via* des relations binaires (*cf* section 1.1.10).

1.1.6 Formules

Les formules sont définies de la manière suivante :

- Tout terme est une formule.
- Si x est une variable et f une formule dans laquelle x n'est pas quantifiée, alors $\exists x\,(f)$ et $\forall x\,(f)$ sont des formules. On les notera parfois respectivement $\exists x,\ f$ et $\forall x,\ f$ pour plus de lisibilité.
- D'autres formules sont construites à l'aide des autres symboles logiques :
  - Si f est une formule, alors $\neg(f)$ (et $\sharp(f)$, si on l'admet dans la théorie) sont des formules.
  - Si f et g sont deux formules telles qu'aucune variable quantifiée dans l'une n'apparaît dans l'autre, alors $(f) \vee (g)$, $(f) \wedge (g)$, $(f) \Rightarrow (g)$, $(f) \Leftarrow (g)$ et $(f) \Leftrightarrow (g)$ sont des formules.

Une variable apparaissant dans une formule (aussi dite *paramètre* de la formule) est dite *liée* si elle est quantifiée (*i.e.*, si l'une de ses occurrences est immédiatement précédée d'un quantificateur) et *libre* si elle ne l'est pas.[4] On impose parfois (et on le fera par la suite sauf mention contraire) qu'une même variable ne puisse être quantfiée plus d'une fois dans une même formule. Si une formule F contient des variables libres $a_1 a_2 \dots$, et si $\alpha_1 \alpha_2 \dots$ sont autant d'éléments définis par une théorie, on note parfois $F\alpha_1\alpha_2 \dots$ ou $F(\alpha_1\alpha_2 \dots)$ la formule obtenue à partir de F en remplaçant $a_1 a_2 \dots$ par $\alpha_1\alpha_2 \dots$. Comme annoncé ci-dessus, à chaque formule correspond une unique valeur de vérité, vraie ou fausse. Ainsi, une formule non vraie est fausse, une formule vraie est non fausse, une formule fausse est non vraie et une formule non fausse est vraie.

Une formule peut être représentée par un symbole non logique. Ce lien peut être noté par le dit symbole suivi de « : » puis de la dite formule ; on dira de ce lien qu'il *définit* le symbole non logique, qui peut alors être employé comme un terme, avec la valeur de vérité associée à la formule qui lui est liée. Une formule ne peut contenir de symbole non logique qui ne soit précédemment défini.

Parfois, une virgule « , » est utilisée pour séparer deux parties d'une formule et la rendre plus lisible, sans en modifier le sens. Chaque partie d'une formule ainsi définie doit être une formule à part entière.

Une formule faisant partie d'une autre formule est dite *sous-formule*.

NB : Un prédicat ne peut référer à un prédicat que si ce dernier est déjà défini. En particulier, il ne peut référer à lui-même, sans quoi on arrive vite à des paradoxes. (Par exemple, si on pouvait definir in prédicat P par $P : \neg P$, alors il serait vrai s'il est faux et faux s'il est vrai.)

1.1.7 Formule à nombre non spécifié de paramètres

Il est parfois utile de considérer des formules avec un nombre non spécifié de variables. Celles-ci peuvent alors être collectivement désignés par une suite de symboles séparés de points de suspensions, par exemple $a_1 \cdots a_p$. Notons formellement S cette séquence. Les notations $\forall S$ et $\exists S$ désignent, respectivement, les séquences de quantification universelles et existentielles pour chacune des variables. Ainsi,

- Si la séquence S est vide, *i.e.* ne contient aucune variable, alors $\forall S$ et $\exists S$ ne représentent rien : si f est une formule, $\forall S\ f$ et $\exists\ f$ représentent simplement f.
- Si $S = a$ où a est une variable, $\forall S$ représente $\forall a$ et $\exists S$ représente $\exists a$.
- Si $S = ab$ où a et b sont deux variables, $\forall S$ représente $\forall a \forall b$ et $\exists S$ représente $\exists a \exists b$.
- Si $S = a_1 a_2 \cdots a_p$ où a_1, a_2, ..., a_p sont des variables, $\forall S$ représente $\forall a_1 \forall a_2 \dots \forall a_p$ et $\exists S$ représente $\exists a_1 \exists a_2 \dots \exists a_p$.

[4] Afin de simplifier les tournures de phrases, on parlera parfois, quand il n'y a pas de confusion possible, simplement de « variables » ou « paramètres » d'une formule pour désigner ses variables libres.

1.1.8 Quantificateur d'unicité

En logique du premier ordre avec égalité, on définit le quantificateur $\exists!$ de la manière suivante : si P est un prédicat à un paramètre libre x et d'éventuels autres paramètres dénotés par $a_1 \dots a_p$, la formule $\exists!\, x\, Pxa_1 \dots a_p$ est équivalente à $(\exists x\, Pxa_1 \dots a_p) \wedge (\forall x \forall y\, (Pxa_1 \dots a_p \wedge Pya_1 \dots a_p) \Rightarrow (x = y))$.

Moins formellement, on définit l'unicité de la manière suivante : dans le cadre d'une théorie définie en logique du premier ordre avec égalité, si P est un prédicat à un paramètre libre, on dira qu'*il existe au plus un unique objet satisfaisant* P si et seulement si le prédicat suivant est vrai :

$$\forall x\, \forall y\, (P(x) \wedge P(y)) \Rightarrow (x = y)\,.$$

On dira qu'*il existe exactement un objet satisfaisant* P si et seulement si le prédicat suivant est vrai :

$$(\forall x\, \forall y\, (P(x) \wedge P(y)) \Rightarrow (x = y)) \wedge (\exists x\, P(x))\,.$$

Ce dernier pourra être abrégé en :

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

1.1.9 Sémantique

Les règles énoncées ci-dessus, complétées par des règles propres à chaque théorie, permettent (au moins dans certains cas) d'attribuer une *valeur de vérité* à une formule. Les parenthèses (et) (ou [et]), indiquent que, pour évaluer la valeur d'une formule (vraie ou fausse), la formule délimitée par la premiere (à gauche) et la seconde (à droite) est évaluée en tant que formule indépendante. Si une formule est construite à partir d'autres formules, sa valeur peut dépendre des leurs, et peut être explicitée par une table de vérité (voir ci-dessous).

Cinq autres règles sont :

- Les variables n'ont pas de sens intrinsèque. Ainsi, si f est une formule faisant intervenir une variable x, et si y est une variable n'apparaissant pas dans f, alors remplacer toutes les occurrences de x par y dans f ne peut modifier sa valeur de vérité : la formule ainsi obtenue est équivalente à f. On considèrera parfois que la formule obtenue est la même (ou que les deux séquences de symboles représentent la même formule).
- Si f est une formule et x et y deux variables qui ne sont pas quantifiées dans f, alors les formules $\forall x\, \forall y\, f$ et $\forall y\, \forall x\, f$ sont équivalentes.
- La valeur de vérité d'une formule est inchangée par le remplacement d'une sous-formule par une formule équivalente.
- Si une formule peut s'écrire comme une séquence de sous-formules et de connecteurs telle qu'elle prend toujours la même valeur de vérité lorsque ces sous-formules sont remplacées indépendamment par V ou par F, alors elle prend cette valeur de vérité, et est équivalente à V si vraie ou à F si fausse.

On omet parois les parenthèses dans une formule lorsque celles-ci ne modifie pas sa valeur de vérité ; l'ordre d'évaluation des differents termes d'une formule est alors déterminé par les règles suivantes :

- L'évaluation s'effectue de gauche à droite sauf si cela est contraire à une des règles ci-dessous.
- Les prédicats sont évalués en premier.
- Lorsqu'une parenthèse ouvrante est atteinte, la formule se trouvant entre elle et la parenthèse fermante correspondante est évaluée en priorité.
- Ordre d'évaluation des connecteurs et quantificateurs : d'abords les quantificateurs $\exists$ et $\forall$, puis $\neg$, puis (en présence de l'égalité) $=$, puis $\wedge$ et $\vee$ (avec la même priorité), puis $\Rightarrow$, $\Leftarrow$ et $\Leftrightarrow$ (avec la même priorité).

Un connecteur binaire C est dit *transitif* si, pour toutes formules f, g et h, les formules $(f\,\mathrm{C}\,g)\,\mathrm{C}\,h$ et $\mathrm{C}(g\,\mathrm{C}\,h)$ sont équivalentes. Un connecteur binaire C est dit *symmétrique* si, pour toutes formules f et g, les formules $f\,\mathrm{C}\,g$ et $g\,\mathrm{C}\,f$ sont équivalentes.

Dans la suite, si C désigne un connecteur transitif et si f, g et h sont trois formules, on omettra parfois les parenthèses dans des formules de la forme $(f\,\mathrm{C}\,g)\,\mathrm{C}\,h$ ou $f\,\mathrm{C}(g\,\mathrm{C}\,h)$. Plus généralement, on omettra parfois les parenthèses lorsque toutes les manières d'ajouter des parenthèses pour obtenir une formule correctement formée donnent des formules équivalentes.

Si f est une formule et x une variable n'apparaissant pas comme variable liée dans f, la formule $\exists x f$ est vraie s'il existe au moins une valeur possible pour x telle que la formule obtenue en remplaçant x par cette valeur dans f est vraie, et fausse

si toutes les formules obtenues en remplaçant x par chacune de ses valeurs possible sont fausses. Sous les mêmes conditions, la formule $\forall x\, f$ est fausse s'il existe au moins une valeur possible pour x telle que la formule obtenue en remplaçant x par cette valeur dans f est fausse, et vraie si toutes les formules obtenues en remplaçant x par chacune de ses valeurs possible sont vraies. On formalise cela par les règles suivantes :

- si x est une variable et f une formule dans laquelle x n'apparait pas, $\forall x\, f$ est équivalente à f ;
- pour toute variable x et toute formule f, la formule $\forall x\, f$ est équivalente à $\neg(\exists x\, \neg f)$;
- soit f une formule admettant exactement $a_1 a_2 \dots a_n$ pour paramètres libres ; si $\forall a_1\, \forall a_2 \cdots \forall a_n\, f$ est vraie, alors f est équivalente à V ;
- en présence de l'égalité, si $f(x)$ est une formule à un paramètre libre éventuel x et a un objet, alors $\exists x\, (x = a) \wedge f(x)$ est équivalente à $f(a)$.

Ainsi, par exemple, si f est une formule et x une variable, la formule $\forall x\, (f \Leftrightarrow f)$ est vraie. En effet,

- la formule $f \Leftrightarrow f$ est vraie que f soit vraie ou fausse, donc elle est équivalente à V,
- la formule $\forall x\, (f \Leftrightarrow f)$ est donc éuivalente à $\forall x\, \mathsf{V}$, donc à V, et donc vraie.

Quelques conséquences immédiates sont (en remplaçant f par $\neg f$ et en notant que $\neg(\neg f))$ est équivalente à f pour toute formule f) :

- Si f est une formule et x et y deux variables qui ne sont pas quantifiées dans f, alors les formules $\exists x\, \exists y\, f$ et $\exists y\, \exists x\, f$ sont équivalentes.
- si x est une variable, alors $\exists x\, \mathsf{F}$ est fausse (en effet, sa négation est $\forall x\, \mathsf{V}$, qui est vraie) et $\exists x\, \mathsf{V}$ est vraie (en effet, sa négation est $\forall x\, \mathsf{F}$, qui est fausse) ;
- soit f une formule admettant exactement $a_1 a_2 \dots a_n$ pour paramètres libres ; si $\exists a_1\, \exists a_2 \cdots \exists a_n\, f$ est fausse, alors f est équivalente à F ;
- soit f et g deux formules à un paramètre libre ; les formules $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ et $\forall x\, (f(x) \wedge g(x))$ sont équivalentes [5] ; em soit f et g deux formules à un paramètre libre ; si $\forall x\, f(x)$ est vraie, alors les formules $\forall x\, (f(x) \wedge g(x))$ et $\forall x\, g(x)$ sont équivalentes ;
- soit f et g deux formules à un paramètre libre ; si $\exists x\, f(x)$ est fausse, alors les formules $\forall x\, (f(x) \vee g(x))$ et $\forall x\, g(x)$ sont équivalentes (en effet, $\forall x\, \neg f(x)$ est alors vraie, donc f est équivalente à F, et donc $f(x) \vee g(x)$ à $g(x)$) ;
- soit f et g deux formules à un paramètre libre ; si $\exists x\, f(x)$ est fausse, alors la formule $\forall x\, (f(x) \wedge g(x))$ est fausse ;
- soit f et g deux formules à un paramètre libre ; si $\forall x\, f(x)$ est vraie, alors la formule $\forall x\, (f(x) \vee g(x))$ est vraie ;
- soit f une formule à un paramètre libre ; si $\forall x\, f(x)$ est vraie, alors la formule $\exists x\, f(x)$ est vraie ;
- si x est une variable et f une formule dans laquelle x n'apparait pas, $\exists x\, f$ est équivalente à f (en effet, x n'apparait pas dans f, donc $\forall x\, \neg f$ est équivalente à $\neg f$, donc $\neg(\forall x\, \neg f)$ est équivalente à f, et donc $\exists x\, f$ à f) ;
- pour toute variable x et toute formule f dans laquelle x n'est pas une variable quantifiée, la formule $\exists x\, f$ est équivalente à $\neg(\forall x\, \neg f)$.
- soit f et g deux formules à un paramètre libre ; les formules $(\exists x\, f(x)) \vee (\exists y\, g(y))$ et $\exists x\, (f(x) \vee g(x))$ sont équivalentes ;
- soit f et g deux formules et x une variable ; si $\forall x\, f$ et $\forall x\, (f \Rightarrow g)$ sont vraies, alors $\forall x\, g$ est vraie (puisqu'alors $\forall x\, (f \wedge (f \Rightarrow g))$ est vraie) ;
- soit x une variable et f et g deux formules (faisant ou non intervenir x) ; si $\forall x\, f$ et $\exists x\, (f \Rightarrow g)$ sont vraies, alors $\exists x\, g$ est vraie (en effet, $\forall x\, \neg(f \Rightarrow g)$ est fausse, donc $\forall x\, (f \wedge \neg g)$ est fausse, donc $(\forall y\, f) \wedge (\forall x\, \neg g)$ est fausse ; puisque $\forall y\, f$ est vraie, on en déduit que $\forall x\, \neg g$ est fausse, et donc que $\exists x\, g$ est vraie) ;
- soit x une variable et f et g deux formules (faisant ou non intervenir x) ; si $\exists x\, f$ et $\forall x\, (f \Rightarrow g)$ sont vraies, alors $\exists x\, g$ est vraie (en effet, $\forall x\, (g \vee \neg f)$ est vraie, donc, si $\exists x\, g$ était fausse, on aurait $\forall x\, ((g \vee \neg f) \wedge (\neg g))$, donc $\forall x\, \neg f$, ce qui n'est pas le cas puisque $\exists x\, f(x)$ est vraie).

[5] En effet,

- Si $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ est vraie, alors $\forall x\, f(x)$ et $\forall y\, g(y)$ sont vraies, donc f et g sont équivalentes à V, donc $f(x) \wedge g(x)$ également, donc $\forall x\, f(x) \wedge g(x)$ est vraie.
- Si $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ est fausse, alors $\forall x\, f(x) \wedge g(x)$ doit être fausse. En effet, si elle était vraie, alors $f(x) \wedge g(x)$ serait équivalente à V, donc f et g également, et donc $(\forall x\, f(x)) \wedge (\forall y\, g(y))$ serait vraie.

Stricto sensu, il est donc possible de se passer d'un de ces deux quantificateurs, ou de voir l'un d'eux comme fondamental et l'autre comme dérivé. Par exemple, on peut voir le quantificateur $\exists$ comme le seul quantificateur fondamental, et définir $\forall$ *via* l'équivalence de $\forall x\ f$ et $\neg(\exists x\ \neg f)$ pour toute variable x et toute formule f.

Attention : Une formule vraie (au sens où sa valeur de vérité est « vrai ») n'est pas nécessairement équivalente à V. De même, une formule faussee (au sens où sa valeur de vérité est « faux ») n'est pas nécessairement équivalente à F. Par contre, une formule équivalente à V est nécessairement vraie et une formule équivalente à F nécessairement fausse.

1.1.10 Relations binaires

Une théorie définie dans le cadre de la logique du premier ordre peut inclure des relations binaires entre les objets de son domaine de discours, chacune étant représentée par un symbole. Si x et y sont deux variables, et R le symbole dénotant une relation binaire, alors $x\ R\ y$ est un terme. L'égalité est un exemple de reation binaire, avec pour symbole $=$.

Soit P un prédicat dépendant de deux variables. On peut définir une relation binaire R par la formule

$$\forall x \forall y\,((x\ R\ y) \Leftrightarrow Pxy),$$

signifiant que, pour chaque x et chaque y, $x\ R\ y$ est vrai si et seulement si Pxy est vrai. Autrement dit, cette formule signiie que les prédicats Pxy et $x\ R\ y$ sont équivalents.

Lors de l'évaluation d'une formule, et sauf mention contraire, les relations binaires autres que l'égalité sont prioritaires sur cette dernière, mais pas sur le connecteur $\neq$.

1.1.11 Réciproque

Soit f et g deux formules n'ayant pas de quantificateur et $P : f \Rightarrow g$. On suppose que le connecteur reliant f et g peut être évalué en dernier. La *réciproque* de P est la formule $g \Rightarrow f$.

Plus généralement, on définit la réciproque d'une formule formée de variables quantifiées et d'une formule de cette forme par celle obtenue en prenant la contraposée de cette dernière : si Q est une séquence de variables quantifiées (de la forme $\forall a_1 \dots \forall a_n \exists b_1 \dots \exists b_m \dots$, où les formules $\forall a_1 \dots \forall a_n$ et $\forall b_1 \dots \forall b_m$ sont comprises comme pouvant contenir chacune, et indépendamment, aucune, une seule, ou plusieurs variables quantifiées), la réciproque de la formule $Q\ f \to q$ est $Q\ g \Rightarrow f$.

1.1.12 Contraposée

Soit f et g deux formules n'ayant pas de quantificateur et $P : f \Rightarrow g$. On suppose que le connecteur reliant f et g peut être évalué en dernier. La *contraposée* de P est la formule $\neg g \Rightarrow \neg f$. La formule P et sa contraposée ont toujours la même valeur de vérité (elles sont vraies si f est fausse ou g est vraie et fausses sinon).

Plus généralement, on définit la contraposée d'une formule formée de variables quantifiées et d'une formule de cette forme par celle obtenue en prenant la contraposée de cette dernière : si Q est une séquence de variables quantifiées (de la forme $\forall a_1 \dots \forall a_n \exists b_1 \dots \exists b_m \dots$, où les formules $\forall a_1 \dots \forall a_n$ et $\forall b_1 \dots \forall b_m$ sont comprises comme pouvant contenir chacune, et indépendamment, aucune, une seule, ou plusieurs variables quantifiées), la contraposée de la formule $Q f \to q$ est $Q(\neg g \Rightarrow \neg f)$. La contraposée d'une formule a toujours la même valeur de vérité que la formule initiale.

1.1.13 NAND et NOR

Notons que chacun des connecteurs peut être construit à l'aide d'un unique connecteur, que l'on note ici $\circ$, appelé *NAND*, définit de la manière suivante : si f et g sont deux formules, alors $f \circ g$ est une formule, vraie si et seulement si f et g ne sont pas toutes deux vraies. En effet, si f et g sont deux formules, et en considérant que deux formules sont équivalentes si elles prennent toujours la même valeur,

- $\neg f$ est équivalente à $f \circ f$,
- $f \wedge g$ est équivalente à $\neg(f \circ g)$,
- $f \vee g$ est équivalente à $(\neg f) \circ (\neg g)$,
- $f \Rightarrow g$ est équivalente à $(\neg f) \vee g$,
- $f \Leftarrow g$ est équivalente à $f \vee (\neg g)$,
- $f \Leftrightarrow g$ est équivalente à $(f \wedge g) \vee ((\neg f) \wedge (\neg g))$.

Un tel connecteur, permettant de construire tous les autres, est dit *universel*.

Il existe un autre connecteur universel, appelé *NOR*, que l'on note dans ce paragraphe $\times$, défini par : si f et g sont deux formules, alors $f \circ g$ est une formule, vraie si et seulement si f et g sont toutes deux fausses. En effet, si f et g sont deux formules, $\neg f$ est équivalente à $f \times f$ et $f \wedge g$ à $(\neg f) \times (\neg g)$, donc $f \circ g$ est équivalente à $[(f \times f) \times (g \times g)] \times [(f \times f) \times (g \times g)]$. Puisque le connecteur $\circ$ est universel, le connecteur $\times$ l'est donc aussi.

1.1.14 XOR

On définit le connecteur *XOR*, noté $\oplus$, de la manière suivante : si f et g sont deux formules, alors $f \oplus g$ est une formule vraie si f est vraie et g est fausse ou si f est fausse et g est vraie, et fausse sinon. Si f et g sont deux formules, alors $f \oplus g$ est équivalente à $f \Leftrightarrow (\neg g)$.

L'utilité du connecteur XOR découle des trois propriétés suivantes :

- Il est *symmétrique* : si f et g sont deux formules, $f \oplus g$ est équivalente à $g \oplus f$ (en effet, toutes deux sont vraies si une des formules f et g est vraie et l'autre est fausse, et fausse sinon).
- Il est *transitif* : si f, g et h sont trois formules, $(f \oplus g) \oplus h$ est équivalente à $f \oplus (g \oplus h)$ (en effet, toutes deux sont vraies soit si les trois formules f, g et h sont vraies ou si une d'entre elles est vraie et les deux autres sont fausses, et fausses sinon).
- Soit f une formule, $f \oplus f$ est toujours fausse.

Notons aussi que, si f est une formule, $f \oplus \mathsf{F}$ est équivalente à f et $f \oplus \mathsf{V}$ à $\neg f$.

1.1.15 Tables de vérité

Les valeurs de formules construites à partir d'autres formules peuvent être consignées dans des tableaux appelés *tables de vérité*, contenant sur la première ligne plusieurs formules et sur les autres leurs valeurs (un tiret indiquant qu'elle peut prendre la valeur vraie ou fausse). En voici un exemple, pour deux formules f et g :

f	g	$\neg f$	$f \wedge g$	$f \vee g$	$f \Rightarrow g$	$f \Leftarrow g$	$f \Leftrightarrow g$
F	F	V	F	F	V	V	V
F	V	V	F	V	V	F	F
V	F	F	F	V	F	V	F
V	V	F	V	V	V	V	V

On peut utiliser des tables de vérités pour montrer l'équivalence entre plusieurs formules. Montrons par exemple les trois propriétés énoncées Section 1.1.14. Pour trois formules f, g et h, on a :

f	g	h	$f \oplus g$	$g \oplus f$	$(f \oplus g) \oplus h$	$f \oplus (g \oplus h)$	$f \oplus f$
F	F	F	F	F	F	F	F
F	F	V	F	F	V	V	F
F	V	F	V	V	V	V	F
F	V	V	V	V	F	F	F
V	F	F	V	V	V	V	F
V	F	V	V	V	F	F	F
V	V	F	F	F	F	F	F
V	V	V	F	F	V	V	F

On remarque, comme attendu, que

- Les formules $f \oplus g$ et $g \oplus f$ prennent toujours la même valeur.
- Les formules $(f \oplus g) \oplus h$ et $f \oplus (g \oplus h)$ prennent toujours la même valeur.
- La formule $f \oplus f$ est toujours fausse.

1.1.16 Quelques propriétés

Les propriétés suivantes peuvent être facilement démontrées en écrivant les tables de vérités correspondantes :

- Soit f une formule. La formule $f \wedge \mathsf{F}$ est toujours fausse et $f \vee \mathsf{V}$ est toujours vraie.
- Soit f une formule. Les formule $f \wedge \mathsf{V}$, $f \vee \mathsf{F}$, $f \wedge f$, $f \vee f$ et $f \Leftrightarrow \mathsf{V}$ ont la même valeur de vérité que f.

- Le connecteur $\wedge$ est symmétrique : Soit f et g deux formules ; si $f \wedge g$ est vraie, alors f et g sont toutes deux vraies, donc $g \wedge f$ l'est également.
- Le connecteur $\wedge$ est transitif : Soit f, g et h trois formules, $f \wedge (g \wedge h)$ a la même valeur de vérité que $(f \wedge g) \wedge h$. En effet, toute deux sont vraies si et seulement si f, g et h sont toutes trois vraies.
- Soit f, g et h trois formules ; si $f \wedge g$ et $g \wedge h$ sont vraies, alors $f \wedge h$ l'est également.
- Le connecteur $\vee$ est symmétrique : Soit f et g deux formules ; si $f \vee g$ est vraie, alors au moins une des deux formules f et g est vraie, donc $g \vee f$ l'est également.
- Le connecteur $\vee$ est transitif : Soit f, g et h trois formules, $f \vee (g \vee h)$ a la même valeur de vérité que $(f \vee g) \vee h$. En effet, toutes deux son vraies si et seulement si au moins une des deux formules f, g et h est vraie.
- Le connecteur $\Leftrightarrow$ est symmétrique : Soit f et g deux formules ; si $f \Leftrightarrow g$ est vraie, alors $g \Leftrightarrow f$ l'est également.
- Le connecteur $\Leftrightarrow$ est transitif : Soit f, g et h trois formules, $f \Leftrightarrow (g \Leftrightarrow h)$ a la même valeur de vérité que $(f \Leftrightarrow g) \Leftrightarrow h$. En effet, toutes deux son vraies si et seulement si les trois formules f, g et h ont la même valeur de vérité.
- Soit f, g et h trois formules.
  - Si $f \Leftrightarrow g$ et $g \Leftrightarrow h$ sont vraies, alors $f \Leftrightarrow h$ l'est également.
  - Si $f \Rightarrow g$ et $g \Rightarrow h$ sont vraies, alors $f \Rightarrow h$ l'est également.
  - Si $f \Leftarrow g$ et $g \Leftarrow h$ sont vraies, alors $f \Leftarrow h$ l'est également.
- Soit f et g deux formules. Alors, $\neg(f \wedge g)$ a la même valeur de vérité que $(\neg f) \vee (\neg g)$. En effet, toutes deux sont vraies si au moins une des formules f et g est fausse, et fausses sinon.
- Soit f et g deux formules. Alors, $\neg(f \vee g)$ a la même valeur de vérité que $(\neg f) \wedge (\neg g)$. En effet, toutes deux sont vraies si les deux formules f et g sont fausses, et fausses sinon.
- Soit f et g deux formules. Si $f \Leftrightarrow g$ est vraie, alors $\neg f \Leftrightarrow \neg g$ l'est aussi.
- Soit f et g deux formules ; la formule $f \Leftrightarrow g$ est équivalente à $(f \Rightarrow g) \wedge (g \rightarrow f)$.
- Le connecteur $\wedge$ est distributif sur $\vee$: si f, g et h sont trois formules, les deux formules $f \wedge (g \vee h)$ et $(f \wedge g) \vee (f \wedge h)$ ont la même valeur de vérité (toutes deux sont vraies si et seulement si f ainsi qu'au moins une des deux formules g et h sont vraies).
- Le connecteur $\vee$ est distributif sur $\wedge$: si f, g et h sont trois formules, les deux formules $f \vee (g \wedge h)$ et $(f \vee g) \wedge (f \vee h)$ ont la même valeur de vérité (toutes deux sont vraies si f est vraie ou si g et h sont toutes deux vraies et fausses sinon).
- Soit f et g deux formules. Si $f \Rightarrow g$, alors $f \wedge g$ est équivalente à f et $f \vee g$ est équivalente à g.
- Soit f et g deux formules. Alors $f \Leftrightarrow g$ et $(\neq f) \Leftrightarrow (\neg g)$ sont équivalentes. (Elles sont toutes deux vraies si f et g ont la même valeur de vérité et fausses sinon.)
- Soit f, g, h et i quatre formules. Si $f \Rightarrow g$ et $h \Rightarrow i$ sont vraies, alors $(f \wedge h) \Rightarrow (g \wedge i)$ et $(f \vee h) \Rightarrow (g \vee i)$ sont vraies.
- Une conséquence de ces deux derniers points est que, avec les notations du second, si $f \Leftrightarrow g$ et $h \Leftrightarrow i$ sont vraies, alors $(f \wedge \neg h) \Leftrightarrow (g \wedge \neg i)$ est vraie.

Attention : Si f, g et h sont trois formules, savoir que $f \vee g$ et $g \vee h$ sont vraies n'implique pas que $f \vee h$ l'est également. (En effet, si f et h sont fausse alors que g est vraie, les deux premières sont vraies mais la troisième est fausse.)

1.1.17 Valeur de vérité Indéfinie

On peut étendre la logique du premier ordre en posant une troisième valeur de vérité, dite *indéfinie*. La constante de vérité correspondante est notée I. Toute formule est alors associée à une (et une seule) des trois valeurs de vérité vraie, fausse ou indéfinie.

La table de vérité suivante donne les valeurs de formules obtenues à partir de deux formules f et g ainsi que d'un connecteur :

f	g	$\neg f$	$f \wedge g$	$f \vee g$	$f \Rightarrow g$	$f \Leftarrow g$	$f \Leftrightarrow g$
F	F	V	F	F	V	V	V
F	I	V	F	I	V	I	I
F	V	V	F	V	V	F	F
I	F	I	F	I	I	V	I
I	I	I	I	I	I	I	I
I	V	I	I	V	V	I	I
V	F	F	F	V	F	V	F
V	I	F	I	I	I	V	I
V	V	F	V	V	V	V	V

On a alors les équivalences :

- $f \Rightarrow g$ est équivalente à $(\neg f) \vee g$,
- $f \Leftarrow g$ est équivalente à $f \vee (\neg g)$,
- $f \Leftrightarrow g$ est équivalente à $(f \wedge g) \vee ((\neg f) \wedge (\neg g))$.

On a aussi les règles additionelles :

- toute formule vraie est équivalente à V,
- toute formule fausse est équivalente à F,
- toute formule indéfinie est équivalente à I.

Si $f(x)$ est une formule dépendant d'un paramètre libre x, alors,

- si $f(a)$ est vraie pour tout objet a du domaine de a théorie, alors $\forall x\, f(x)$ est vraie,
- si $f(a)$ est vraie ou indéfinie pour tout objet a du domaine de a théorie et qu'il existe au moins un d'entre eux pour lequel $f(a)$ est indéfinie, alors $\forall x\, f(x)$ est indéfinie,
- si $f(a)$ est fausse pour au moins un objet a du domaine de a théorie, alors $\forall x\, f(x)$ est fausse.

Cela implique (en prenant la négation) :

- si $f(a)$ est fausse pour tout objet a du domaine de a théorie, alors $\exists x\, f(x)$ est fausse,
- si $f(a)$ est fausse ou indéfinie pour tout objet a du domaine de a théorie et qu'il existe au moins un d'entre eux pour lequel $f(a)$ est indéfinie, alors $\exists x\, f(x)$ est indéfinie,
- si $f(a)$ est vraie pour au moins un objet a du domaine de a théorie, alors $\exists x\, f(x)$ est vraie.

Le point de vue canonique en logique mathématique est de considérer que les deux seules valeurs de vérité possibles sont « vraie » et « fausse ». Un point de vue intermédiaire est de considérer que seules les formules ayant au moins une variable libre peuvent prendre la valeur indéfinie. Dans ce qui suit, on tâchera de ne tenir que des raisonnement valables avec ou sans la valeur de vérité indéfinie. Sauf mention contraire explicite, on considèrera qu'une formule peut prendre une des trois valeurs de vérité.

1.1.18 Quelques schémas de raisonnement

Pour démontrer qu'une formule est vraie, on remplacera souvent certains quantificateurs et connecteurs par des mots ayant la même signification afin de les rendre plus faciles à suivre, en suivant les règles énoncées ci-dessus. Nous présentons ici brièvement quelques idées souvent utilisées pour démontrer des formules, de manière informelle. On se place dans le cadre d'une théorie comprenant la logique du premier ordre et portant sur un certain domaine de discours définissant des objets.

Raisonnement par l'absurde : Un type de raisonnement revenant souvent est le raisonnement par l'absurde : si f et g sont deux formules, si $f \Rightarrow g$ est vraie et g est fausse, alors f est nécessairement fausse. En pratique, pour montrer qu'une formule f est fausse, on peut donc trouver une formule g telle que g est fausse et $f \Rightarrow g$.

Plus formellement, si f et g sont deux formules, on a :

$$\big((f \Rightarrow g) \wedge (\neg g)\big) \Leftrightarrow \big(((\neg f) \vee g) \wedge (\neg g)\big) \Leftrightarrow \big(((\neg f) \wedge (\neg g)) \vee (g \wedge (\neg g))\big) \Leftrightarrow \big(((\neg f) \wedge (\neg g)) \vee \mathsf{F}\big) \Leftrightarrow \big((\neg f) \wedge (\neg g)\big).$$

Donc, si $(f \Rightarrow g) \wedge (\neg g)$ est vraie, alors $\neg f$ est vraie, donc f est fausse.

Prouver une propriété de la forme $\forall x P(x) \Rightarrow Q(x)$: Soit P et Q deux prédicats à un paramètre libre. Pour prouver que la formule $\forall x\, P(x) \Rightarrow Q(x)$ est vraie, on pourra prendre un objet x pouvant être n'importe-quel objet du domaine de discours de la théorie et montrer que, si $P(x)$ est vrai, alore $Q(x)$ l'est également.

Prouver l'unicité d'un objet satisfaisant une propriété en montrant que deux objets la satisfaisant sont égaux : On se place ici dans le cadre de la logique du premier ordre avec égalité. Soit P un prédicat à un paramètre libre. Pour montrer qu'il existe au plus un unique objet x tel que $P(x)$ est satisfait, on pourra montrer que si x et y sont deux objets tels que $P(x)$ et $P(y)$ sont vrais, alors $x = y$. Pour montrer qu'il en existe exactement un, on montrera en outre qu'il existe un objet x tel que $P(x)$ est vrai.

Équivalence : Soit f et g deux formules. Si on peut montrer qur $f \Rightarrow g$ et $g \Rightarrow f$ sont vraies, alors $f \Leftrightarrow g$ est vraie.

1.1.19 Un exemple : arc-en-ciel à minuit ?

Pour rendre cela un peu plus concret, éxaminons un exemple d'application. On se restreint ici à la logique propositionelle, sans variables ni quantificateurs. Considérons les prédicats suivants :

- P_1 : « Le soleil brille. »
- P_2 : « Il pleut. »
- P_3 : « Il y a un arc-en-ciel. »
- P_4 : « Il fait jour. »
- P_5 : « Il est minuit. »
- P_6 : « Si le soleil brille, il fait jour. »
- P_7 : « À minuit, il ne fait pas jour. »
- P_8 : « Il y a un arc-en-ciel si et seulement si le soleil brille et il pleut. »

Alors,

- P_6 est équivalent à : $P_1 \Rightarrow P_4$.
- P_7 est équivalent à : $P_5 \Rightarrow \neg P_4$.
- P_8 est équivalent à : $P_3 \Rightarrow (P_1 \wedge P_2)$.

Posons-nous la question : en admettant P_6, P_7 et P_8, peut-il y avoir un arc-en-ciel à minuit ? Évidemment, non ! En effet, la contraposée de P_6 est $\neg P_4 \Rightarrow \neg P_1$. Si P_7 et P_6 (et donc sa contraposée) sont vrais, alors $(P_5 \Rightarrow \neg P_4) \wedge (\neg P_4 \Rightarrow \neg P_1)$ est vrai. Puisque le connecteur $\Rightarrow$ est transitif, cela implique $P_5 \Rightarrow \neg P_1$. Or, la contraposée de P_8 est $\neg(P_1 \wedge P_2) \Rightarrow \neg P_3$. Si P_8 est vrai, sa contraposée l'est aussi. Si, de plus, P_1 est faux, alors $\neg(P_1 \wedge P_2)$ est vrai, et donc $\neg P_3$ est vrai. Donc, si P_8 est vrai, $\neg P_1 \Rightarrow \neg P_3$. En utilisant une dernière fois la transitivité du connecteur $\Rightarrow$, on obtient donc $P_5 \Rightarrow \neg P_1$ si P_6, P_7 et P_8 sont vrais. Cela peut se récrire formellement :

$$P_6 \wedge P_7 \wedge P_8 \Rightarrow (P_5 \Rightarrow \neg P_1).$$

1.1.20 Premier théorème d'incomplétude de Gödel

Les deux théorèmes d'incomplétude de Gödel énoncent, en un certain sens, des limites au pouvoir démonstratif d'une théorie mathématique rigoureuse—autrement dit, si une théorie (suffisamment complexe, en un sens défini ci-dessous) est *cohérente*, *i.e.* si aucun prédicat faux ne peut être démontré, alors tous les prédicat vrais ne peuvent être démontrés. Le premier d'entre eux exprime que, dans une théorie fondée sur la logique du premier ordre et suffisamment complexe pour y définir les entiers naturels, il existe des prédicats dont il est impossible de déterminer la valeur de vérité. On peut l'énoncer de manière informelle comme suit :

Tout système formel F d'axiomes cohérent permettant de définir une arithmétique élémentaire est incomplet, au sens où il existe des prédicats exprimés dans le language de F dont la valeur de vérité ne peut être démontrée vraie ni fausse à partir de F.

Cet énoncé est imprécis, entre autres puisqu'il ne définit pas ce qu'est une « arithmétique élémentaire ». Pour le préciser, considérons une théorie dont l'alphabet contient (au moins) les symboles suivants :

- Un symbole 0 représentant une constante.
- Un symbole x représentant une variable, ainsi qu'un symbole $*$ permettant de construire d'autres variables x^*, x^{**}, x^{***}, ... Ces variables sont dites *primaires*, et aussi appelées *paramètres*.
- Un symbole « successeur » S définissant une fonction d'une seule variable.
- Deux opérations binaires $+$ (addition) et $\times$ (multiplication).
- Les opérateurs logiques de conjonction $\wedge$, disjonction $\vee$ et négation $\neg$.
- Les quantificateurs $\exists$ et $\forall$.

- Deux relations binaires = (égalité) et <.
- Les parenthèses (et).

Les formules de la théorie sont des chaines (finies) de symboles, avec les règles suivantes :

- Si y désigne une constante, Sy est une constante, dite *successeur* de y. On note 1 le successeur 0 et on suppose $1 \neq 0$.
- Si y désigne une variable, Sy est une variable, dite *secondaire*.
- Si y et z sont chacune une constante ou une variable, alors $y = z$ et $y < z$ sont des formules.
- Si f est une formule, alors (f) en est une.
- Si f est une formule, alors $\neg f$ en est une.
- Si f et g sont deux formules n'ayant aucune variable quantifiée en commun, alors $f \wedge g$ et $f \vee g$ en sont également.
- Soit f une formule et v une variable primaire telle que ni $\forall v$ ni $\exists v$ n'apparaît dans f. Alors $\forall v\ f$ et $\exists v\ f$ sont des formules.

Notons que l'arithmétique usuelle satisfait ces propriétés (voir section sub:constN). Une variable x apparaissant dans une formule F est dite *libre* si ni $\exists x$ ni $\forall x$ n'apparaissent dans F.

On peut se limiter aux formules sans variable libre en remplaçant les règles ci-dessus par les suivantes (cela n'aura pas d'incidence sur la suite) :

- Si y désigne une constante, Sy est une constante.
- Si y et z sont deux constantes, alors $y = z$ et $y < z$ sont des formules.
- Si f est une formule, alors (f) en est une.
- Si f est une formule, alors $\neg f$ en est une.
- Si f et g sont deux formules, alors $f \wedge g$ et $f \vee g$ en sont également.
- Soit f une formule, c une constante et v une variable. Soit g la séquence de symboles obtenue en remplaçant c par v dans f. Alors, $\forall v\ g$ et $\exists v\ g$ sont des formules.

Ces éléments permettent, sous certains axiomes, de définir un ensemble de nombres $\mathbb{N}$, contenant 0 et stable par S, ayant les mêmes propriétés que celui défini dans les sections suivantes (notamment celles des opérations binaires + et $\times$ et le fait de définir < comme une relation d'ordre).

On suppose un système d'axiomes permettant de définir un ensemble de nombres $\mathbb{N}$ satisfaisant les propriétés établies en section sub:constN, constituant la base de l'arithmétique usuelle. En particulier, + et $\times$ sont des fonctions de $\mathbb{N} \times \mathbb{N}$ vers $\mathbb{N}$ et l'on peut définir les nombres premiers comme dans la section subsub:defNombresPremiers. Pour fixer les idées, on pourra considérer que l'on se place dans le cadre de la théorie des ensembles et de l'arithmétique définies dans les sections ci-dessous.[6]

La théorie est dite *cohérente* si aucune formule ne peut être montrée à la fois vraie et fausse. Elle est dite *ω-cohérente* si, pour toute formule f et toute variable n, il est impossible de montrer $\exists n\ f$ si $\neg f$ est démontrable pour toute constante n. Notons que la seconde notion implique la première (en choisissant pour n une variable n'apparaissant pas dans f, $\exists n\ f$ est équivalente à f). Dans la suite, on suppose la théorie ω-cohérente.

Enfin, la théorie est supposée *effective*, c'est-à-dire qu'il est théoriquement possible d'écrire un algorithme ayant un nombre fini d'instructions donnant un par un tous ses axiomes et uniquement ses axiomes. (On peut donner à cette définition un sens plus précis dans le cadre de l'arithmétique usuelle, et en définissant un ensemble d'instructions possibles pour un algorithme.) On considère qu'un algorithme à un nombre fini d'instructions démontrant une formule F peut être décrit par une formule de la théorie, par exemple par une formule de la forme $P \Rightarrow F$, où P est soit un axiome de la théorie soit une formule démontrable.

Premier théorème d'incomplétude de Gödel : Sous ces conditions, il existe une formule F sans variable libre dont on ne peut montrer (par un algorithme fini) ni qu'elle est vraie ni qu'elle est fausse.

L'essence de la preuve est de construire, dans le cadre de cette théorie, un prédicat Z équivalent à l'impossibilité de le démontrer lui-même. Ainsi, si Z est vrai, il n'est pas démontrable, et si Z est faux il est démontrable (ce qui est impossible si la théorie est cohérente). Dans le langage usuel, de tels énoncés paradoxaux sont aisés à formuler car un énoncé peut référer directement à lui-même. Par exemple, la phrase « Cette phrase n'est pas démontrable. » ne peut être démontrée que si elle n'est pas vraie [7]. Pour démontrer le premier théorème d'incomplétude de Gödel, il suffit en quelque sorte de montrer qu'un tel énoncé existe et forme un prédicat dans le cadre de toute théorie satisfaisant les propriétés énoncées ci-dessus.

---

[6] Pour faire le lien avec la section 1.4, on peut poser l'équivalence suivante :
- les constantes sont les entiers naturels, *i.e.*, les éléments de $\mathbb{N}$;
- les relations = et < sont, respectivement, la relation d'égalité et la première relation d'ordre sur $\mathbb{N}$;
- S est l'application successeur : pour tout entier naturel n, $Sn = n + 1$.

[7] Dans le même ordre d'idée, la phrase « Cette phrase est fausse. » ne peut être ni vraie ni fausse.

La démonstration de Gödel repose sur les *nombres de Gödel* associés à chaque formule. De manière générale (et une fois une théorie de l'arithmétique construite, voir section sec:arithmetique ; on se limite ici aux entiers naturels), une *numérotation de Gödel* est une fonction injective (une définition rigoureuse des fonctions dans le cadre de la théorie des ensembles sera donnée section ??) associant un nombre à chaque symbole ou formule.

La numérotation originelle de Gödel, que nous nommerons dans la suite *encodage de Gödel*, noté $\mathbf{G}$, est obtenue de la manière suivante :

- On choisit une suite (infinie) de nombres premiers distincts, notée p.[8]
- À chaque symbole de la théorie ou variable primaire x est associé un nombre $\mathbf{G}(x)$, de sorte que chaque nombre est associé à au plus un symbole ou une variable primaire.[9]
- Si n est un entier naturel et x_1, x_2, ..., x_n sont des symboles, le nombre associé à la séquence de symboles $x_1x_2 \dots x_n$ est $p_1^{\mathbf{G}(x_1)} \times p_2^{\mathbf{G}(x_2)} \times \dots \times p_n^{\mathbf{G}(x_n)}$. Plus formellement, $\mathbf{G}(x_1x_2 \dots x_n) = \prod_{i=1}^{n} p_i^{\mathbf{G}(x_i)}$.

D'après l'unicité de la décomposition en produits de facteurs premiers (voir section subsub:dec_fact_prem), deux formules distinctes ne peuvent avoir le même encodage. Puisque toute formule est une séquence finie de symboles, à chaque formule est ainsi associé un unique nombre et chaque nombre est associé à au plus une formule.

Exemple : Si trois variables primaires x, y et z sont représentées respectivement par les nombres 1, 2 et 3, si $+$ et $=$ sont respectivement représentés par les nombres 4 et 5, et si la suite p commence par (2, 3, 5, 7, 11), alors $\mathbf{G}(x + y = z) = 2^1 \times 3^4 \times 5^2 \times 7^5 \times 11^3 = 90598973850$.

Donnons une esquisse de preuve du premier théorème d'incomplétude. Soit F une formule. Si F est démontrable, alors il existe un prédicat P qui prouve F. On peut ainsi, par exemple, définir la fonction Dem de $\mathbb{N} \times \mathbb{N}$ vers $\{0, 1\}$, illustrant que « n démontre m », par : pour tous entiers naturels n et m,

- Si n est un nombre de Gödel associé à une formule P, m est un nombre de Gödel associé à une formule F et si P démontre F, alors $\text{Dem}(n, m) = 1$.
- Sinon, $\text{Dem}(n, m) = 0$.

(Cette fonction ne sera pas utilisée dans la suite, mais sert d'illustration.)

On définit la fonction q de $\mathbb{N} \times \mathbb{N}$ vers $\{0, 1\}$ par : pour tous entiers naturels n et m,

- Si n est un nombre de Gödel associé à un prédicat P, m est un nombre de Gödel associé à une formule F à un paramètre libre et si P démontre $F(\mathbf{G}(F))$, alors $q(n, m) = 0$.
- Sinon, $q(n, m) = 1$.[10]

Alors, pour toute formule F à un paramètre libre, la formule $\forall y\, q(y, \mathbf{G}(F)) = 1$ est équivalente à : « il n'existe pas de preuve de $F(\mathbf{G}(F))$ ». En effet, s'il existe un prédicat P démontrant $F(\mathbf{G}(F))$, alors $q(\mathbf{G}(P), \mathbf{G}(F)) = 0$, donc $\exists y\, \neg(q(y, \mathbf{G}(F)) = 1)$ est vrai, donc $\forall y\, q(y, \mathbf{G}(F)) = 1$ est faux, et s'il n'en existe pas, alors, pour tout nombre y, soit y encode un prédicat P et P ne peut montrer $F(\mathbf{G}(F))$, donc $q(y, \mathbf{G}(F)) = 1$, soit y n'encode pas de formule, et donc $q(y, \mathbf{G}(F)) = 1$ également.

Définissons le prédicat à un paramètre libre P par : $P(x) : \forall y\, q(y, x) = 1$. Considérons maintenant le prédicat Z défini par : $Z : P(\mathbf{G}(P))$. De manière informelle, Z est équivalent à $\forall y\, q(y, \mathbf{G}(P))$, et donc à « il n'existe pas de preuve de Z ». Nous avons donc construit un prédicat vrai si et seulement si il n'est pas démontrable.

Montrons un peu plus formellement que Z est démontrable si et seulement si il est faux.

- Supposons que Z est démontrable. Alors, il existe une formule, notons-là F, démontrant Z. Donc, F démontre $P(\mathbf{G}(P))$. Donc, $q(\mathbf{G}(F), \mathbf{G}(P)) = 0$. Donc, $q(\mathbf{G}(F), \mathbf{G}(P)) = 1$ est faux. Donc, $\forall y\, q(y,\mathbf{G}(P)) = 1$ est faux. Donc, $P(\mathbf{G}(P))$ est faux. Donc, Z est faux.
- Supposons que Z est faux. Alors, $P(\mathbf{G}(P))$ est faux. Donc, $\forall y\, q(y,\mathbf{G}(P)) = 1$ est faux. Donc, $\exists y\, \neg(q(y,\mathbf{G}(P)) = 1)$ est vrai. Puisque, dans cette expression, $q(y,\mathbf{G}(P))$ ne peut prendre que les valeurs 0 et 1, on en déduit qu'il existe un entier y tel que $q(y,\mathbf{G}(P)) = 0$[11], et donc qu'il existe une formule F telle que $y = \mathbf{G}(F)$ et F prouve $P(\mathbf{G}(P))$, et donc Z.

Ainsi, la valeur de vérité du prédicat Z ne peut être déterminée. En effet,

- Si Z et vrai, alors Z n'est pas démontrable.
- Si la théorie est cohérente, Z ne peut être faux (car alors il serait démontrable).

[8] Cela est possible car il existe une infinité de nombres premiers (voir section ??).

[9] Cela est possible car l'ensemble des symboles est fini et celui des variables primaires est dénombrable, donc l'ensemble contenant les symboles et variables primaires est dénombrable (voir définition section ??).

[10] En particulier, si n est un nombre de Gödel associé à un prédicat P, m est un nombre de Gödel associé à une formule F à un paramètre libre et si P ne démontre pas $F(\mathbf{G}(F))$, alors $q(n, m) = 1$.

[11] En effet, il existe un entier y tel que $q(y,\mathbf{G}(P)) = 1$ est faux, et donc $q(y,\mathbf{G}(P)) = 0$ est vrai.

1.1.21 Second théorème d'incomplétude de Gödel

******

1.2 Théorie ZFC

1.2.1 La théorie de Zermelo

La théorie de Zermelo, aussi dite « théorie Z » est une axiomatisation, dans le cadre de la logique du premier ordre avec égalité, de la théorie des ensembles. Elle fait intervenir des objets, appelés *ensembles*[12], et leurs relations, notamment des relations binaires. Une de ces relations est l'*appartenance*, désignée par le symbole $\in$. Si x et y sont deux ensembles, alors $x \in y$ est une proposition bien formée (il s'agit d'un terme). Si elle est vraie, on dira que x *est un élément de* y, que x *appartient à* y, que x *est dans* y, que y *contient* x, ou que y *possède* x. On définit aussi la relation $\ni$ par : $x \ni y$ est équivalente à $y \in x$. On a donc : $\forall x \, \forall y \, (x \ni y) \Leftrightarrow (y \in x)$ et la relation $\notin$ par $\forall x \, \forall y \, (x \notin y) \Leftrightarrow \neg(x \in y)$. Pour l'évaluation d'une formule, les relations $\in$ et $\ni$ sont (comme toute autre relation binaire) prioritaires par rapport à l'égalité, mais pas par rapport à $\neg$.

On définit la relation d'inclusion $\subset$ par : $a \subset b$ est équivalent à $\forall x \, (x \in a) \Rightarrow (x \in b)$, autrement dit,

$$\forall a \, \forall b \, ((a \subset b) \Leftrightarrow (\forall x \, (x \in a) \Rightarrow (x \in b))) \, .$$

Si $a \subset b$, on dira que a *est un sous-ensemble de* b, que a *est inclus dans* b, ou que a *est une partie de* b. Notons que, pour tout ensemble a, $a \subset a$ est vrai.[13] On définit aussi la relation $\supset$ par :

$$\forall a \, \forall b \, ((a \supset b) \Leftrightarrow (\forall x \, (x \in a) \Leftarrow (x \in b))) \, .$$

Lemme : Soit $\forall a \, \forall b \, (a = b) \Leftrightarrow ((a \subset b) \wedge (b \subset a))$.

Démonstration : La formule $(a \subset b) \wedge (b \subset a)$ est équivalente à : $(\forall x (x \in a) \Rightarrow (x \in b)) \wedge (\forall y (y \in a) \Rightarrow (y \in b))$, et donc à $\forall x \, ((x \in a) \Rightarrow (x \in b)) \wedge ((x \in b) \Rightarrow (x \in a))$. Si f et g sont deux formules, $(f \Rightarrow g) \wedge (g \Rightarrow a)$ est équivalente à $f \Leftrightarrow g$. Donc, $(a \subset b) \wedge (b \subset a)$ est équivalente à $\forall x \, (x \in a) \Leftrightarrow (x \in b)$, et donc à $a = b$. Donc, $((a \subset b) \wedge (b \subset a)) \Leftrightarrow (a = b)$ est équivalente à V. Donc, $\forall a \, \forall b \, ((a \subset b) \wedge (b \subset a)) \Leftrightarrow (a = b)$ est vraie.

□

La théorie Z comporte six axiomes (l'axiome d'extensionnalité et les cinq axiomes de construction) ainsi qu'un schéma d'axiomes, correspondant à un axiome par formule à un paramètre libre.

Axiome d'extensionnalité : *Si deux ensembles possèdent les mêmes éléments, alors ils sont égaux.*

$$\forall a \, \forall b \, (\forall x \, ((x \in a) \Leftrightarrow (x \in b)) \Rightarrow (a = b)) \, .$$

La réciproque est une conséquence directe des propriétés de l'égalité en logique du premier ordre.[14] On définit la relation $\neq$ par : $\forall a \, \forall b \, (a \neq b) \Leftrightarrow \neg(a = b)$.

Lemme : On définit la relation R sur les ensembles par : soit a et b deux ensembles ($a \ R \ b$) a la même valeur de vérité que $(\forall x \, (x \in a) \Leftrightarrow (x \in b))$. Alors, les trois prédicats suivants sont vrais :

- $\forall x \, (x \ R \ x)$ (réciprocité)
- $\forall x \, \forall y \, (x \ R \ y) \Rightarrow (y \ R \ x)$ (réflexivité)
- $\forall x \, \forall y \, \forall z \, ((x \ R \ y) \wedge (y \ R \ z)) \Rightarrow (x \ R \ z)$.

Cela suggère que l'axiome d'extensionalité est compatible avec la définition de l'égalité en logique du premier ordre (même s'il manque le schéma d'axiomes de Leibniz pour assurer la cohérence).

Démonstration :

[12] Un ensemble est parfois appelé *espace* ; mais ce terme est en général utilisé seulement en présence d'une structure additionnelle.

[13] En effet, soit x un ensemble, $x \in a$ a toujours la même valeur de vérité que lui-même, donc $(x \in a) \Rightarrow (x \in a)$ est vrai.

[14] En effet, soit deux ensembles a et b tels que $a = b$, et soit x un ensemble, et P le prédicat à un paramètre libre définit par $Py : x \in y$, puisque $a = b$, on doit avoir $P(a) \Leftrightarrow P(b)$, et donc $(x \in a) \Leftrightarrow (x \in b)$.

- Soit x un ensemble. Pour tout y, $y \in x$ a la même valeur de vérité que $y \in x$ (trivialement, puisqu'il s'agit de la même formule). Donc, $\forall y\,(y \in x) \Leftrightarrow (y \in x)$. Donc, $x\ R\ x$.
- Soit x et y deux ensembles tels que $x\ R\ y$. Puisque $x = y$, on a : $\forall z\ z \in x \Leftrightarrow z \in y$. Puisque le connecteur $\Leftrightarrow$ est symétrique, on a donc : $\forall z\ z \in y \Leftrightarrow z \in y$. Donc, $y\ R\ x$.
- Soit x, y et z trois ensembles tels que $x\ R\ y$ et $y\ R\ z$. Pour tout ensemble a, on a $a \in x \Leftrightarrow a \in y$ et $a \in y \Leftrightarrow a \in z$. Donc, par transitivité du connecteur $\Leftrightarrow$, $a \in x \Leftrightarrow a \in z$. Cela étant valable pour tout ensemble a, on en déduit que $x\ R\ z$.

□

Démonstration bis : À titre d'exercice, re-faisons ces courtes démonstrations de manière plus formelle.

- Soit f la formule à deux paramètres libres x et y donnée par : $f : y \in x$. Puisque $f \Leftrightarrow f$ est équivalente à V, la formule $\forall x\,\forall y\,(f \Leftrightarrow f)$ est vraie. Donc, $\forall x\,\forall y\,(y \in x) \Leftrightarrow (y \in x)$ est vraie. Donc, $\forall x\ x\ R\ x$ est vraie.
- Soit f la formule à deux paramètres libres a et x donnée par : $f : a \in x$, et g la formule à deux paramètres libres a et y donnée par : $g : a \in y$. Les deux formules $f \Leftrightarrow g$ et $g \Leftrightarrow f$ sont équivalentes (elles sont toutes deux vraies si f et g ont la même valeur de vérité et fausses sinon). Donc, les formules $\forall a\,(f \Leftrightarrow g)$ et $\forall a\,(g \Leftrightarrow f)$ sont équivalentes. Puisque $\forall a\,(f \Leftrightarrow g)$ est équivalente à $x\ R\ y$ et $\forall a\,(g \Leftrightarrow f)$ à $y\ R\ x$, on en déduit que $x\ R\ y$ et $y\ R\ x$ sont équivalentes. Donc, $(x\ R\ y) \Rightarrow (y\ R\ x)$ est équivalente à $h \Rightarrow h$, où h est la formule donnée par $h : x\ R\ y$. Puisque $h \Rightarrow h$ est vraie que h soit vraie ou fausse, elle est équivalente à V. Donc, $\forall x \forall y (h \Rightarrow h)$ est vraie. Donc, $\forall x \forall y (x\ R\ y) \Rightarrow (y\ R\ x)$ est vraie.
- Soit f la formule à deux paramètres libres a et x donnée par : $f : a \in x$, g la formule à deux paramètres libres a et y donnée par : $g : a \in y$, et h la formule à deux paramètres libres a et z donnée par : $h : a \in z$. Alors, $((f \Leftrightarrow g) \wedge (g \Leftrightarrow h)) \Rightarrow (f \Leftrightarrow h)$ est vraie quelles que soient les valeurs de vérité de f, g et h. Donc, si $\forall a\,((f \Leftrightarrow g) \wedge (g \Leftrightarrow h))$ est vraie, alors $\forall a\,(f \Leftrightarrow h)$ est vraie. Donc, si $\forall a\,(f \Leftrightarrow g)$ et $\forall a\,(g \Leftrightarrow h)$ sont vraies, alors $\forall a\,(f \Leftrightarrow h)$ est vraie. Puisque $\forall a\,(f \Leftrightarrow g)$ est équivalente à $x\ R\ y$, $\forall a\,(g \Leftrightarrow h)$ est équivalente à $y\ R\ z$, et $\forall a\,(f \Leftrightarrow h)$ est équivalente à $x\ R\ z$, on en déduit que $((x\ R\ y) \wedge (y\ R\ z)) \Rightarrow (x\ R\ z)$ est toujours vraie. Donc, $\forall x\,\forall y\,\forall z\,((x\ R\ y) \wedge (y\ R\ z)) \Rightarrow (x\ R\ z)$ est vraie .

□

Lemme : La relation $\subset$ satisfait les trois propriétés suivantes :

- *Réflexivité :* $\forall x\ x \subset x$.
- *Antisymétrie :* $\forall x\,\forall y\,(x \subset y) \wedge (y \subset x) \Rightarrow (x = y)$.
- *Transitivité :* $\forall x \forall y \forall z\,(x \subset y) \wedge (y \subset z) \Rightarrow (x \subset z)$.

Démonstration :

- Soit x un ensemble. Pour tout élément e de x, on a (par définition), $e \in x$. Donc, le prédicat $\forall e\,(e \in x) \Rightarrow (e \in x)$ est vrai. Donc, $x \subset x$.
- Soit x et y deux ensembles tels que $x \subset y$ et $y \subset x$. Soit e un ensemble. Si $e \in x$ est vrai, alors $e \in y$ est vrai aussi puisque $x \subset y$. Si $e \in x$ est faux, alors $e \in y$ est faux aussi, sans quoi on aurait $e \in y$ et donc $e \in x$ puisque $y \subset x$. Cela montre que $\forall e\,(e \in x) \Leftrightarrow (e \in y)$ est vrai. Donc, d'après l'axiome d'extensionnalité, $x = y$ est vrai.
- Soit x, y et z trois ensembles tels que $x \subset y$ et $y \subset z$. Soit e un ensemble. Si $e \in x$, alors $e \in y$ puisque $x \subset y$, et donc $e \in z$ puisque $y \subset z$. Cela montre que le prédicat $\forall e\,(e \in x) \Rightarrow (e \in z)$ est vrai. Donc, $x \subset z$.

□

Démonstration bis :

- Soit f la formule $f : e \in x$. La formule $f \Rightarrow f$ est vraie que f soit vraie ou fausse, donc elle est équivalente à V. Donc, $\forall e\,(f \Rightarrow f)$ est équivalente à V. Donc, $\forall e\,((e \in x) \Rightarrow (e \in x))$ est équivalente à V. Donc, $x \subset x$ est équivalente à V. Donc, $\forall x\ x \subset x$ est vraie.
- La formule $(x \subset y) \wedge (y \subset x)$ est équivalente à : $(\forall e\,(e \in x \Rightarrow e \in y)) \wedge (\forall f\,(f \in y \Rightarrow f \in x))$, et donc à $\forall e\,((e \in x \Rightarrow e \in y) \wedge (e \in y \Rightarrow e \in x))$. Puisque $(e \in x \Rightarrow e \in y) \wedge (e \in y \Rightarrow e \in x)$ est équivalente à $(e \in x \Leftrightarrow e \in y)$, la formule $(x \subset y) \wedge (y \subset x)$ est équivalente à $x = y$. Donc, $((x \subset y) \wedge (y \subset x)) \Rightarrow (x = y)$ est équivalente à V. Donc, $\forall x\,\forall y\,((x \subset y) \wedge (y \subset x)) \Rightarrow (x = y)$ est vraie.
- La formule $(x \subset y) \wedge (y \subset z)$ est équivalente à $(\forall e\ e \in x \Rightarrow e \in y) \wedge (\forall f\ f \in y \Rightarrow f \in z)$, donc à $\forall e\,((e \in x \Rightarrow e \in y) \wedge (e \in y \Rightarrow e \in z))$. Soit f, g et h trois formules, $((f \Rightarrow g) \wedge (g \Rightarrow h))$ est équivalente à $(f \Rightarrow h) \wedge (f \Rightarrow g)$. Donc, la formule $(x \subset y) \wedge (y \subset z)$ est équivalente à $\forall e\,((e \in x \Rightarrow e \in z) \wedge (e \in x \Rightarrow e \in y))$, et donc à $(\forall e\,(e \in x \Rightarrow e \in z)) \wedge (\forall f\,(f \in x \Rightarrow f \in y))$, et donc à $(x \subset z) \wedge (x \subset y)$. Puisque, si g et h sont deux formules, $g \wedge h \Rightarrow g$ est toujours vraie, $((x \subset z) \wedge (x \subset y)) \Rightarrow (x \subset z)$ est équivalente à V, donc on en déduit que $((x \subset y) \wedge (y \subset z)) \Rightarrow (x \subset z)$ est équivalente à V, donc $\forall x\,\forall y\,((x \subset y) \wedge (y \subset z)) \Rightarrow (x \subset z)$ est vraie.

□

Lemme : La proposition $\forall a\, \forall b\, (a = b) \Leftrightarrow [(a \subset b) \wedge (b \subset a)]$ est vraie. Autrement dit, pour tous ensembles a et b, la formule $a = b$ est équivalente à $(a \subset b) \wedge (b \subset a)$.

Démonstration : Soit a et b deux ensembles.

- Supposons d'abord que $a = b$. Soit x tel que $x \in a$. Puisque $a = b$, on a $x \in b$. Donc, $\forall x\, (x \in a) \Rightarrow (x \in b)$. Donc, $a \subset b$. Puisque l'égalité est symétrique, on montre de même en échangeant les rôles de a et b que $b \subset a$. Donc, $(a \subset b) \wedge (b \subset a)$.
- Supposons maintenant que $(a \subset b) \wedge (b \subset a)$. Soit x un ensemble. Si $x \in a$, et puisque $a \subset b$, alors $x \in b$. De même, si $x \in b$, et puisque $b \subset a$, alors $x \in a$. Donc, $\forall x\, (x \in a) \Leftrightarrow (x \in b)$. Donc, $a = b$.

On a donc montré que les formules $a = b$ et $(a \subset b) \wedge (b \subset a)$ son équivalentes, au sens où chacune est vraie qi l'autre l'est (et donc, également, fausse si l'autre l'est).

□

Démonstration bis : La formule $(a \subset b) \wedge (b \subset a)$ est équivalente à : $(\forall x\, (x \in a \Rightarrow x \in b)) \wedge (\forall y\, (y \in b \Rightarrow y \in a))$, et donc à $\forall x\, ((x \in a \Rightarrow x \in b) \wedge (x \in b \Rightarrow x \in a))$. Si f et g sont deux formules, $(f \Rightarrow g) \wedge (g \Rightarrow f)$ est équivalente à $f \Leftrightarrow g$ (toutes deux sont vraies si f et g sont toutes deux vraies ou toutes deux fausses, fausses si l'une est vraie et l'autre est fausse, et (en présence de la valeur de vérité I) indéfinies si f ou g l'est). Donc, $(x \in a \Rightarrow x \in b) \wedge (x \in b \Rightarrow x \in a)$ est équivalente à $x \in a \Leftrightarrow x \in b$. Donc, la formule $(a \subset b) \wedge (b \subset a)$ est équivalente à $\forall x\, (x \in a \Leftrightarrow x \in b)$, et donc à $a = b$.

Donc, la formule $((a \subset b) \wedge (b \subset a)) \Leftrightarrow (a = b)$ est équivalente à $(a = b) \Leftrightarrow (a = b)$, et donc toujours vraie, et donc équivalente à V. Donc, la formule $\forall a\, \forall b\, ((a \subset b) \wedge (b \subset a)) \Leftrightarrow (a = b)$ est vraie.

□

Axiome de la paire : *La paire formée par deux ensembles est un ensemble :*

$$\forall a\, \forall b\, \exists c\, \forall x\, ((x \in c) \Leftrightarrow ((x = a) \vee (x = b))).$$

Si a et b sont deux ensembles, on note $\{a, b\}$ leur paire. Il s'agit de l'ensemble contenant a et b mais aucun autre (au sens de « non égal à a ni à b ») ensemble. Cet ensemble est unique d'après l'axiome d'extensionnalité. Si de plus $b = a$, alors $\{a, b\}$ ne contient qu'un seul élément. Il peut alors être abrégé en $\{a\}$. Puisque, pour tout x, la formule $(x = a) \vee (x = a)$ est équivalente à $x = a$, on a :

$$\forall x\, (x \in \{a\}) \Leftrightarrow (x = a).$$

Axiome de la réunion : *Pour tout ensemble a, il existe un ensemble qui est l'union des éléments de a :*

$$\forall a\, \exists b\, \forall x\, ((x \in b) \Leftrightarrow (\exists y\, ((y \in a) \wedge (x \in y)))).$$

La réunion d'un ensemble a (noté b dans la formule ci-dessus) est notée $\cup a$. Cet ensemble est unique d'après l'axiome d'extensionnalité. Si a et b sont deux ensembles, $\{a, b\}$ est aussi un ensemble d'après l'axiome de paire. La réunion de cet ensemble est notée $a \cup b$, et appelé *union* de a et b. Soit a, b et c trois ensembles. On note $\{a, b, c\}$ l'ensemble $\{a, b\} \cup \{c\}$.

Lemme : Soit a, b et x trois ensembles. Le prédicat $x \in a \cup b$ est équivalent à $(x \in a) \vee (x \in b)$.

Démonstration : Le prédicat $x \in a \cup b$ est équivalent à $\exists y\, y \in \{a, b\} \wedge x \in y$, donc à $\exists y\, (y = a \vee y = b) \wedge x \in y$, donc à $\exists y\, ((y = a \wedge x \in y) \vee (y = b \vee x \in y))$, donc à $(\exists y\, y = a \wedge x \in y) \vee (\exists z\, z = b \wedge x \in z))$. Si f est ue formule dépendant de deux paramètres libres x et y et si a est un ensemble, alors $\exists (y = a) \wedge f(x,y)$ est équivalente à $f(x,a)$. En effet, si $f(x,a)$ est fausse, alors $(y = a) \wedge f(x,y)$ est fausse pour toute valeur de y et, si elle est vraie, alors elle est vraie pour une valeur de y (et cette valeur est a). Donc, $x \in a \cup b$ est équivalente à $(x \in a) \vee (x \in b)$.

□

Axiome de l'ensemble des parties : *La collection des parties d'un ensemble est un ensemble :*

$$\forall a\, \exists b\, \forall x\, ((x \in b) \Leftrightarrow (x \subset a)).$$

Cet ensemble est unique d'après l'axiome d'extensionnalité. L'ensemble des parties (ou enseble des sous-ensembles) d'un ensemble x est aussi appelé *ensemble puissance* de x et noté $\mathscr{P}(x)$.

Schéma d'axiomes de compréhension : *Pour tout prédicat* $\boldsymbol{P}$ *à une variable libre x et chaque ensemble a, il existe un ensemble qui a pour éléments l'ensemble des éléments de a vérifiant la propriété* $\boldsymbol{P}$*, c'est-à-dire :*

$$\forall a\, \exists b\, \forall x\, [(x \in b) \Leftrightarrow ((x \in a) \wedge Px)].$$

Avec les mêmes notations, cet ensemble est noté $\{x \in a | Px\}$. Il est unique d'après l'axiome d'extensionnalité. (En effet, si deux ensembles satisfont l'énoncé de l'axiome obtenu pour un même ensemble et une même propriété, alors tout élément de l'un appartient à l'autre.) Ce schéma d'axiomes implique qu'il existe un ensemble vide, noté $\varnothing$, pourvu qu'au moins un ensemble a existe—ce qui est nécessairement le cas puisque, en logique du premier ordre, les domaines d'interprétation des variables d'objets de base, ici les ensembles, sont non vides. On peut en effet le définir par : $\varnothing = \{x \in a | x \neq x\}$. Puisque tout ensemble x satisfait $x = x$, il n'existe aucun x tel que $x \in \varnothing$; autrement dit, la formule suivante est vraie : $\forall x\, x \notin \varnothing$. Cet ensemble est unique d'après l'axiome d'extensionnalité.

Notons que, puisque $\forall x\, x \notin \varnothing$ est vraie, $\exists x\, x \in \varnothing$ est fausse et $x \notin \varnothing$ est équivalente à V et $x \in \varnothing$ à F.

Lemme : Le prédicat suivant est vrai : $\forall x \varnothing \subset x$.

Démonstration : Soit x un ensemble. La formule $\varnothing \subset x$ est équivalente à : $\forall e\, (e \in \varnothing) \Rightarrow (e \in x)$. Or, pour tout ensemble e, $e \in \varnothing$ est faux, donc $(e \in \varnothing) \Rightarrow (e \in x)$ est vrai. Donc, $\forall e\, (e \in \varnothing) \Rightarrow (e \in x)$ est vrai. Donc, $\varnothing \subset x$ est vrai.

□

Démonstration bis : On veut montrer que le prédicat $P : \forall x \forall e\, (e \in \varnothing \Rightarrow e \in x)$ est vrai. P est équivalent à : $\forall x \forall e\, ((e \in x) \vee \neg(e \in \varnothing))$, c'est-à-dire, à : $\forall x \forall e\, ((e \in x) \vee (e \notin \varnothing))$. Puisque $\forall e\, e \notin \varnothing$ est vrai, $e \notin \varnothing$ est équivalent à V, donc $\forall e\, ((e \in x) \vee (e \notin \varnothing))$ est équivalent à $\forall e\, ((e \in x) \vee \mathsf{V})$, donc à $\forall e\, \mathsf{V}$, et donc à V. Donc, P est vrai.

□

Lemme : Le prédicat suivant est vrai : $\forall x\, x \subset \varnothing \Rightarrow x = \varnothing$.

Démonstration : Soit x un ensemble satisfaisant $x \subset \varnothing$. Pour tout ensemble y, on a $y \notin \varnothing$, donc $y \notin x$.

□

Démonstration bis : On veux montrer le prédicat $P : \forall x\, (x \subset \varnothing) \Rightarrow (x = \varnothing)$. Il est équivalent à : $\forall x\, (x \subset \varnothing) \Rightarrow ((x \subset \varnothing) \wedge (\varnothing \subset x))$, donc à $\forall x\, \neg(x \subset \varnothing) \vee ((x \subset \varnothing) \wedge (\varnothing \subset x))$, donc à $\forall x\, (\neg(x \subset \varnothing) \vee (x \subset \varnothing)) \wedge (\neg(x \subset \varnothing) \vee (\varnothing \subset x))$. Puisque $\neg(x \subset \varnothing) \vee (x \subset \varnothing)$ est toujours vrai (soit f la formule $x \subset \varnothing$, il s'agit de $\neg f \vee f$, qui est vrai que f soit vraie ou fausse), P est équivalent à $\forall x\, (\neg(x \subset \varnothing) \vee (\varnothing \subset x))$. On a vu que $\forall x \varnothing \subset x$ est vrai. Donc, $\varnothing \subset x$ est équivalente à V. Donc, P est équivalente à $\forall x\, (\neg(x \subset \varnothing) \vee \mathsf{V})$, donc à $\forall x\, \mathsf{V}$, et donc à V. Donc, P est vrai.

□

L'axiome de compréhension peut aussi être utilisé pour définir la différence de deux ensembles. Soit A et B deux ensembles. On note $A \backslash B$ l'ensemble $\{x \in A | x \notin B\}$.

Notons qu'il s'agit bien d'un schéma d'axiomes, c'est-à-dire une méthode permettant de construire des axiomes, et non d'un seul axiome : puisqu'on ne peut pas quantifier les prédicats en logique du premier ordre, ce schéma définit un axiome pour chaque prédicat à un paramètre libre. En théorie Z, on considère le prédicat obtenu à partir de tout prédicat P à une variable libre comme vrai.

Ce schéma peut être reformulé en notant que, si P est un prédicat à une variable libre x et d'autres variables libres éventuelles $a_1 \cdots a_p$, et si $\alpha 1 \ldots \alpha_p$ est une collection d'ensembles pouvant remplacer $a_1 \ldots a_p$, alors le prédicat Q défini par $Q : Px\alpha 1 \cdots \alpha_p$ a une unique variable libre x. Le schéma d'axiomes de compréhension peut ainsi être reformulé de la manière suivante : *Pour tout prédicat P à une variable libre x et d'éventuels autres variables libres collectivement notées $a_1 \ldots a_p$, pour chaque valeur des variables $a_1 \cdots a_p$ et chaque ensemble b, il existe un ensemble qui a pour éléments l'ensemble des éléments de b vérifiant la propriété $Pxa_1 \ldots a_p$, c'est-à-dire :*

$$\forall a_1 \ldots a_p \forall b\, \exists c\, \forall x\, [(x \in c) \Leftrightarrow ((x \in b) \wedge Pxa_1 \ldots a_p)].$$

(Dans cette formule, il est entendu que le premier quantificateur est absent si P n'a qu'une seule variable libre.)

Lemme : Soit A et B deux ensembles. Alors, $(A \backslash B) \cup B = A \cup B$.

Démonstration : Soit x un élément de $A \cup B$. Si $x \in B$, alors $x \in (A \backslash B) \cup B$. Sinon, $x \in A$, donc $x \in A \backslash B$, donc $x \in (A \backslash B) \cup B$. Donc, dans tous les cas, $x \in (A \backslash B) \cup B$.

Soit x un élément de $(A \backslash B) \cup B$. Alors, $x \in A \backslash B$ ou $x \in B$. Si $x \in A \backslash B$, alors $x \in A$ puisque $A \backslash B \subset A$, donc $x \in A \cup B$. Si $x \in B$, alors $x \in A \cup B$. Donc, dans tous les cas, $x \in A \cup B$.

On a donc montré que : $\forall x\, (x \in A \cup B) \Leftrightarrow (x \in (A \backslash B) \cup B)$, et donc que $(A \backslash B) \cup B = A \cup B$.

□

Démonstration bis : Le prédicat $x \in A \cup B$ est équivalent à $(x \in A) \vee (x \in B)$. Le prédicat $x \in (A \backslash B) \cup B$ est équivalent à $(x \in A \backslash B) \vee (x \in B)$, et donc à $((x \in A) \wedge (x \notin B)) \vee (x \in B)$. Ce dernier est équivalent à $((x \in A) \vee (x \in B)) \wedge ((x \notin$

$B) \vee (x \in B)$). Pour toute formule f, $(\neg f) \vee f$ est vrai que f soit vraie ou fausse, donc équivalent à V. Donc, $x \in (A \backslash B) \cup B$ est équivalent à $((x \in A) \vee (x \in B)) \wedge \mathsf{V}$, donc à $(x \in A) \vee (x \in B)$, et donc à $x \in A \cup B$. Donc, $(x \in A \cup B) \Leftrightarrow (x \in (A \backslash B) \cup B)$ est équivalent à $(x \in A \cup B) \Leftrightarrow (x \in A \cup B)$. Pour toute formule f, $f \Leftrightarrow f$ est vrai que f soit vraie ou fausse, et donc équivalent à V. Donc, $\forall x\, (x \in A \cup B) \Leftrightarrow (x \in (A \backslash B) \cup B)$ est vrai.

□

Lemme : Soit A et B deux ensembles tels que $B \subset A$. Alors, $A \cup B = A$.

Démonstration : Soit x un élément de $A \cup B$. Alors, $x \in A$ ou $x \in B$. Si $x \in B$, et puisque $B \subset A$, $x \in A$. Donc, $x \in A$.
Soit x un élément de A, on a $x \in A \cup B$.
Ainsi, $A \cup B = A$.

□

Démonstration bis : Puisque $B \subset A$, le prédicat $\forall x\, (x \in B) \Rightarrow (x \in A)$ est vrai. Donc, le prédicat $(x \in B) \Rightarrow (x \in A)$ est équivalent à V. Donc, le prédicat $(x \in A) \vee (x \notin B)$ est équivalent à V.

Le prédicat $x \in A \cup B$ est équivalent à $(x \in A) \vee (x \in B)$. Puisque, pour tout prédicat P, $P \wedge \mathsf{V}$ est équivalent à P, $x \in A \cup B$ est équivalent à $((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \notin B))$, et donc à $(x \in A) \vee ((x \in B) \wedge (x \notin B))$. Puisque, pour tout prédicat P, $P \wedge \neg P$ est équivalent à F, cela est équivalent à $(x \in A) \vee \mathsf{F}$, et donc à $x \in A$. Donc, $x \in A \cup B$ est équivalent à $x \in A$. Donc, $\forall x\, x \in A \cup B \Leftrightarrow x \in A$ est vrai. Donc, $A \cup B = A$.

□

Axiome de l'infini : *Il existe un ensemble contenant l'ensemble vide et clos par application du successeur* $x \mapsto x \cup \{x\}$. Formellement, cet axiome s'écrit :

$$\exists Y\, (\varnothing \in Y) \wedge (\forall y\, ((y \in Y) \Rightarrow (y \cup \{y\} \in Y))).$$

L'ensemble ainsi défini contient $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, ...

Notation : Soit E un ensemble et P un prédicat dépendant des variables x, a, ..., b. On peut noter par
- $\forall x \in E\, P(x, a, \ldots, b)$ le prédicat $\forall x\, x \in E \Rightarrow P(x, a, \ldots, b)$,
- $\exists x \in E\, P(x, a, \ldots, b)$ le prédicat $\exists x\, x \in E \wedge P(x, a, \ldots, b)$.

1.2.2 Intersection

Soit a et b deux ensembles. On appelle *intersection* de a et b, notée $a \cap b$, l'ensemble

$$a \cap b = \{x \in a | x \in b\}.$$

Cet ensemble existe d'après le schéma d'axiomes de compréhension, en considérant la formule à un paramètre $Px : x \in b$. Il est unique d'après l'axiome d'extensionnalité. On a : $\forall x\, x \in a \cap b \Leftrightarrow (x \in a \wedge x \in b)$. Notons que cette définition est symétrique : $\forall a\, \forall b\, (a \cap b) = (b \cap a)$. Elle est aussi transitive : si a, b et c sont trois ensembles, on a $(a \cap b) \cap c = a \cap (b \cap c)$. (Ces deux propriétés sont des conséquence de la symétrie et de la transitivité du connecteur $\wedge$.) On pourra noter ce l'ensemble $a \cap (b \cap c)$ par $a \cap b \cap c$.

De même, on a : $\forall x\, x \in a \cup b \Leftrightarrow (x \in a \vee x \in b)$. On en déduit aisément que $a \cup b = b \cup a$ et, si c est un ensemble, $(a \cup b) \cup c = a \cup (b \cup c)$. On pourra noter ce l'ensemble $a \cup (b \cup c)$ par $a \cup b \cup c$.

Lemme : Soit E un ensemble. Alors $E \cup \varnothing = E$ et $E \cap \varnothing = \varnothing$.

Démonstration : Soit e un ensemble. Si $e \in E$, alors $(e \in E) \vee (e \in \varnothing)$ est vrai, donc $e \in (E \cup \varnothing)$. Sinon, et puisque $e \in \varnothing$ est faux, alors $(e \in E) \vee (e \in \varnothing)$ est faux, donc $e \in (E \cup \varnothing)$ est faux. On a donc : $\forall e\, (e \in E) \Leftrightarrow (e \in (E \cup \varnothing))$. Donc, $E = E \cup \varnothing$.
Soit e un ensemble. Puisque $e \in \varnothing$ est faux, $(e \in \varnothing) \wedge (e \in E)$ est faux. Donc, $e \in (E \cap \varnothing)$ est faux. Cela montre que $E \cap \varnothing = \varnothing$.

□

Démonstration bis :
- Notons P_1 et P_2 les prédicats à un paramètre libre suivants : $P_1(x) : x \in E \cup \varnothing$, $P_2(x) : x \in E$. P_1 est équivalent à $(x \in E) \vee (x \in \varnothing)$. Puisque $x \in \varnothing$ est équivalent à F, P_1 est équivalent à $x \in E$. Donc, P_1 est équivalent à P_2. Donc, $P_1 \Leftrightarrow P_2$ est équivalent à V. Donc, $\forall x\, P_1 \Leftrightarrow P_2$ est vrai. Donc, $E \cup \varnothing = E$.

- Notons P_1 le prédicat à un paramètre libre : $P_1(x) : x \in E \cap \varnothing$. P_1 est équivalent à $(x \in E) \wedge (x \in \varnothing)$. Puisque $x \in \varnothing$ est équivalent à F, P_1 est équivalent à F, et donc à $x \in \varnothing$. Donc, $P_1 \Leftrightarrow (x \in \varnothing)$ est équivalent à V. Donc, $\forall x\, P_1 \Leftrightarrow (x \in \varnothing)$ est vrai. Donc, $E \cap \varnothing = \varnothing$.

□

1.2.3 Schéma d'axiomes de remplacement

La théorie de Zermelo plus cet axiome donne la théorie ZF.

Énoncé : *Soit F une formule à deux variables libres (notées en première et second position) et d'éventuels paramètres notés $a_1 \dots a_p$. Alors,*

$$\forall a_1 \dots a_p \left(\forall x \forall y \forall z \left[(Fxya_1 \dots a_p \wedge Fxza_1 \dots a_p) \Rightarrow (z = y) \right] \right) \Rightarrow \left(\forall b \exists c \forall z \left[(z \in c) \Leftrightarrow (\exists x \left[(x \in b) \wedge (Fxza_1 \dots a_p) \right]) \right] \right).$$

Lemme : Pour un choix donné des paramètres tel que le membre de gauche de l'implication est satisfait et pour tout b, l'ensemble c définit par $\forall z \left[(z \in c) \Leftrightarrow (\exists x \left[(x \in b) \wedge (Fxza_1 \dots a_p) \right]) \right]$ est unique d'après l'axiome d'extensionnalité.

La démonstration de ce lemme est relativement triviale. Écrivons-là cependant explicitement par soucis de clarté.

Démonstration : Soit F une formule à deux variables libres notées en première et seconde position et d'éventuels paramètres, collectivement notés a. Fixons les paramètres a tels que la formule

$$\forall x \forall y \forall z \left[(Fxya \wedge Fxza) \Rightarrow (z = y) \right]$$

est vraie.

Soit b un ensemble. Soit c_1 et c_2 deux ensembles satisfaisant :

$$(z \in c_1) \Leftrightarrow (\exists x \left[(x \in b) \wedge (Fxza) \right])$$

et

$$(z \in c_2) \Leftrightarrow (\exists x \left[(x \in b) \wedge (Fxza) \right]).$$

Alors, ,

- Soit z un ensemble. Si $z \in c_1$, il existe un élément x de b tel que $Fxza$ est vrai. Donc, $z \in c_2$.
- Soit z un ensemble. Si $z \in c_2$, il existe un élément x de b tel que $Fxza$ est vrai. Donc, $z \in c_1$.

Les deux ensembles c_1 et c_2 sont donc égaux d'après l'axiome d'extensionnalité.

□

Si F est une formule à deux variables libres sans autres paramètres, le schéma d'axiomes de remplacement donne :

$$\left(\forall x \forall y \forall z \left[(Fxy \wedge Fxz) \Rightarrow (z = y) \right] \right) \Rightarrow \left(\forall b \exists c \forall z \left[(z \in c) \Leftrightarrow (\exists x \left[(x \in b) \wedge (Fxz) \right]) \right] \right).$$

Lemme : Le schéma d'axiomes de compréhension est une conséquence du schéma d'axiomes de remplacement, obtenue en prenant $Fxy : (x = y) \wedge P(x)$.

Démonstration : (On peut aisément étendre cette démonstration au cas où le prédicat P a d'autres paramètres que x en ajoutant les mêmes paramètres à F.) On admet le schéma d'axiomes de remplacement. Soit P un prédicat à un paramètre libre. Soit F la formule à deux paramètres libres définie par $Fxy : (x = y) \wedge P(x)$. Pour tous y et z, si Fxy et Fxz, alors $x = y$ et $x = z$, donc $y = z$ par réflexivité et transitivité de l'égalité. Soit b un ensemble. D'après l'axiome obtenu par le schéma d'axiomes de compréhension pour la formule F, on peut choisir un ensemble c tel que :

$$\forall z\, (z \in c) \Leftrightarrow \left(\exists x \left((x \in b) \wedge (Fxz) \right) \right).$$

Cette formule est équivalente à :

$$\forall z\, (z \in c) \Leftrightarrow \left(\exists x \left((x \in b) \wedge (x = z) \wedge P(x) \right) \right).$$

Puisque la relation $\wedge$ est symétrique et transitive, la formule $\exists x\,((x \in b) \wedge (x = z) \wedge P(x))$ est équivalente à $\exists x\,((x = z) \wedge ((x \in b) \wedge P(x)))$. Or, pour tout z, la formule $\exists x\,((x = z) \wedge ((x \in b) \wedge P(x)))$ est équivalente à $(z \in b) \wedge P(z)$. En effet,

- Si cette dernière est vraie, alors, puisque $z = z$ est toujours vrai par réciprocité de l'égalité, $(z = z) \wedge ((z \in b) \wedge P(z))$ est vraie, et donc il existe une valeur de x (z) telle que $(x \in b) \wedge (x = z) \wedge P(x)$ est vraie.
- Si elle est fausse, alors il n'existe aucune valeur de x telle que $(x = z) \wedge ((x \in b) \wedge P(x))$ est vraie puisque, si $x = z$ est vrai, $(x \in b) \wedge P(x)$ a la même valeur de vérité que $(z \in b) \wedge P(z)$ et est donc fausse.

Ainsi, l'ensemble c satisfait :

$$\forall z\,(z \in c) \Leftrightarrow \big((z \in b) \wedge P(z)\big).$$

On a donc montré que :

$$\forall b\,\exists c\,\forall z\,(z \in c) \Leftrightarrow \big((z \in b) \wedge P(z)\big).$$

□

Lemme: En présence du schéma d'axiomes de remplacement, l'axiome de la paire est une conséquence des autres.

Démonstration: Tout d'abord, d'après le schéma d'axiomes de compréhension, l'ensemble vide $\varnothing$ existe. Son seul sous-ensemble est lui-même. En effet, on a $\varnothing \subset \varnothing$ (puisque chaque ensemble est un sous-ensemble de lui-même ; une autre façon de voir cela est que $(x \in \varnothing) \Rightarrow (x \in \varnothing)$ est vraie pour tout x puisque le membre de gauche est toujours faux) et, si $a \subset \varnothing$, alors $\forall x\, x \notin a$ (sans quoi on aurait $x \in a$ et donc $x \in \varnothing$, ce qui est impossible par définition de l'ensemble vide), et donc $a = \varnothing$. Donc, l'ensemble des parties de $\varnothing$ est l'ensemble ne contenant que $\varnothing$. Cet ensemble est noté $\{\varnothing\}$. Ce nouvel ensemble contient deux sous-ensembles : $\varnothing$ et $\{\varnothing\}$. (Ce sont bien des sous-ensembles car tout élément d'un de ces ensembles doit être $\varnothing$, qui est un élément de $\{\varnothing\}$ et, si $a \subset \{\varnothing\}$, a ne peut contenir d'autre élément que $\varnothing$; il doit donc être égal soit à $\varnothing$ (s'il ne contient pas $\varnothing$) soit à $\{\varnothing\}$ (s'il le contient).) D'après l'axiome de l'ensemble des parties, l'ensemble $\{\varnothing, \{\varnothing\}\}$ contenant uniquement $\varnothing$ et $\{\varnothing\}$ existe donc.

Soit A et B deux ensembles. Considérons la formule à deux variables libres F définie par :

$$Fxy : [(x = \varnothing) \wedge (y = A)] \vee [(x = \{\varnothing\}) \wedge (y = B)].$$

Notons que $\{\varnothing\} \neq \varnothing$ puisque $\varnothing \in \{\varnothing\}$ et $\varnothing \notin \varnothing$. F satisfait :

$$\forall x\,\forall y\,\forall z\,([(Fxy) \wedge (Fxz)] \Rightarrow [y = z]).$$

(Car, si le membre de gauche est vrai, soit $x = \varnothing$, $y = A$, $z = A$, soit $x = \{\varnothing\}$, $y = B$, $z = B$.) Soit C l'ensemble défini par l'axiome de remplacement pour F, en prenant pour l'ensemble noté b dans la définition l'ensemble $\{\varnothing, \{\varnothing\}\}$. Alors, pour tout d, $d \in C$ si et seulement si il existe x tel que $x \in \{\varnothing, \{\varnothing\}\}$ et Fxd. On a donc deux (et seulement deux) possibilités : $x = \varnothing$ et $d = A$, ou $x = \{\varnothing\}$ et $d = B$. Donc, $[d \in C] \Leftrightarrow [(d = A) \vee (d = B)]$. L'ensemble C est donc la paire $\{A, B\}$.[15]

□

En admettant le schéma d'axiomes de remplacement, on peut donc s'affranchir du schéma d'axiomes de compréhension et de l'axiome de la paire. La théorie ZF est ainsi définie par quatre axiomes et un schéma d'axiomes.

1.2.4 Axiome de fondation

Cet axiome peut être inclus ou non dans la théorie ZFC, selon les auteurs. Dans la suite, on ne l'inclura pas sauf mention contraire explicite.

Énoncé : *Tout ensemble x non vide possède un élément y n'ayant aucun élément commun avec x:*
$\forall\, x,\ [x \neq \varnothing \Rightarrow (\exists y\, y \in x\ \wedge\ y \cap x = \varnothing)]$.

Corolaire 1 : Aucun ensemble ne peut être un élément de lui-même.

[15] Montrons cela plus rigoureusement. Tout d'abords, A et B appartiennent à C. En effet, on a $\varnothing \in \{\varnothing, \{\varnothing\}\}$ et $F\varnothing A$, donc $A \in C$, et $\{\varnothing\} \in \{\varnothing, \{\varnothing\}\}$ et $F\{\varnothing\}\,B$, donc $B \in C$.
Soit X un élément de C. On peut choisir un élément x de $\{\varnothing, \{\varnothing\}\}$ tel que FxX. Cela laisse deux possibilités : $x = \varnothing$ ou $x = \{\varnothing\}$. Si $x = \varnothing$, FxX implique $X = A$. Si $x = \{\varnothing\}$, FxX implique $X = B$. Dans les deux cas, on a bien $(X = A) \wedge (X = B)$.
Ainsi, $(X \in C) \Leftrightarrow ((X = A) \vee (X = B))$ est vrai.

Démonstration : Soit y un ensemble quelconque, et considérons l'ensemble $x = \{y\}$. (Cet ensemble existe d'après l'axiome de la paire : il s'agit de la paire formée par y et lui-même.) Alors, x est non vide et ne contient qu'un élément (y). D'après l'axiome de fondation, on a donc $y \cap x = \emptyset$. Puisque $y \in x$, cela implique $y \notin y$ (sans quoi on aurait $y \in y \cap x$).

□

Corolaire 2 : Soit deux ensembles x et y. Si $x \in y$, alors $y \notin x$.

Démonstration : Soit x et y deux ensembles tels que $x \in y$. Considérons l'ensemble $z = \{x,y\}$ (qui existe d'après l'axiome de la paire). L'ensemble z est non vide et ne contient que les éléments x et y. Donc, d'après l'axiome de fondation, $x \cap z = \emptyset$ ou $y \cap z = \emptyset$. Mais $x \in y$, donc $x \in (y \cap z)$, donc la formule $y \cap z = \emptyset$ est fausse. On a donc $x \cap z = \emptyset$, et donc, puisque $y \in z$, $y \notin x$.

□

1.2.5 Couples

Définition : Soit deux ensembles x et y. D'après l'axiome de la paire, $\{x\}$ et $\{x, y\}$ existent. En utilisant à nouveau l'axiome de la paire, l'ensemble $\{\{x\}, \{x, y\}\}$ existe. On l'appelle le *couple* de x et y, noté (x,y).

Lemme : Soit a, b, c et d quatre ensembles tels que $(a,b) = (c,d)$. Alors $a = c$ et $b = d$.

Démonstration : On distingue deux cas selon que a et b sont égaux ou non. Supposons d'abord que $a = b$. Alors, $(a,b) = \{\{a\}\}$. Puisque $\{c\} \in (c,d)$ et $(c,d) = (a,b)$, on en déduit que $\{c\} \in \{\backslash lbracea\}\}$ et donc $\{c\} = \{a\}$. Donc, $c \in \{a\}$, et donc $c = a$. Par ailleurs, $\{c, d\} \in (c,d)$, donc $\{c, d\} = \{a\}$, et donc $d = a$. Puisque $b = a$, on a donc bien $c = a$ et $d = b$.

Supposons maintenant $a \neq b$. Puisque $\{c\} \in (c,d)$, et $(c,d) = (a,b)$, on a $\{c\} = \{a\}$ ou $\{c\} = \{a, b\}$. Montrons que la seconde égalité est impossible. Si elle était vraie, puisque $a \in \{a, b\}$, on aurait $a \in \{c\}$, donc $a = c$, et, puisque $b \in \{a,b\}$, on aurait $b \in \{c\}$, donc $b = c$, et donc (par symétrie et transitivité de l'égalité) $b = a$, ce qui est impossible $a \neq b$. Ainsi, $\{c\} = \{a, b\}$ est nécessairement fausse, et donc $\{c\} = \{a\}$. Donc, $c \in \{a\}$, et donc $c = a$.

Puisque $\{a,b\} \in (a,b)$ et $(a,b) = (c,d)$, on a $\{a,b\} \in (c,d)$. Donc, $\{a,b\} = \{c\}$ ou $\{a,b\} = \{c, d\}$. On vient de voir que la première égalité est fausse, donc $\{a,b\} = \{c, d\}$. Donc, $b \in \{c, d\}$. Donc, $b = c$ ou $b = d$. Puisque $a = c$ et $b \neq a$, la première égalité est fausse. Donc, $b = d$.

□

Soit x et y deux ensembles et $z = (x,y)$. On dit parfois que x est la *première composante* de z et y sa *deuxième composante*, ou *seconde composante*.

1.2.6 Produit Cartésien

Soit a et b deux ensembles, c l'ensemble des parties de a et d l'ensemble des parties de $a \cup b$. Soit e l'ensemble des parties de $c \cup d$. Soit P le prédicat à une variables x définit par :

$$Px : \exists\alpha\, \exists\beta\, (\alpha \in a) \wedge (\beta \in b) \wedge (x = (\alpha, \beta)).$$

On note $a \times b$ et on appelle *produit Cartésien de a et b* l'ensemble des éléments de e satisfaisant la propriété P. Cet ensemble existe d'après le schéma d'axiomes de compréhension.

Soit a et b deux ensembles et c un sous-ensemble de $a \times b$. On appelle *domaine* de c l'ensemble $\{x \in a | \exists y\, y \in b \wedge (x,y) \in c\}$.

Lemme : Soit a, b, a' et b' quatre ensembles tels que $a' \subset a$ et $b' \subset b$. Alors $a' \times b' \subset a \times b$.

Démonstration : Soit z un élément de $a' \times b'$. On peut choisit un élément x de a' et un élément y de b' tels que $z = (x,y)$. Puisque a' est un sous-ensemble de a, on a $x \in a$. Puisque b' est un sous-ensemble de b, on a $y \in b$. Donc, $(x,y) \in a \times b$. Donc, $z \in a \times b$.

□

Lemme : Soit E un ensemble. On a : $E \times \emptyset = \emptyset$ et $\emptyset \times E = \emptyset$.

Démonstration :

- Supposons par l'absurde qu'il existe un ensemble z tel que $z \in E \times \emptyset$. Alors, il existe un élément x de E et un élément y de $\emptyset$ tels que $z = (x,y)$. Puisque $y \in \emptyset$ est faux pour tout ensemble y, cela est impossible. Ainsi, $z \in E \times \emptyset$ est faux pour tout ensemble z, et donc $E \times \emptyset = \emptyset$.

- Supposons par l'absurde qu'il existe un ensemble z tel que $z \in \emptyset \times E$. Alors, il existe un élément x de $\emptyset$ et un élément y de E tels que $z = (x,y)$. Puisque $x \in \emptyset$ est faux pour tout ensemble x, cela est impossible. Ainsi, $z \in \emptyset \times E$ est faux pour tout ensemble z, et donc $\emptyset \times E = \emptyset$.

□

1.2.7 Graphe de relation binaire

Soit a et b deux ensembles. Un *graphe de relation binaire* sur a et b est un sous-ensemble de $a \times b$. À un graphe de relation binaire G est associé une relation binaire R définie par : $\forall a \, \forall b \, (aRb) \Leftrightarrow ((a,b) \in G)$. On dira alors que la relation R est *définie sur a et b*.

1.2.8 Relation d'ordre

Soit E un ensemble. Une relation binaire $\leq$ définie sur $E \times E$ est dite *relation d'ordre* sur E si elle satisfait les trois propriétés suivantes :

- *Réflexivité :* $\forall x \; x \in E \Rightarrow x \leq x$.
- *Antisymétrie :* $\forall x \, \forall y \; x \in E \wedge y \in E \wedge (x \leq y) \wedge (y \leq x) \Rightarrow x = y$.
- *Transitivité :* $\forall x \, \forall y \, \forall z \; x \in E \wedge y \in E \wedge z \in E \wedge (x \leq y) \wedge (y \leq z) \Rightarrow x \leq z$.

Une relation d'ordre $\leq$ sur E est dite *relation d'ordre total* si la formule suivante est vraie : $\forall x \in E \, \forall y \in E \, (x \leq y) \vee (y \leq x)$. Un élément e de E tel que : $\forall f \; f \in E \wedge f \leq e \Rightarrow f = e$ est dit *minimal* (pour l'ensemble E et pour la relation $\leq$) ; on dit aussi que E admet e pour élément minimal pour la relation $\leq$. Un élément e de E tel que $\forall x \in E \, e \leq x$ est dit *plus petit élément*, ou *minimum*, de E (pour la relation $\leq$). Un élément e de E tel que : $\forall f \; f \in E \wedge e \leq f \Rightarrow f = e$ est dit *maximal* (pour l'ensemble E et pour la relation $\leq$) ; on dit aussi que E admet e pour élément maximal pour la relation $\leq$. Un élément e de E tel que $\forall x \in E \; x \leq e$ est dit *plus grand élément*, ou *maximum*, de E (pour la relation $\leq$). Un ensemble muni d'une relation d'ordre est dit *ordonné*. Un ensemble muni d'une relation d'ordre total est dit *totalement ordonné*.

Remarque : Soit E un ensemble et F un sous-ensemble de E. Soit $\leq$ une relation d'ordre sur E. Alors, $\leq$ est une relation d'ordre sur F. En outre, si $\leq$ est une relation d'ordre total sur E, elle l'est qussi sur F.

Remarque : Un ensemble a au plus un minimum et au plus un maximum.

Démonstration : Soit E un ensemble et $\leq$ une relation d'ordre sur E.

- Soit a et b deux minima de E pour la relation $\leq$. Alors $a \leq b$ (puisque a est un minimum) et $b \leq a$ (puisque b est un minimum). Donc, $a = b$.
- Soit a et b deux maxima de E pour la relation $\leq$. Alors $b \leq a$ (puisque a est un maximum) et $a \leq x$ (puisque b est un maximum). Donc, $a = b$.

□

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Alors, E admet au plus un plus minimum et au plus un maximum.

Démonstration : Soit x et y deux minima de E. Alors, $x \leq y$ et $y \leq x$, donc $x = y$.
Soit x et y deux maxima de E. Alors, $y \leq x$ et $x \leq y$, donc $x = y$.

□

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Soit e un élément de E. Alors,

- Si e est un minimum de E pour $\leq$, alors e est un élément minimal de E pour $\leq$.
- Si e est un maximum de E pour $\leq$, alors e est un élément maximal de E pour $\leq$.

Démonstration :

- Supposons que e est un minimum de E pour $\leq$.. Soit x un élément de E tel que $x \leq e$. Alors, puisque e est un minimum, $x \leq e \wedge e \leq x$. Donc, $x = e$.
- Supposons que e est un maximum de E pour $\leq$.. Soit x un élément de E tel que $e \leq x$. Alors, puisque e est un maximum, $e \leq x \wedge x \leq e$. Donc, $x = e$.

□

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre total sur E. Alors, E admet au plus un élément maximal et au plus un élément minimal pour la relation $\leq$.

Démonstration : Soit a et b deux éléments maximaux de E pour la relation $\leq$. Puisque $\leq$ est une relation d'ordre total sur E, $a \leq b$ ou $b \leq a$. Puisque a est un élément maximal, $a \leq b$ implique $b = a$. Puisque b est un élément maximal, $b \leq a$ implique $a = b$. Donc, et puisque l'égalité est symétrique, on a dans tous les cas $a = b$. Cela montre que E admet au plus un seul élément maximal pour la relation $\leq$.

Soit a et b deux éléments minimaux de E pour la relation $\leq$. Puisque $\leq$ est une relation d'ordre total sur E, $a \leq b$ ou $b \leq a$. Puisque b est un élément minimal, $a \leq b$ implique $a = b$. Puisque a est un élément minimal, $b \leq a$ implique $b = a$. Donc, et puisque l'égalité est symétrique, on a dans tous les cas $a = b$. Cela montre que E admet au plus un seul élément minimal pour la relation $\leq$.

□

Remarques :

- Un élément minimal d'un ensemble totalement ordonné est aussi le minimum de cet ensemble.
- Un élément maximal d'un ensemble totalement ordonné est aussi le maximum de cet ensemble.

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Soit e un élément de E tel que : $\forall x \in E\, e \leq x$. Alors e est un élément minimal de E pour $\leq$.

Démonstration : Soit x un élément de E tel que $x \leq e$. On a $(x \leq e) \wedge (e \leq x)$. Par antisymétrie de la relation $\leq$, on en déduit $x = e$.

□

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre total sur E. Soit e un élément de E. Alors, le prédicat $\forall f \in E\, e \leq f$ est équivalent à dire que e est l'élément minimal de E.

Démonstration :

- Supposons le prédicat $\forall f \in E\, e \leq f$ vrai. Soit f un élément de E tel que $f \leq e$. On a alors $e \leq f$ et $f \leq e$, donc $f = e$ par antisymétrie de la relation $\leq$. Ainsi, e est un élément minimal de E pour $\leq$. Puisque $\leq$ est une relation d'ordre total, cet élément minimal est unique.
- *(Nous adoptions ici une approche un brin pédestre.)* Supposons que e est l'élément minimal de E pour $\leq$. Soit f un élément de E. Puisque $\leq$ est une relation d'ordre total, $e \leq f \vee f \leq e$ est vrai. Puisque e est l'élément minimal de E pour $\leq$, $f \leq e \Rightarrow f = e$ est vrai. *(Ici, on pourrait directement conclure que, puisque $f \leq e$ implique $f = e$ et donc $e \leq f$, la première formule est équivalente à $e \leq f$. Dans la suite, nous montrons cela plus formellement* via *le calcul des prédicats.)* Cette dernière formule peut se récrire en : $f = e \vee \neg(f \leq e)$. La conjonction de ces deux prédicats donne : $(e \leq f \vee f \leq e) \wedge (f = e \vee \neg(f \leq e))$. En développant cette formule, il vient : $(e \leq f \wedge f = e) \vee (e \leq f \wedge \neg(f \leq e)) \vee (f \leq e \wedge f = e) \vee (f \leq e \wedge \neg(f \leq e))$. Cette formule peut être simplifiée en : $(f = e) \vee (e \leq f \wedge \neg(f \leq e)) \vee (f = e) \vee \mathsf{F}$, ou en $(f = e) \vee (e \leq f \wedge \neg(f \neq e))$. Cette formule ne peut être vraie que si $e \leq f$ (sans quoi $f = e$ et $e \leq f$ seraient fausses). Donc, $e \leq f$. Nous avons donc montré que $\forall f \in E\, e \leq f$ est vrai.

□

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre sur E. La relation $\geq$ sur E définie par : $\forall x\, \forall y\, x \in E \wedge y \in E \Rightarrow (x \geq y \Leftrightarrow y \leq x)$ est une relation d'ordre sur E. En outre, si $\leq$ est une relation d'ordre total, alors $\geq$ l'est aussi.

Démonstration :

- *Réflexivité :* Soit x un élément de E. On a $x \leq x$ par réflexivité de la relation $\leq$, donc $x \geq x$.
- *Antisymétrie :* Soit x et y deux éléments de E tels que $x \geq y$ et $y \geq x$. Alors, $y \leq x$ et $x \leq y$. Par antisymétrie de la relation $\leq$, on en déduit que $x = y$.
- *Transitivité :* Soit x, y et z trois éléments de E tels que $x \geq y$ et $y \geq z$. Alors, $y \leq x$ et $z \leq y$. Par transitivité de la relation $\leq$, on en déduit que $z \leq x$, et donc $x \geq z$.
- Supposons que $\leq$ est une relation d'ordre total. Soit x et y deux éléments de E. Alors, $x \leq y$ ou $y \leq x$. Donc, $y \geq x$ ou $x \geq y$.

□

Soit E un ensemble, $\leq$ une relation d'ordre total sur E et F un sous-ensemble de E. On dit que F est *borné supérieurement* (dans E et pour la relation $\leq$) s'il existe un élément m de E tel que : $\forall e\, (e \in F) \Rightarrow (e \leq m)$. On dit alors que cet élément est une *borne supérieure* de F (dans E et pour la relation $\leq$). On dit que F est *borné inférieurement* (dans E et pour la relation $\leq$) s'il existe un élément m de E tel que : $\forall e\, (e \in F) \Rightarrow (m \leq e)$. On dit alors que cet élément est une *borne inférieure* de F (dans E et pour la relation $\leq$).

Une relation binaire $<$ antisymétrique, transitive et telle que $\forall x\, x \in E \Rightarrow \neg(x < x)$ (antireflexivité) est dite *relation d'ordre strict*. (cette dernière propriété et l'antisymétrie impliquent qu'il n'existe pas d'éléments x et y de E tels que $(x < y) \wedge (y < x)$.) Si $\leq$ est une relation d'ordre sur un ensemble E, alors la relation $<$ définie par : pour tout éléments a et b de E, $a < b \Leftrightarrow (a \leq b) \wedge (a \neq b)$ est une relation d'ordre strict. En effet,

- Soit x un élément de E, $x \neq x$ est fausse, donc $x < x$ est fausse.
- Soit x et y deux éléments de E tels que $x < y$ et $y < x$, alors $x \leq y$ et $y \leq x$, donc $x = y$. La relation $<$ est bien antisymétrique.
- Soit x, y et z trois éléments de E tels que $x < y$ et $y < z$. Alors $x \leq y$ et $y \leq z$, donc $x \leq z$. Par ailleurs, si on avait $x = z$, alors $y \leq x$, et donc $y = x$, ce qui est impossible puisque $x < y$. Donc, $x \neq z$. On en déduit que $x < z$. Ainsi, la relation $<$ est bien transitive.

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre sur E. La relation $<$ sur E définie par : $\forall x\, \forall y\, x \in E \wedge y \in E \Rightarrow (x < y \Leftrightarrow (y \leq x \wedge x \neq y))$ est une relation d'ordre strict sur E.

Démonstration :

- *Antiréflexivité :* Soit x un élément de E. Puisque $x = x$, la formule $x \neq x$ est fausse, donc $x < x$ est fausse.
- *Antisymétrie :* Soit x et y deux éléments de E tels que $x < y$ et $y < x$. Alors, $x \leq y$ et $y \leq x$. Puisque $\leq$ est une relation d'ordre, cela implique $x = y$.
- *Transitivité :* Soit x, y et z trois éléments de E tels que $x < y$ et $y < z$. On a $x \leq y$ et $y \leq z$. Puisque $\leq$ est une relation d'ordre, cela implique $x \leq z$. Par ailleurs, z ne peut pas être égal à x car on aurait alors $x \leq y$ et $y \leq x$, d'où $y = x$, ce qui est incompatible avec $x < y$. Donc, $x \leq z$ est fausse, et donc $x < z$ est vraie.

□

Lemme : Soit E un ensemble et $<$ une relation d'ordre strict sur E. La relation $\leq$ sur E définie par : $\forall x\, \forall y\, x \in E \wedge y \in E \Rightarrow (x \leq y \Leftrightarrow (y \leq x \vee x = y))$ est une relation d'ordre sur E.

Démonstration :

- *Réflexivité :* Soit x un élément de E. Puisque $x = x$ est vrai par réflexivité de l'égalité, $x \leq x$ est vrai.
- *Antisymétrie :* Soit x et y deux éléments de E tels que $x \leq y$ et $y \leq x$. Alors, $x < y$ ou $x = y$. De même, $y < x$ ou $x = y$. Puisque $x < y$ et $y < x$ ne peuvent être simultanément vrais, on en déduit que $x = y$.
- *Transitivité :* Soit x, y et z trois éléments de E tels que $x \leq y$ et $y \leq z$. On a $x < y$ ou $x = y$. Dans le second cas, le second prédicat de l'hypothèse donne $x \leq z$. Supposons maintenant $x < y$. On a de même $y < z$ ou $y = z$. Dans le second cas, le premier prédicat de l'hypothèse donne $x \leq z$. Supposons maintenant $y < z$. Puisque $x < y$, $y < z$, et car $<$ est une relation d'ordre strict, donc transitive, on en déduit $x < z$, et donc $x \leq z$. Le prédicat $x \leq z$ est donc vrai dans tous les cas.

□

Lemme : Soit E un ensemble, $\leq$ une relation d'ordre sur E, et $<$ la relation d'ordre strict sur E définie par : $\forall x \forall y\, (x \in E \wedge y \in E) \Rightarrow (x < y \Leftrightarrow (x \leq y \wedge x \neq y))$. Alors, soit x, y et z trois éléments de E,

- Si $x < y$ et $y \leq z$, alors $x < z$.
- Si $x \leq y$ et $y < z$, alors $x < z$.

Démonstration : Notons d'abord que, dans les deux cas, on a $x \leq y$ et $y \leq z$, donc $x \leq z$ par transitivité de la relation $\leq$. In suffit donc de montrer que $x \neq z$. Supposons par l'absurde que $x = z$. Alors,

- Dans le premier cas, on a $x < y$, donc $x \leq y$, et $y \leq x$. On a donc $y = x$. Mais cela est incompatible avec $x < y$.
- Dans le second cas, on a $x \leq y$ et $y < x$, donc $y \leq x$. On a donc $y = x$. Mais cela est incompatible avec $y < x$.

Dans les deux cas, la formule $x = z$ est donc nécessairement fausse, donc $x \neq z$ est vraie.

□

Lemme : Soit E un ensemble, $\leq$ une relation d'ordre sur E, et $<$ la relation d'ordre strict sur E définie par : $\forall x \forall y\, (x \in E \wedge y \in E) \Rightarrow (x < y \Leftrightarrow (x \leq y \wedge x \neq y))$. Soit x et y deux éléments de E. Si $y < x$ est vrai, alors $x \leq y$ est faux.

Démonstration : Supposons que $y < x$ est vrai. Alors, $y \leq x$ et $x \neq y$ sont vrais. Si $x \leq y$ était vrai, on aurait $x \leq y \wedge y \leq x$, donc $x = y$, ce qui est faux. On en déduit que $x \leq y$ est faux.

□

Lemme : Soit E un ensemble, $\leq$ une relation d'ordre sur E, et $<$ la relation d'ordre strict sur E définie par : $\forall x \forall y\, (x \in E \wedge y \in E) \Rightarrow (x < y \Leftrightarrow (x \leq y \wedge x \neq y))$. Alors, soit x et y deux éléments de E, les formules $x \leq y$ et $(x < y) \vee (x = y)$ sont équivalentes.

Démonstration : Puisque la formule $(x = y) \vee (x \neq y)$ est toujours vraie, on a : $(x \leq y) \Leftrightarrow ((x \leq y) \wedge ((x = y) \vee (x \neq y)))$. Utilisant la distributivité de $\wedge$ sur $\vee$, cela donne : $(x \leq y) \Leftrightarrow (((x \leq y) \wedge (x = y)) \vee ((x \leq y) \wedge (x \neq y)))$. Puisque la relation $\leq$ est réflexive, $(x = y) \Rightarrow (x \leq y)$, donc $(x \leq y) \wedge (x = y)$ est équivalente à $x = y$. En outre, par définition de la relation $<$, $(x \leq y) \wedge (x \neq y)$ est équivalente à $x < y$. Donc, $(x \leq y) \Leftrightarrow ((x = y) \vee (x < y))$.

□

Lemme : Soit E un ensemble et $<$ une relation d'ordre strict sur E. La relation $>$ sur E définie par : $\forall x \, \forall y \, x \in E \wedge y \in E \Rightarrow (x > y \Leftrightarrow y < x)$ est une relation d'ordre strict sur E.

Démonstration :

- Soit x un élément de E. Le prédicat $x < x$ est faux puisque $<$ est une relation d'ordre strict, donc $x > x$ l'est aussi.
- *Antisymétrie :* Soit x et y deux éléments de E tels que $x > y$ et $y > x$. Alors, $y < x$ et $x < y$. Par antisymétrie de la relation $<$, on en déduit que $x = y$.
- *Transitivité :* Soit x, y et z trois éléments de E tels que $x > y$ et $y > z$. Alors, $y < x$ et $z < y$. Par transitivité de la relation $<$, on en déduit que $z < x$, et donc $x > z$.

□

Soit E un ensemble, $\leq$ une relation d'ordre sur E et $<$ la relation d'ordre strict définie par : pour tout éléments a et b de E, $a < b \Leftrightarrow (a \leq b) \wedge (a \neq b)$. Alors, soit a, b et c trois éléments de E tels que $a \leq b$ et $b < c$, on a $a < c$. En effet, on a $a \leq c$ par transitivité de la relation $\leq$ et $a \neq c$ (sans quoi on aurait $b < a$, et donc $b \leq a$, donc $b = a$, ce qui est contradictoire avec $b < a$).

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre total définie sur E. Alors la relation $>$ définie sur E par : pour tous éléments x et y de E, $a > b \Leftrightarrow \neg(a \leq b)$ est une relation d'ordre strict.

Démonstration :

- *Antiréflexivité :* Soit x un élément de E. La formule $x \leq x$ est vraie, donc $x > x$ est fausse.
- *Antisymétrie :* Soit x et y deux éléments de E tels que $x > y$ et $y > x$. Alors, $\neg(x \leq y)$ et $\neg(y \leq x)$. Puisque $\leq$ est une relation d'ordre total, cela implique $y \leq x$ et $x \leq y$, et donc $x = y$.
- *Transitivité :* Soit x, y et z trois éléments de E tels que $x > y$ et $y > z$. On a $\neg(x \leq y)$ et $\neg(y \leq z)$. Puisque $\leq$ est une relation d'ordre total, cela implique $y \leq x$ et $z \leq y$, et donc $z \leq x$. Par ailleurs, z ne peut pas être égal à x car on aurait alors $y \leq x$ et $x \leq y$, d'où $y = x$, ce qui est incompatible avec $x > y$. Donc, $x \leq z$ est fausse, et donc $x > z$.

□

Lemme : Soit E un ensemble et $<$ une relation d'ordre strict définie sur E, telle que : $\forall x \in E \, \forall y \in E (x < y) \vee (y < x) \vee (x = y)$. Alors la relation $\geq$ définie sur E par : pour tous éléments x et y de E, $a \geq b \Leftrightarrow \neg(a < b)$ est une relation d'ordre total.

Démonstration :

- *Réflexivité :* Soit x un élément de E. La formule $x < x$ est fausse, donc $x \geq x$ est vraie.
- *Antisymétrie :* Soit x et y deux éléments de E tels que $x \geq y$ et $y \geq x$. Alors, $\neg(x < y)$ et $\neg(y < x)$. Donc, $x = y$.
- *Transitivité :* Soit x, y et z trois éléments de E tels que $x \geq y$ et $y \geq z$. On a $\neg(x < y)$ et $\neg(y < z)$. Donc, $(y < x) \vee (x = y)$ et $(z < y) \vee (y = z)$. Si $x = y$, alors $y \leq z$ implique $x \leq z$. Si $y = z$, alors $x \leq y$ implique $x \leq y$. Si $x \neq y$ et $y \neq z$, on a $y < x$ et $z < y$. Par transitivité de la relation $<$, on a donc $z < x$. Par antisymétrie, on a donc $\neq (x < z)$, et donc $x \geq z$. La formule $x \geq z$ est ainsi vraie dans tous les cas.
- Soit x et y deux éléments de E. On a $(x < y) \vee (y < x) \vee (x = y)$. Si $x < y$ est vraie, alors $y < x$ est fausse, donc $y \geq x$ est vraie. Si $y < x$ est vraie, alors $x < y$ est fausse, donc $x \geq y$ est vraie. Enfin, si $x = y$ est vraie, alors $x \leq y$ est vraie. Dans tous les cas, on a bien $(x \leq y) \vee (y \leq x)$.

Vocabulaire : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Soit $\geq$, $<$ et $>$ les relations définies par : pour tous éléments a et b de E,

- $a \geq b \Leftrightarrow b \geq a$,
- $a < b \Leftrightarrow (a \leq b \wedge a \neq b)$,
- $a > b \Leftrightarrow b < a$.

Alors, soit a et b deux éléments de E, et s'il n'y a pas d'ambigüité,

- si $a \leq b$, on dira que *a est inférieur ou égal à b*,
- si $a \geq b$, on dira que *a est supérieur ou égal à b*,
- si $a < b$, on dira que *a est strictement inférieur à b*,
- si $a > b$, on dira que *a est strictement supérieur à b*.

Notation : Soit E un ensemble, $\geq$ une relation d'ordre sur E, et $<$ la relation d'ordre strict sur E définie par : pour tous éléments a et b de E, $a < b \Leftrightarrow (a \leq b \wedge a \neq b)$. Si a_0, a_1, a_2, ..., a_n sont des éléments de E (avec a_n possiblement absent) et R_1, R_2, ..., R_n (où R_n est absent si a_n l'est) des symboles chacun identique à $\leq$ ou $<$, alors la formule

$$a_0 \; R_1 \; a_1 \; R_2 \; a_2 \ldots$$

signifie :

$$(a_0 \; R_1 \; a_1) \wedge (a_1 \; R_2 \; a_2) \ldots .$$

Définition : Soit E un ensemble et $\leq$ une relation d'ordre sur E. La relation $\leq$ est dit un *bon ordre* sur E si tout sous-ensemble non vide de E admet un plus petit élément. L'ensemble E est alors dit *bien ordonné*.

Lemme : Soit E un ensemble et $\leq$ un bon ordre sur E. Alors $\leq$ est une relation d'ordre total sur E.

Démonstration : Soit x et y deux éléments de E. Alors, $\{x, y\}$ est un sous-ensemble non vide de E (il contient au moins x). Donc, il contient un plus petit élément. Si ce plus petit élément est x, alors $x \leq y$. Sinon, ce plus petit élément est y, donc $y \leq x$. Dans tous les cas, on a $x \leq y \vee y \leq x$.

□

1.2.9 Induction transfinie

Lemme (induction transfinie) : Soit E un ensemble non vide, $\leq$ une relation de bon ordre sur E et P un prédicat à un paramètre libre. On note $<$ la relation d'rodre strict sur E définie par :

$$\forall x \in E \, \forall y \in E \; x < y \Leftrightarrow ((x \leq y) \wedge (x \neq y)).$$

Soit m le plus petit élément de E pour $\leq$ (qui existe puisque $\leq$ est une relation de bon ordre sur E). On suppose que les prédicats suivants sont vrais :

- $P(m)$,
- $\forall x \in E \, (\forall y \in E \; y < x \Rightarrow P(y)) \Rightarrow P(x)$.

Alors, $P(x)$ est vrai pour tout élément x de E.

Démonstration : Supposons par l'absurde que ce n'est pas le cas. Soit S l'ensemble défini par :

$$S = \{x \in E \mid \neg \, P(x)\}.$$

Alors, S est un sous-ensemble de E (par construction) et non vide (par hypothèse). Il admet donc un plus petit élément, noté n. Puisque n est un élément de S, $P(n)$ est faux.

Mais, pour tout élément y de E, si $x < n$, alors $x \notin S$ (puisaue n est un élément minimal de S), donc $P(x)$ est vrai. Donc, $\forall y \in E \; y < n \Rightarrow P(y)$ est vrai. Donc, $P(n)$ est vrai. On obtient donc une contradiction ($\neg \, P(n) \wedge P(n)$), montrant que l'hypothèse de départ est fausse.

□

1.2.10 Partition

Soit E et P deux ensembles. On dit que P *est une partition de* E si les quatre propriétés suivantes sont satisfaites :

- $\forall p \, (p \in P) \Rightarrow (p \subset E)$,
- $\emptyset \notin P$,
- $\forall e \, (e \in E) \Rightarrow (\exists p \; p \in P \wedge e \in p)$
- $\forall p \, \forall q \, (p \in P) \wedge (q \in P) \wedge ((p \cap q) \neq \emptyset) \Rightarrow (p = q)$.

1.2.11 Relation d'équivalence

Soit E un ensemble. Une relation binaire $\sim$ définie sur $E \times E$ est dite *relation d'équivalence* sur E si elle satisfait les trois propriétés suivantes :

- *Réflexivité :* $\forall x \; x \in E \Rightarrow x \sim x$
- *Symétrie :* $\forall x \, \forall y \, (x \in E) \wedge (y \in E) \wedge (x \sim y) \Rightarrow (y \sim x)$.
- *Transitivité :* $\forall x \, \forall y \, \forall z \, (x \in E) \wedge (y \in E) \wedge (z \in E) \wedge (x \sim y) \wedge (y \sim z) \Rightarrow (x \sim z)$.

Soit E un ensemble et $\sim$ une relation d'équivalence sur E. Pour tout $x \in E$, on définit la *classe d'équivalence* de x pour $\sim$, notée ici $[x]$, par : $[x] = \{y \in E | y \sim x\}$. Les éléments d'une classe d'équivalence sont parfois appelés ses *représentants*, ou *représentations*. Notons que, pour tout élément x de E, $[x] \subset E$. Donc, l'ensemble des classes d'équivalences existe d'après le schéma d'axiomes de compréhensions. (Pour voir cela, prendre pour ensemble l'ensemble des parties de E et pour propriété $Py : \exists x\,(x \in E) \wedge (y = [x])$.)

Lemme : Soit x et y deux éléments de E. Si $x \sim y$, alors $[x] = [y]$.

Démonstration : Supposons $x \sim y$. Soit $z \in [x]$. On a $z \sim x$. Par symétrie et transitivité de la relation $\sim$, on en déduit $z \sim y$. Donc, $z \in [y]$. On en déduit $[x] \subset [y]$. Par symétrie, on a aussi $y \sim x$, et donc, en utilisant le même argument et échangeant les rôles de x et y, on montre que $[y] \subset [x]$. Ainsi, $[y] = [x]$.

□

Lemme : L'ensemble des classes d'équivalence de E pour la relation $\sim$ forme une partition de E.

Démonstration : Notons F cet ensemble. Vérifions qu'il satisfait les quatre propriétés d'une partition de E.

- Soit $f \in F$. On peut choisir un élément y de E tel que $f = [y]$. Puisque $[y] \subset E$, on en déduit $f \subset E$.
- Pour tout élément f de F, il existe x tel que $x \in E$ et $f = [x]$, et donc $x \in f$, ce qui montre que $f \neq \emptyset$. Donc, $\emptyset \notin F$.
- Soit $x \in E$. On a $x \in [x]$ et $[x] \in F$.
- Soit $f \in F$ et $g \in F$ tels que $f \cap g \neq \emptyset$. On peut choisir un élément x de $f \cap g$. Soit $y \in E$ et $z \in E$ tels que $f = [y]$ et $g = [z]$. On a $x \sim y$ et $x \sim z$. Par symétrie et transitivité de la relation $\sim$, on en déduit $y \sim z$. Donc, $[y] = [z]$, et donc $f = g$.

□ blank[medium]

Définition : Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence de $\mathscr{R}$ est noté $E/\mathscr{R}$ et appelé *ensemble quotient* de E par $\mathscr{R}$.

1.2.12 Fonctions

Soit a un ensemble. La séquence de symboles « $\forall x\,(x \in a) \Rightarrow$ » incluse dans une formule est parfois simplifiée en « $\forall x \in a$ » ou en « $\forall x \in a,$ ». La séquence de symboles « $\exists x\,(x \in a) \wedge$ » incluse dans une autre formule est parfois simplifiée en « $\exists x \in a$ » ou en « $\exists x \in a,$ ». Ainsi, si f est une formule, la formule $\forall x \in a,\, f$ (éventuellement sans la virgule) est considérée comme identique à $\forall x\,(x \in a) \Rightarrow f$ (au sens où ces suites de symboles représentent la même formule) et $\exists x \in a,\, f$ (éventuellement sans la virgule) est considérée comme identique à $\exists x\,(x \in a) \wedge f$.

Définition : Soit deux ensembles X et Y. Une *fonction*, ou *application*, f de X vers Y (ou de X dans Y, ou de X sur Y) est un ensemble (parfois appelé *graphe*) tel que :

$$\forall z\,[(z \in f) \Rightarrow (\exists x\,\exists y\,[(x \in X) \wedge (y \in Y) \wedge (z = (x,y))])],$$

$$\forall x\,[\,(x \in X) \Rightarrow [\exists y\,(x,y) \in f\,]]$$

et

$$\forall y\,\forall y'\,([\exists x\,((x,y) \in f \wedge (x,y') \in f)] \Rightarrow (y = y')).$$

La première condition est équivalente à dire que f est un sous-ensemble de $X \times Y$, *i.e.*, à : $f \subset X \times Y$. La seconde et la troisième sont équivalentes à dire que, pour tout élément x de X, il existe un unique élément y de Y tel que $(x,y) \in f$, c'est-à-dire : $\forall x\,[(x \in X) \Rightarrow [\exists!\, y\,(x,y) \in f\,]]$. Avec ces mêmes notations, pour tout x appartenant à X, on note $f(x)$ (ou, quand il n'y a pas d'ambigüité, $f\,x$) l'unique élément y de Y tel que $(x,y) \in f$. On dit alors que y est l'*image* de x ou que x est un *antécédent* de y par f. On dit aussi que f *associe* y à x.

On dit que f est *définie sur* X, ou que X est le *domaine de définition* de f. L'ensemble des éléments de y tels qu'il existe un élément x de X satisfaisant $f(x) = y$ est appelé *image* de f, notée $\mathrm{Im}(f)$ (c'est donc l'ensemble $\{y \in Y | \exists x\,(x \in X) \wedge f(x) = y\}$). La notation $f : X \to Y$, signifie que f est une fonction de X vers Y. Avec les mêmes notations, si X' est un sous-ensemble de X et s'il n'y a pas d'ambiguité[16], on appellera *image de X' par f* l'ensemble des éléments y de Y tels qu'il existe un élément x de X' tel que $f(x) = y$.

[16] Une telle ambiguité pourrait survenir dans des cas particuliers si $X' \in X$.

Pour tout sous-ensemble Y' de Y, on note $f^{-1}(Y')$ l'ensemble $\{x \in X | f(x) \in Y'\}$, appelé *image inverse* de G par f. S'il n'y a pas d'ambigüité, et si $y \in Y$, on notera parfois $f^{-1}(y)$ l'ensemble $f^{-1}(\{y\})$. (Les ensembles ainsi obtenus pour différentes valeurs de y sont deux à deux disjoints. En effet, soit y et z deux éléments de Y et x un élément de X. Si $x \in f^{-1}(y) \cap f^{-1}(z)$, on a $f(x) = y$ et $f(x) = z$, et donc $y = z$. Ainsi, si $y \neq z$, $f^{-1}(y) \cap f^{-1}(z)$ est vide.) Notons que, pour tout élément y de F, on a $f^{-1}(y) \neq \emptyset \Leftrightarrow y \in \mathrm{Im}(f)$.

Soit X et Y deux ensembles. L'ensemble des fonctions de X vers Y existe : il s'agit du sous-ensemble de l'ensemble des parties de $X \times Y$ (qui existe d'après l'axiome de l'ensemble des parties) satisfaisant la seconde et la troisième conditions ci-dessus (qui existe donc d'après le schéma d'axiomes de compréhension)[17]. Cet ensemble est noté $\mathcal{F}(X,Y)$, ou parfois (quand il n'y a pas d'ambigüité) Y^X. Notons que, si deux fonctions f et g de X vers Y satisfont $\forall x \in X,\ f(x) = g(x)$, alors $f = g$. Une fonction f de X vers Y peut ainsi être définie de manière unique par la donnée de $f(x)$ pour tout élément x de X.

Lemme : Soit E et F deux ensembles non vides et P un prédicat à deux paramètres libres tel que, pour tout élément e de E, il existe un unique élément f de F tel que Pef est vrai, *i.e.*,

$$\forall e \in E,\ (\exists f \in F,\ Pef) \wedge (\forall f \in F,\ \forall g \in F,\ Pef \wedge Peg \Rightarrow f = g).$$

Alors l'ensemble G définit par $G = \{g \in E \times F | \exists e \in E\, \exists f \in F\, g = (e,f) \wedge Pef\}$ est une fonction de E vers F.

Démonstration : Montrons que l'ensemble G satisfait les trois conditions pour être une fonction de E vers F.

- Soit g un élément de G. Par définition de cet ensemble, on peut choisir un élément e de E et un élément f de F tel que $g = (e,f)$. Donc, $g \in E \times F$. Cela montre que G est un sous-ensemble de $E \times F$.
- Soit e un élément de E. Par définition de P, on peut choisir un élément f de F tel que Pef est vrai. Alors, (e,f) est un élément de G.
- Soit e un élément de E et y et y' deux éléments de F tels que $(e,f) \in G$ et $(e,f') \in G$. Alors, Pef et Pef' sont vrais. Donc, $f = f'$.

□

Lemme : Soit E et F deux ensembles et f et g deux fonctions de E vers F. On suppose que : $\forall x \in E,\ f(x) = g(x)$ est vrai. Alors, $f = g$.

Démonstration : Soit z un élément de f. On peut choisir un élément x de E et un élément y de F tel que $z = (x,y)$. Puisque $x \in E$, on peut choisir un élément y' de F tel que $(x,y') \in g$. On a alors $y = f(x)$ et $y' = g(x)$. Puisque $f(x) = g(x)$, on en déduit $y' = y$. Donc, $(x,y) \in g$, et donc $z \in g$. Cela montre que $f \subset g$.

Soit z un élément de g. On peut choisir un élément x de E et un élément y de F tel que $z = (x,y)$. Puisque $x \in E$, on peut choisir un élément y' de F tel que $(x,y') \in f$. On a alors $y = g(x)$ et $y' = f(x)$. Puisque $g(x) = f(x)$, on en déduit $y' = y$. Donc, $(x,y) \in f$, et donc $z \in f$. Cela montre que $g \subset f$.

On a donc bien $f = g$.

□

Soit E et F deux ensembles et f une fonction de E vers F. On dit que

- f est *injective* (ou *une injection*) si $\forall x\ \forall y\, [f(x) = f(y) \Rightarrow x = y]$. Puisque chaque élément de f est dans $E \times F$, cela est équivalent à : $\forall x \in E\ \forall y \in F\, [f(x) = f(y) \Rightarrow x = y]$.
- f est *surjective* (ou *une surjection*) si $\forall y \in F\ \exists x\, [f(x) = y]$. Puisque chaque élément de f est dans $E \times F$, cela est équivalent à : $\forall y \in F\ \exists x \in E\, [f(x) = y]$.
- f est *bijective* (ou *une bijection*) si elle est à la fois injective et surjective, ce qui est équivalent à : $\forall y \in F\ \exists!\, x\, [f(x) = y]$ et à : $\forall y \in F\ \exists!\, x \in E\, [f(x) = y]$.

Lemme : Soit E un ensemble. Soit I l'ensemble $\{z \in E \times E\, \exists x \in E\, z = (x,x)\}$. Alors, I est une bijection de E vers E, appelée *fonction identité* sur E. En outre, pour tout élément x de E, $I(x) = x$.

Démonstration :

- Montrons d'abord que I est une fonction de E vers E.

[17] Pour être tout à fait rigoureux, le prédicat à employer pour utiliser l'axiome de compréhension est la conjonction de ces deux conditions, qui peut s'écrire : $(\forall x\, [(x \in X) \Rightarrow [\exists y\, (x,y) \in f]]) \wedge [\forall w\, \forall w'\, ([\exists z\, ((z,w) \in f \wedge (z,w') \in f)] \Rightarrow (w = w'))]$.

  - Soit z un élément de I. Alors il existe un élément x de E tel que $z = (x,x)$. Donc, il existe un élément y de E (il suffit de prendre $y = x$) tel que $z = (x,y)$. La première condition est donc satisfaite.
  - Soit x un élément de E. On a $(x,x) \in I$. Donc, il existe un élément y de E (il suffit de prendre $y = x$) tel que $(x,y) \in E$. La deuxième condition est donc satisfaite.
  - Soit y et y' deux éléments de E et x un élément de E tel que $(x,y) \in I$ et $(x,y') \in I$. Alors, il existe deux éléments x' et x'' de E tels que $(x,y) = (x',x')$ et $(x,y') = (x'',x'')$. La première égalité donne $x = x'$ et $y = x'$, donc $x = y$. La seconde égalité donne $x = x''$ et $y' = x''$, donc $x = y'$. Donc, $y = y'$. La troisième condition est donc satisfaite.
- Soit x un élément de E. On a $(x,x) \in I$, donc $I(x) = x$.
- Montrons qu'elle est injective. Soit x et y deux éléments de E tels que $I(x) = I(y)$. Alors, puisque $I(x) = x$ et $I(y) = y$, et par réflexivité et transitivité de l'égalité, $x = y$.
- Montrons qu'elle est surjective. Soit y un élément de E. Alors, $I(y) = y$, donc il existe un élément x de E (il suffit de prendre $x = y$) tel que $I(x) = y$.

□

Lemme : Soit E et F deux ensembles, f une fonction de E vers F, I_E la fonction identité sur E et I_F la fonction identité sur F. Alors, $f \circ I_E = I_F \circ f = f$.

Démonstration : Tout d'abord, puisque I_E est une fonction de E vers E, I_F une fonction de F vers F, et f une fonction de E vers F, $f \circ I_E$ et $I_F \circ f$ sont deux fonctions de E vers F. Soit x un élément de E. On a : $(f \circ I_E)(x) = f(I_E(x)) = f(x)$ et $(I_F \circ f)(x) = I_F(f(x)) = f(x)$. Cela étant vrai pour tout élément x de E, on en déduit $f \circ I_E = f$ et $I_F \circ f = f$.

□

Soit E un ensemble.

- S'il existe une fonction de E vers $\emptyset$, alors $E = \emptyset$ (en effet, soit f une telle fonction, si E contenait un élément x, $f(x)$ serait un élément de $\emptyset$, ce qui est impossible).
- La seule fonction de $\emptyset$ vers E est $\emptyset$. Elle est toujours injective. Elle est surjective (et donc bijective) si et seulement si $E = \emptyset$.

Soit E et F deux ensembles. Alors,

- Si E est non vide et s'il existe une injection f de E vers F, alors il existe une surjection de F vers E. En effet, une telle surjection peut être construite de la manière suivante. Soit a un élément de E. Soit P la propriété à deux variables libres définie par : $Pyx : [(y \in \mathrm{Im}(f)) \wedge (f(x) = y)] \vee [(y \notin \mathrm{Im}(f)) \wedge (x = a)]$. Alors, l'ensemble $\{z \in F \times E | \exists x \, \exists y \, (z = (y,x)) \wedge (Pyx)\}$ est une fonction de F vers E et est surjective.
- S'il existe une surjection f de E vers F, et si l'on admet l'axiome du choix (voir ci-dessous), alors il existe une injection de F vers E. En effet, soit X l'ensemble des $f^{-1}(y)$ pour $y \in F$ (cet ensemble existe d'après l'axiome de l'ensemble des parties et le schéma d'axiome de compréhension : il s'agit de l'ensemble des parties p de F telles que $\exists y (y \in F) \wedge (p = f^{-1}(y))$), soit g une fonction qui à chaque élément de cet ensemble associe un de ses éléments[18], et soit h l'ensemble $\{z \in F \times E | \exists x \in E \, \exists y \in F \, (x = g(f^{-1}(y))) \wedge (z = (y,x))\}$; alors h est une fonction injective de F vers E. (Elle est bien injective. En effet, si y et y' sont deux élément de f ayant la même image x, alors $x \in f^{-1}(y)$ et $x \in f^{-1}(y')$, donc $f(x) = y$ et $f(x) = y'$, donc $y = y'$.)

Ces deux résultats étant importants, récrivons-les et démontrons-les plus formellement.

Lemme : Soit E et F deux ensembles. On suppose que E est non vide et qu'il existe une injection de E vers F. Alors, il existe une surjection de F vers E.

Démonstration : Soit f une injection de E vers F. Soit a un élément de E (un tel élément existe puisque E est non vide). Définissons la propriété P à deux paramètres libres par :

$$Pxy : \left[(y \in \mathrm{Im}(f)) \wedge (f(x) = y)\right] \vee \left[(y \notin \mathrm{Im}(f)) \wedge (x = a)\right].$$

Soit g l'ensemble défini par :

$$g = \{z \in F \times E | \exists x \exists y \, (z = (y,x)) \wedge (Pxy)\}.$$

Montrons que g est une fonction de F vers E et qu'elle est surjective:

[18] Cela est possible car, pour tout élément y de F, $f^{-1}(y)$ est non vide puisque f est surjective.

- Soit z un élément de g. Alors, on peut choisir un élément x de F et un élément y de E tels que $z = (x,y)$. La première condition pour être une fonction est donc satisfaite.
- Soit y un élément de F. Si $y \in \mathrm{Im}(f)$, alors on peut choisir un élément x de E tel que $f(x) = y$. On a donc $(y,x) \in F \times E$ et Pxy. Donc, $(y,x) \in g$. On a donc montré que $\exists x (y,x) \in g$. La deuxième condition pour être uns fonction est donc bien satisfaite.
- Soit x et x' deux éléments de E et y un élément de F tels que $(y,x) \in g$ et $(y,x') \in g$. Alors, Pxy et $Px'y$ sont vraies. Si $y \in \mathrm{Im}(f)$, cela implique $f(x) = y$ et $f(x') = y$, donc $f(x) = f(x')$, et donc (puisque f est injective) $x = x'$. Sinon, cela implique $x = a$ et $x' = a$, donc $x = x'$. Dans tous les cas, on a $x = x'$. La troisième condition pour être une fonction est donc satisfaite.
- Soit x un élément de E. On a $f(x) \in \mathrm{Im}(f)$ et $f(x) = f(x)$, donc $Pxf(x)$ est vraie. Puisque $x \in E$ et $f(x) \in F$, $(f(x),x) \in F \times E$. Donc, $(f(x),x) \in g$. Il existe donc un élément y de F (égal à $f(x)$) tel que $g(y) = x$. Cela montre que g est surjective.

□

Lemme : Soit E et F deux ensembles. On suppose qu'il existe une surjection de E vers F. On admet également l'axiome du choix (voir ci-dessous). Alors, il existe une injection de F vers E.

Démonstration : Soit f une surjection de E vers F. Soit $\mathscr{E}$ l'ensemble des parties de E. Soit X l'ensemble définit par :

$$X = \{p \in \mathscr{E} | \exists y (y \in F) \wedge (p = f^{-1}(\{y\}))\}.$$

Soit p un élément de X. On peut choisir un élément y de F tel que $p = f^{-1}(\{y\})$. Puisque f est surjective, on peut choisir un élément x de E tel que $f(x) = y$. Donc, $f(x) \in \{y\}$. Donc, $x \in f^{-1}(\{y\})$. Donc, $x \in p$. Cela montre que X ne contient pas $\emptyset$.

D'après l'axiome du choix, il existe donc une fonction de X vers $\cup X$ qui à chaque élément x de X associe un élément de x. Soit g une telle fonction. Puisque chaque élément de X est un sous-ensemble de E, $\cup X$ en est également un. En effet, soit e un élément de $\cup X$, il existe un élément x de X tel que $e \in x$; puisque $x \subset E$, on a donc $e \in E$. Donc, g est une fonction de X vers E. Notons h l'ensemble défini par :

$$h = \{z \in F \times E | \exists x \in E \, \exists y \in F \, (x = g(f^{-1}(\{y\}))) \wedge (z = (y,x))\}.$$

Montrons que h est une fonction de F vers E.

- Par définition, h est un sous-ensemble de $F \times E$, et satisfait donc la première condition.
- Soit y un élément de F. Alors, $f^{-1}(\{y\})$ est un élément de X. Soit x l'élément de E défini par $x = g(f^{-1}(\{y\}))$. On a $(y,x) \in h$.
- Soit y un élément de F et x et x' deux éléments de E tels que $(y,x) \in h$ et $(y,x') \in h$. Alors, $x = g(f^{-1}(\{y\}))$ et $x' = g(f^{-1}(\{y\}))$. Donc, $x = x'$.

L'ensemble h est donc bien une fonction de F vers E.

Montrons que h est injective. Soit y et y' deux éléments de F tels que $h(y) = h(y')$. Puisque $h(y) = g(f^{-1}(\{y\}))$ et $g(f^{-1}(\{y\})) \in f^{-1}(\{y\})$, on a $h(y) \in f^{-1}(\{y\})$, et donc $f(h(y)) = y$. De même, puisque $h(y') = g(f^{-1}(\{y'\}))$ et $g(f^{-1}(\{y'\})) \in f^{-1}(\{y'\})$, on a $h(y') \in f^{-1}(\{y'\})$, et donc $f(h(y')) = y'$. Puisque $h(y) = h(y')$, on en déduit que $y = y'$. Ainsi, h est bien injective.

□

Soit E et F deux ensembles, f une fonction de E vers F et E' un sous-ensemble de E. Pour simplifier les notations, on note parfois $\{f(x) | x \in E'\}$ ou $F(E')$ l'ensemble $\{y \in F | \exists x (x \in E') \wedge (f(x) = y)\}$.

Composition de deux fonctions : Soit E, F et G trois ensembles. Soit f une fonction de E vers F et g une fonction de F vers G. La *composée* de g et f, notée $g \circ f$, est la fonction de E vers G définie par : $\forall x \in E \, (g \circ f)(x) = g(f(x))$. Plus formellement, $g \circ f = \{z \in E \times G | \exists x \in E \, z = (x,g(f(x)))\}$.

Lemme : L'ensemble ainsi défini est bien une fonction de E vers G.

Démonstration :

- Soit z un élément de $g \circ f$. Alors, on peut choisir un élément x de E tel que $z = (x,g(f(x)))$. Puisque f est une fonction de E vers F, $f(x) \in F$. Puisque g est une fonction de F vers G, $g(f(x)) \in F$. Donc, $z \in E \times G$.
- Soit x un élément de E. Alors $(x,g(f(x))) \in g \circ f$.
- Soit y et y' deux ensembles. Soit x un ensemble tel que $(x,y) \in g \circ f$ et $(x,y') \in g \circ f$. Alors, on peut choisir un élément x' de E tel que $(x,y) \in (x',g(f(x')))$ et un élément x'' de E tel que $(x,y') = (x'',g(f(x'')))$. On a donc $x = x'$, $y = g(f(x'))$, $x = x''$ et $y' = g(f(x''))$. Donc, $y = g(f(x))$ et $y' = g(f(x))$. Donc, $y = y'$.

□

Remarque : Avec les mêmes notations, si f et g sont deux injections, alors $g \circ f$ en est aussi une. En effet, soit x et y deux éléments de G tels que $(g \circ f)(x) = (g \circ f)(y)$, on a $g(f(x)) = g(f(y))$, donc $f(x) = f(y)$, et donc $x = y$.

Remarque : Avec les mêmes notations, si f et g sont deux surjections, alors $g \circ f$ en est aussi une. En effet, soit z un élément de G, il existe un élément y de F tel que $g(y) = z$ et un élément x de E tel que $f(x) = y$; on a donc $(g \circ f)(x) = z$.

Remarque : Avec les mêmes notations, si f et g sont deux bijections, alors $g \circ f$ en est aussi une. En effet, il s'agit d'une injection et d'une surjection d'après les deux points précédents.

Lemme (associativité de la composition de fonctions) : Soit E, F, G et H quatre ensembles. Soit f, g et h des fonctions respectivement de E vers F, de F vers G et de G vers H. Alors $h \circ (g \circ f) = (h \circ g) \circ f$.

Démonstration : Montrons d'abord que $h \circ (g \circ f)$ et $(h \circ g) \circ f$ sont deux fonctions de E vers H. Puisque f est une fonction de E vers F et g une fonction de F vers G, $g \circ f$ et une fonction de E vers G. Donc, $h \circ (g \circ f)$ est une fonction de E vers H. Puisque g est une fonction de F vers G et h une fonction de G vers H, $h \circ g$ et une fonction de F vers H. Donc, $(h \circ g) \circ f$ est une fonction de E vers H.

Montrons maintenant qu'elles sont égales. Soit x un élément de E. On a : $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$. Par ailleurs, $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$. Donc, $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$. On en déduit que $h \circ (g \circ f) = (h \circ g) \circ f$.

□

Inverse d'une bijection : Soit E et F deux ensembles et f une bijection de E vers F. L'ensemble $\{z \in F \times E | \exists x \in E \, \exists y \in F \, z = (y,x) \wedge (x,y) \in f\}$ est une fonction de F vers E (puisque, pour chaque élément y de F, il existe un unique élément x de E tel que $(x,y) \in f$). On montre facilement qu'il s'agit d'une bijection (pour chaque élément x de E, il existe un unique élément y de F dont l'image est x : il s'agit de $f(x)$ (son image est bien x par définition et, soit z un élément de F tel que $z \neq y$, l'image de z est l'antécédent de z par f, distinct de x)), appelée *inverse* de f et notée f^{-1}.

Ce résultat étant important, récrivons-le et démontrons-le plus formellement.

Lemme : Soit E et F deux ensembles. On suppose qu'il existe une bijection, notée f, de E vers F. Alors il existe une unique fonction g de F vers E telle que, pour tout élément x de E, $g(f(x)) = x$. En outre, cette fonction est bijective.

Démonstration : Soit g l'ensemble défini par :

$$g = \{z \in F \times E | \exists x \in E \, \exists y \in F \, z = (y,x) \wedge (x,y) \in f\}.$$

Montrons d'abord que g est une fonction de F vers E.

- Soit z un élément de g. Alors, il existe un élément y de F et un élément x de E tels que $z = (y,x)$.
- Soit y un élément de F. Puisque f est surjective, on peut choisir un élément x de E tel que $f(x) = y$. Alors, $(y,x) \in F \times E$ et $(x,y) \in f$, donc $(y,x) \in g$.
- Soit y un élément de F et x et x' deux éléments de E tels que $(y,x) \in g$ et $(y,x') \in g$. Alors, $(x,y) \in f$ et $(x',y) \in f$, donc $f(x) = y$ et $f(x') = y$, donc $f(x) = f(x')$. Puisque f est injective, on en déduit que $x = x'$.

Ainsi, g est bien une fonction de F vers E.

Montrons qu'elle est unique. Soit h une fonction de F vers E telle que, pour tout élément x de E, $h(f(x)) = x$. Soit y un élément de F. Puisque f est surjective, on peut choisir un élément x de E tel que $y = f(x)$. On a alors $g(y) = x$ et $h(y) = x$. Donc, $h(y) = g(y)$. Cela étant vrai pour tout élément y de F, on en déduit que $h = g$.

Montrons maintenant que g est bijective.

- Soit y et y' deux éléments de F tels que $g(y) = g(y')$. Puisque $(y,g(y)) \in g$, on a $(g(y),y) \in f$, donc $f(g(y)) = y$. De même, puisque $(y',g(y')) \in g$, on a $(g(y'),y') \in f$, donc $f(g(y')) = y'$. Puisque $g(y') = g(y)$, cela implique $f(g(y)) = y'$, et donc $y = y'$. Cela montre que g est injective.
- Soit x un élément de E. Notons y l'élément de F définit par $y = f(x)$. Alors, $(y,x) \in F \times E$ et $(x,y) \in F$. Donc, $(y,x) \in g$. Donc, $g(y) = x$. Cela montre que g est surjective.

Puisque g est injective et surjective, il s'agit bien d'une bijection.

□

Définition : Soit E et F deux ensembles, E' un sous-ensemble de E, et f une fonction de E vers F. On appelle *restriction de f à E'* la fonction g de E' vers F définie par : pour tout élément e de E', $g(e) = f(e)$.

Notation: Soit E, F et G trois ensembles. Soit f une fonction de E vers F et G une fonction de E vers G. On pourra noter $\{(f(e), g(e))|e \in E\}$ l'ensemble $\{x \in F \times G|\exists e \in E\, x = (f(e), g(e))\}$. Si $f(e)$ est donnée par une formule explicite, alors $f(e)$ peut être remplacée par cette formule, et de même pour $g(e)$.

1.2.13 Axiome du choix

Énoncé : *Pour tout ensemble X d'ensembles non vides, il existe une fonction sur X qui à chaque ensemble x appartenant à X associe un élément de x :*

$$\forall X \left[(\varnothing \notin X) \Rightarrow \left(\exists f : X \to \cup X\, \forall x\, [(x \in X) \Rightarrow (\exists y\, [((x,y) \in f) \wedge (y \in x)])]\right)\right].$$

Cette formule peut se récrire plus simplement (au prix d'avoir une partie mal définie pour $x \notin X$) :

$$\forall X \left[(\varnothing \notin X) \Rightarrow \left(\exists f : X \to \cup X\, \forall x \in X\, (f(x) \in x)\right)\right].$$

La théorie ZF plus l'axiome du choix est appelée théorie ZFC.

1.2.14 Théorie de Tarski-Grothendieck

Définition : Un ensemble U est dit *univers de Grothendieck* si les quatre proptiétés suivantes sont vraies :

- L'ensemble U est *transitif* : pour tout élément x de U et tout élément y de x, $y \in U$.
- Pour tous éléments x et y de U, $\{x, y\} \in U$.
- Pour tout élément x de U, l'ensemble des sous-ensembles de x, $\mathcal{P}(x)$, est un élément de U.
- Pour tout sous-ensemble S de U, l'union des éléments de S, $\cup S$, est un élément de U.

Formellement, cela peut s'écrire :

- $\forall x\, \forall y\, (x \in U \wedge y \in x) \Rightarrow y \in U$.
- $\forall x\, \forall y\, (x \in U \wedge y \in U) \Rightarrow \{x, y\} \in U$.
- $\forall x\, x \in U \Rightarrow \mathcal{P}(x) \in U$.
- $\forall S\, S \subset U \Rightarrow \cup S \in U$.

Axiome de Tarski : Pour tout ensemble E, il existe un univers de Grothendieck U tel que $E \in U$.

La *théorie de Tarski-Grothendieck* ceomprend les axiomes de la théorie ZF plus l'axiome de Tarski. Sauf mention contraire explicite, on ne supposera pas l'axiome de Tarski ici.

1.2.15 Lemme de Zorn (en théorie ZFC)

Dans cette section seulement, on définit la notion de *chaine* de la manière suivante. Soit X un ensemble et $\leq$ une relation d'ordre sur X. Un sous-ensemble C de X est une *chaine* de X pour $\leq$ si $\leq$ est une relation d'ordre total sur C, autrement dit, si

$$\forall x \in C\, \forall y \in C\, x \leq y \vee y \leq x.$$

Pour toute chaine C de X pour $\leq$ et tout élément x de C, on note $P(C, x)$ l'ensemble définit par

$$P(C, x) = \{y \in C | y < x\},$$

où $<$ est la relation d'ordre stricte définie par : pour tous éléments x et y de C, $x < y$ est équivalent à $(x \leq y) \wedge (x \neq y)$.

Notons que tout sous-ensemble d'une chaine est une chaine.[19] En particulier, pour toute chaine C et tout élément x de C, $P(C, x)$ est une chaine.

Énoncé : Soit X un ensemble et $\leq$ une relation d'ordre sur X. On suppose que toute chaine de X pour $\leq$ admet une borne supérieure dans X. Alors X admet (au moins) un élément maximal pour la relation $\leq$.

On se propose de montrer cet énoncé. Pour ce faire, supposons par l'absurde que l'on puisse choisir un ensemble X et une relation d'ordre $\leq$ sur X tels que toute chaine de X pour $\leq$ admet une borne supérieure dans X, mais que X n'admet aucun élément maximal pour la relation $\leq$, et montrons que cela mène à une contradiction.

[19] Montrons cela. Avec les notations précédentes, soit C une chaine et C' un sous-ensemble de C. Soit x et y deux éléments de C'. Puisque C' est un sous-ensemble de C, $x \in C$ et $y \in C$. Puisque C est une chaine, on a donc $x \leq y \vee y \leq x$. Cela montre que C' est également une chaine.

On définit la relation d'ordre $\geq$ et les deux relations d'ordre strict $<$ et $>$ sur X comme suit : pour tous éléments x et y de X,

- $x \geq y$ est équivalent à $y \leq x$,
- $x < y$ est équivalent à $x \leq y \wedge x \neq y$,
- $x > y$ est équivalent à $y < x$.

Notons que, pour tous éléments x et y de X, $x > y$ est équivalent à $x \geq y \wedge x \neq y$.[20] L'absence d'élément maximal implique que, pour tout élément x de X, il existe un élément y de X tel que $x \leq y$ et $x \neq y$ (sans quoi x serait un élément maximal), et donc $x < y$.

Soit C une chaine de X pour $\leq$. On peut choisir une borne supérieure u de C dans X, et un élément x de X, dit *borne supérieure stricte de* C tel que $x > u$. Alors, pour tout élément e de C, on a $e \leq u$ (puisque u est une borne supérieure de C) et $u < x$, donc $u \leq x$, donc $e \leq x$. En outre, avec les mêmes notations, on a $e \neq x$, sans quoi on aurait $x \leq u$ et $u < x$, donc $x \leq u$ et $u \leq x$, donc $u = x$, ce qui est impossible puisque $u < x$. Donc, pour tout élément e de C, on a $e < x$.

On note $\mathscr{X}$ l'ensemble des sous-ensembles de X. Soit $\mathscr{C}$ l'ensemble des chaines de X. Il s'agit d'un sous-ensemble de l'ensemble des sous-ensembles de X, définit par : $\mathscr{C} = \{C \in \mathscr{X} | \forall x \in C \, \forall y \in C \, x \leq y \vee y \leq x\}$. Pour toute chaine C, on note S_C l'ensemble des bornes supérieures strictes de C (dans X). Alors, $\left\{ \left(C, S_C\right) | C \in \mathscr{C} \right\}$ est une fonction de $\mathscr{C}$ vers $\mathscr{X}$. (En effet, chaque élément C de $\mathscr{C}$ a une unique image S_C.) En outre, pour tout élément C de $\mathscr{C}$, S_C est non vide. Soit $\mathscr{S}$ l'ensemble définit par : $\mathscr{S} = \{S \in \mathscr{X} | \exists C \in \mathscr{C} \; S = S_C\}$. Alors, $\mathscr{S}$ est un ensemble d'ensembles non vide (puisque toute chaine admet au moins une borne supérieure stricte). D'après l'axiome du choix, on peut donc choisir une fonction g de $\mathscr{S}$ vers X telle que, pour tout élément S de $\mathscr{S}$, $g(S) \in S$. Soit $f = \{(C, g(S_C)) | C \in \mathscr{C}\}$. Alors, f est une fonction de $\mathscr{C}$ vers X et, pour tout élément C de $\mathscr{C}$, $f(C)$ est une borne supérieure stricte de C.

Pour toute chaine C de X et tout élément x de C, on définit le sous-ensemble $P(C, x)$ de C par :

$$P(C, x) = \{y \in C | y < x\}.$$

Soit C une chaine de X. Un sous-ensemble D de C est dit *segment initial* de C s'il existe un élément x de C tel que $D = P(C, x)$.

On dit d'un sous-ensemble A de X qu'il est *conforme* s'il satisfait les deux conditions suivantes :

- la relation $\leq$ est un bon ordre sur A (il s'agit alors d'un ordre total sur A, donc A est une chaine),
- pour tout élément x de A, on a $x = f(P(A,x))$.

Montrons le résultat intermédiaire suivant :

Lemme : Soit A et B deux sous-ensembles conformes de X tels que $A \neq B$. Alors A est un segment initial de B ou B est un segment initial de A.

Démonstration : Supposons que $A \neq B$. Alors, il existe un élément de A qui n'est pas un élément de B ou un élément de B qui n'est pas un élément de A. Supposons qu'il existe un élément de A qui n'est pas un élément de B. (Sinon, on se ramène à ce cas en échangeant les rôles de A et B.) Alors, l'ensemble $A \backslash B$ est non vide.

L'ensemble $A \backslash B$ est un sous-ensemble non vide de A. Puisque $\leq$ est un bon ordre sur A, $A \backslash B$ admet un élément minimal, noté x dans la suite de cette démonstration. Montrons que $P(A, x) = B$.

Soit y un élément de $P(A,x)$. Alors, $y \in A$ et $y < x$. Puisque x est un élément minimal de $A \backslash B$ pour $\leq$, on en déduit que $y \neq A \backslash B$ (sans quoi on aurait $x \leq y$). Donc, $y \in B$ (sans quoi on aurait $y \in A \wedge y \notin B$, et donc $y \in A \backslash B$). Ainsi, $P(A,x) \subset B$.

Il reste à montrer que $B \subset P(A,x)$. Supposons par l'absurde que ce n'est pas le cas. Alors, il existe un élément de B qui n'est pas un élément de $P(A,x)$. Donc, $B \backslash P(A, x)$ est non vide. Puisque $\leq$ est un bon ordre sur B, et puisque $B \backslash P(A,x)$ est un sous-ensemble de B, on en déduit que $B \backslash P(A,x)$ admet un élément minimal, noté y dans la suite de cette démonstration.

Notons que x n'appartient pas à $P(B, y)$ (qui est un sous-ensemble de B). Donc, $x \in A \backslash P(B,y)$. Donc, $A \backslash P(B,y)$ est non vide. Puisqu'il s'agit d'un sous-ensemble de A, il admet donc un élément minimal, noté z dans la suite. Puisque z est un élément minimal de $A \backslash P(B,y)$, qui contient x, on a $z \leq x$.

Nous allons montrer que $P(A,z) = P(B,y)$. Puisque A et B sont conformes, on a $z = f(P(A,z))$ et $y = f(P(B,y))$, et on aura donc $z = y$. Puisque $y \in B$ et $x \notin B$, $x \neq y$; on aura donc $z \neq x$, donc $z < x$, donc (puisque $z \in A$) $z \in P(A,x)$, et donc $y \in P(A,x)$, ce qui est impossible puisque y est un élément de $B \backslash P(A,x)$. Cela montrera que l'hypothèse de départ est fausse et que $B \subset P(A,x)$. On pourra alors conclure que $B = P(A,x)$.

Soit a un élément de $P(A,z)$. Alors, $a \in A$ et $a < z$. Puisque z est un élément minimal de $A \backslash P(B,y)$, le prédicat $a \in A \backslash P(B,y)$ est faux (sans quoi on aurait $z \leq a$, ce qui est impossible puisque $a < z$). Donc, $a \in P(B,y)$ (sans quoi on aurait $a \in A \wedge a \notin P(B,y)$, et donc $a \in A \backslash P(B,y)$). Cela montre que $P(A,z) \subset P(B,y)$.

[20] En effet, $x > y$ est équivalent à $y < x$, donc à $y \leq x \wedge x \neq y$. Puisque $y \leq x$ est équivalent à $x \geq y$, on en déduit que $x > y$ est donc équivalent à $x \geq y \wedge x \neq y$.

Soit b un élément de $P(B,y)$. Alors, $b \in B$ et $b < y$. Puisque y est un élément minimal de $B \setminus P(A,x)$, b ne peut appartenir à $B \setminus P(A,x)$ (sans quoi on aurait $y \leq b$, ce qui est impossible puisque $b < y$), donc $b \in P(A,x)$, donc $b \in A$ et $b < x$. Si $z = x$, alors $b < z$, donc $b \in P(A, z)$. Sinon, $z < x$, donc, puisque x est un élément minimal de $A \setminus B$, on a $z \in B$ (sans quoi on aurait $z \in A \setminus B$ et donc $x \leq z$). Dans ce cas, puisque $z \in A \setminus P(B, y)$, on a $z \geq y$ (sans quoi on aurait $z \leq y$ puisque $\leq$ est une relation d'ordre total sur B, et $z \neq y$, donc $z < y$ et donc $z \in P(B,y)$), donc, puisque $b < y$, $b < z$, et donc $b \in P(A, z)$. Cela montre que $P(B, y) \subset P(A, z)$.

Nous avons donc montré que $P(A, z) = P(B, y)$, ce qui conclut la preuve.

□

Soit A un sous-ensemble conforme de X non vide et x un élément de A. Soit y un élément de X tel que $y < x$. Supposons $y \notin A$. Alors y ne peut appartenir à aucun sous-ensemble conforme de X.

En effet, supposons par l'absurde qu'il existe un sous-ensemble conforme B de X tel que $y \in B$. On a $A \neq B$ (puisque $y \notin A$ et $y \in B$), donc l'un des deux ensembles A et B est un segment initial de l'autre. Puisque $y \in B$ et $y \notin A$, B ne peut être un sous-ensemble de A, dons B n'est pas un segment initial de A. Donc, A est un segment initial de B. On peut donc choisir un élément z de B tel que $A = \{w \in B | w < z\}$. Puisque $y \notin A$, $y < z$ doit être faux [21], donc $z = y$ ou $y \leq z$ est faux ; dans les deux cas (puisque $\leq$ est une relation d'ordre total sur B) $z \leq y$ est vrai. Puisque $y < x$, on a $y \leq x$, donc $z \leq x$. Mais, puisque $x \in A$, on a aussi $x < z$, donc $x \leq z$ et $x \neq x$ sont vrais, donc $z \leq x$ est faux. On en déduit que y ne peut appartenir à aucun sous-ensemble conforme de X.

Notons U l'union de tous les sous-ensembles conformes de X.[22]

Lemme : U est un sous-ensemble conforme de X.

Démonstration :

- Soit u un élément de U. On peut choisir un sous-ensemble conforme Y de X tel que $u \in Y$. Puisque Y est un sous-ensemble de X, cela implique $u \in X$. Donc, U et un sous-ensemble de X.
- Montrons que $\leq$ est un bon ordre sur U, et donc que U est une chaine. Soit V un sous-ensemble non vide de U. Soit v un élément de V. Puisque $v \in V$, $v \in U$, donc on peut choisir un sous-ensemble conforme A de X tel que $v \in A$. L'ensemble A est donc non vide et est un sous-ensemble de lui-même. Puisque $\leq$ est un bon ordre sur A, on en déduit que A admet un minimum a. Alors, a est un minimum de U. En effet, soit u un élément de u,
  - Si $u \in A$, alors $u < a$ est faux puisque a est un plus petit élément de A.
  - Sinon, $u < a$ est faux, sans quoi u n'appartiendrait à aucun sous-ensemble conforme de X, et donc n'appartiendrait pas à U.
- Soit x un élément de U. On peut choisir un sous-ensemble conforme A de X tel que $x \in A$. Puisque A est conforme, on a $x = f(P(A,x))$. Montrons que $P(U, x) = P(A, x)$; on aura alors $x = f(P(U,x))$, d'où le résultat attendu.
  - Soit y un élément de $P(A, x)$. Alors, $y \in A$ et $y < x$. Puisque A est un sous-ensemble de U, on a donc $y \in U$ et $y < x$. Donc, $u \in P(U, x)$.
  - Soit y un élément de $P(U, x)$. Alors, $y < x$. En outre, $y \in A$, sans quoi y n'appartiendrait à aucun sous-ensemble conforme de X, et donc n'appartiendrait pas à U. Donc, $y \in P(A, x)$.

    On a donc bien $P(U,x) = P(A,x)$.

□

Notons x l'élément $f(U)$.

Lemme : $U \cup \{x\}$ est un sous-ensemble conforme de X.

Démonstration :

- Montrons que $\leq$ est un bon ordre sur $U \cup \{x\}$. Soit V un sous-ensemble non vide de $U \cup \{x\}$.
  - Si $x \notin V$, V est un sous-ensemble non vide de U, donc, puisque $\leq$ est un bon ordre sur U, V admet un plus petit élément.

[21] En effet, si $y < z$ est vrai, on a $y \in B \wedge y < z$, donc $y \in A$.

[22] Cet ensemble existe bien. En effet,

- l'ensemble des sous-ensembles de X existe d'après l'axiome de l'ensemble des parties,
- l'ensemble des sous-ensembles conformes de X existe donc d'après le schéma d'axiomes de compréhension avec le prédicat $P(x)$ équivalent à « x est conforme »,
- l'union des sous-ensembles conformes de X existe donc d'après l'axiome de la réunion.

– Si $x \in V$, alors $V \backslash \{x\}$ est un sous-ensemble de U (en effet, soit y un élément de cet ensemble, $y \in V$, donc $y \in U \cup \{x\}$, et $y \neq x$, donc $y \in U$). Si $V \backslash \{x\}$ est non vide, il admet un plus petit élément v. Puisque x est une borne supérieure stricte de U, on a $v < x$. Donc, pour tout élément y de V, $v < y$ (par définition d'un plus petit élément si $y \neq x$ et par l'argument précédent sinon). Donc, v est un plus petit élément de V. Si $V \backslash \{x\}$ est vide, alors $V = \{x\}$, donc x est un plus petit élément de V. (En effet, pour tout élément y de V, $y = x$.)

- Soit y un élément de $U \cup \{x\}$.
  – Si $y \neq x$, on a $y \in U$. Puisque U est conforme, on a donc $y = f(P(U, y))$. Montrons que $P(U \cup \{x\}, y) = P(U, y)$. On aura alors $y = f(P(U \cup \{x\}, y))$.
    ⋆ Soit z un élément de $P(U, y)$. Alors, $z \in U$, donc $z \in U \cup \{x\}$, et $z < y$. Donc, $z \in P(U \cup \{x\}, y)$.
    ⋆ Soit z un élément de $P(U \cup \{x\}, y)$. Alors $z \in U \cup \{x\}$ et $z < y$. Puisque x est une borne supérieure de U, $x < y$ est faux, donc $z \neq x$. Donc, $z \in U$, donc $z \in P(U, y)$.

    Ainsi, on a bien $P(U \cup \{x\}, y) = P(U, y)$.
  – Sinon, $y = x$, donc $y = f(U)$. Montrons que $P(U \cup \{x\}, x) = U$. On aura alors $y = f(P(U \cup \{x\}, x))$, et donc $y = f(P(U \cup \{x\}, y))$.
    ⋆ Soit z un élément de U. Alors, $z \in U \cup \{x\}$. Soit u une borne supérieure de U dans X telle que $x > u$ (un tel u existe par définition de x). Alors, $z \leq u$ et $u < x$, donc $u \leq x$, donc $z \leq x$ et $z \neq x$ (sans quoi on aurait $u < z$), donc $z < x$. Donc, $z \in P(U \cup \{x\}, x)$.
    ⋆ Soit z un élément de $P(U \cup \{x\}, x)$. Alors, $z \in U \cup \{x\}$ et $z < x$, donc $z \neq x$, donc $z \in U$.

□

Par définition de U, on a donc $U \cup \{x\} \subset U$, donc $x \in U$. Par définition, x est une borne supérieure stricte de U, donc on peut choisir une borne supérieure u de U dans X tel que $x > u$, et donc $u \leq x$. Mais, puisque $x \in U$ et u est une borne supérieure de U, on a aussi $x \leq u$. Donc, $u \leq x \wedge x \leq u$, donc $x = u$. Donc, $u = x$ et $x > u$, ce qui est impossible. On en déduit que l'hypothèse de départ est fausse, ce qui prouve le lemme de Zorn.

1.3 Quelques notations et résultats

1.3.1 Résumé des notations

Résumons ici quelques notations utiles pour la suite, de manière informelle :

- Valeurs de vérité : V (« vrai »), I (« indéfini »), F (« faux »).
- Le symbole ¬ représente la négation : si P est une proposition, la proposition $\neg P$ est fausse si P est vraie et inversement. Sa table de vérité est donnée ci-dessous :

P	$\neg P$
V	F
I	I
F	V

- Les symboles $\wedge$ et $\vee$ représentent respectivement les connecteurs « et » et « ou ». Les symboles $\Rightarrow$ et $\Leftarrow$ représentent l'implication vers la droite et vers la gauche. Le symbole $\Leftrightarrow$ représente l'équivalence. Soit P et Q deux propositions, on a ainsi la table de vérité suivante :

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftarrow Q$	$P \Leftrightarrow Q$
V	V	V	V	V	V	V
V	I	I	V	I	V	I
V	F	F	V	F	V	F
I	V	I	V	V	I	I
I	I	I	I	I	I	I
I	F	F	I	I	V	I
F	V	F	V	V	F	F
F	I	F	I	V	I	I
F	F	F	F	V	V	V

- Les symboles $\forall$ et $\exists$ représentent respectivement les quantificateurs universel (« pour tout ») et existentiel (« il existe »).
- On note $\in$ la relation d'appartenance et $\notin$ sa négation : $\forall x \forall y \, x \notin y \nLeftrightarrow (x_i n y)$.
- L'ensemble vide est noté $\varnothing$.
- Soit a un ensemble. On note $\{a\}$ l'ensemble contenant uniquement a.
- Soit a et b deux ensembles. On note $\{a, b\}$ la paire de a et b, *i.e.* l'ensemble définit par :

$$\forall x \, x \in \{a, b\} \Leftrightarrow ((x = a) \wedge (x = b))$$

- Soit E un ensemble et P un prédicat à un paramètre libre. L'ensemble $\{x \in E | Px\}$ (noté F dans la formule ci-dessous) est le sous-ensemble de E défini par :

$$\forall x \, x \in F \Leftrightarrow x \in E \wedge Px.$$

  On note (a,b) le couple formé par a et b, définit par : $(a,b) = \{\{a\}, \{a, b\}\}$.
- Soit E et F deux ensembles. L'*union* de E et F, notée $E \cup F$, est l'ensemble défini par :

$$E \cup F = \{x | (x \in E) \vee (x \in F)\}.$$

  L'*intersection* de E et F, notée $E \cap F$, est l'ensemble défini par :

$$E \cap F = \{x | (x \in E) \wedge (x \in F)\}.$$

  La *différence* de E et F, notée $E \backslash F$, est l'ensemble défini par :

$$E \backslash F = \{x | (x \in E) \wedge (x \notin F)\}.$$

- Soit E et F deux ensembles. On dit que E est inclus dans F, et on note $E \subset F$ ou $F \supset E$, si la proposition suivante est vraie : $\forall \, x \, x \in E \Rightarrow x \in F$.

1.3.2 Ensemble de tous les ensembles

Lemme : Il n'existe pas d'ensemble de tous les ensembles.

Démonstration : Supposons par l'absurde que l'ensemble de tous les ensembles existe, et notons-le U. Définissons l'ensemble X par : $X = \{e \in U | e \notin e\}$ [23], et considérons la propriété $P : X \in X$. Alors,

- Si P est vraie, $X \in X$, donc, par définition de cet ensemble, X n'est pas un élément de X, et donc P est fausse.
- Si P est fausse, $X \notin X$, donc, par définition de cet ensemble, X est un élément de X, et donc P est vraie.

Ainsi, la propriété P ne peut être ni vraie ni fausse, ce qui constitue une contradiction. On en déduit que l'hypothèse de départ est fausse.

□

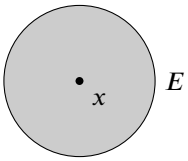
NB: Si on inclus la valeur de vérite « indéfinie » dans la théorie, alors cette démonstration montre seulement que, avec les mêmes notations, la propriété P est indéfinie.

[23] Cet ensemble existe d'après le schéma d'axiomes de compréhensions. En ré-utilisant les notations de l'énoncé de cet axiomes, il s'agit de l'ensemble obtenu en prenant $a = U$ et $Px : x \notin x$.

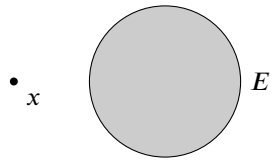
NB: Le résultat est évident si l'on inclus l'axiome de fondation dans la théorie, puisqu'alors aucun ensemble ne peut être élément de lui-même.

1.3.3 Représentations schématiques

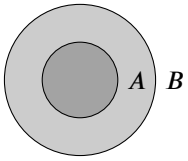
Nous donnons ici des représentations schématiques de certains des concepts définis ci-dessus. Ces schémas sont destinés à donner une représentation intuitive de ces concepts, et n'ont aucunement prétention à aucune forme de rigueur.



$x \in E$

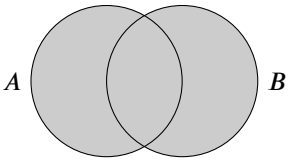


$x \notin E$

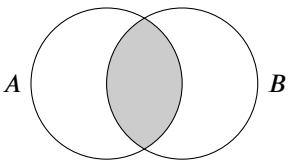


$A \subset B$

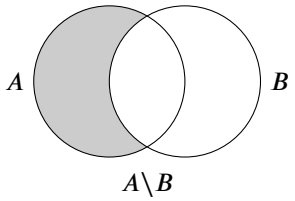
Sur chacun des quatre schémas suivants, la zone grisée correspond à l'ensemble en légende.



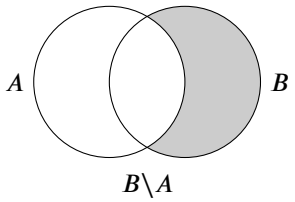
$A \cup B$



$A \cap B$

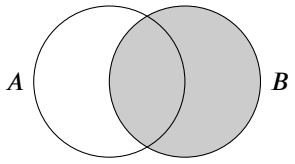


$A \setminus B$

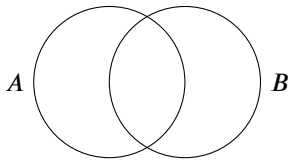


$B \setminus A$

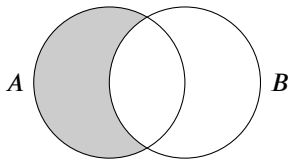
Certains résultats se voient aisément schématiquement :



$(B \setminus A) \cup (A \cap B) = B$

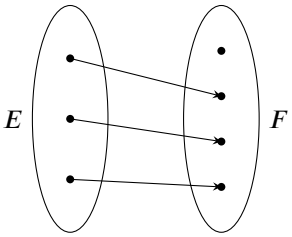


$(B \setminus A) \cap (A \cap B) = \varnothing$

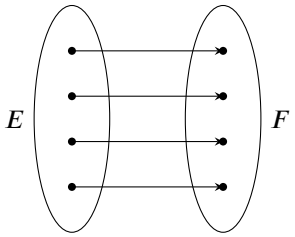


$(A \cup B) \setminus B = A \setminus B$

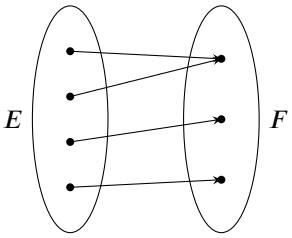
Une fonction d'un ensemble E vers un ensemble F peut être représentée par des flèches allant de chaque élément de E vers son image.



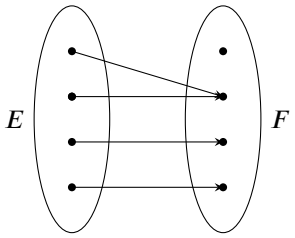
Exemple d'injection



Exemple de bijection



Exemple de surjection



Exemple de fonction ni injective ni surjective

1.4 Construction de $\mathbb{N}$

1.4.1 Définition

L'ensemble des entiers naturels, noté $\mathbb{N}$, est défini de la manière suivante. Notons Cl le prédicat à un paramètre libre défini par :

$$\mathrm{Cl}(A) : (\varnothing \in A) \wedge (\forall a\,(a \in A \Rightarrow a \cup \{a\} \in A)).$$

D'après l'axiome de l'infini, il existe un ensemble A tel que $\mathrm{Cl}(A)$ est vrai. Soit Ent le prédicat à un paramètre libre défini par :

$$\mathrm{Ent}(x) : \forall A\,(\mathrm{Cl}(A) \Rightarrow x \in A).$$

Soit I un ensemble tel que $\mathrm{Cl}(I)$ est vrai. L'ensemble $\mathbb{N}$ est défini par :

$$\mathbb{N} = \{x \in I | \mathrm{Ent}(x)\}.$$

Notons que cette définition ne dépend pas du choix de I. Notons aussi que $\varnothing \in \mathbb{N}$ et $\forall n\, n \in \mathbb{N} \Rightarrow n \cup \{n\} \in \mathbb{N}$.

Démonstration :

- Montrons d'abord que $\varnothing \in \mathbb{N}$. Puisque $\mathrm{Cl}(I)$ est vrai, $\varnothing \in I$. Soit A un ensemble tel que $\mathrm{Cl}(A)$ est vrai. Alors, $\varnothing \in A$. Donc, $\mathrm{Ent}(\varnothing)$ est vrai. On a donc $\varnothing \in I \wedge \mathrm{Ent}(\varnothing)$. Donc, $\varnothing \in \mathbb{N}$.
- Soit n un élément de $\mathbb{N}$. Alors, $n \in I$. Puisque $\mathrm{Cl}(I)$ est vrai, on en déduit que $n \cup \{n\} \in I$. Soit A un ensemble tel que $\mathrm{Cl}(A)$ est vrai. Puisque $\mathrm{Ent}(n)$ est vrai, $n \in A$. Alors, puisque $\mathrm{Cl}(A)$ est vrai, $n \cup \{n\} \in A$. On en déduit que $\mathrm{Ent}(n \cup \{n\})$ et vrai. On a donc $n \cup \{n\} \in I \wedge \mathrm{Ent}(n \cup \{n\})$. Donc, $n \cup \{n\} \in \mathbb{N}$.
- Motrons finalement que la définition de $\mathbb{N}$ ne dépends pas du choix de I. Soit J un ensemble tel que $\mathrm{Cl}(J)$ est vrai. Soit $\mathbb{M}$ l'ensemble défini par : $\mathbb{M} = \{x \in J | \mathrm{Ent}(x)\}$. Il s'agit de montrer que $\mathbb{M} = \mathbb{N}$.
  Soit x un élément de $\mathbb{N}$. Puisque Cl(J) et Ent(x) sont vrais, $x \in J$ est vrai aussi. Donc, $x \in J \wedge \mathrm{Ent}(x)$. Donc, $x \in \mathbb{M}$. Cela montre que $\mathbb{N} \subset \mathbb{M}$.
  Soit y un élément de $\mathbb{M}$. Puisque Cl(I) et Ent(y) sont vrais, $y \in I$ est vrai aussi. Donc, $y \in I \wedge \mathrm{Ent}(x)$. Donc, $y \in \mathbb{N}$. Cela montre que $\mathbb{M} \subset \mathbb{N}$.
  On a donc $\mathbb{M} = \mathbb{N}$.

□

On notera souvent 0 l'ensemble $\varnothing$. Pour tout élément n de $\mathbb{N}$, on notera $n + 1$ l'ensemble $n \cup \{n\}$, appelé *successeur* de n. Cela définit une application Suc de $\mathbb{N}$ vers lui-même, qui à un élément n associe $n + 1$. Notons que, pour tout entier naturel n,

on a $n \subset n+1$. Les premiers entiers sont notés de la manière suivante en base 10 (voir section ?? pour une définition générale de la base) :

n	$n+1$
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10

NB: Notons que Cl($\mathbb{N}$) est vraie et, si E est un ensemble tel que Cl(E) est vraie, alors $\mathbb{N} \subset E$. En ce sens, $\mathbb{N}$ est le plus petit ensemble satisfaisant Cl.

Démonstration :

Tout d'abord, on a vu ci-dessus que $\varnothing \in \mathbb{N}$ et $\forall n\, n \in \mathbb{N} \Rightarrow n \cup \{n\} \in \mathbb{N}$. Donc, Cl($\mathbb{N}$) est vrai.

Soit E un ensemble tel que Cl(E) est vrai. Soit x un élément de $\mathbb{N}$. Alors, Ent(x) est vrai, donc $x \in E$. Ainsi, N $\subset E$.

□

Un élément de $\mathbb{N}$ est dit *entier naturel* (ou parfois simplement *entier* quand il n'y a pas de confusion possible avec d'autres définitions). Il est dit *non nul* s'il est différent de 0.

Lemme : Soit n un élément de $\mathbb{N}$ et m un ensemble tel que $m \subset n+1$. Alors $n \in m$ ou $m \subset n$.

Démonstration : Si $n \in m$, le résultat est vrai. Supposons que $n \notin m$. Soit x un élément de m. Puisque $m \subset n+1$, on a $x \in n+1$, et donc $x \in n$ ou $x \in \{n\}$. La seconde option est impossible puisqu'elle impliquerait $x = n$, et donc $n \in m$, en contradiction avec notre hypothèse. Donc, $x \in n$. Cela étant vrai pour tout élément x de m, on en déduit $m \subset n$.

□

Définition : On note $\mathbb{N}^*$ l'ensemble $\mathbb{N}\backslash\{0\}$.

1.4.2 Relation d'ordre : définition

On définit une relation binaire, notée $\leq$, sur $\mathbb{N}$ par : pour tous éléments n et m de $\mathbb{N}$,

$$n \leq m \Leftrightarrow n \subset m.$$

Il sagit d'une relation d'ordre puisque la relation $\subset$ est réflexive, antisymétrique et transitive. On définit la relation d'ordre strict $<$ par pour tous éléments n et m de $\mathbb{N}$,

$$n < m \Leftrightarrow (n \leq m \wedge m \neq n).$$

Notons que, pour tout élément n de $\mathbb{N}$, $0 \leq n$ (puisque l'ensemble vide est un sous-ensemble de tout ensemble) et $n < n+1$ (en effet, on a $n \subset n+1$, donc $n \leq n+1$, et $n \neq n+1$; nous démontrerons ce point dans la section ??—pour le moment, nous avons seulement montré que $n \leq n+1$). Par antisymétrie, le premier point implique que le seul élément n de $\mathbb{N}$ satisfaisant $n \leq 0$ est 0 lui-même.

On définit aussi la relation d'ordre $\geq$ et la relation d'ordre strict $>$ sur $\mathbb{N}$ par : pour tous éléments n et m de $\mathbb{N}$, $n \geq m \Leftrightarrow m \leq n$ et $n > m \Leftrightarrow m < n$.

1.4.3 Principe de récurrence

Lemme (principe de récurrence) : Soit P une formule à un paramètre libre. On suppose que $P(0)$ est vraie et que, pour tout élément n de $\mathbb{N}$, $P(n) \Rightarrow P(n+1)$ est vraie. Alors, $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

On dira parfois, dans ce contexte, que P est vraie « au rang n » pour signifier que $P(n)$ est vrais. Ainsi, démontrer P parrécurrence revient à montrer que $P(0)$ est vraie et que, pour tout entier naturel n, « si P est vraie au rang n, alors P est vraie au rang $n+1$ ».

Démonstration : Soit E l'ensemble défini par $E = \{n \in \mathbb{N} | P(n)\}$. Puisque $P(0)$ et vraie, on a $0 \in E$. En outre, pour tout $n \in E$, $P(n)$ est vrai, donc $P(n+1)$ est vrai aussi, et donc $n+1 \in E$. Donc, Cl(E) est vraie. Donc, $\mathbb{N} \subset E$. Soit $n \in \mathbb{N}$, on a donc $n \in E$, et donc $P(n)$ est vraie.

□

Lemme (Récurrence finie) : Soit E un sous-ensemble non vide de $\mathbb{N}$ tel que : $\forall n \in E$, $\forall m \in \mathbb{N}$, $m \leq n \Rightarrow m \in E$. Soit P une formule à un paramètre libre. On suppose que $P(0)$ est vraie et que, pour tout $n \in E$ tel que $n+1 \in E$, $P(n) \Rightarrow P(n+1)$ est vraie. Alors, $P(n)$ est vraie pour tout $n \in E$.

Démonstration : Notons que $0 \in E$. Définissons la formule Q à un paramètre libre par $Q(n) : P(n) \vee (n \notin E)$. Alors $Q(0)$ est vraie. En outre, soit $n \in \mathbb{N}$ tel que $Q(n)$ est vraie, soit $n+1 \in E$, donc $n \in E$, donc $P(n)$ est vraie, donc $P(n+1)$ est vraie, et donc $Q(n+1)$ est vraie, soit $n+1 \notin E$ et donc $Q(n+1)$ est vraie. Par récurrence, $Q(n)$ est vraie pour tout $n \in \mathbb{N}$. Soit $n \in E$. Puisque $Q(n)$ est vraie et que $n \notin E$ ne peut être vraie, on en déduit que $P(n)$ est vraie.

□

Donnons un exemple facile de démonstration par récurrence.

Lemme : Soit n un entier naturel. Alors $n = 0$ ou il existe un entier naturel m tel que $n = m + 1$.

Remarque : On montre section 1.4.4 que deux entiers naturels a et b satisfaisant $a + 1 = b + 1$ sont égaux. Donc, l'entier naturel m défini par l'énoncé du lemme est unique.

Démonstration : Soit P le prédicat à un paramètre défini par : $P(n) : n = 0 \vee (\exists m \in \mathbb{N},\ n = m + 1)$. Tout d'abord, $P(0)$ est vrai puisque $0 = 0$ est vrai. Soit n un élément de $\mathbb{N}$. Alors $P(n+1)$ est vrai puisqu'il existe un entier naturel m tel que $n + 1 = m + 1$—il suffit de prendre $m = n$. Par récurrence, $P(n)$ est donc vrai pour tout élément n de $\mathbb{N}$.

□

Définition : Soit n un entier naturel tel que $n \neq 0$. L'entier naturel m tel que $n = m + 1$ est noté $n - 1$. Notons que, pour tout entier naturel n, $(n + 1) - 1 = n$ et, si $n \neq 0$, $(n - 1) + 1 = n$.

Cet exemple est conceptuellement très simple car la seconde étape du raisonnement ne fait pas appel au fait que le prédicat est vrai au rang précédent. Donnons maintenant un exemple légèrement moins aisé, et plus proche de la manière dont la démonstration par récurrence fonctionne la plupart du temps. On admet momentanément que, pour tout entier naturel n, $n+1 \neq n$, et donc $n \notin n$. (Cela sera démontré, sans utiliser le lemme suivant, section 1.4.4.)

Lemme : Soit n et m deux entiers naturels. S'il existe une bijection de n vers m, alors $n = m$.

Démonstration : Considérons le prédicat suivant, dépendant d'un paramètre libre n : *Pour tout entier naturel m, s'il existe une bijection de n vers m, alors n = m.*

Pour $n = 0$, le résultat est aisé : la seule fonction de 0 vers un ensemble est $\emptyset$, dont l'image est $\emptyset$. Si E est un ensemble et s'il existe une biection de 0 vers E, alors $E = \emptyset = 0$.

Soit n un entier naturel pour lequel le prédicat est vrai. Soit m un entier naturel et f une bijection de $n+1$ vers m. Puisqu'une telle bijection existe et $n + 1$ est non vide (il contient au moins n), m ne peut être égal à 0 (il contient au moins les images des éléments de $n + 1$). Donc, d'après le lemme précédent, on peut choisir un entier naturel k tel que $m = k + 1$. Montrons qu'il existe une bijection de n vers k. On aura alors $n = k$, donc $n + 1 = k + 1$, et donc $n + 1 = m$, et le lemme sera montré par récurrence.

On a : $m = k \cup \{k\}$. Soit g la fonction de m vers m définie par $g(k) = f(n)$, $g(f(n)) = k$ (notons que cela est toujours possible car ces deux conditions sont équivalentes si $f(n) = k$) et $g(x) = x$ pour tout élément x de m tel que $x \notin \{k, f(n)\}$. Supposons avoir montré que g est une bijection de m vers m. Alors, $g \circ f$ est une bijection de $n + 1$ vers m et $(g \circ f)(n) = k$. Soit h la fonction de n vers k définie par : pour tout élément x de n, $h(x) = (g \circ f)(x)$. (Son image est bien incluse dans k puisque, pour tout élément x de n, $(g \circ f)(x) \in m$ et $(g \circ f)(x) \neq k$ puisque $x \neq n$ (car $x \in n$ et $n \notin n$).) Montrons que h est une bijection. Soit x et y deux éléments de n tels que $h(x) = h(y)$. Alors, $(g \circ f)(x) = (g \circ f)(y)$. Puisque $g \circ f$ est une bijection, cela implique $x = y$. Donc, h est injective. Soit y un élément de k. Puisque $g \circ f$ est bijective, on peut choisir un élément x de $n + 1$ tel que $(g \circ f)(x) = y$. En outre, $y \in k$, donc $y \neq k$. Puisque $(g \circ f)(n) = k$, cela implique $x \neq n$, et donc $x \in n$. On a donc $h(x) = y$. Donc, h est surjective. La fonction h est ainsi une bijection de n vers k.

Il nous reste à montrer que la fonction g est bijective. Montrons d'abord qu'elle est injective. Soit x et y deux éléments de m tels que $g(x) = g(y)$. Si ni x ni y ne sont dans $\{f(n), k\}$, alors $g(x) = x$ et $g(y) = y$, donc $x = y$. Si $x \in \{f(n), k\}$, alors $y \in \{f(n), k\}$ (sans quoi on aurait $g(x) \in \{f(n), k\}$ et $g(y) \notin \{f(n), k\}$). De même, si $y \in \{f(n), k\}$, alors $x \in \{f(n), k\}$. Supposons $x = k$. Alors, $g(x) = f(n)$, donc $g(y) = f(n)$. Si $y = f(n)$, on a $g(y) = k$, ce qui contredit $g(x) = g(y)$ sauf si $f(n) = k$. Donc, $y = k$ ou $y = f(n)$ et $f(n) = k$. Dans les deux cas, on a $y = k$, et donc $y = x$. Enfin, supposons $x = f(n)$. Alors, $g(x) = k$, donc $g(y) = k$. Si $y = k$, on a $g(y) = f(n)$, ce qui contredit $g(x) = g(y)$ sauf si $k = f(n)$. Donc, $y = f(n)$ ou $y = k$ et $k = f(n)$. Dans les deux cas, on a $y = f(n)$, et donc $y = x$. Ainsi, g est bien injective.

Montrons qu'elle est surjective. Soit y un élément de m. Si $y \notin \{k, f(n)\}$, on a $g(y) = y$. Si $y \in \{k, f(n)\}$, on a $y = k$ ou $y = f(n)$. Dans le premier cas, $g(f(n)) = y$. Dans le second cas, $g(k) = y$. Dans tous les cas, il existe donc un élément x de m tel que $g(x) = y$. Ainsi, g est surjective. Il s'agit donc bien d'une bijection.

□

Pour prouver par récurrence qu'un prédicat P dépendant d'une variable libre n est vraie pour tout entier naturel n supérieur ou égal à un entier naturel n_0, on pourra procéder comme suit :

- Montrer que $P(n_0)$ est vrai.
- Pour tout entier naturel n tel que $n \geq n_0$ et $P(n)$ est vrai, montrer que $P(n+1)$ est vrai.

Dans ce schéma de raisonnement, n pourra être appelé *rang*, et le prédicat P dit *vraie au rang n* si $P(n)$ est vrai.

1.4.4 Relation d'ordre : propriétés

Lemme : Pour tout élément n de $\mathbb{N}$, $0 \leq n$.

Démonstration : Évident car $\varnothing \subset E$ pour tout ensemble E.

□

Lemme : Pour tout élément n de $\mathbb{N}$, $n \leq 0 \Rightarrow n = 0$.

Corolaire : Il n'existe aucun élément n de $\mathbb{N}$ tel que $n < 0$.

Démonstration : Conséquence directe du lemme précédent et de l'antisymétrie de $\leq$.

□

Lemme : Pour tout élément n de $\mathbb{N}$, on a $n \neq 0 \Rightarrow 0 \in n$.

Démonstration : On procède par récurrence. Soit $P : n \neq 0 \Rightarrow 0 \in n$. Pour $n = 0$, le résultat est évident car $n \neq 0$ est fausse, donc $P(0)$ est vraie. Soit n un élément de $\mathbb{N}$ tel que $P(n)$ est vraie. Si $n = 0$, $n + 1 = \{\varnothing\}$, donc $0 \in n + 1$, donc $P(n + 1)$ est vraie. Si $n \neq 0$, $0 \in n$, donc, puisque $n \subset n + 1$, $0 \in n + 1$, donc $P(n + 1)$ est vraie. Par récurrence, on en déduit que $P(n)$ est vraie pour tout élément n de $\mathbb{N}$.

□

Lemme : Soit n un élément de $\mathbb{N}$. Pour tout élément m de $\mathbb{N}$ tel que $n \leq m$, on a $m \notin n$. En particulier, pour tout élément n de $\mathbb{N}$, on a $n + 1 \neq n$. Puisque $n \subset n + 1$, $n \leq n + 1$, donc cela implique $n < n + 1$.

Démonstration : Montrons d'abord que la première partie du lemme implique bien le cas particulier. Soit n un élément de $\mathbb{N}$. On a $n \in n + 1$. Si la première partie du lemme est vraie, on a aussi $n \notin n$, d'où $n + 1 \neq n$.

Montrons maintenant la première partie du lemme. On procède par récurrence. La propriété attendue est évidente pour 0 puisqu'il s'agit de l'ensemble vide.

Soit n un élément de $\mathbb{N}$ et supposons que, pour tout élément m de $\mathbb{N}$ tel que $n \leq m$, $m \notin n$. Soit m un élément de $\mathbb{N}$ tel que $n + 1 \leq m$. Puisque $n \subset n + 1$ et $n + 1 \subset m$, on a $n \subset m$, et donc $n \leq m$. Donc, $m \notin n$. En outre, $n \in n + 1$ et $n \notin n$ (puisque $n \leq n$), donc $n + 1 \subset n$ ne peut être vrai, donc $m \neq n$, donc $m \notin \{n\}$. Puisque $n + 1 = n \cup \{n\}$, on en déduit $m \notin n + 1$. La propriété attendue est donc vraie pour $n + 1$.

Par récurrence, la propriété est vraie pour tout élément n de $\mathbb{N}$.

□

Lemme : Soit n un élément de $\mathbb{N}$. Pour tout élément m de $\mathbb{N}$ tel que $m \in n$, on a $n > m$.

Démonstration : On procède par récurrence sur n. Pour $n = 0$, le résultat est évident puisqu'aucun élément m de $\mathbb{N}$ ne satisfait $m \in 0$. Soit n un élément de $\mathbb{N}$ satisfaisant la propriété énoncée dans le lemme. Soit m un élément de $\mathbb{N}$ tel que $m \in n + 1$. Alors, $m \in n$ ou $m = n$.

- Si $m \in n$, on a $n > m$. En outre, d'après le lemme précédent, on a $n + 1 > n$. Donc, $n + 1 > m$.

- Si $m = n$, on a $n + 1 > m$ d'après le lemme précédent.

Ainsi, $n + 1$ satisfait également la propriété énoncée dans le lemme. Par récurrence, on en déduit qu'elle est vraie pour tout élément n de $\mathbb{N}$.

□

Lemme : Soit n un élément de $\mathbb{N}$. Pour tout élément m de $\mathbb{N}$ tel que $m < n$, on a $m \in n$.

Démonstration : On procède par récurrence. Pour $n = 0$, le résultat est évident puisqu'il n'existe aucun élément m de $\mathbb{N}$ tel que $m < 0$. Soit n un élément de $\mathbb{N}$ tel que, pour tout élément m de $\mathbb{N}$ tel que $m < n$, $m \in n$. Soit m un élément de $\mathbb{N}$ tel que $m < n + 1$. Montrons d'abord que $n \notin m$. Si on avait $n \in m$, alors on aurait $m > n$ d'après le lemme précédent, d'où $n \subset m$ et (puisque $n \in m$) $n + 1 \subset m$, en contradiction avec $m < n + 1$. Donc, $n \notin m$. Donc, puisque $m \subset n + 1$, $m \subset n$. (En effet, soit x un élément de m, on a $x \in n + 1$, donc $x \in n$ ou $x \in \{n\}$; la seconde option est impossible car $n \notin m$, donc $m \in n$.) Donc, $m \leq n$. Si $m = n$, on a $m \in n + 1$. Sinon, $m < n$, donc $m \in n$, et donc $m \in n + 1$. Dans les deux cas, $m \in n + 1$. Ainsi, la propriété énoncée dans le lemme est vraie pour $n + 1$. Par récurrence, on en déduit qu'elle l'est pour tout élément n de $\mathbb{N}$.

□

Corolaire : Soit n et m deux éléments de $\mathbb{N}$. D'après les deux lemmes précédents, les propositions $m \in n$ et $m < n$ sont équivalentes.

Lemme : Soit n un élément de $\mathbb{N}$. Pour tout élément m de $\mathbb{N}$ tel que $m \notin n$, on a $n \leq m$.

Démonstration : On procède par récurrence sur n. Pour $n = 0$, le résultat est évident car $0 \leq m$ pour tout élément m de $\mathbb{N}$. Soit n un élément de $\mathbb{N}$ tel que, pour tout élément m de $\mathbb{N}$ tel que $m \notin n$, $n \leq m$. Soit m un élément de $\mathbb{N}$ tel que $m \notin n + 1$. Alors, $m \notin n$ (donc $n \leq m$) et $m \neq n$, donc $n < m$. D'après le lemme précédent, cela implique $n \in m$. Puisque $n < m$, on a en outre $n \subset m$. Donc, $n + 1 \subset m$. Donc, $n + 1 \leq m$. On en déduit que le résultat est vrai pour $n + 1$. Par récurrence, il est vrai pour tout élément n de $\mathbb{N}$.

□

Corolaire : Soit n et m deux élément de $\mathbb{N}$. Les formules $m \notin n$ et $n \leq m$ sont équivalentes.

Démonstration : Soit n et m deux éléments de $\mathbb{N}$. Si $n \leq m$, alors $n \subset m$. Puisque $m \notin m$, cela implique $m \notin n$. Donc, $(n \leq m) \Rightarrow (m \notin n)$. Le lemme précédent montre en outre que $(n \leq m) \Leftarrow (m \notin n)$. Donc, $(n \leq m) \Leftrightarrow (m \notin n)$.

□

Corolaire : Soit n et m deux éléments de $\mathbb{N}$ tels que $n \notin m$ et $m \notin n$. Alors $m \leq n$ et $n \leq m$, et donc $n = m$.

Lemme : La relation d'ordre $\leq$ sur $\mathbb{N}$ est une relation d'ordre total.

Démonstration : Soit n et m deux éléments de $\mathbb{N}$. Alors, $m \in n$ ou $m \notin n$. Dans le premier cas, $n > m$, donc $m < n$, et donc $m \leq n$. Dans le second cas, $n \leq m$.

□

Corolaire : Soit n et m deux éléments de $\mathbb{N}$. Si $n \leq m$ est fausse, alors $m \leq n$ est vraie (d'après le lemme précédent) et $n \neq m$ est vraie (car $n \leq n$), donc $m < n$ est vraie. Donc, $\neg(n \leq m) \Rightarrow (m < n)$. Par ailleurs, si $m < n$, alors $n \leq m$ est fausse (sans quoi on aurait $m \subset n$ et $n \subset m$, et donc $m = n$). Ainsi, $\neg(n \leq m)$ est équivalente à $m < n$, et donc à $n > m$. De même, $\neg(n \geq m)$ est équivalente à $m > n$, et donc à $n < m$.

Corolaire : Soit n et m deux éléments de $\mathbb{N}$. Puisque $\leq$ est une relation d'ordre totale, on a $n \leq m$ ou $n \geq m$. Donc, $n < m$ ou $n = m$ ou $n > m$.

Notons que, si deux éléments n et m de $\mathbb{N}$ satisfont $n + 1 = m + 1$, on a soit $n = m$ soit $n \in m$ et $m \in n$.[24] La seconde possibilité implique $m < n$ et $n < m$, qui ne peuvent être stisfaites simultanément (car cela impliquerait $m \leq n$ et $n \leq m$, d'où $n = m$, ce qui est incompatible avec $m < n$). On en déduit le lemme suivant :

Lemme : Soit n et m deux éléments de $\mathbb{N}$. Si $n + 1 = m + 1$, alors $n = m$.

Lemme : Soit n un élément de $\mathbb{N}$. Pour tout élément m de $\mathbb{N}$ tel que $m < n + 1$, on a $m \leq n$. La réciproque est évidente puisque $n < n + 1$: pour tout élément m de $\mathbb{N}$, si $m \leq n$, $m < n + 1$. Donc, pour tout élément m de $\mathbb{N}$, on a $m < n + 1 \Leftrightarrow m \leq n$.

[24] En effet, puisque $n \in n + 1$ et $m \in m + 1$, la formule $n + 1 = m + 1$ implique $(n \in m + 1) \wedge (m \in n + 1)$, d'où $((n = m) \vee (n \in m)) \wedge ((m = n) \vee (m \in n))$. En utilisant deux fois la distributivité de $\wedge$ sur $\vee$ ainsi que sa symétrie, cette formule se récris $((n = m) \wedge (m = n)) \vee ((n = m) \wedge (m \in n)) \vee ((n \in m) \wedge (m = n)) \vee ((n \in m) \wedge (m \in n))$. Puisque $(n = m) \wedge (m \in n)$ et $(n \in m) \wedge (m = n)$ ne peuvet être vraies, et par symétrie de l'égalité, cette formule est équivalente à $(n = m) \vee (n \in m) \wedge (m \in n)$.

Corolaire : En prenant la négation de la formule de chaque côté du connecteur $\Leftrightarrow$, on obtient, pour tout élément m de $\mathbb{N}$: $m \geq n+1 \Leftrightarrow m > n$.

Démonstration : Soit m un élément de $\mathbb{N}$ tel que $m < n+1$. Alors $m \subset n \cup \{n\}$. Si $n \in m$, on a $m > n$, donc $n \subset m$, et donc $n+1 \subset m$ et donc $n+1 \leq m$, ce qui est impossible par hypothèse. On en déduit que $n \notin m$, donc que $m \subset n$, et donc que $m \leq n$. Ainsi, $\forall m \in \mathbb{N}\, m < n+1 \Rightarrow m \leq n$. Cela montre la première partie du lemme, de laquelle le reste découle.

□

Lemme : Pour tout entier naturel n, on a : $n = \{m \in \mathbb{N} | m < n\}$.

Démonstration : On procède par récurrence. Tout d'abord, il n'existe aucun entier naturel m tel que $m < 0$. Donc, $\{m \in \mathbb{N} | m < 0\} = \emptyset = 0$. Soit n un entier naturel tel que $n = \{m \in \mathbb{N} | m < n\}$. Puisque $n+1 = n \cup \{n\}$, on a : $n+1 = \{m \in \mathbb{N} | m < n \vee m = n\}$. Cela peut se récrire : $n+1 = \{m \in \mathbb{N} | m \leq n\}$. D'après le lemme précédent, cela est équivalent à : $n+1 = \{m \in \mathbb{N} | m < n+1\}$. Par récurrence, le résultat attendu est donc vrai pour tout entier naturel.

□

Lemme (récurrence en partant d'un rang non nul) : Soit n un entier naturel et P un prédicat à un paramètre. On suppose que $P(n)$ est vrai et que, pour tout entier naturel m tel que $m \geq n$, $P(m) \Rightarrow P(m+1)$. Alors, $\forall m \in \mathbb{N},\ m \geq n \Rightarrow P(n)$.

Démonstration : On procède par récurrence. Soit Q le prédicat à un paramètre libre défini par $Q(m) : m \geq n \Rightarrow P(n)$. Si $n = 0$, $P(0)$ est vrai, donc $Q(0)$ l'est aussi. Si $n \neq 0$, $n > 0$, donc $0 \geq n$ est fausse et $Q(0)$ est vraie. Dans tous les cas, $Q(0)$ est vraie.

Soit m un entier naturel tel que $Q(m)$ est vrai. Alors,

- Si $m+1 < n$, $n \geq m+1$ est fausse, donc $Q(m+1)$ est vrai.
- Si $m+1 = n$, $P(m+1)$ est vrai, donc $Q(m+1)$ est vrai.
- Si $m+1 > n$, $m \geq n$, donc $P(m)$ est vrai (puisque $Q(m)$ l'est), donc $P(m+1)$ est vrai, donc $Q(m+1)$ est vrai.

On a donc montré que, pour tout entier naturel m, $Q(m) \Rightarrow Q(m+1)$. Par récurrence, $Q(m)$ est donc vrai pour tout entier naturel m.

□

Définition : Soit a et b deux entiers naturels. On définit l'ensemble $[\![a, b]\!]$ par :

$$[\![a, b]\!] = \{n \in \mathbb{N} | (n \geq a) \wedge (n \leq b)\}.$$

Notons que $[\![a, b]\!] = \emptyset$ si $a > b$. En effet, dans ce cas, tout élément x de $\mathbb{N}$ satisfaisant $x \geq a$ satisfait $x > b$, et donc ne satistfait pas $x \geq b$.

Lemme : Soit n un entier naturel. On a : $[\![0, n-1]\!] = n$.

Démonstration :

- Soit x un élément de $[\![0, n-1]\!]$. Puisque $[\![0, n-1]\!]$ est un sous-ensemble de $\mathbb{N}$, $x \in \mathbb{N}$. En outre, $x \leq n-1$. Puisque $(n-1)+1 = n$, $n-1 < n$, et donc $x < n$. Donc, $x \in n$.
- Soit x un élément de n. Puisque n est un sous-ensemble de $\mathbb{N}$, $x \in \mathbb{N}$. Donc, $x \geq 0$. En outre, $x < n$. Donc, $x \leq n-1$. Donc, $x \in [\![1,n-1]\!]$.

□

1.4.5 Récurrence forte

Lemme (principe de récurrence forte) : Soit P une formule à un paramètre libre. On suppose que $P(0)$ est vraie et que, pour tout élément n de $\mathbb{N}$, la formule $(\forall m \in \mathbb{N}\, m \leq n \Rightarrow P(m)) \Rightarrow P(n+1)$ est vrai. Alors, pour tout élément n de $\mathbb{N}$, $P(n)$ est vraie.

Démonstration : Considérons la formule à un paramètre libre Q définie par $Q(n) : \forall m \in \mathbb{N}\, m \leq n \Rightarrow P(m)$. Notons que, d'après la seconde hypothèse faite sur P, pour tout élément n de $\mathbb{N}$ $Q(n) \Rightarrow P(n+1)$. Montrons que $Q(n)$ est vraie pour tout élément n de $\mathbb{N}$. Tout d'abord, $Q(0)$ est équivalente à $P(0)$ (car le seul élément m de $\mathbb{N}$ tel que $m \leq 0$ est 0). Donc, $Q(0)$ est vraie. Soit $n \in \mathbb{N}$ tel que $Q(n)$ est vraie. Soit $m \in \mathbb{N}$ tel que $m \leq n+1$. Alors, $m \leq n$ ou $m = n+1$. Si $m \leq n$, $P(m)$ est vraie car $Q(n)$ est vraie. Si, $m = n+1$, $P(m)$ est vraie puisque $Q(n)$ est vraie et $Q(n) \Rightarrow P(n+1)$. Donc, $Q(n+1)$ est vraie. Par récurrence, on en déduit que $Q(n)$ est vraie pour tout élément n de $\mathbb{N}$.

Montrons que cela implique le lemme. Soit n un élément de $\mathbb{N}$. On a vu que $Q(n)$ est vraie. Donc, pour tout élément m de $\mathbb{N}$ tel que $m \leq n$, $P(m)$ est vraie. Puisque $n \leq n$ par reflexivité de la relation d'ordre, $P(n)$ est vraie.

□

1.4.6 Suites ; définition par récurrence

Définition : Soit E un ensemble non vide. Une *suite* u d'éléments de E est une fonction de $\mathbb{N}$ vers E. Si u est une suite d'éléments de E et n un élément de $\mathbb{N}$, l'élément $u(n)$ de E est parfois noté u_n. Si f est une formule dépendant d'un paramètre libre telle que, pour tout élément n de $\mathbb{N}$, $f(n) = u(n)$, la suite u est parfois notée $(f(n))_{n\in\mathbb{N}}$. Si u est une suite et n une variable, dans la formule u_n, n est parfois appelé *indice*.

Lemme (définition par récurrence) : Soit E un ensemble non vide et f une fonction de $\mathbb{N} \times E$ vers E. Soit e_0 un élément de E. Il existe une unique fonction u de $\mathbb{N}$ vers E telle que $u(0) = e_0$ et, pour tout $n \in \mathbb{N}$, $u(n + 1) = f(n, u(n))$.

Ce lemme permet notamment de *définir* une suite par récurrence, étant donnés son image de 0 et une fonction f donnant son image de $n + 1$ connaissant celle de n.

Démonstration : *Unicité :* Soit u et v deux fonctions satisfaisant les propriétés de l'énoncé. Tout d'abord, on a $u(0) = e_0$ et $v(0) = e_0$ par hypothèse, et donc $u(0) = v(0)$. Soit n un élément de $\mathbb{N}$ et supposons $u(n) = v(n)$. Alors, $u(n + 1) = f(n, u(n))$ donne $u(n + 1) = f(n, v(n))$, d'où $u(n + 1) = v(n + 1)$. Par récurrence, on a donc $u(n) = v(n)$ pour tout élément n de $\mathbb{N}$.

Éxistence : Une fonction v d'un sous-ensemble non vide de $\mathbb{N}$ dans E est dite *f-inductive* si elle satisfait les trois propriétés suivantes :

- son domaine D satisfait $\forall x \in D,\ \forall n \in \mathbb{N},\ n \leq x \Rightarrow n \in D$,
- si 0 est dans son domaine, alors $v(0) = e_0$,
- si n est un élément de $\mathbb{N}$ tel que n et $n + 1$ sont tous deux dans son domaine, alors $v(n + 1) = f(n, v(n))$.

Chacune de ces fonctions est un sous-ensemble de $\mathbb{N} \times E$.

Soit v une fonction f-injective. Puisque son domaine est non nul, on peux choisir un élément x de D. Puisque D est un sous-ensemble de $\mathbb{N}$, on a $x \in \mathbb{N}$. Donc, $0 \leq x$, et donc $0 \in D$. Cela montre que 0 appartient au domaine de définition de toute fonction f-inductive.

Soit u l'union de toutes les fonctions f-inductives. (Cet ensemble existe d'après l'axiome de compréhension obtenu avec l'ensemble des parties de $\mathbb{N} \times E$ et la conjonction des trois propriétés définissant une fonction f-inductive.) Montrons que u est une fonction de $\mathbb{N}$ dans E satisfaisant les propriétés de l'énoncé.

Tout d'abord, $\{(0,e_0)\}$ (vu comme une fonction de $\{0\}$ vers E) est f-inductive, donc $(0,e_0) \in u$, et donc 0 appartient au domaine de u. Soit $n \in \mathbb{N}$ tel que n appartient au domaine de u. Soit v une fonction f-inductive dont le domaine contient n et $v' = v \cup \{n + 1, f(n, f(v(n)))\}$. On vérifie facilement que v' est une fonction f-inductive avec pour domaine $D \cup \{n + 1\}$, où D est le domaine de v. (Il s'agit bien d'une fonction car v en est une et, si $n + 1$ est aussi dans le domaine de v, on a $v(n+1) = f(n, f(v(n)))$; elle satisfait la première propriété car un entier m satisfaisant $m \leq n+1$ est égal à $n+1$ s'il contient n ou satisfait $m \leq n$ (et est donc dans le domaine de v) sinon, la seconde car l'image de 0 est égale à $v(0)$, donc à e_0, la troisième pour tout entier m satisfaisant $m \neq n$ car v est f-inductive (si m et $m + 1$ sont dans son domaines, alors ils sont aussi dans celui de v, d'où le résultat), et la troisième pour l'entier n car $v'(n + 1) = f(n,v(n))$ et $v(n) = v'(n)$.) Donc, $n + 1$ appartient au domaine de u. Cela montre (par récurrence) que le domaine de u est $\mathbb{N}$.

Soit $n \in \mathbb{N}$ et v et v' deux fonctions f-inductives dont les domaines contiennent n. On montre facilement par récurrence finie que $v(n) = v'(n)$. (Cela est vrai pour $n = 0$ car $v(0)$ et $v'(0)$ sont tous deux égaux à e_0 et, si un entier m est tel que $m + 1$ appartienne à leurs domaine de définition, alors m y appartient également (puisque $m < m + 1$) ; si de plus $v'(m) = v(m)$, alors $v'(m + 1) = f(m,v'(m)) = f(m,v(m)) = v(m + 1)$, donc $v'(m + 1) = v(m + 1)$.) Donc, u est bien une fonction.

Par ailleurs, on a $u(0) = e_0$. Soit $n \in \mathbb{N}$, $n + 1$ appartient à $\mathbb{N}$, donc au domaine de u, donc on peut choisir une fonction v f-inductive telle que $n + 1$ appartienne au domaine de v. Puisque $n < n + 1$, n est aussi dans le domaine de v. On a donc $v(n + 1) = f(n, v(n)) = f(n,u(n))$, et donc $u(n + 1) = f(n, u(n))$.

□

Ce résultat étant particulièrement important pour la suite, nous en donnons ci-dessous une démonstration formulée un brin différemment, et un peu plus détaillée. On reprend les notations du lemme.

Montrons tout d'abord que, si une fonction de $\mathbb{N}$ dans E satisfaisant les deux propriétés de l'énoncé existe, alors elle est unique. On suppose avoir deux telles fonctions, notées u et v. Montrons qu'elles sont nécéssairement égales. Pour ce faire, il suffit de montrer que, pour tout élément n de $\mathbb{N}$, $u(n) = v(n)$. On procède par récurrence. D'après la première propriété de l'énoncé, on a $u(0) = e_0$ et $v(0) = e_0$. Donc, $u(0) = v(0)$. Considérons maintenant un élément n de $\mathbb{N}$ tel que $u(n) = v(n)$. On a $f(n, u(n)) = f(n, v(n))$. Or, on a aussi, d'après la deuxième propriété de l'énoncé : $f(n, u(n)) = u(n+1)$ et $f(n, v(n)) = v(n+1)$. Donc, $u(n + 1) = v(n + 1)$. Cela étant vrai pour tout élément n de $\mathbb{N}$ tel que $u(n) = v(n)$, et puisque $u(0) = v(0)$, on en déduit par récurrence que, pour tout élément n de $\mathbb{N}$, $u(n) = v(n)$, et donc que $u = v$. Ainsi, il existe au plus une fonction satisfaisant les conditions de l'énoncé.

Montrons maintenant qu'une telle fonction existe bien. Pour ce faire, définissons d'abord la notion de fonction f-injective [25] de la manière suivante. Une fonction f-injective est une fonction, notée v dans la suite de cette définition, d'un sous-ensemble non vide D de $\mathbb{N}$ vers E telle que les conditions suivantes sont satisfaites :

- Pour tout élément x de D, pour tout élément n de $\mathbb{N}$ tel que $n \leq x$, $n \in D$. (C'est-à-dire : $\forall x \in D$, $\forall n \in \mathbb{N}$, $n \leq x \Rightarrow x \in D$; dans la suite, on note P_1 le prédicat obtenu en remplaçant D par la formule $\{x \in \mathbb{N} | \exists y \in \mathbb{N}\,(x,y) \in v\}$.)
- Si $0 \in D$, $v(0) = e_0$. (C'est-à-dire : $0 \in D \Rightarrow v(0) = e_0$; dans la suite, on note P_2 le prédicat obtenu en remplaçant D par la formule $\{x \in \mathbb{N} | \exists y \in \mathbb{N}\,(x,y) \in v\}$.) .)
- Si n est un élément de D tel que $n+1 \in D$, alors $v(n+1) = f(n, v(n))$. (C'est-à-dire : $\forall n \in D$, $n+1 \in D \Rightarrow v(n+1) = f(n, v(n))$; dans la suite, on note P_3 le prédicat obtenu en remplaçant D par la formule $\{x \in \mathbb{N} | \exists y \in \mathbb{N}\,(x,y) \in v\}$.))

Notons que la première condition impose $0 \in D$. En effet, D doit être non vide et, soit x un élément de D (un tel élément existe donc), on a $x \in \mathbb{N}$, donc $0 \leq x$, et donc $0 \in D$. La seconde condition peut donc être simplifiée en $v(0) = e_0$.

Toute fonctions f-injective est un sous-ensemble de $\mathbb{N} \times E$. En effet, si v est une telle fonction et z un élément de v, on peut choisir un élément x du domaine D de v et un élément y de E tels que $z = (x,y)$. Puisque D est un sous-ensemble de $\mathbb{N}$, on a $x \in \mathbb{N}$, et donc $z \in \mathbb{N} \times E$.

En appliquant l'axiome de compréhension avec l'ensemble des parties de $\mathbb{N} \times E$ et la propriété $P : P_1 \wedge P_2 \wedge P_3$, on montre que l'ensemble des fonctions f-inductives existe. Notons qu'il existe au moins une fonction f-injective : $\{(0, e_0)\}$. Il s'agit d'une fonction de $\{0\}$ vers E (en effet, son seul élément est dans $\{0\} \times E$, l'unique élément de $\{0\}$ a une image e_0, et, si x est un élément de $\{0\}$, et y et y' deux images de x, alors $y = e_0$ et $y' = e_0$, donc $y = y'$) ; son domaine est $\{0\}$, qui est bien un sous-ensemble de $\mathbb{N}$; le seul élément n de $\mathbb{N}$ satisfaisant $n \leq 0$ est 0 lui-même, qui est bien dans D ; on a $v(0) = e_0$; il n'existe aucun élément n de D tel que $n+1 \in D$ puisque $0 + 1 \neq 0$. Notons u l'union de tous les éléments de l'ensemble des fonctions f-injectives. (L'ensemble u existe d'après l'axiome de la réunion.) Nous nous proposons de montrer que u est une fonction de $\mathbb{N}$ vers E puis qu'elle satisfait les deux propriétés du lemme.

En tant qu'union de sous-ensembles de $\mathbb{N} \times E$, u en est un également.[26] Pour montrer que u est une fonction de $\mathbb{N}$ vers E, il suffit donc de montrer que, pour tout élément n de $\mathbb{N}$, il existe un unique élément e de E tel que $(n,e) \in u$. On procède par récurrence. Pour $n = 0$, le résultat est facile à démontrer : $\{(0, e_0)\}$ est une fonction f-inductive, donc $(0, e_0) \in u$. En outre, soit e un élément de e tel que $(0,e) \in E$, il existe une fonction f-inductive v telle que $(0,e) \in v$. La première propriété du lemme donne alors $e = e_0$. Ainsi, il existe un unique élément e de E (e_0) tel que $(0, e_0) \in u$.

Soit n un élément de $\mathbb{N}$ et supposons qu'il existe un unique élément de E, noté e dans la suite de ce paragraphe tel que $(n,e) \in u$. Soit e_1 et e_2 deux éléments de E tels que $(n+1, e_1) \in u$ et $(n+1, e_2) \in u$. On peut trouver deux fonctions f-injectives v_1 et v_2 dont les domaines contiennent $n+1$ et telles que $v_1(n+1) = e_1$ et $v_2(n+1) = e_1$. Puisque $n \leq n+1$, n appartient aussi à leurs domaines de définition. Puisque $(n, v_1(n)) \in u$ et $(n, v_2(n)) \in u$, on a $v_1(n) = e$ et $v_2(n) = e$. Donc, d'après le troisième critère de définition d'une fonction f-infductive, $v_1(n+1) = f(n,e)$ et $v_2(n+1) = f(n,e)$. Donc, $e_1 = f(n,e)$ et $e_2 = f(n,e)$. Donc, $e_1 = e_2$. Il existe donc au plus un élément e' de E tel que $(n+1, e') \in u$. Montrons qu'il existe bien. Soit v une fonction f-inductive dont le domaine de définition contient n. Montrons que $v \cup \{(n+1, f(n, v(n)))\}$ est une fonction f-inductive. Cela montrera que $(n+1, f(n,v(n))) \in u$. Par récurrence, nous aurons alors montré que u est bien une fonction, et que l'image par u d'un élément n de $\mathbb{N}$ est $v(n)$, où v est une fonction f-injective (quelconque) dont le domaine contient n.

Notons v' l'ensemble $v \cup \{(n+1, f(n, v(n)))\}$ et D le domaine de v. Montrons que v' est une fonction de $D \cup \{n+1\}$ dans E. Soit $m \in D$. Puisque v est une fonction de D vers E, on peut choisir un unique élément e de E tel que $(m,e) \in v$. On a alors $(m,e) \in v'$. Si $m \neq n+1$, il n'existe pas d'autre élément de v' dont la première composante soit n (car le seul élément de v' qui ne soit pas dans v a $n+1$ pour première composante ; un élément de v' dont la première composante est m doit donc être un élément de v, et sa deuxième composante ne peut alors être que e puisque v est une fonction). Si $m = n+1$, on a $v(n+1) = f(n, v(n))$ car v est f-injective. Donc, $(n+1, f(n,v(n))) \in v$ et $v' = v$, donc v' et une fonction et n'a pas plus d'un élément avec $n+1$ comme première composante. Par ailleurs, si $n+1$ n'est pas un élément de D, alors le seul élément de v' dont la première composante est $n+1$ est $(n+1, f(n,v(n)))$ (tout autre élément de v' appartient à v, et a donc sa première composante dans D). Ainsi, dans les deux cas (que $n+1$ soit ou non un élément de D) v' est une fonction.

Montrons qu'elle est f-injective. Son domaine de définition est celui de v, auquel on ajoute éventuellement $n+1$. Pour tout élément m de ce domaine distinct de $n+1$, m est dans le domaine de v, donc pour tout élément k de $\mathbb{N}$ tel que $k \leq m$, k est

[25] Cette définition est un peu bancale puisqu'elle dépend de f mais aussi de e_0. Une appellation plus appropriée serait « f-injective avec élément initial e_0 ». Pour simplifier, et puisque cette notion n'est utilisée que dans cette preuve où e_0 est fixé, nous la raccourcissons en « f-injective », l'élément initial étant implicite.

[26] En effet, soit $z \in u$, il existe un élément v de l'ensemble des fonctions f-injectives tel que $z \in v$. Soit D son domaine. On a $z \in D \times E$ Puisque D est un sous-ensemble de $\mathbb{N}$, $D \times E$ est un sous-ensemble de $\mathbb{N} \times E$, donc $z \in \mathbb{N} \times E$.)

dans le domaine de v et donc dans celui de v'. Soit m un élément de $\mathbb{N}$ tel que $m \leq n+1$. On a $m < n+1$ ou $m = n+1$. Dans le premier cas, on a $m \leq n$. Puisque n est dans le domaine de v et car v est f-injective, m y est également, et est donc dans celui de v'. Dans le second cas m est bien dans le domaine de v' puisque $(n+1, f(n,v(n))) \in v'$. Ainsi, la fonction v' satisfait P_1.

On a $v'(0) = v(0)$, donc, puisque v est f-injective, $v'(0) = e_0$. La fonction v' satisfait donc P_2.

Enfin, soit m un élément du domaine de v',

- Si $m \neq n$ et, et si $m+1$ est dans le domaine de v', alors $m+1$ est dans le domaine de v (en effet, si $m \neq n$, $m+1 \neq n+1$). Donc, puisque $m \leq m+1$, m est dans le domaine de v. Puisque v est f-injective, $v(m+1) = f(m, v(m))$. Puisque $v'(m) = v(m)$ et $v'(m+1) = v(m+1)$, on en déduit $v'(m+1) = f(m, v'(m))$.
- Si $m = n$, on a $v'(m+1) = f(n, v(n))$. Puisque $v'(n) = v(n)$, on en déduit $v'(m+1) = f(m,v'(m))$.

Ainsi, v' satisfait P_3. Cette fonction est donc bien f-injective.

Il ne reste plus qu'à montrer que u satisfait les deux propriétés de l'énoncé. Nous avons vu plus haut que $u(0) = e_0$. Soit n un élément de $\mathbb{N}$. Alors, $n+1$ appartient à $\mathbb{N}$ et donc au domaine de u, donc il on peut choisir une fonction f-injective v dont le domaine contient $n+1$. Puisque $n \leq n+1$, n appartient aussi au domaine de v. On a donc $v(n+1) = f(n, v(n))$. Puisque $u(n) = v(n)$ et $u(n+1) = v(n+1)$, on en déduit $u(n+1) = f(n, u(n))$.

□

Définition : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Soit u une suite d'éléments de E. On dit que u est *majorée* s'il existe un élément e de E tel que : $\forall n \in \mathbb{N}\, u_n \leq e$. On dit que u est *minorée* s'il existe un élément e de E tel que : $\forall n \in \mathbb{N}\, e \leq u_n$. Un élément e de E satisfaisant $\forall n \in \mathbb{N}\, u_n \leq e$ est dit *majorant* de u. Un élément e de E satisfaisant $\forall n \in \mathbb{N}\, e \leq u_n$ est dit *minorant* de u. Une suite à la fois majorée et minorée est dite *bornée* ; son majorant et son minorant sont aussi appelés *bornes*.

Définition : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Soit u une suite d'éléments de E. On dit que u est *croissante* si, pour tous entiers naturels n et m, $n \leq m \Rightarrow u_n \leq u_m$. On dit que u est *décroissante* si, pour tous entiers naturels n et m, $n \leq m \Rightarrow u_m \leq u_n$.

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Soit u une suite d'éléments de E. On suppose que $u_{n+1} \geq u_n$ pour tout entier naturel n. Alors, u est croissante.

Démonstration : Soit n un entier naturel. On veut montrer que, pour tout entier naturel m supérieur ou égal à n, $u_n \leq u_m$. On procède par récurrence sur $m - n$, noté k. Si $k = 0$, alors $m = n$, donc $u_n = u_m$ et $u_n \leq u_m$.

Supposons le résultat attendu pour un entier naturel k, *i.e.*, $u_n \leq u_{n+k}$. Puisque u est croissante, $u_{n+k} \leq u_{(n+k)+1}$. Donc, $u_n \leq u_{(n+k)+1}$. Donc, $u_n \leq u_{n+(k+1)}$. Le résultat attendu est vrai au rang $k+1$. Par récurrence, il l'est pour tout entier naturel k.

□

Lemme : Soit E un ensemble et $\leq$ une relation d'ordre sur E. Soit u une suite d'éléments de E. On suppose que $u_n \geq u_{n+1}$ pour tout entier naturel n. Alors, u est décroissante.

Démonstration : Soit n un entier naturel. On veut montrer que, pour tout entier naturel m supérieur ou égal à n, $u_m \leq u_n$. On procède par récurrence sur $m - n$, noté k. Si $k = 0$, alors $m = n$, donc $u_m = u_n$ et $u_m \leq u_n$.

Supposons le résultat attendu pour un entier naturel k, *i.e.*, $u_{n+k} \leq u_n$. Puisque u est décroissante, $u_{(n+k)+1} \leq u_{n+k}$. Donc, $u_{(n+k)+1} \leq u_n$. Donc, $u_{n+(k+1)} \leq u_n$. Le résultat attendu est vrai au rang $k+1$. Par récurrence, il l'est pour tout entier naturel k.

□

1.4.7 Sous-ensembles de $\mathbb{N}$, bornes, et éléments extrémaux

Lemme : Tout sous-ensemble non-vide de $\mathbb{N}$ admet un unique élément minimal pour la relation $\leq$.

Démonstration :

- *Unicité :* Soit E un sous-ensemble de $\mathbb{N}$ non vide et n et m deux de ses éléments minimaux. Puisque $\leq$ est une relation d'ordre totale et puisqu'ils sont minimaux, on a $n \leq m$ et $m \leq n$. Donc, $n = m$.
- *Existence :* On montre par récurrence forte la propriété suivante : Soit n un élément de $\mathbb{N}$, tout sous-ensemle de $\mathbb{N}$ contennat n admet un élément minimal. Pour $n = 0$, cela est évident car, pour tout élément e de E, $e \in \mathbb{N}$ et donc $0 \leq e$; 0 est donc un élément minimal de E. Soit n un élément de $\mathbb{N}$ et supposons la propriété vraie pour tout élément m de $\mathbb{N}$ tel que $m \leq n$. Soit E un sous-ensemble de $\mathbb{N}$ contenant $n+1$. Si $n+1$ est un élément minimal pour E, alors E admet un élément minimal. Sinon, on peut choisir un élément m de E tel que $n+1 \leq m$ est faux, et donc $m < n+1$ est vrai. Puisque $m < n+1$, on a $m \leq n$. Donc, E admet un élément infèrieur ou égal à n, et donc un élément minimal. Par récurrence

sorte, la propriété est vraie pour tout élément n de $\mathbb{N}$. Soit E un sous-ensemble non vide de $\mathbb{N}$, il existe un élément n de $\mathbb{N}$ tel que $n \in E$, donc E a un élément minimal.

□

Ce résultat étant important, donnons-en un énoncé et une démonstration un peu plus détaillés.

Lemme : Soit E un sous-ensemble non vide de $\mathbb{N}$. Alors il existe un unique élément e de E tel que $\forall x \in E\, e \leq x$. Puisque $\leq$ est une relation d'ordre total sur $\mathbb{N}$, cela est équivalent à dire que E admet un unique élément minimal.

Démonstration : Montrons d'abord l'unicité. (Elle découle directement du fait que $\leq$ est une relation d'ordre total sur $\mathbb{N}$.) Soit e_1 et e_2 deux tels éléments de E. Alors $e_1 \leq e_2$ (propriété de e_1) et $e_2 \leq e_1$ (propriété de e_2). Donc, $e_1 = e_2$. On en déduit qu'un tel élément, s'il existe, est unique.

Montrons maintenant l'existence. Soit P le prédicat à un paramètre libre défini par :

$$P(n) : \forall E\,(E \subset \mathbb{N} \wedge n \in E) \Rightarrow (\exists e \in E\, \forall x \in E\, e \leq x).$$

On se propose de montrer que $P(n)$ est vrai pour tout élément n de $\mathbb{N}$ par récurrence forte.

Montrons d'abord que $P(0)$ est vrai. Soit E un sous-ensemble de $\mathbb{N}$ tel que $0 \in E$. Pour tout élément x de E, on a $x \in \mathbb{N}$, donc $0 \leq x$. Donc, 0 est un élément minimal de E.

Soit n un élément de $\mathbb{N}$ et supposons que $P(m)$ est vrai pour tout élément m de $\mathbb{N}$ tel que $m \leq n$. Soit E un sous-ensemble de $\mathbb{N}$ tel que $n+1 \in E$. Alors,

- S'il existe un élément x de E tel que $x < n+1$, on a $x \leq n$, donc $P(x)$ est vrai, et donc E admet un élément minimal.
- Sinon, pour tout élément x de E, $x < n+1$ est faux, donc $n+1 < x$ est vrai, donc $n+1 \leq x$ et vrai ; $n+1$ est donc un élément minimal de E.

Dans les deux cas, E admet un élément minimal. On en déduit que $P(n+1)$ est vrai. Par récurrence forte, on en déduit que $P(n)$ est vrai pour tout élément n de $\mathbb{N}$.

Soit E un sous-ensemble non vide de $\mathbb{N}$. Puisque E est non vide, il contient au moins un élément n. Puisque E est un sous-ensemble de $\mathbb{N}$, $n \in \mathbb{N}$. Donc, $P(n)$ est vrai. Donc, E admet un élément minimal. Cela prouve le lemme.

□

Lemme : Tout sous-ensemble non-vide de $\mathbb{N}$ borné supérieurement admet un unique élément maximal.

Démonstration : On procède par récurrence sur une borne supérieure. La formule P que l'on veut démontrer peut s'écrire :

$$P(n) : \forall E\,((E \subset \mathbb{N}) \wedge (\forall e\,(e \in E) \Rightarrow (e \leq n))) \Rightarrow (\exists !\, m\,(m \in E) \wedge (\forall e\,(e \in E) \Rightarrow (e \leq m))).$$

Soit E un sous-ensemble non vide de $\mathbb{N}$ borné supérieurement par 0. Soit e un élément de E. On a $x \leq 0$, donc $x = 0$. Ainsi, $E = \varnothing$ ou $E = \{0\}$. Puisque E est non vide, on en déduit $E = \{0\}$. L'entier 0 est donc un élément maximal de E (puisque $0 \leq 0$) et cet élément maximal est unique (puisque E ne contient qu'un élément).

Soit n un entier naturel. On suppose que $P(n)$ est vrai. Soit E un sous-ensemble non vide de $\mathbb{N}$ borné supérieurement par $n+1$. Si $n+1 \notin E$, alors n est aussi une borne supérieure de E. En effet, soit x un élément de E, on a $x \leq n+1$, donc $x = n+1$ ou $x < n+1$. Puisque E ne contient pas $n+1$, on a $x < n+1$, et donc $x \leq n$. Puisque $P(n)$ est vrai, E admet donc un unique élément maximal.

Supposons maintenant que $n+1 \in E$. Alors, $n+1$ est un élément maximal de E. Puisque $\leq$ est une relation d'ordre total qur $\mathbb{N}$, cet élément est unique.

Dans les deux cas, $P(n+1)$ est donc vrai. Par récurrence, cela montre que $P(n)$ est vrai pout tout élément n de $\mathbb{N}$.

□

1.4.8 Addition

Définition de l'addition : Soit E l'ensemble des fonctions de $\mathbb{N}$ dans $\mathbb{N}$. On définit la suite Add d'éléments de E par récurrence de la manière suivante : [27]

- On définit Add(0) par : pour tout élément m de $\mathbb{N}$, $\mathrm{Add}(0)(m) = m$.

[27] Il s'agit bien d'une définition par récurrence, obtenue, en reprenant les notation du premier lemme de la section 1.4.6, avec

- e_0 égal à la fonction identité sur $\mathbb{N}$,
- f la fonction de $\mathbb{N} \times \mathscr{F}(\mathbb{N},\mathbb{N})$ vers $\mathscr{F}(\mathbb{N},\mathbb{N})$ définie par : pour tout élément n de $\mathbb{N}$ et tout élément g de $\mathscr{F}(\mathbb{N},\mathbb{N})$, $f(n,g)$ est la fonction définie par : pour tout élément m de $\mathbb{N}$, $f(n,g)(m) = g(m)+1$.

- Pour tout élément n de $\mathbb{N}$, on définit $\text{Add}(n+1)$ par : pour tout élément m de $\mathbb{N}$, $\text{Add}(n+1)(m) = \text{Add}(n)(m) + 1$.

Notons que, pour tout élément m de $\mathbb{N}$, on a $\text{Add}(1)(m) = m + 1$. Dans la suite, pour tous éléments n et m de $\mathbb{N}$, on notera l'entier $\text{Add}(n)(m)$ par $m+n$. Pour tous éléments n et m de $\mathbb{N}$, on a donc $m + 0 = m$ et $m + (n + 1) = (m + n) + 1$.

Lemme : Pour tout élément n de $\mathbb{N}$, on a $0 + n = n$.

Démonstration : On procède par récurrence. Soit P le prédicat à un paramètre libre n définit par : $P(n) : 0 + n = n$. Par définition de l'addition, $0 + 0 = 0$, donc $P(0)$ est vrai. Soit n un élément de $\mathbb{N}$ tel que $P(n)$ est vrai. On a par définition de l'addition : $0 + (n + 1) = (0 + n) + 1$. Puisque $P(n)$ est vraie, $0 + n = n$, donc, $0 + (n + 1) = n + 1$. Donc, $P(n + 1)$ est vraie. Par récurrence, on en déduit que $P(n)$ est vrai pour tout élément n de $\mathbb{N}$, et donc le lemme.

□

Lemme : Pour tout élément n de $\mathbb{N}$, on a $1 + n = n + 1$.

Démonstration : On procède par récurrence. Soit P le prédicat à un paramètre libre n définit par : $P(n) : 1 + n = n + 1$. Par définition de l'addition, $1 + 0 = 1$. Puisque $0 + 1 = 1$, $P(0)$ est vrai. Soit n un élément de $\mathbb{N}$ tel que $P(n)$ est vrai. On a par définition de l'addition : $1 + (n + 1) = (1 + n) + 1$. Puisque $P(n)$ est vraie, $1 + n = n + 1$, donc, $1 + (n + 1) = (n + 1) + 1$. Donc, $P(n + 1)$ est vraie. Par récurrence, on en déduit que $P(n)$ est vrai pour tout élément n de $\mathbb{N}$, et donc le lemme.

□

Lemme : L'addition est commutative : si n et m sont deux éléments de $\mathbb{N}$, alors $n + m = m + n$.

Démonstration : On procède par récurrence. Soit P le prédicat à un paramètre libre n définit par : $P(n) : \forall m \in \mathbb{N},\ n+m = m+n$. Soit m un élément de $\mathbb{N}$. On a $m + 0 = m$ et $0 + m = m$. Donc, $0 + m = m + 0$. On en déduit que $P(0)$ est vrai.

Soit n un élément de $\mathbb{N}$ tel que $P(n)$ est vrai. Montrons par récurrence que, pour tout élément m de $\mathbb{N}$, $(n + 1) + m = m + (n + 1)$. Cela montrera que $P(n + 1)$ est vrai. Par récurrence, on en déduira que $P(n)$ est vrai pour tout élément n de $\mathbb{N}$, et donc le lemme.

On a : $(n + 1) + 0 = n + 1$ et $0 + (n + 1) = n + 1$. La propriété attendue est donc vraie pour $m = 0$. Soit m un élément de $\mathbb{N}$ tel que $(n + 1) + m = m + (n + 1)$. On a : $(n + 1) + (m + 1) = ((n + 1) + m) + 1$. Par hypothèse de récurrence, cela donne $(n + 1) + (m + 1) = (m + (n + 1)) + 1$ En utilisant la définition de l'addition, il vient : $(n + 1) + (m + 1) = ((m + n) + 1) + 1$. Par ailleurs, $(m + 1) + (n + 1) = ((m + 1) + n) + 1$ par définition de l'addition. Puisque $P(n)$ est vraie, cela donne $(m + 1) + (n + 1) = (n + (m + 1)) + 1$. En utilisant à nouveau la définition de l'addition, il vient : $(m + 1) + (n + 1) = ((n + m) + 1) + 1$. Enfin, puisque $P(n)$ est vraie, $n + m = m + n$; on déduit donc $(n + 1) + (m + 1) = (m + 1) + (n + 1)$. Par récurrence, cela est vrai pour tout élément m de $\mathbb{N}$.

□

Lemme : L'addition est associative : si n, m et k sont trois éléments de $\mathbb{N}$, alors $(n + m) + k = n + (m + k)$.

Démonstration : On procède par récurrence. Soit P le prédicat à un paramètre libre k définit par : $P(k) : \forall n \in \mathbb{N},\ \forall m \in \mathbb{N},\ (n + m) + k = n + (m + k)$. Soit n et m deux éléments de $\mathbb{N}$. On a : $n + (m + 0) = n + m$ (car $m + 0 = m$) et $(n + m) + 0 = n + m$. Cela montre que $P(0)$ est vrai. Soit k un élément de $\mathbb{N}$ tel que $P(k)$ est vrai. Soit n et m deux éléments de $\mathbb{N}$. On a : $(n + m) + (k + 1) = ((n + m) + k) + 1$. Puisque $P(k)$ est vrai, cela implique $(n + m) + (k + 1) = (n + (m + k)) + 1$. Par définition de l'addition, il vient $(n + m) + (k + 1) = n + ((m + k) + 1)$. En utilisant à nouveau la définition de l'addition, on obtient : $(n + m) + (k + 1) = n + (m + (k + 1))$. Cela montre que $P(k + 1)$ est vrai. Par récurrence, on a donc montré que $P(k)$ est vrai pour tout élément k de $\mathbb{N}$.

□

Notons que la démonstration de la commutativité peut être simplifiée en admettant l'associativité (et n'a pas été utilisée pour montrer cette dernière) de la manière suivante. Soit P le prédicat à un paramètre libre n définit par : $P(n) : \forall m \in \mathbb{N},\ n+m = m+n$ et n un élément de $\mathbb{N}$ tel que $P(n)$ est vrai. Pour tout élément m de $\mathbb{N}$, on a alors $(n + 1) + m = n + (1 + m) = n + (m + 1) = (n+m)+1 = (m+n)+1 = m+(n+1)$. Donc, $P(n+1)$ est vraie. On montre ainsi que, pour tout élément n de $\mathbb{N}$, $P(n) \Rightarrow P(n+1)$, sans utiliser de seconde récurrence.

Lemme : Soit n et m deux éléments de $\mathbb{N}$ tels que $n \neq 0$. Alors $m + n > m$.

Démonstration : On procède par récurrence. Soit P le prédicat à un paramètre libre définit par : $P(n) : n = 0 \vee (\forall m \in \mathbb{N},\ m+n > m)$. Alors, $P(0)$ est vrai. Soit n un élément de $\mathbb{N}$ tel que $P(n)$ est vrai. Soit m un élément de $\mathbb{N}$. On a : $m + (n + 1) = (m + n) + 1$. Donc, $m + (n + 1) > m + n$. Puisque $P(n)$ est vrai, $n = 0$ (et donc $m + n = m$) ou $n \neq 0$ et $m + n > m$. Dans tous les cas, $m + n \geq m$. Donc, $m + (n + 1) > m$. On en déduit que $P(n + 1)$ est vrai. Par récurrence, $P(n)$ est vrai pour tout élément n de $\mathbb{N}$.

□

Corolaire : Soit n et m deux éléments de $\mathbb{N}$ tels que $n + m = 0$. Alors $n = 0$ et $m = 0$.

Démonstration : Si $m \neq 0$, on a donc $n + m > n$ d'après le lemme. Puisque $n \geq 0$, on en déduit que $n + m > 0$, ce qui contredit l'énoncé. Donc, $n = 0$. On montre de meme, en échangeant les rôles de n et m et en utilisant la commutativité de l'addition, que $m = 0$.

□

Lemme : Soit n et m deux éléments de $\mathbb{N}$. Alors $m + n \geq m$.

Démonstration : Si $n = 0$, $m + n = m$, donc $m + n \geq m$. Si $n \neq 0$, $m + n > m$ d'après le lemme précédent, donc $m + n \geq m$.

□

Lemme : Soit n et m deux éléments de $\mathbb{N}$. Alors $n + m \geq m$ et, si $n \neq 0$, $n + m > n$.

Démonstration : On se ramène aux deux lemmes précédents en notant que $n + m = m + n$ par commutativité de l'addition.

□

Lemme : Soit n, m et k trois éléments de $\mathbb{N}$ tels que $m + n = k + n$. Alors $m = k$.

Démonstration : Notons tout d'abord que, pour $n = 1$, le résultat a déjà été démontré section 1.4.4. Soit P le prédicat à un paramètre libre donné par, pour tout élément n de $\mathbb{N}$: $P(n) : \forall m \in \mathbb{N},\ \forall k \in \mathbb{N},\ m + n = k + n \Rightarrow m = k$. On veut montrer par récurrence sur n que $P(n)$ est vrai pour tout élément n de $\mathbb{N}$. Pour $n = 0$, le résultat est aisé à voir : soit m et k deux éléments de $\mathbb{N}$ tels que $m + 0 = k + 0$; alors, puisque $m + 0 = m$ et $k + 0 = k$, on a $m = k$. Donc, $P(0)$ est vrai. Soit n un élément de $\mathbb{N}$ tel que $P(n)$ est vrai. Soit m et k deux éléments de $\mathbb{N}$ tels que $m + (n + 1) = k + (n + 1)$. Par associativité de l'addition, on a $(m + n) + 1 = (k + n) + 1$. Donc, $m + n = k + n$. Puisque $P(n)$ est vrai, on a donc $m = k$. Donc, $P(n + 1)$ est vrai. Par récurrence, on en déduit que $P(n)$ est vrai pour tout élément n de $\mathbb{N}$.

□

Lemme : Soit n, m et k trois éléments de $\mathbb{N}$. On a $(n + k \leq m + k) \Leftrightarrow (n \leq m)$.

Démonstration : On procède par récurrence sur k. Soit n et m deux entiers naturels. Soit P le prédicat à un paramètre libre k définit par : $P(k) : (n + k \leq m + k) \Leftrightarrow (n \leq m)$.

$P(0)$ est évidemment vrai puisqu'il sécrit $(n \leq m) \Leftrightarrow (n \leq m)$.

Soit k un entier naturel tel que $P(k)$ est vrai. Si $n + (k + 1) \leq m + (k + 1)$, alors, par transitivité de l'addition, $(n + k) + 1 \leq (m + k) + 1$. Puisque $n + k < (n + k) + 1$, on a donc $n + k < (m + k) + 1$, et donc $n + k \leq m + k$.

Sinon, et puisque $\leq$ est une relation d'ordre total, on a $m + (k + 1) \leq n + (k + 1)$. Par le même argument (en échangeant le rôles de n et m), il vient $m + k \leq n + k$. En outre, $m + k \neq n + k$ (sans quoi on aurait $(m + k) + 1 = (n + k) + 1$, donc $n + (k + 1) = m + (k + 1)$, donc $n + (k + 1) \leq m + (k + 1)$). Donc, $n + k \leq m + k$ est faux.

On a donc : $(n + (k + 1) \leq m + (k + 1)) \Leftrightarrow (n + k \leq m + k)$. Puisque $P(k)$ est vrai, on en déduit $(n + (k + 1) \leq m + (k + 1)) \Leftrightarrow (n \leq m)$. Donc, $P(k + 1)$ est vrai.

Par récurrence, $P(k)$ est ainsi vrai pour tout entier naturel k.

□

Corolaire : Avec les mêmes notations, en prenant la négation des deux côtés, il vient : $(n + k) \geq (m + k) \Leftrightarrow (n \geq m)$. En outre, puisque $(n = m) \Rightarrow (n + k = m + k)$ et, d'après un lemme précédent, $(n + k = m + k) \Rightarrow (n = m)$, on a $(n + k = m + k) \Leftrightarrow (n = m)$. Donc, $(n + k) < (m + k) \Leftrightarrow (n < m)$ et $(n + k) \geq (m + k) \Leftrightarrow (n \geq m)$.

1.4.9 Soustraction

Lemme : Soit n et m deux éléments de $\mathbb{N}$ tels que $m \leq n$. Alors il existe un unique élément k de $\mathbb{N}$ tel que $n = m + k$.

Définition : Soit n et m deux éléments de $\mathbb{N}$ tels que $m \leq n$. On note $n-m$ l'élément k de $\mathbb{N}$ tel que $n = m + k$.

Démonstration :

- *Unicité :* Soit k et l deux éléments de $\mathbb{N}$ tels que $n = m + k$ et $n = m + l$. Alors, par symétrie et associativité de l'égalité, $m + k = m + l$. Par commutativité de l'addition, on a donc $k + m = l + m$. Donc, $k = l$.
- *Existence :* On procède par récurrence sur n. Le prédicat P à un paramètre libre que nous souhaitons montrer est $P(n) : \forall m \in \mathbb{N},\ m \leq n \Rightarrow (\exists k \in \mathbb{N},\ m + k = n)$. Considérons d'abord le cas $n = 0$. Soit m un élément de $\mathbb{N}$ tel que $m \leq n$, alors $m = 0$. Donc, $m + 0 = 0 = n$. Le résultat attendu est donc vrai pour $n = 0$. Soit n un élément de $\mathbb{N}$ tel que $P(n)$ est vrai. Soit m un élément de $\mathbb{N}$ tel que $m \leq n + 1$. Alors, $m = n + 1$ ou $m < n + 1$. Dans le premier cas, $m + 0 = n + 1$. Dans le second cas, $m \leq n$. On peut donc choisir un élément l de $\mathbb{N}$ tel que $m + l = n$. Alors, par associativité de l'addition,

$m + (l + 1) = n + 1$. Dans tous les cas, il existe donc bien un élément k de $\mathbb{N}$ tel que $m + k = n + 1$. Le résultat attendu est donc vrai pour $n + 1$. Par récurrence, il l'est pour tout élément n de $\mathbb{N}$.

□

Lemme : Soit n un entier naturel. Alors, $n - 0 = n$ et $n - n = 0$.

Démonstration : Tout d'abord, on a $0 \leq n$ puisque n est un entier naturel et $n \leq n$ puisque $n = n$. Donc, $n - 0$ et $n - n$ existent. On a : $n = 0 + n$, donc $n - 0 = n$, et $n = n + 0$, donc $n - n = 0$.

□

Remarque : Soit n et m deux entiers naturels. Alors, par définition, $(n + m) - m = n$.

Lemme : Soit n, et m deux éléments de $\mathbb{N}$ tels que $n > m$ et $m > 0$. Alors $n - m < n$.

Démonstration : On a : $n = (n - m) + m$. Puisque $m > 0$, on en déduit $n > n - m$.

□

Lemme : Soit n, m et k trois entiers naturels tels que $n \geq m$. Alors, $n \geq m + k \Leftrightarrow (n - m) \geq k$ et, si $n \geq m + k$, $n - (m + k) = (n - m) - k$.

Démonstration :

- Si $n - m \geq k$, alors $(n - m) + m \geq k + m$, donc $n \geq k + m$. Sinon, $n - m < k$, donc $(n - m) + m < k + m$, et donc $n < k + m$.
- Si $n - m \geq k$, on a : $((n - m) - k) + (m + k) = ((n - m) - k) + (k + m) = (((n - m) - k) + k) + m = (n - m) = m = n$.

□

Lemme : Soit n, m et k trois entiers naturels tels que $n \leq m$. Alors, $k + (m - n) = (k + m) - n$.

Démonstration : Tout d'abord, $k + m \geq m$ et $m \geq n$, donc $k + m \geq n$. On a : $(k + (m - n)) + n = k + ((n - m) + n)k + m$.

□

Lemme : Soit n, m et k trois éléments de $\mathbb{N}$ tels que $m > k$. Alors $m + n > k + n$.

Démonstration : Puisque $m > k$, on peut choisir un entier naturel q tel que $m = k + q$. En outre puisque $m \neq k$, $q \neq 0$. Donc, $n + m = n + (k + q)$. Par associativité de l'addition, il vient $n + m = (n + k) + q$. Puisque $q > 0$, on en déduit $n + m > n + k$.

□

Corolaire : Soit n, m et k trois éléments de $\mathbb{N}$ tels que $m \geq k$. Alors $m + n \geq k + n$.

Démonstration : Puisque $m \geq k$, on a $m = k$ ou $m > k$. Si $m = k$, on a $m + n = k + n$. Si $m > k$, on a $m + n > k + n$ d'après le lemme précédent. Dans les deux cas, on a bien $m + n \geq k + n$.

□

Lemme : Soit n, m et k trois entiers naturels tels que $n \leq m$. Alors, $(n - m) + k = (n + k) - m$.

Démonstration : Tout d'abord, $n \geq m$ et $n + k \geq n$, donc $n + k \geq m$. On a : $((n - m) + k) + m = ((n - m) + m) + k = n + k$ Donc, $(n - m) + k = (n + k) - m$.

□

Lemme : Soit n, m et k trois entiers naturels tels que $n \geq m$ et $n - m \geq k$. Alors, $(n - m) - k = n - (m + k)$.

Démonstration : Tout d'abord, puisque $n - m \geq k$, on a $(n - m) + m \geq k + m$, donc $n \geq k + m$. Donc, $n - (m + k)$ existe. En outre, on a $((n - m) - k) + (m + k) = ((n - m) - k) + (k + m) = (((n - m) - k) + k) + m = (n - m) + m = n$. Donc, $(n - m) - k = n - (m + k)$.

□

Lemme : Soit n, m et k trois entiers naturels tels que $n \leq m$ et $k \geq m - n$. Alors, $k - (m - n) = (k + n) - m$.

Démonstration : Tout d'abord, puisque $k \geq m - n$, on a $k + n \geq m$. On a : $(k - (m - n)) + m = (k - (m - n)) + ((m - n) + n) = ((k - (m - n)) + (m - n)) + n = k + n$ et $((k + n) - m) + m = k + n$. Donc, $(k - (m - n)) + m = (k + n) - m$.

□

Lemme : Soit n, m et k trois entiers naturels tels que $n \geq m$, $n \geq k$ et $n - m = n - k$. Alors, $m = k$.

Démonstration : Puisque $n - m = n - k$, on a $n = (n - k) + m$. Donc, $n = (n + m) - k$. Donc, $n + k = n + m$. On en déduit que $k = m$.

□

Lemme : Soit n, m et k trois éléments de $\mathbb{N}$ tels que $m + n > k + n$. Alors $m > k$ Avec le corolaire précédent, on a donc $(m + n > k + n) \Leftrightarrow (m > k)$.

Démonstration : On procède par l'absurde. Si $m > k$ est faux, alors $m \leq k$ est vrai, donc $m + n \leq k + n$ est vrai, ce qui est en conradiction avec $m + n > k + n$.

□

Corolaire : Soit n, m et k trois éléments de $\mathbb{N}$ tels que $m + n \geq k + n$. Alors $m \geq k$. Avec le corolaire précédent, on a donc $(m + n \geq k + n) \Leftrightarrow (m \geq k)$.

Démonstration : Puisque $m + n \geq k + n$, on a $m + n = k + n$ ou $m + n > k + n$. Si $m + n = k + n$, on a $m = k$. Si $m + n > k + n$, on a $m > k$ d'après le lemme précédent. Dans les deux cas, on a bien $m + n \geq k + n$.

□

Lemme : Soit n, m et k trois éléments de $\mathbb{N}$ tels que $n \geq m$ et $n \geq k$. Alors $(n - m \geq n - k) \Leftrightarrow (m \leq k)$, $(n - m = n - k) \Leftrightarrow (m = k)$ et $(n - m < n - k) \Leftrightarrow (m < k)$.

Démonstration : Supposons d'abords $m \leq k$. Alors, $((n - k) + (k - m)) + m = (n - k) + ((k - m) + m) = (n - k) + k = n$. Donc, $(n - k) + (k - m) = n - m$ Donc, $n - k \leq n - m$, donc $n - m \geq n - k$.

Supposons mantenant $n - m \geq n - k$. Alors, $m + ((n - m) - (n - k)) = (m + (n - m)) - (n - k) = n - (n - k) = k$. Donc, $m \leq k$. Cela montre que $(n - m \geq n - k) \Leftrightarrow (m \leq k)$.

Par ailleurs, si $m = k$, alors $n - m = n - k$ et, si $n - m = n - k$, alors $n + k = n + m$ (obtenu en ajoutant $k + m$ des deux côtés) et donc $k = m$. Cela montre $(n - m = n - k) \Leftrightarrow (m = k)$.

La troisième équivalence découle directement des deux précédentes en notant que, pour tous entiers naturels a et b, $a < b \Leftrightarrow (a \leq b \wedge a \neq b)$.

□

Lemme : Soit n un entier naturel. On note (ici seulement) $\mathbb{N}_{\geq n}$ l'ensemble défini par : $\mathbb{N}_{\geq n} = \{m \in \mathbb{N} | m \geq n\}$. Alors, il existe une bijection entre $\mathbb{N}$ et $\mathbb{N}_{\geq n}$.

Démonstration : Soit f la fonction de $\mathbb{N}$ vers $\mathbb{N}_{\geq n}$ définie par : pour tout entier naturel m, $f(m) = n + m$. (Notons que $n + m \geq n$ pour tout entier naturel m, donc $f(m)$ est bien un élément de $\mathbb{N}_{\geq n}$.) Montrons que f est une bijection.

Soit l et k deux entier naturels tels que $f(l) = f(k)$. Alors, $n + l = n + k$. Donc, $l = k$. Cela montre que f est injective.

Soit m un élément de $\mathbb{N}_{\geq n}$. Alors, $m \geq n$. Soit k l'entier naturel $m - n$. On a : $f(k) = n + (m - n) = m$. Donc, m a un antécédant par f. Cela montre que f est injective.

La fonction f est donc injective et surjective. Il s'agit donc d'une bijection.

□

La figure 1.1 illustre la fonction décrite dans cette démonstration pour $n = 0$, $n = 1$ et $n = 2$.

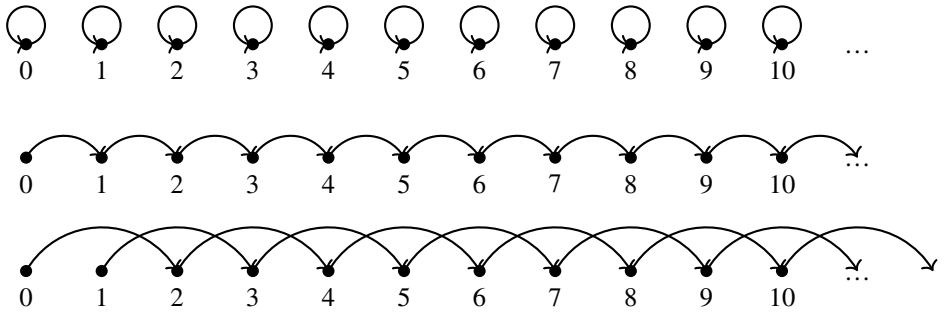


Figure 1.1 Illustration de bijections de $\mathbb{N}$ vers quelques-uns de ses sous-ensembles : la fonction identité sur $\mathbb{N}$ et les fonctions $f_1 : \mathbb{N} \to \mathbb{N}^*$ et $f_2 : \mathbb{N} \to \mathbb{N} \backslash \{0, 1\}$ définies par : pour tout entier naturel x, $f_1(x) = x + 1$ et $f_2(x) = x + 2$.

1.4.10 Multiplication

Définition de la multiplication : Soit E l'ensemble des fonctions de $\mathbb{N}$ dans $\mathbb{N}$. On définit la suite Mul d'éléments de E par récurrence de la manière suivante :

- Pour tout élément m de $\mathbb{N}$, $\text{Mul}(0)(m) = 0$.
- Pour tout élément n de $\mathbb{N}$, pour tout élément m de $\mathbb{N}$, $\text{Mul}(n+1)(m) = \text{Mul}(n)(m) + m$.

Notons que, pour tout élément m de $\mathbb{N}$, on a $\text{Mul}(1)(m) = m$. Dans la suite, si m et n sont deux éléments de $\mathbb{N}$, on notera $m \times n$ l'entier $\text{Mul}(n)(m)$. Pour tous éléments n et m de $\mathbb{N}$, on a donc $m \times 0 = 0$, $m \times 1 = m$ et $m \times (n+1) = (m \times n) + m$.

La multiplication est prioritaire sur l'addition. Par exemple, si a, b et c sont trois éléments de $\mathbb{N}$, $a \times b + c$ est équivalent à $(a \times b) + c$ et $a + b \times c$ à $a + (b \times c)$. Le symbole $\times$ est parfois omis quand il n'y a pas de confusion possible. Ainsi, si n et m sont deux entiers naturels, $n \times m$ pourra s'écrire nm.

Lemme : Pour tout entier naturel n, on a $0 \times n = 0$.

Démonstration : On procède par récurrence sur n. Puisque 0 est un entier naturel et par définition de la multiplication, $0 \times 0 = 0$. Donc, le résultat attendu est vrai pour $n = 0$. Soit n un entier naturel tel que $0 \times n = 0$. Alors, $0 \times (n+1) = 0 + 0$. Puisque $0 + 0 = 0$, on en déduit $0 \times (n+1) = 0$. Par récurrence, le résultat attendu est donc vrai pour tout entier naturel.

□

Lemme : Pour tous entiers naturels n et m, on a $(m+1) \times n = (m \times n) + n$.

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre défini par : $P(n) : \forall m \in \mathbb{N},\ (m+1) \times n = (m \times n) + n$. Pour tout entier naturel m, on a $(m+1) \times 0 = 0$ et $(m \times 0) + 0 = 0 + 0 = 0$. Donc, $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. Soit m un entier naturel. Par définition de la multiplication, $(m+1) \times (n+1) = ((m+1) \times n) + (m+1)$. Puisque $P(n)$ est vrai, cela donne $(m+1) \times (n+1) = ((m \times n) + n) + (m+1)$. En utilisant deux fois l'associativté et la commutativité de l'addition, cela donne $(m+1) \times (n+1) = ((m \times n) + m) + (n+1)$. Utilisant à nouveau la définition de la multiplication, cela se récrit en : $(m+1) \times (n+1) = (m \times (n+1)) + (n+1)$. Cela étant vrai pour tout élémnt m de $\mathbb{N}$, on en déduit que $P(n+1)$ est vrai.

Par récurrence, $P(n)$ est donc vrai pour tout entier naturel n, ce qui prouve le lemme.

□

Lemme : La multiplication est commutative : pour tous entiers naturels n et m, on a $m \times n = n \times m$.

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre défini par : $P(n) : \forall m \in \mathbb{N},\ m \times n = n \times m$. Pour tout entier naturel m, on a $m \times 0 = 0$ et $0 \times m = 0$. Donc, $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. Soit m un entier naturel. On a : $m \times (n+1) = (m \times n) + m$. Puisque $P(n)$ est vrai, $m \times n = n \times m$. Donc, $m \times (n+1) = (n \times m) + m$. En utilisant le lemme précédent, il vient : $m \times (n+1) = (n+1) \times m$. On en déduit que $P(n+1)$ est vrai.

Par récurrence, $P(n)$ est donc vrai pour tout entier naturel n.

□

Corolaire : Pour tout entier naturel n, $1 \times n = n \times 1 = n$.

Corolaire : Pour tous entiers naturels n et m, $(n+1) \times m = m \times (n+1) = (m \times n) + m = (n \times m) + m$.

Lemme : La multiplication est distributive sur l'addition : pour tous entiers naturels n, m et k, on a $n \times (m+k) = (n \times m) + (n \times k)$. (Puisque la multiplication est commutative, on en déduit que, pour tous entiers naturels n, m et k, on a $(m+k) \times n = (m \times n) + (k \times n)$.)

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre libre défini par : $P(n) : \forall m \in \mathbb{N},\ \forall k \in \mathbb{N},\ n \times (m+k) = (n \times m) + (n \times k)$.

Soit m et k deux entiers naturels. On a : $0 \times (m+k) = 0$ et $(0 \times m) + (0 \times k) = 0 + 0 = 0$. Donc, $0 \times (m+k) = (0 \times m) + (0 \times k)$. Donc, $P(0)$ est vrai.

Soit n un entier naturel et supposons que $P(n)$ est vrai. Soit m et k deux enters naturels. Alors, $(n+1) \times (m+k) = (n \times (m+k)) + (m+k)$. Donc, puisque $P(n)$ est vrai, $(n+1) \times (m+k) = ((n \times m) + (n \times k)) + (m+k)$. Puisque l'addition est associative et commutative, cela implique $(n+1) \times (m+k) = ((n \times m) + m) + ((n \times k) + k)$. Donc, $(n+1) \times (m+k) = ((n+1) \times m) + ((n+1) \times k)$. Donc, $P(n+1)$ est vrai.

Par récurrence, on en déduit que $P(n)$ est vrai pour tout entier naturel n, et donc le lemme.

□

Lemme : La multiplication est associative : pour tous entiers naturels n, m et k, on a $n \times (m \times k) = (n \times m) \times k$.

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre libre défini par : $P(n) : \forall m \in \mathbb{N},\ \forall k \in \mathbb{N},\ n \times (m \times k) = (n \times m) \times k$.

Soit m et k deux entiers naturels. On a : $0 \times (m \times k) = 0$ et $(0 \times m) \times k = 0 \times k = 0$. Donc, $0 \times (m \times k) = (0 \times m) \times k$. On en déduit que $P(0)$ est vrai. Soit n un entier naturel et supposons que $P(n)$ est vrai. Soit m et k deux enters naturels. Alors, $(n+1) \times (m \times k) = (n \times (m \times k)) + (m \times k)$. Puisque $P(n)$ est vrai, cela donne $(n+1) \times (m \times k) = ((n \times m) \times k) + (m \times k)$. En utilisant la distributivité de la multiplication sur l'addition, ceci devient : $(n+1) \times (m \times k) = ((n \times m) + m) \times k$, et donc $(n+1) \times (m \times k) = ((n+1) \times m) \times k$. On en déduit que $P(n+1)$ est vrai.

Par récurrence, on en déduit que $P(n)$ est vrai pour tout entier naturel n, et donc le lemme.

□

Lemme : Soit n, m et k trois entiers naturels. Si $n \neq 0$ et $m > k$, alors $n \times m > n \times k$.

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre défini par : $P(n) : n \neq 0 \Rightarrow \forall m \in \mathbb{N},\ \forall k \in \mathbb{N},\ m > k \Rightarrow n \times m > n \times k$. Puisque $0 \neq 0$ est fausse, $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. Si $n = 0$, $n + 1 = 1$; alors, soit m et k deux entiers naturels tels que $m > k$, puisque $nm = m$ et $nk = k$, on a $nm > nk$, donc $P(n+1)$ est vrai. Supposons maintenant $n \neq 0$. Soit m et k deux entiers naturels tels que $m > k$. Alors, $nm > nk$. Donc, $nm + k > nk + k$. Puisque $m > k$, on a $m \geq k$, donc $k \leq m$, donc, on peut choisir un élément q de $\mathbb{N}$ tel que $m = k + q$. Puisque $nm + k + q \geq nm + k$, on en déduit $nm + m > nk + k$. Donc, $(n+1)m > (n+1)k$. Cela montre que $P(n) \Rightarrow P(n+1)$ pour tout entier naturel n.

Par récurrence, on en déduit que $P(n)$ est vrai pour tout entier naturel n, et donc le lemme.

□

Corolaire : Soit n, m et k trois entiers naturels tels que $m > k$. Alors $n \times m \geq n \times k$.

Démonstration : Si $n \neq 0$, on a $n \times m > n \times k$ d'après le lemme, et donc $n \times m \geq n \times k$. Si $n = 0$, on a $n \times m = n \times k = 0$, et donc $n \times m \geq n \times k$. Le résultat attendu est donc vrai dans les deux cas.

□

Corolaire : Soit n et m deux entiers naturels tels que $n \times m = 0$. Alors $n = 0$ ou $m = 0$.

Démonstration : Supposons par l'absurde $n \neq 0$ et $m \neq 0$. Alors, $m > 0$, donc, d'après le lemme précédent, $n \times m > n \times 0$, donc $n \times m > 0$, ce qui contredit l'énoncé.

□

Corolaire : Soit a, b, c et d quatre entiers naturels tels que $a > c$ et $b > d$. Alors $ab > cd$.

Démonstration : Puisque $a > c$, $a > 0$. Donc, puisque $b > d$, $a \times b > a \times d$. En outre, puisque $a > c$, $a \times d \geq c \times d$. Donc, $a \times b > c \times d$.

□

Corolaire : Soit n, m et k trois entiers naturels tels que $n \neq 0$ et $n \times m = n \times k$. Alors $m = k$.

Démonstration : On ne peut avoir $m > k$ car cela impliquerait $nm > nk$, donc $m \leq k$. De même, ne peut avoir $k > m$ car cela impliquerait $nk > nm$; donc $k \leq m$. On en déduit que $m = k$.

□

Corolaire : Soit n et m deux entiers naturels tels que $n > 1$ et $m > 0$. Alors $n \times m > m$.

Démonstration : Puisque $m > 0$ et $n > 1$, $m \times n > m \times 1$, ce qui donne $n \times m > m$.

□

Corolaire : Soit n et m deux entiers naturels tels que $n \geq 1$. Alors $n \times m \geq m$.

Démonstration : Si $m = 0$, on a $n \times m = 0$, donc $n \times m = m$. Si $n = 1$, on a $n \times m = m$. Si aucune de ces conditions n'est satisfaite, $m > 0$ et $n > 1$, donc, d'après le corolaire précédent, $n \times m > m$. Dans tous les cas, on a bien $n \times m \geq m$.

□

Définition (factoriel d'un entier naturel) : On définit par récurrence le factoriel d'un entier naturel, noté par un point d'exclamation à sa droite, de la manière suivante[28] :

- On pose $0! = 1$.
- Pour tout entier naturel n, on pose $(n+1)! = (n!) \times (n+1)$.

[28] Il s'agit bien d'une définition par récurrence, obtenue en prenant (avec les notations du lemme de la section 1.4.6) $E = \mathbb{N}$, $e_0 = 1$ et pour f la fonction de $\mathbb{N} \times \mathbb{N}$ vers $\mathbb{N}$ définie par : $\forall x \in \mathbb{N}\, \forall y \in \mathbb{N}\ f(x,y) = y \times (x+1)$.

Le factoriel est prioritaire sur la multiplication et sur l'addition.

Lemme : Soit n, m et k trois entiers naturels tels que $m \geq k$. Alors, $n(m-k) = nm - nk$.

Démonstration : Tout d'abord, puisque $m \geq k$, $nm \geq mk$, donc $nm - nk$ existe.

Montrons l'égalité par récurrence sur n. Soit P le prédicat à un paramètre libre définit par : $P(n) : \forall m \in \mathbb{N} \forall k \in \mathbb{N}\, m \geq k \Rightarrow n(m-k) = nm - nk$.

Soit m et k deux entiers naturels tels que $m \geq k$. On a $0 \times (m-k) = 0$ et $0 \times m + 0 \times = 0 + 0 = 0$. Donc, $P(0)$ est vrai.

Soit n un enitier naturel tel que $P(n)$ est vrai. Soit m et k deux entiers naturels tels que $m \geq k$. Alors, $(n+1)(m-k) = n(m-k) + (m-k)$. Puisque $P(n)$ est vrai, il vient : $(n+1)(m-k) = (nm - nk) + (m-k)$. Donc, $(n+1)(m-k) + (n+1)k = (nm - nk) + (m-k) + (n+1)k = (nm - nk) + (m-k) + nk + k = (nm - nk) + nk + (m-k) + k = nm + m = (n+1)m$. Donc, $(n+1)(m-k) = (n+1)m - (n+1)k$. On en déduit que $P(n+1)$ est vrai.

Par récurrence, $P(n)$ est donc vrai pour tout élément n de $\mathbb{N}$, ce qui prouve le lemme.

□

1.4.10.1 Puissance

Puissance d'entiers naturels : Soit E l'ensemble des fonctions de $\mathbb{N}$ dans $\mathbb{N}$. On définit la suite Exp d'éléments de E par récurrence de la manière suivante :

- Pour tout élément m de $\mathbb{N}$, $\text{Exp}(0)(m) = 1$.
- Pour tout élément n de $\mathbb{N}$, pour tout élément m de $\mathbb{N}$, $\text{Exp}(n+1)(m) = \text{Exp}(n)(m) \times m$.

Notons que, pour tout élément m de $\mathbb{N}$, on a $\text{Exp}(1)(m) = m$. Dans la suite, pour tous éléments n et m de $\mathbb{N}$, on notera l'entier $\text{Exp}(n)(m)$ par m^n. Pour touts éléments n et m de $\mathbb{N}$, on a donc $m^0 = 1$, $m^1 = m$ et $m^{n+1} = m^n \times m$. L'exponentiation est prioritaire sur la multiplication et l'addition. Par exemple, si a, b et c sont trois éléments de $\mathbb{N}$, $a^b \times c$ est équivalent à $(a^b) \times c$ et $a^b + c$ est équivalent à $(a^b) + c$.

Lemme : Pour tout entier naturel n, $1^n = 1$.

Démonstration : On procède par récurrence sur n. Pour $n = 0$, le résultat est vrai par définition de la puissance. Soit m un entier naturel tel que $1^m = 1$. Alors $1^{m+1} = 1^m \times 1 = 1 \times 1 = 1$. Le résultat est donc vrai pour $n = m + 1$. Par récurrence, on en déduit qu'il est vrai pour tout entier naturel n.

□

Lemme : Pour tout entier naturel n, $0^{n+1} = 0$.

Démonstration : Soit n un entier naturel. On a : $0^{n+1} = 0^n \times 0$. Puisque 0^n est un entier naturel, $0^n \times 0 = 0$. Donc, $0^{n+1} = 0$.

□[medium]

Corolaire : Soit n un entier naturel tel que $n \neq 0$. Alors, $n > 0$, donc $n - 1$ existe et est un entier naturel. Soit $m = n - 1$. On a : $0^n = 0^{m+1}$. Donc, $0^n = 0$.

Lemme : Soit n et m deux entiers naturels tels que $m \neq 0$. Alors $m^n \neq 0$.

Démonstration : On procède par récurrence qur n. Pour $n = 0$, le résultat est évident car $m^0 = 1$. Supposons le résultat vrai pour un entier naturel n. Alors, $m^{n+1} = m^n \times m$. Puisque $m^n \neq 0$ et $m \neq 0$, $m^{n+1} \neq 0$. Par récurrence, on en déduit le lemme.

□

Lemme : Soit n, m et p trois entiers naturels. Alors, $p^{n+m} = p^n \times p^m$.

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre libre défini par : $P(n) : \forall p \in \mathbb{N}, \forall m \in \mathbb{N},\ p^{n+m} = p^n \times p^m$. Soit p et m deux entiers naturels. Puisque $0 + m = m$, on a $p^{0+m} = p^m$. Par ailleurs, puisque $p^0 = 1$, $p^0 \times p^m = p^m$. Donc, $p^{0+m} = p^0 \times p^m$. Cela montre que $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. On veut montrer que $P(n+1)$ est vrai. Soit m et p deux entiers naturels. Par commutativité et transitivité de l'addition, on a : $p^{m+(n+1)} = p^{m+(1+n)} = p^{(m+1)+n}$. Puisque $P(n)$ est vrai, on en déduit que $p^{m+(n+1)} = p^{m+1} \times p^n$. Par définition de la puissance d'entiers, cela donne $p^{m+(n+1)} = (p^m \times p) \times p^n$. En utilisant l'associativité et la commutativité de la multiplication, il vient : $p^{m+(n+1)} = p^m \times (p^n \times p)$. Enfin, utiliser à nouveau la définition de la puissance d'entiers donne : $p^{m+(n+1)} = p^m \times p^{n+1}$. Cela montre que $P(n+1)$ est vrai. Par récurrence, le prédicat $P(n)$ est donc vrai pour tout entier naturel n, ce qui prouve le lemme.

□

Lemme : Soit n, m et p trois entiers naturels tels que $m > p$. Alors, $m^{n+1} > p^{n+1}$.

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre défini par : $P(n) : \forall m \in \mathbb{N}, \forall p \in \mathbb{N}, m > p \Rightarrow m^{n+1} > p^{n+1}$. Soit m et p deux entiers naturels tels que $m > p$. On a $m^{0+1} = m^1 = m$ et $p^{0+1} = p^1 = p$. Donc, $m^{0+1} > p^{0+1}$. On en déduit que $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. Soit m et p deux entiers naturels tels que $m > p$. On a $m^{(n+1)+1} = m^{n+1} \times m$ et $p^{(n+1)+1} = p^{n+1} \times p$. Puisque $P(n)$ est vrai, on a $m^{n+1} > p^{n+1}$. Donc, $m^{(n+1)+1} > p^{n+1} \times m$. Puisque $m > p$, $p^{n+1} \times m \geq p^{n+1} \times p$, et donc $p^{n+1} \times m \geq p^{(n+1)+1}$. Donc, $m^{(n+1)+1} > p^{(n+1)+1}$. On en déduit que $P(n+1)$ est vrai.

Par récurrence, $P(n)$ est donc vrai pour tout entier naturel n, ce qui prouve le lemme.

□

Corolaire : Soit n un entier naturel tel que $n \neq 0$. Alors, $n > 0$, donc $n - 1$ existe et est un entier naturel. Soit $q = n - 1$. Soit m et p deux entiers naturels tels que $m > p$. Alors, $m^n = m^{q+1}$ et $p^n = p^{q+1}$. D'après le lemme précédent, on en déduit $m^n > p^n$.

Corolaire : Soit m et p deux entiers naturels tels que $m \geq p$. Par définition de la puissance, $m^0 = p^0 = 1$. En outre, si $m = p$, alors $m^n = p^n$ pour tout entier naturel n et, si $m > p$, $m^n > p^n$ pour tout entier naturel n distinct de 0 d'après le corolaire précédent. On en déduit que, pour tout entier naturel n, $m^n \geq p^n$.

Lemme : Soit n, m et p trois entiers naturels tels que $m > p$. Alors, si $n > 1$, $n^m > n^p$. (Rappelons que l'on a : $1^m = 1^p = 1$.)

Démonstration : On procède par récurrence sur m. Soit P le prédicat à un paramètre défini par : $P(m) : \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, (m > p) \wedge (n > 1) \Rightarrow n^m > n^p$. Pour $m = 0$, il n'existe aucun entier naturel p tel que $m > p$, donc $P(0)$ est vrai.

Soit m un entier naturel tel que $P(m)$ est vrai. Soit n et p deux entiers naturels tels que $m + 1 > p$ et $n > 1$. Alors, $p = m$ ou $p < m$. Dans le second cas, puisque $P(m)$ est vrai, on a $n^m > n^p$. Donc, dans les deux cas, $n^m \geq n^p$. En outre, $n \neq 0$, donc $n^m \neq 0$. Puisque $n > 1$ et $n^{m+1} = n^m \times n$, on en déduit que $n^{m+1} > n^m$, et donc $n^{m+1} > n^p$. Donc, $P(m+1)$ est vrai.

Par récurrence, $P(m)$ est donc vrai pour tout entier naturel m.

□

1.4.11 Puissances de fonctions

Soit E un ensemble et f une fonction de E vers E. On définit les puissances de f, f^n, pour $n \in \mathbb{N}$ de la manière suivante :

- f^0 est la fonction identité, qui à tout élément x de E associe x.
- Pour tout élément n de $\mathbb{N}$, $f^{n+1} = f \circ f^n$. (Cela définit bien une fonction de E vers E, commecomposée de deux fonctions de E vers E.)

(Il s'agit d'une définition par récurrence d'une suite de fonctions de E vers E.) Notons que, pour tout entier naturel n tel que $n \neq 0$, on a $f^n = f \circ f^{n-1}$ (puisque n = (n-1) + 1). Notons aussi que $f^1 = f$. La puissance est prioritaire sur $\circ$.

Lemme : Soit E un ensemble et f une fonction de E vers E. Soit n un entier naturel. Alors, $f^n \circ f = f^{n+1}$.

Démonstration : On procède par récurrence sur n. Soit P le prédicat à un paramètre libre défini par : $P(n) : f^n \circ f = f^{n+1}$. Les deux fonctions $(f^0) \circ f$ et f^1 sont deux fonctions de E dans E (la première, comme composée de fonctions de E dans E). Soit x un élément de E. On a : $(f^0 \circ f)(x) = f^0(f(x)) = f(x) = f^1(x)$. Donc, $f^0 \circ f = f^1$. Donc, et puisque $1 = 0 + 1$, $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. Les deux fonctions $(f^{n+1}) \circ f$ et $f^{(n+1)+1}$ sont deux fonctions de E dans E (la première, comme composée de fonctions de E dans E). En outre, on a $f^{(n+1)+1} = f \circ f^{n+1}$. Puisque $P(n)$ est vrai, cela donne $f^{(n+1)+1} = f \circ (f^n \circ f)$. Puisque la composition de fonctions est associative, cela donne : $f^{(n+1)+1} = (f \circ f^n) \circ f$. Enfin, en utilisant la définition de la puissance de fonction, il vient : $f^{(n+1)+1} = f^{n+1} \circ f$. Cela montre que $P(n+1)$ est vrai.

Par récurrence, on conclut que $P(n)$ est vrai pour tout entier naturel n, ce qui prouve le lemme.

□

Lemme : Soit E un ensemble et f une fonction de E vers E. Soit n et m deux entiers naturels. Alors, $f^{n+m} = (f^n) \circ (f^m)$.

Démonstration : *(La démonstration est essentiellement identique à celle donnée pour la puissance d'entiers, en utilisant l'associativité de $\circ$ et le résultat ci-dessus en guise de commutativité. Nous la donnons ici explicitement afin d'être complets.)*

On procède par récurrence sur n. Soit P le prédicat à un paramètre libre défini par : $P(n) : \forall m \in \mathbb{N}, f^{n+m} = f^n \circ f^m$. Puisque f^0 est la fonction identité, on a $f^0 \circ f^m = f^m$ pour tout entier naturel m. Puisque $0 + m = m$ pour tout entier naturel m, on en déduit que $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. Soit m un entier naturel. On a d'après le lemme précédent : $f^{n+1} \circ f^m = (f^n \circ f) \circ f^m$. En utilisant l'associativité de $\circ$, il vient : $f^{n+1} \circ f^m = f^n \circ (f \circ f^m)$. La définition de la puissance de fonction donne alors : $f^{n+1} \circ f^m = f^n \circ f^{m+1}$. Puisque $P(n)$ est vrai, cela donne : $f^{n+1} \circ f^m = f^{n+(m+1)}$. Enfin, en utilisant la commutativité et l'associativité de l'addition, il vient : $f^{n+1} \circ f^m = f^{(n+1)+m}$. On en déduit que $P(n+1)$ est vrai.

Par récurrence, on conclut que $P(n)$ pour tout entier naturel n, et donc le lemme.

□

Lemme : Soit E un ensemble et f une fonction de E vers E. Soit n et m deux entiers naturels. Alors, $f^n \circ f^m = f^m \circ f^n$.

Démonstration :[29] On procède par récurrence sur n. Soit P le prédicat à un paramètre libre défini par : $P(n) : \forall m \in \mathbb{N},\ f^n \circ f^m = f^m \circ f^n$. Soit m un entier naturel. Puisque f^0 est la fonction identité sur E, on a $f^0 \circ f^m = f^m$ et $f^m \circ f^0 = f^m$. Donc, $f^0 \circ f^m = f^m \circ f^0$. Cela étant vrai pour tout entier natiurel m, on en déduit que $P(0)$ est vrai.

Soit n un entier naturel tel que $P(n)$ est vrai. Soit m un entier naturel. Les deux fonctions $f^{n+1} \circ f^m$ et $f^m \circ f^{n+1}$ sont les composées de deux fonctions de E dans E. Ce sont donc encore des fonctions de E dans E. On a : $f^{n+1} \circ f^m = (f^n \circ f) \circ f^m$. L'associativité de la composition de fonctions donne : $f^{n+1} \circ f^m = f^n \circ (f \circ f^m)$. En utilisant la définition de la puissance de fonction, il vient : $f^{n+1} \circ f^m = f^n \circ f^{m+1}$. Puisque $P(n)$ est vrai, cela donne : $f^{n+1} \circ f^m = f^m \circ f^{n+1}$. Cela étant vrai pour tout élément m de $\mathbb{N}$, on en déduit que $P(n+1)$ est vrai.

Par récurrence, on en déduit que $P(n)$ est vrai pour tout entier naturen n, ce qui prouve le lemme.

□

1.4.12 Puissances d'ensembles

Soit E un ensemble et n un entier naturel. On note E^n l'ensemble des fonctions de n vers E. (Notons que cela est cohérent avec les notations définies section ??) Soit n éléments de E notés e_0, e_1, ..., e_{n-1}. On note (quand il n'y a pas d'ambiguité avec d'autres notations) $\left(e_0, e_1, \dots e_{n-1}\right)$ la fonction f de n vers E telle que $f(0) = e_0$, $f(1) = e_1$, ..., $f(n-1) = e_{n-1}$. Quand il n'y a pas d'ambiguité, si f est une fonction de n vers E^n et i un élément de [[1,n]], on note parfois f_i l'élément $f(i-1)$ de E.

Soit n un entier naturel et E un ensemble. Une fonction de n vers E est parfois appelée *séquence de n éléments de E* ou *n-uplet d'éléments de E*.

1.4.13 Produit cartésien de plusieurs ensembles

Soit n un entier naturel non nul et E_1, E_2, ..., E_n des ensembles (où le dernier symbole est absent si $n \leq 2$ et le symbole E_2 est absent si $n = 1$). On note $E_1 \times E_2 \times \cdots \times E_n$ l'ensemble $(\cdots (E_1 \times E_2) \times \cdots) \times E_n$.

Soit e_1 un élément de E_1, E_2 un élément de E_2, ..., e_n un élément de E_n. L'élément $((\cdots (e_1, e_2), \dots), e_n)$ pourra être noté $(e_1, e_2, \dots e_n)$ s'il n'y a pas d'ambiguité.

1.5 Construction de $\mathbb{Z}$

1.5.1 Définition

On définit l'ensemble $\mathbb{Z}$ par :

$$\mathbb{Z} = \left\{ z \in \mathbb{N} \times \mathbb{N} \;\middle|\; (\exists n \in \mathbb{N},\ z = (0,n)) \vee (\exists n \in \mathbb{N}^*,\ z = (1,n)) \right\}.$$

Pour tout élément n de $\mathbb{N}$, on note parfois et s'il n'y a pas de confusion possible simplement n l'élément $(0,n)$ et, si $n \neq 0$, $-n$ l'élément $(1,n)$. On note $\mathbb{Z}^*$ l'ensemble $\mathbb{Z} \backslash \{(0,0)\}$. On qualifie les éléments de $\mathbb{Z}$ d'*entiers* ou *entiers relatifs*, et ceux de $\mathbb{N}$ d'*entiers naturels*.

On définit deux fonctions sgn : $\mathbb{Z} \to \{0, 1\}$ et abs : $\mathbb{Z} \to \mathbb{N}$ de la manière suivante. Soit a un élément de $\mathbb{Z}$. On peut choisir un élément ϵ de $\{0, 1\}$ et un élément n de $\mathbb{N}$ tels que $a = (\epsilon, n)$. On pose alors $\text{sgn}(a) = \epsilon$ et $\text{abs}(a) = n$. Le premier est appelé *signe* de l'entier a et le second, aussi noté $|a|$, sa *valeur absolue*.

Notons que, si a et b sont deux entiers tels que $|a| = |b|$ et $\text{sgn}(a) = \text{sgn}(b)$, alors $a = b$.

Un entier est dit *nul* s'il est égal à (0,0).

Soit a et b deux entiers, on a $\text{sgn}(a) = \text{sgn}(b)$ ou $\text{sgn}(a) = 1 - \text{sgn}(b)$.

Quand il n'y a pas d'ambiguité, un entier naturel n pourra être identifié à l'entier relatif $(0,n)$. En particulier, (0,0) est parfois simplement noté 0. Les définitions données dans la suite de cette section sont compatibles avec cette identification.

[29] La démonstration est évidente en utilisant le lemme précédent et la commutativité de l'addition : en admettant ces éléments, on a $f^n \circ f^m = f^{n+m} = f^{m+n} = f^m \circ f^n$. Nous donnons ici unr démonstration alternative, plus pédestre.

1.5.2 Relation d'ordre

Définition : On définit la relation binaire $\leq$ sur $\mathbb{Z}$ de la manière suivante.

- Soit n et m deux éléments de $\mathbb{N}$, (0,n) $\leq$ (0,m) si et seulement si $n \leq m$.
- Soit n et m deux éléments de $\mathbb{N}^*$,(1,n) $\leq$ (1,m) si et seulement si $m \leq n$,
- Soit n un élément de $\mathbb{N}^*$ et m un élément de $\mathbb{N}$, (1,n) $\leq$ (0,m) est vrai et (0,m) $\leq$ (1,n) est faux.

On définit aussi la relation $<$ par : $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, a < b \Leftrightarrow ((a \leq b) \wedge (a \neq b))$, la relation $\geq$ par : $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, a \geq b \Leftrightarrow b \leq a$, et la relation $>$ par : $\forall a \in \mathbb{Z}$, $\forall b \in \mathbb{Z}$, $a > b \Leftrightarrow ((a \geq b) \wedge (a \neq b))$. On a alors:

- Soit n et m deux éléments de $\mathbb{N}$,
  - (0,n) $<$ (0,m) si et seulement si $n < m$,
  - (0,n) $\geq$ (0,m) si et seulement si $n \geq m$,
  - (0,n) $>$ (0,m) si et seulement si $n > m$.
- Soit n et m deux éléments de $\mathbb{N}^*$,
  - (1,n) $<$ (1,m) si et seulement si $n > m$,
  - (1,n) $\geq$ (1,m) si et seulement si $n \leq m$,
  - (1,n) $>$ (1,m) si et seulement si $n < m$.
- Soit n un élément de $\mathbb{N}^*$ et m un élément de $\mathbb{N}$,
  - (1,n) $<$ (0,m) est vrai,
  - (0,m) $<$ (1,n) est faus,
  - (1,n) $\geq$ (0,m) est faux,
  - (0,m) $\geq$ (1,n) est vrai,
  - (1,n) $>$ (0,m) est faux,
  - (0,m) $>$ (1,n) est vrai.

Notons que, pour tous entiers a et b, $a > b$ est équivalent à $\neg(a \leq b)$ et $a < b$ est équivalent à $a \geq b$.

Lemme : La relation $\leq$ est une relation d'ordre sur $\mathbb{Z}$.

Démonstration : Vérifions qu'elle satisfait les trois propriétés définissant une relation d'ordre :

- *Réflexivité :* Soit x un entier relatif. On peut choisir un élément ϵ de $\{0, 1\}$ et un entier naturel n tel que $x = (\epsilon, n)$. Puisque $n = n$, on a $n \leq n$ (dans les deux cas $\epsilon = 0$ ou $\epsilon = 1$), donc $x \leq x$.
- *Antisymétrie :* Soit x et y deux éléments de $\mathbb{Z}$ tels que $x \leq y$ et $y \leq x$. On peut choisir deux éléments ϵ et η de $\{0, 1\}$ et deux entiers naturels n et m tels que $x = (\epsilon, n)$ et $y = (\eta, m)$. Montrons d'abord que $\epsilon = \eta$. Si $\epsilon = 0$, alors $x \leq y$ implique $\eta = 0$ d'après la contraposée du troisième point de la définition. Si $\epsilon = 1$, alors $y \leq x$ implique $\eta = 1$ par le même argument. Dans les deux cas, on a bien $\epsilon = \eta$. Donc, $y = (\epsilon, m)$. D'après les deux premières lignes de la définition de la relation $\leq$ sur $\mathbb{Z}$ (et la commutativité du connecteur $\wedge$ dans le cas $\epsilon = 1$), $(x \leq y) \wedge (y \leq x)$ implique donc $(n \leq m) \wedge (m \leq n)$.[30] Donc, $n = m$. On en déduit que $x = y$.
- *Transitivité :* Soit x, y et z trois éléments de $\mathbb{Z}$ tels que $x \leq y$ et $y \leq z$. Alors,
  - Si $\text{sgn}(z) = 1$, on doit avoir $\text{sgn}(y) = 1$ (puisque $y \leq z$) et sgn(x) = 1 (puisque $x \leq y$). On peut donc choisir trois entiers naturels n, m et k tels que $x = (1,n)$, $y = (1,m)$ et $z = (1,k)$. En outre, on a $n \geq m$ puisque $x \leq y$ et $m \geq k$ puisque $y \leq z$. Donc, $n \geq k$. Donc, (1,n) $\leq$ (1,k), et donc $x \leq z$.
  - Si $\text{sgn}(z) = 0$ et $\text{sgn}(y) = 1$, on a $\text{sgn}(x) = 1$ puisque $x \leq y$. Donc, $x \leq z$.
  - Si $\text{sgn}(z) = 0$, $\text{sgn}(y) = 0$, et $\text{sgn}(x) = 1$, alors $x \leq z$.
  - Si $\text{sgn}(z) = 0$, $\text{sgn}(y) = 0$, et $\text{sgn}(x) = 0$, alors on peut choisir trois entier naturels n, m et k tels que $x = (0,n)$, $y = (0,m)$ et $z = (0,k)$. Puisque $x \leq y$ et $y \leq k$, on a $n \leq m$ et $m \leq k$. Donc, $n \leq k$, donc (0,n) $\leq$ (0,k) et $x \leq z$.

□

Corolaire : La relation $\geq$ est une relation d'ordre et les relations $<$ et $>$ sont des relations d'ordre strict sur $\mathbb{Z}$.

Lemme : La relation $\leq$ est une relation d'ordre total sur $\mathbb{Z}$.

[30] En effet,

- Si $\epsilon = 0$, $x \leq y$ implique $n \leq m$ et $y \leq x$ implique $m \leq n$.
- Sinon, $\epsilon = 1$, donc $x \leq y$ implique $m \leq n$ et $y \leq x$ implique $n \leq m$.

Démonstration : Soit a et b deux éléments de $\mathbb{Z}$. On peut choisir deux éléments ϵ et η de $\{0, 1\}$ et deux éléments n et m de $\mathbb{N}$ tels que $a = (\epsilon, n)$ et $b = (\eta, m)$.

- Si $\epsilon = 0$ et $\eta = 1$, on a $b \leq a$.
- Si $\epsilon = 1$ et $\eta = 0$, on a $a \leq b$.
- Si $\epsilon = 0$, $\eta = 0$ et $n \leq m$, on a $a \leq b$.
- Si $\epsilon = 0$, $\eta = 0$ et $\neg(n \leq m)$, on a $n > m$, donc $m \leq n$, et donc $b \leq a$.
- Si $\epsilon = 1$, $\eta = 1$ et $n \leq m$, on a $b \leq a$.
- Si $\epsilon = 1$, $\eta = 1$ et $\neg(n \leq m)$, on a $n > m$, donc $m \leq n$, et donc $a \leq b$.

Dans tous les cas, on a donc $(a \leq b) \vee (b \leq a)$.

□

Corolaire : La relation $\geq$ est une relation d'ordre total sur $\mathbb{Z}$.

Définitions : Un entier x est dit :

- *positif* si $x \geq 0$,
- *négatif* si $x \leq 0$,
- *strictement positif* si $x > 0$,
- *strictement négatif* si $x < 0$.

1.5.3 Addition

Définition : On définit l'opération + sur $\mathbb{Z}$ (vue comme une fonction de $\mathbb{Z} \times \mathbb{Z}$ vers $\mathbb{Z}$) de la manière suivante. Soit n et m deux élément de $\mathbb{N}$. Alors,

- $(0,n) + (0,m) = (0, n + m)$,
- si $n \neq 0$ et $m \neq 0$, $(1,n) + (1,m) = (1, n + m)$;
- si $n \neq 0$ et $n \leq m$, $(1,n) + (0,m) = (0, m - n)$;
- si $n \neq 0$ et $n > m$, $(1,n) + (0,m) = (1, n - m)$;
- si $m \neq 0$ et $n < m$, $(0,n) + (1,m) = (1, m - n)$;
- si $m \neq 0$ et $n \geq m$, $(0,n) + (1,m) = (0, n - m)$.

Lemme : Soit z un élément de $\mathbb{Z}$. Alors $z + 0 = z$ et $0 + z = z$.

Démonstration : Éxaminons tour à tour les deux cas possibles, notant que $0 = (0,0)$:

- S'il existe un entier naturel n tel que $z = (0,n)$, alors $z + 0 = (0,n) + (0,0) = (0,n + 0) = (0,n) = z$ et $0 + z = (0,0) + (0,n) = (0,0 + n) = (0,n) = z$.
- S'il existe un entier naturel non nul n tel que $z = (1,n)$, alors $n > 0$, donc $z + 0 = (1,n) + (0,0) = (1,n - 0) = (1,n) = z$ et $0 + z = (0,0) + (1,n) = (1,n - 0) = (1,n) = z$.

□

Lemme : L'addition est commutative : pour tous éléments a et b de $\mathbb{Z}$, $a + b = b + a$.

Démonstration : Éxaminons les différents cas possibles :

- Si $\text{sgn}(a) = 0$ et $\text{sgn}(b) = 0$, alors $a + b = (0, |a| + |b|)$ et $b + a = (0, |b| + |a|)$. Puisque l'addition d'entiers naturels est commutative, on a $|a| + |b| = |b| + |a|$, et donc $a + b = b + a$.
- Si $\text{sgn}(a) = 1$ et $\text{sgn}(b) = 1$, alors $a + b = (1, |a| + |b|)$ et $b + a = (1, |b| + |a|)$. Puisque l'addition d'entiers naturels est commutative, on a $|a| + |b| = |b| + |a|$, et donc $a + b = b + a$.
- Si $\text{sgn}(a) = 0$, $\text{sgn}(b) = 1$ et $|a| \geq |b|$, alors $a + b = (0, |a| - |b|)$ et $b + a = (0, |a| - |b|)$, donc $a + b = b + a$.
- Si $\text{sgn}(a) = 0$, $\text{sgn}(b) = 1$ et $|a| < |b|$, alors $a + b = (1, |b| - |a|)$ et $b + a = (1, |b| - |a|)$, donc $a + b = b + a$.
- Si $\text{sgn}(a) = 1$, $\text{sgn}(b) = 0$ et $|a| > |b|$, alors $a + b = (1, |a| - |b|)$ et $b + a = (1, |a| - |b|)$, donc $a + b = b + a$.
- Si $\text{sgn}(a) = 1$, $\text{sgn}(b) = 0$ et $|a| \leq |b|$, alors $a + b = (0, |b| - |a|)$ et $b + a = (0, |b| - |a|)$, donc $a + b = b + a$.

Dans tous les cas, on a bien $a + b = b + a$.

□

Lemme : L'addition est associative : pour tous éléments a, b et c de $\mathbb{Z}$, $a + (b + c) = (a + b) + c$.

Démonstration : Soit a, b et c trois éléments de $\mathbb{Z}$. On peut choisir trois éléments κ, μ et ν de $\{0, 1\}$ et trois éléments k, m et n de $\mathbb{N}$ tels que $a = (\kappa, k)$, $b = (\mu, m)$ et $c = (\nu, n)$. Alors,

- Si $\kappa = \mu = \nu = 0$, on a $(a+b)+c = (0,k+m)+c = (0,(k+m)+n)$ et $a+(b+c) = a+(0,m+n) = (0,k+(m+n))$. Puisque l'addition d'entiers naturels est associative, $(k+m)+n = k+(m+n)$. Donc, $(0,(k+m)+n) = (0,k+(m+n))$, et donc $(a+b)+c = a+(b+c)$.
- Si $\kappa = \mu = \nu = 1$, on a $(a+b)+c = (1,k+m)+c = (1,(k+m)+n)$ et $a+(b+c) = a+(1,m+n) = (1,k+(m+n))$. Puisque l'addition d'entiers naturels est associative, $(k+m)+n = k+(m+n)$. Donc, $(1,(k+m)+n) = (1,k+(m+n))$, et donc $(a+b)+c = a+(b+c)$.
- Si $\kappa = \mu = 0$ et $\nu = 1$, on a $(a+b)+c = (0,k+m)+c$. Donc, $(a+b)+c = (0,(k+m)-n)$ si $k+m \geq n$ et $(a+b)+c = (1,n-(k+m))$ sinon. Éxaminons les différentes possibilités pour $a+(b+c)$.
  - Si $n > m$ et $(n-m) > k$, alors $n > k+m$ et $a+(b+c) = a+(1,n-m) = (1,(n-m)-k) = (1,n-(k+m))$. Donc, $a+(b+c) = (a+b)+c$.
  - Si $n > m$ et $(n-m) \leq k$, alors $n \leq k+m$ et $a+(b+c) = a+(1,n-m) = (0,k-(n-m)) = (0,(k+m)-n)$. Donc, $a+(b+c) = (a+b)+c$.
  - Si $n \leq m$, alors $n \leq k+m$ et $a+(b+c) = a+(0,m-n) = (0,k+(m-n)) = (0,(k+m)-n)$. Donc, $a+(b+c) = (a+b)+c$.
- Si $\kappa = \mu = 1$ et $\nu = 0$, on a $(a+b)+c = (1,k+m)+c$. Donc, $(a+b)+c = (1,(k+m)-n)$ si $k+m > n$ et $(a+b)+c = (0,n-(k+m))$ sinon. Éxaminons les différentes possibilités pour $a+(b+c)$.
  - Si $n \geq m$ et $(n-m) \geq k$, alors $n \geq k+m$ et $a+(b+c) = a+(0,n-m) = (0,(n-m)-k) = (0,n-(k+m))$. Donc, $a+(b+c) = (a+b)+c$.
  - Si $n \geq m$ et $(n-m) < k$, alors $n < k+m$ et $a+(b+c) = a+(0,n-m) = (1,k-(n-m)) = (1,(k+m)-n)$. Donc, $a+(b+c) = (a+b)+c$.
  - Si $n < m$, alors $n < k+m$ et $a+(b+c) = a+(1,m-n) = (1,k+(m-n)) = (1,(k+m)-n)$. Donc, $a+(b+c) = (a+b)+c$.
- Si $\mu = \nu$ et $\mu \neq \kappa$, on se ramène aux deux cas précédents en notant que a et c jouent des rôles interchangeables. En effet, si on définit les trois entiers $\overline{a}$, $\overline{b}$ et $\overline{c}$ par $\overline{a} = c$, $\overline{b} = b$ et $\overline{c} = a$, on a $\overline{a}+(\overline{b}+\overline{c}) = (\overline{a}+\overline{b})+\overline{c}$ d'après les deux cas précédents. En utilisant quatre fois la commutativité de l'addition, cela donne $(\overline{c}+\overline{b})+\overline{a} = \overline{c}+(\overline{b}+\overline{a})$, et donc $(a+b)+c = a+(b+c)$.
- Si $\mu = \nu$ et $\mu \neq \kappa$, on se ramène au cas précédent de la manière suivante. Puisque $\text{sgn}(a) = \text{sgn}(c)$ et $\text{sgn}(a) \neq \text{sgn}(b)$, et par commutativité de l'addition, on a : $(a+b)+c = (b+a)+c = b+(a+c)$. En utilisant la commutativité de l'addition, il vient : $(a+b)+c = (a+c)+b$. Puisque $\text{sgn}(a) = \text{sgn}(c)$, on a d'après les cas précédents : $(a+c)+b = a+(c+b) = a+(b+c)$. Donc, $(a+b)+c = a+(b+c)$.

□

Lemme : Soit n et m deux éléments de $\mathbb{Z}$. Alors,
- si $n = (0,0)$, $n+m = m$,
- si $n > (0,0)$, $n+m > m$,
- si $n < (0,0)$, $n+m < m$.

Démonstration : Considérons les différents cas possibles :
- Si $n = (0,0)$, on a vu que $n+m = m$.
- Supposons que $n > (0,0)$. Alors, on peut choisir un entier naturel non nul a tel que $n = (0,a)$. Distinguons deux cas :
  - Si $m \geq 0$, on peut choisir un entier naturel b tel que $m = (0,b)$. On a alors $n+m = (0,a+b)$. Puisque $a > 0$, $a+b > b$, donc $n+m > m$.
  - Sinon, on peut choisir un entier naturel non nul b tel que $m = (1,b)$. Si $b \leq a$, on a $n+m = (0,a-b)$ et, puisque b est non nul, donc $n+m > m$. Sinon, $n+m = (1,b-a)$. Puisque $a > 0$, $b-a < b$, donc $n+m > m$.
- Supposons que $n < (0,0)$. Alors, on peut choisir un entier naturel non nul a tel que $n = (1,a)$. Distinguons deux cas :
  - Si $m < 0$, on peut choisir un entier naturel non nul b tel que $m = (1,b)$. On a alors $n+m = (1,a+b)$. Puisque $a > 0$, $a+b > b$, donc $n+m < m$.
  - Sinon, on peut choisir un entier naturel b tel que $m = (0,b)$. Si $b \leq a$, on a $n+m = (1,a-b)$, donc $n+m < m$. Sinon, $n+m = (0,b-a)$. Puisque $a > 0$, $b-a < b$, donc $n+m < m$.

□

Lemme : Soit a, b et c trois éléments de $\mathbb{Z}$. Alors, $(a+c \leq b+c) \Leftrightarrow (a \leq b)$ et $(a+c < b+c) \Leftrightarrow (a < b)$.

Démonstration : On peut choisir trois éléments α, β et γ de $\{0, 1\}$ et trois éléments n, m et k de $\mathbb{N}$ tels que $a = (\alpha, n)$, $b = (\beta, m)$ et $c = (\gamma, k)$. Alors,

- Si $\alpha = \beta = \gamma = 0$, $a + c \leq b + c$ est équivalent à $n + k \leq m + k$ et $a \leq b$ à $n \leq m$. Puisque $(n + k \leq m + k) \Leftrightarrow (n \leq m)$, on en déduit $(a + c \leq b + c) \Leftrightarrow (a \leq b)$. De même, $a + c < b + c$ est équivalent à $n + k < m + k$ et $a < b$ à $n < m$. Puisque $(n + k < m + k) \Leftrightarrow (n < m)$, on en déduit $(a + c < b + c) \Leftrightarrow (a < b)$.
- Si $\alpha = \beta = \gamma = 1$, $a + c \leq b + c$ est équivalent à $n + k \geq m + k$ et $a \leq b$ à $n \geq m$. Puisque $(n + k \geq m + k) \Leftrightarrow (n \geq m)$, on en déduit $(a + c \geq b + c) \Leftrightarrow (a \geq b)$. De même, $a + c < b + c$ est équivalent à $n + k > m + k$ et $a < b$ à $n > m$. Puisque $(n + k > m + k) \Leftrightarrow (n > m)$, on en déduit $(a + c < b + c) \Leftrightarrow (a < b)$.
- Si $\alpha = 0$, $\beta = 1$ (ce qui implique $m > 0$) et $\gamma = 0$, $a \leq b$ et $a < b$ sont faux. On a deux possibilités :
  - Si $k < m$, $a + c = (0, n + k)$ et $b + c = (1, m - k)$, donc $a + c \leq b + c$ et $a + c < b + c$ sont faux.
  - Si $k \geq m$, $a + c = (0, n + k)$ et $b + c = (0, k - m)$. Puisque $m > 0$, $k - m < k$ (puisque $k = (k - m) + m$). Puisque $k \leq k + n$, on a $k - m < k + n$, donc $b + c < a + c$, donc $a + c \leq b + c$ et $a + c < b + c$ sont faux.
- Si $\alpha = 0$, $\beta = 1$ et $\gamma = 1$, $a \leq b$ et $a < b$ sont faux. On a deux possibilités :
  - Si $k \leq n$, $a + c = (0, n - k)$ et $b + c = (1, m + k)$, donc $a + c \leq b + c$ et $a + c < b + c$ sont faux.
  - Si $k > n$, $a + c = (1, k - n)$ et $b + c = (1, m + k)$. Puisque $k - n \leq k$ (puisque $k = (k - n) + n$) et $k < k + m$ (puisque $m > 0$), on a $k - n < k + m$, donc $b + c < a + c$, donc $a + c \leq b + c$ et $a + c < b + c$ sont faux.
- Si $\alpha = 1$, $\beta = 0$ et $\gamma = 0$, $a \leq b$ et $a < b$ sont vrais. On a deux possibilités :
  - Si $k < n$, $a + c = (1, n - k)$ et $b + c = (0, m + k)$, donc $a + c \leq b + c$ et $a + c \neq b + c$, et donc $a + c < b + c$, sont vrais.
  - Si $k \geq n$, $a + c = (0, k - n)$ et $b + c = (0, k + m)$. Puisque $k - n < k + m$ ($k - n < k$ puisque $n > 0$ et $k \leq k + m$), on a donc $a + c \leq b + c$ et $a + c \neq b + c$, et donc $a + c < b + c$.
- Si $\alpha = 1$, $\beta = 0$ et $\gamma = 1$, $a \leq b$ et $a < b$ sont vrais. On a deux possibilités :
  - Si $k \leq m$, $a + c = (1, n + k)$ et $b + c = (0, m - k)$, donc $a + c \leq b + c$ et $a + c \neq b + c$, et donc $a + c < b + c$, sont vrais.
  - Si $k > m$, $a + c = (1, n + k)$ et $b + c = (1, k - m)$. Puisque $k - m < k + n$ ($k + n > k$ puisque $n > 0$ et $k - m \leq k$), on a donc $a + c \leq b + c$ et $a + c \neq b + c$, et donc $a + c < b + c$.
- Supposons $\alpha = \beta = 0$ et $\gamma = 1$. Alors,
  - Si $k \leq n$ et $k \leq m$, on a $a + c = (0,n - k)$ et $b + c = (0,m - k)$. Donc, $(a + c \leq b + c) \Leftrightarrow (n - k \leq m - k)$ et $(a + c = b + c) \Leftrightarrow (n - k = m - k)$. Puisque $(n - k) + k = n$ et $(m - k) + k = m$, $(n - k \leq m - k) \Leftrightarrow (n \leq m)$ et $(n - k = m - k) \Leftrightarrow (n = m)$. Donc, $(n - k \leq m - k) \Leftrightarrow (a \leq b)$ et $(n - k = m - k) \Leftrightarrow (a = b)$. Donc, $(a + c \leq b + c) \Leftrightarrow (a \leq b)$ et $(a + c = b + c) \Leftrightarrow (a = b)$. Donc, $(a + c \leq b + c) \Leftrightarrow (a \leq b)$ et $(a + c < b + c) \Leftrightarrow (a < b)$.
  - Si $k > n$ et $k > m$, on a $a + c = (1,k - n)$ et $b + c = (1,k - m)$. Donc, $(a + c \leq b + c) \Leftrightarrow (k - n \geq k - m)$ et $(a + c = b + c) \Leftrightarrow (k - n = k - m)$. Or, $k - n \geq k - m$ est équivalent à $n \leq m$ et $k - n = k - m$ à $n = m$. Donc, $(k - n \geq k - m) \Leftrightarrow (a \leq b)$ et $(k - n = k - m) \Leftrightarrow (a = b)$. Donc, $(a + c \leq b + c) \Leftrightarrow (a \leq b)$ et $(a + c < b + c) \Leftrightarrow (a < b)$.
  - Si $k \leq n$ et $k > m$, alors $m < n$, donc $b < a$, donc $a \leq b$ et $a < b$ sont faux. En outre, $a + c = (0, n - k)$ et $b + c = (1, k - m)$, donc $b + c < a + c$, donc $a + c \leq b + c$ et $a + c < b + c$ sont faux.
  - Si $k > n$ et $k \leq m$, alors $n < m$, donc $a < b$, donc $a \leq b$ et $a < b$ sont vrais. En outre, $a + c = (1, k - n)$ et $b + c = (0, m - k)$, donc $a + c < b + c$, donc $a + c \leq b + c$ et $a + c < b + c$ sont vrais.
- Supposons $\alpha = \beta = 1$ et $\gamma = 0$. Alors,
  - Si $k < n$ et $k < m$, on a $a + c = (1,n - k)$ et $b + c = (1,m - k)$. Donc, $(a + c \leq b + c) \Leftrightarrow (n - k \geq m - k)$ et $(a + c = b + c) \Leftrightarrow (n - k = m - k)$. Puisque $(n - k) + k = n$ et $(m - k) + k = m$, $(n - k \geq m - k) \Leftrightarrow (n \geq m)$ et $(n - k = m - k) \Leftrightarrow (n = m)$. Donc, $(n - k \geq m - k) \Leftrightarrow (a \leq b)$ et $(n - k = m - k) \Leftrightarrow (a = b)$. Donc, $(a + c \leq b + c) \Leftrightarrow (a \leq b)$ et $(a + c = b + c) \Leftrightarrow (a = b)$. Donc, $(a + c \leq b + c) \Leftrightarrow (a \leq b)$ et $(a + c < b + c) \Leftrightarrow (a < b)$.
  - Si $k \geq n$ et $k \geq m$, on a $a + c = (0,k - n)$ et $b + c = (0,k - m)$. Donc, $(a + c \leq b + c) \Leftrightarrow (k - n \leq k - m)$ et $(a + c = b + c) \Leftrightarrow (k - n = k - m)$. Or, $k - n \leq k - m$ est équivalent à $n \geq m$ et $k - n = k - m$ à $n = m$. Donc, $(k - n \leq k - m) \Leftrightarrow (a \leq b)$ et $(k - n = k - m) \Leftrightarrow (a = b)$. Donc, $(a + c \leq b + c) \Leftrightarrow (a \leq b)$ et $(a + c < b + c) \Leftrightarrow (a < b)$.
  - Si $k < n$ et $k \geq m$, alors $m < n$, donc $b > a$, donc $a \leq b$ et $a < b$ sont vrais. En outre, $a + c = (1, n - k)$ et $b + c = (0, k - m)$, donc $b + c > a + c$, donc $a + c \leq b + c$ et $a + c < b + c$ sont vrais.
  - Si $k \geq n$ et $k < m$, alors $n < m$, donc $a > b$, donc $a \leq b$ et $a < b$ sont faux. En outre, $a + c = (0, k - n)$ et $b + c = (1, m - k)$, donc $a + c > b + c$, donc $a + c \leq b + c$ et $a + c < b + c$ sont faux.

Dans tous les cas, on a bien $(a + c \leq b + c) \Leftrightarrow a \leq b$ et $(a + c < b + c) \Leftrightarrow a < b$.

□

Lemme : Soit a et b deux éléments de $\mathbb{Z}$. Alors, $|a+b| \leq |a| + |b|$.

Démonstration : Si a et b sont de même signe, alors, par définition de l'addition $|a+b| = |a| + |b|$, donc $|a+b| \leq |a| + |b|$. Sinon, en notant M le maximum de $\{|a|, |b|\}$ et m son minimum, on a $|a+b| = M - m$ et $|a| + |b| = M + m$. Puisque $M + m = (M - m) + (2 \times m)$, on a $M - m \leq M + m$, donc $|a+b| \leq |a| + |b|$.

□

1.5.4 Opposé

Définition : On définit l'opération $-$ sur $\mathbb{Z}$, vue comme une fonction de $\mathbb{Z}$ vers $\mathbb{Z}$, de la manière suivante :

- $-(0,0) = (0,0)$;
- soit n un entier naturel non nul, $-(0,n) = (1,n)$.
- soit n un entier naturel non nul, $-(1,n) = (0,n)$.

Pour tout entier n, l'entier $-n$ est apelé son *opposé*. Notons que, pour tout entier z, on a $z = 0 \Leftrightarrow -z = 0$.

Lemme : Soit z un élément de $\mathbb{Z}$. Alors $-(-z) = z$.

Démonstration : Éxaminons tout à tour les trois cas possibles :

- Si $z = (0,0)$, alors $-z = z$, donc $-(-z) = -z = z$.
- S'il existe un entier naturel non nul n tel que $z = (0,n)$, alors $-z = (1,n)$, donc $-(-z) = (0,n) = z$.
- S'il existe un entier naturel non nul n tel que $z = (1,n)$, alors $-z = (0,n)$, donc $-(-z) = (1,n) = z$.

Dans tous les cas, on a donc bien $-(-z) = z$.

□

Lemme : Soit z un élément de $\mathbb{Z}$. Alors $z + (-z) = (0,0)$.

Démonstration : Éxaminons tout à tour les trois cas possibles :

- Si $z = (0,0)$, alors $-z = z$, donc $z + (-z) = (0,0) + (0,0) = (0,0)$.
- S'il existe un entier naturel non nul n tel que $z = (0,n)$, alors $-z = (1,n)$, donc $z + (-z) = (0,n) + (1,n) = (0,n-n) = (0,0)$.
- S'il existe un entier naturel non nul n tel que $z = (1,n)$, alors $-z = (0,n)$, donc $z + (-z) = (1,n) + (0,n) = (0,n-n) = (0,0)$.

Dans tous les cas, on a donc bien $z + (-z) = (0,0)$.

□

Corolaire : Soit n et m deux éléments de $\mathbb{Z}$. Alors, $-n = -m \Leftrightarrow n = m$.

Démonstration :

- Si $n = m$, alors $-n = -m$ par propriété de l'égalité.
- Si $-n = -m$, alors $-(-n) = -(-m)$, donc $n = m$.

□

Lemme : Soit n et m deux éléments de $\mathbb{Z}$. Alors,

- $n \leq m \Leftrightarrow (-n) \geq (-m)$,
- $n < m \Leftrightarrow (-n) > (-m)$.

Démonstration : Notons d'abord que, d'après le lemme précédent, la première proposition est équivalente à la seconde.
Considérons les différents cas possibles :

- Si $n = (0,0)$ et $m = (0,0)$, alors $-n = (0,0)$ et $-m = (0,0)$, donc $n = m$ et $-n = -m$, donc $n \leq m$ et $(-n) \geq (-m)$.
- S'il existe un entier naturel a tel que $n = (0,0)$ et $m = (0,a)$, alors $-n = (0,0)$ et $-m = (1,a)$, donc $n \leq m$ et $(-n) \geq (-m)$.
- S'il existe un entier naturel a tel que $n = (0,0)$ et $m = (1,a)$, alors $-n = (0,0)$ et $-m = (0,a)$, donc $n > m$ et $(-n) < (-m)$.
- S'il existe un entier naturel a tel que $n = (0,a)$ et $m = (0,0)$, alors $-n = (1,a)$ et $-m = (0,0)$, donc $n > m$ et $(-n) < (-m)$.
- S'il existe un entier naturel a tel que $n = (1,a)$ et $m = (0,0)$, alors $-n = (0,a)$ et $-m = (0,0)$, donc $n \leq m$ et $(-n) \geq (-m)$.
- S'il existe deux entiers naturels on nuls a et b tels que $n = (0,a)$ et $m = (0,b)$, alors $-n = (1,a)$ et $-m = (1,b)$, alors $n \leq m \Leftrightarrow a \leq b$ et $(-n) \geq (-m) \Leftrightarrow a \leq b$.
- S'il existe deux entiers naturels on nuls a et b tels que $n = (0,a)$ et $m = (1,b)$, alors $-n = (1,a)$ et $-m = (0,b)$, alors $n > m$ et $(-n) < (-m)$.

- S'il existe deux entiers naturels on nuls a et b tels que $n = (1,a)$ et $m = (0,b)$, alors $-n = (0,a)$ et $-m = (1,b)$, alors $n \leq m$ et $(-n) \geq (-m)$.
- S'il existe deux entiers naturels non nuls a et b tels que $n = (1,a)$ et $m = (1,b)$, alors $-n = (0,a)$ et $-m = (0,b)$, alors $n \leq m \Leftrightarrow b \leq a$ et $(-n) \geq (-m) \Leftrightarrow b \leq a$.

Dans tous les cas, $n \leq m$ est bien équivalent à $(-n) \leq (-m)$.

□

Lemme : Soit a et b deux entiers. Alors, $-(a+b) = (-a) + (-b)$.

Démonstration :

Si $a = 0$, on a $-(a+b) = -b$ et $(-a)+(-b) = 0+(-b) = -b$. Si $b = 0$, on a $-(a+b) = -a$ et $(-a)+(-b) = (-a)+0 = -a$. Dans les deux cas, on a bien $-(a+b) = (-a)+(-b)$.

Supposons maintenant $a \neq 0$ et $b \neq 0$. Distinguons quatres cas possibles :

- Si $\text{sgn}(a) = 0$ et $\text{sgn}(b) = 0$, alors $-(a+b) = -((0,|a|) + (0,|b|)) = -(0, |a| + |b|) = (1, |a| + |b|)$ et $(-a)+(-b) = (-(0,|a|)) + (-(0,|b|)) = (1,|a|) + (1,|b|) = (1, |a| + |b|)$. Donc, $-(a+b) = (-a)+(-b)$.
- Si $\text{sgn}(a) = 0$ et $\text{sgn}(b) = 1$, alors
  - Si $|a| = |b|$, $b = -a$, donc $a+b = 0$, donc $-(a+b) = 0$ et $(-a)+(-b) = (-a)+a = 0$. Donc, $-(a+b) = (-a)+(-b)$.
  - Si $|a| > |b|$, $-(a+b) = -((0,|a|)+(1,|b|)) = -(0,|a|-|b|) = (1,|a|-|b|)$ et $(-a)+(-b) = (-(0,|a|))+(-(1,|b|)) = (1,|a|) + (0,|b|) = (1,|a|-|b|)$. Donc, $-(a+b) = (-a)+(-b)$.
  - Si $|a| < |b|$, $-(a+b) = -((0,|a|)+(1,|b|)) = -(1,|b|-|a|) = (0,|b|-|a|)$ et $(-a)+(-b) = (-(0,|a|))+(-(1,|b|)) = (1,|a|) + (0,|b|) = (0,|b|-|a|)$. Donc, $-(a+b) = (-a)+(-b)$.
- Si $\text{sgn}(a) = 1$ et $\text{sgn}(b) = 0$, alors
  - Si $|a| = |b|$, $b = -a$, donc $a+b = 0$, donc $-(a+b) = 0$ et $(-a)+(-b) = (-a)+a = 0$. Donc, $-(a+b) = (-a)+(-b)$.
  - Si $|a| > |b|$, $-(a+b) = -((1,|a|)+(0,|b|)) = -(1,|a|-|b|) = (0,|a|-|b|)$ et $(-a)+(-b) = (-(1,|a|))+(-(0,|b|)) = (0,|a|) + (1,|b|) = (0,|a|-|b|)$. Donc, $-(a+b) = (-a)+(-b)$.
  - Si $|a| < |b|$, $-(a+b) = -((1,|a|)+(0,|b|)) = -(0,|b|-|a|) = (1,|b|-|a|)$ et $(-a)+(-b) = (-(1,|a|))+(-(0,|b|)) = (0,|a|) + (1,|b|) = (1,|b|-|a|)$. Donc, $-(a+b) = (-a)+(-b)$.
- Si $\text{sgn}(a) = 1$ et $\text{sgn}(b) = 1$, alors $-(a+b) = -((1,|a|) + (1,|b|)) = -(1, |a| + |b|) = (0, |a| + |b|)$ et $(-a)+(-b) = (-(1,|a|)) + (-(1,|b|)) = (0,|a|) + (0,|b|) = (0, |a| + |b|)$. Donc, $-(a+b) = (-a)+(-b)$.

1.5.5 Soustraction

Définition : On définit l'opération $-$ sur $\mathbb{Z}$ (vue comme une fonction de $\mathbb{Z} \times \mathbb{Z}$ vers $\mathbb{Z}$) de la manière suivante. Soit n et m deux élément de $\mathbb{Z}$. Alors,

- si $n = (0,0)$, alors $m - n = m$;
- sinon, $m - n = m + (-n)$.

Lemme : Pour tout élément z de $\mathbb{Z}$, on a :

- $z - z = 0$,
- $z - 0 = z$,
- $0 - z = -z$.

Démonstration : Soit z un élément de $\mathbb{Z}$. On a :

- $z - z = z + (-z) = 0$,
- $z - 0 = z$ par définition,
- $0 - z = 0 + (-z) = -z$.

□

Lemme : Soit n et m deux éléments de $\mathbb{Z}$. Alors $(n - m) + m = n$.

Démonstration : On a : $(n-m)+m = (n+(-m))+m = n+((-m)+m) = n+0 = n$.

□

Lemme : Soit a et b deux élément de $\mathbb{Z}$. Alors

- Si $b > -a$, $a + b > 0$.
- Si $b < -a$, $a + b < 0$.

Démonstration : Notons d'abords que le premier résultat implique le second. En effet, si $b < -a$, on a $-b > -(-a)$, donc, si le premier résultat est vrai, $(-a) + (-b) > 0$, donc $-(a + b) > 0$, donc $a + b < 0$. Montrons donc seulement le premier résultat. Pour ce faire supposons $b > -a$ et distinguons trois cas possibles :

- Si $a \geq 0$ et $b \geq 0$, alors a et b ne peuvent être tous deux nuls (sans quoi on aurait $b = -a$). Donc, $|a| + |b| > 0$, donc $a + b$ (égal à $(0, |a| + |b|)$) est strictement supérieur à 0.
- Si $a \geq 0$ et $b < 0$, $b > -a$ implique $a \neq 0$ (sans quoi on aurait $-a = 0$ et donc $b > 0$) et $|b| < |a|$ (puisque $b = (1, |b|)$, $-a = (1, |a|)$, et $b > -a$), donc $a + b = (0, |a| - |b|)$ et $a - b > 0$.
- Si $a < 0$, alors $-a > 0$, donc $b > 0$. En outre, puisque $-a = (0, |a|)$ et $b = (0, |b|)$, on doit avoir $|b| > |a|$. Donc, $a + b = (0, |b| - |a|)$ et $a + b > 0$.

□

Corolaire : Soit a et b deux élément de $\mathbb{Z}$. Alors

- Si $b > a$, $b + (-a) > 0$, donc $b - a > 0$.
- Si $b < a$ $b + (-a) < 0$, $b - a < 0$.

Puisque, en outre, $b - a = 0$ est équivalent à $b = a$, on a :

- $b = a \Leftrightarrow b - a = 0$,
- $b > a \Leftrightarrow b - a > 0$,
- $b < a \Leftrightarrow b - a < 0$,
- $b \geq a \Leftrightarrow b - a \geq 0$,
- $b \leq a \Leftrightarrow b - a \leq 0$.

Lemme : Soit a, b et c trois élément de $\mathbb{Z}$ tels que $b > c$. Alors, $a + b > a + c$

Démonstration : On a : $(a + b) - (a + c) = (a + b) + ((-a) + (-c)) = b - c$. Puisque $b > c$, $b - c > 0$, donc $(a + b) - (a + c) > 0$. Si $a + b \leq a + c$ éait vrai, on aurait $a + b = a + c$, et donc $(a + b) - (a + c) = 0$, ou $a + b < a + c$, et donc $(a + b) - (a + c) < 0$. Puisqu'aucun de ces deux prédicats est vrai, $a + b \leq a + c$ est faux, donc $a + b > a + c$ est vrai.

□

1.5.6 Multiplication

Définition : On définit l'opération $\times$ sur $\mathbb{Z}$ (vue comme une fonction de $\mathbb{Z} \times \mathbb{Z}$ vers $\mathbb{Z}$) de la manière suivante. Soit a et b deux entiers, alors

- si $a = 0$, alors $a \times b = b \times a = 0$,
- si $a \neq 0$ et $b \neq 0$, $a \times b = (\epsilon, |a| \times |b|)$, où ϵ est égal à 0 si $\text{sgn}(a) = \text{sgn}(b)$ et 1 sinon.

Ces règles sont équivalentes à : soit n et m deux élément de $\mathbb{N}$, alors

- $(0,n) \times (0,m) = (0, n \times m)$;
- si $n \neq 0$, $(0,0) \times (1,n) = (0, 0)$ et $(1, n) \times (0, 0) = (0,0)$;
- si $n \neq 0$ et $m \neq 0$, $(1,n) \times (0,m) = (1, n \times m)$;
- si $n \neq 0$ et $m \neq 0$, $(0,n) \times (1,m) = (1, n \times m)$;
- si $n \neq 0$ et $m \neq 0$, $(1,n) \times (1,m) = (0, n \times m)$.

Notons que, dans tous les cas, pour tous entiers relatifs a et b, $|a \times b| = |a| \times |b|$. Notons aussi que, pour tout entier relatif a, $(1,1) \times a = -a$. Le symbole $\times$ est parfois omis quand il n'y a pas de confusion possible.

Lemme : Soit a et b deux entiers relatifs. Si $a \times b = 0$, alors $a = 0$ ou $b = 0$.

Démonstration : On peut choisir deux entiers naturels n et m et deux éléments ϵ et η de $\{0, 1\}$ tels que $a = (\epsilon, n)$ et $b = (\eta, m)$. On peut aussi choisir un élément μ de $\{0, 1\}$ tel que $a \times b = (\mu, n \times m)$. (Avec $\mu = 0$ si $\epsilon = \eta$ ou $n = 0$ ou $m = 0$, et $\mu = 1$ si $\epsilon \neq \eta$, $n \neq 0$ et $m \neq 0$.) Si $a \times b = (0,0)$, on a donc $n \times m = 0$, donc $n = 0$ ou $m = 0$. Si $n = 0$, ϵ doit être égal à 0 (puisque $(\epsilon,n) \in \mathbb{Z}$), donc $a = (0,0)$. Sinon, $m = 0$, donc η doit être égal à 0 (puisque $(\eta,m) \in \mathbb{Z}$), donc $b = (0,0)$.

□

Lemme : Soit a et b deux entiers relatifs. Alors,

- Si $a = 0$ ou $b = 0$, alors $a \times b = 0$.
- Si $a > 0$ et $b > 0$, alors $a \times b > 0$.
- Si $a > 0$ et $b < 0$, alors $a \times b < 0$.
- Si $a < 0$ et $b > 0$, alors $a \times b < 0$.
- Si $a < 0$ et $b < 0$, alors $a \times b > 0$.

- Si $|a| = 1$, alors $|a \times b| = |b|$.
- Si $|a| > 1$ et $m \neq 0$, alors $|a \times b| > |b|$.

Démonstration :
- Les six premiers points sont des conséquences directes de la définition de la multiplication.
- Les deux derniers points sont des conséquences diectes du fait que $|a \times b| = |a| \times |b|$.

□

Lemme : La multiplication est commutative : pour tous éléments a et b de $\mathbb{Z}$, $a \times b = b \times a$.

Démonstration : Soit a et b deux entiers relatifs. Soit n et m deux entiers naturels et ϵ et η deux éléments de $\{0, 1\}$ tels que $a = (\epsilon, n)$ et $b = (\eta, m)$. Alors,
- Si $n = 0$ ou $m = 0$, alors $a = (0,0)$ ou $b = (0,0)$, donc $a \times b = (0,0)$ et $b \times a = (0,0)$, donc $a \times b = b \times a$.
- Sinon, on a $a \times b = (\mu, n \times m)$ et $b \times a = (\mu, m \times n)$, où μ est égal à 0 si $\epsilon = \eta$ et 1 sinon. Puisque la multiplication d'entiers naturels est commutative, $n \times m = m \times n$, donc $a \times b = b \times a$.

□

Lemme : Soit n, m et k trois entiers relatifs. Alors,
- Si $n = 0$, $n \times m = n \times k$.
- Si $n \neq 0$, $n \times m = n \times k \Leftrightarrow m = k$.
- Si $n > 0$, $n \times m > n \times k \Leftrightarrow m > k$.
- Si $n < 0$, $n \times m > n \times k \Leftrightarrow m < k$.

Démonstration :
- Si $n = 0$, $n \times m = 0$ et $n \times k = 0$, donc $n \times m = n \times k$.
- Supposons $n \neq 0$. Supposons $n \times m = n \times k$.
  - On a $|n \times m| = |n \times k|$, donc $|n| \times |m| = |n| \times |k|$. Puisque $n \neq 0$, $|n| \neq 0$, donc cela implique $|m| = |k|$.
  - Si $\text{sgn}(n \times m) = 0$, alors $\text{sgn}(n \times k) = 0$, donc $\text{sgn}(n) = \text{sgn}(m)$ et $\text{sgn}(n) = \text{sgn}(k)$, donc $\text{sgn}(m) = \text{sgn}(k)$. Sinon, $\text{sgn}(n \times m) = 1$, donc $\text{sgn}(n \times k) = 1$, donc $\text{sgn}(m) = 1 - \text{sgn}(n)$ et $\text{sgn}(k) = 1 - \text{sgn}(n)$, donc $\text{sgn}(m) = \text{sgn}(k)$.
    Donc, $m = k$.
    Réciproquement, si $m = k$, alors $n \times m = n \times k$.
- Supposons que $n > 0$. Alors,
  - Si $m \geq 0$ et $k \geq 0$, $n \times m = (0, |n| \times |m|)$ et $n \times k = (0, |n| \times |k|)$. Donc, $n \times m > n \times k \Leftrightarrow |n| \times |m| > |n| \times |k|$. Puisque $n > 0$, $|n| \neq 0$, donc $|n| \times |m| > |n| \times |k| \Leftrightarrow |m| > |k|$ donc cela donne : $n \times m > n \times k \Leftrightarrow |m| > |k|$. Puisque $m > k \Leftrightarrow |m| > |k|$, on en déduit $n \times m > n \times k \Leftrightarrow m > k$.
  - Si $m \geq 0$ et $k < 0$, $m > k$ est vrai. En outre, $n \times m \geq 0$ et $n \times k < 0$, donc $n \times m > n \times k$ est vrai.
  - Si $m < 0$ et $k \geq 0$, $m > k$ est faux. En outre, $n \times m < 0$ et $n \times k \geq 0$, donc $n \times m > n \times k$ est faux.
  - Si $m < 0$ et $k < 0$, $n \times m = (1, |n| \times |m|)$ et $n \times k = (1, |n| \times |k|)$. Donc, $n \times m > n \times k \Leftrightarrow |n| \times |m| < |n| \times |k|$. Puisque $|n| > 0$, cela donne : $n \times m > n \times k \Leftrightarrow |m| < |k|$. Puisque $m > k \Leftrightarrow |m| < |k|$, on en déduit $n \times m > n \times k \Leftrightarrow m > k$.
- Supposons que $n < 0$. Alors,
  - Si $m \geq 0$ et $k \geq 0$, $n \times m = (1, |n| \times |m|)$ et $n \times k = (1, |n| \times |k|)$. Donc, $n \times m > n \times k \Leftrightarrow |n| \times |m| < |n| \times |k|$. Puisque $|n| > 0$, cela donne : $n \times m > n \times k \Leftrightarrow |m| < |k|$. Puisque $m < k \Leftrightarrow |m| < |k|$, on en déduit $n \times m > n \times k \Leftrightarrow m < k$.
  - Si $m \geq 0$ et $k < 0$, $m > k$ est vrai. En outre, $n \times m \leq 0$ et $n \times k > 0$, donc $n \times m > n \times k$ est faux.
  - Si $m < 0$ et $k \geq 0$, $m > k$ est faux. En outre, $n \times m > 0$ et $n \times k \leq 0$, donc $n \times m > n \times k$ est vrai.
  - Si $m < 0$ et $k < 0$, $n \times m = (0, |n| \times |m|)$ et $n \times k = (0, |n| \times |k|)$. Donc, $n \times m > n \times k \Leftrightarrow |n| \times |m| > |n| \times |k|$. Puisque $|n| > 0$, cela donne : $n \times m > n \times k \Leftrightarrow |m| > |k|$. Puisque $m < k \Leftrightarrow |m| > |k|$, on en déduit $n \times m > n \times k \Leftrightarrow m < k$.

□

Lemme : La multiplication est associative : pour tous éléments a, b et c de $\mathbb{Z}$, $a \times (b \times c) = (a \times b) \times c$.

Démonstration : On distingue différents cas :
- Si $a = 0$, $(a \times b) \times c = 0 \times c = 0$ et $a \times (b \times c) = 0$.
- Si $b = 0$, $(a \times b) \times c = 0 \times c = 0$ et $a \times (b \times c) = a \times 0 = 0$.
- Si $c = 0$, $(a \times b) \times c = 0$ et $a \times (b \times c) = a \times 0 = 0$.
- Supposons que a, b et c sont non nuls. Distinguons alors selon les valeurs possibles de $(\text{sgn}(a), \text{sgn}(b), \text{sgn}(c))$, qui est un élément de $\{0, 1\}^3$:

– S'il est égal à (0,0,0), on a $(a \times b) \times c = (0, |a| \times |b|) \times c = (0, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (0, |b| \times |c|) = (0, |a| \times (|b| \times |c|))$.
– S'il est égal à (0,0,1), on a $(a \times b) \times c = (0, |a| \times |b|) \times c = (1, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (1, |b| \times |c|) = (1, |a| \times (|b| \times |c|))$.
– S'il est égal à (0,1,0), on a $(a \times b) \times c = (1, |a| \times |b|) \times c = (1, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (1, |b| \times |c|) = (1, |a| \times (|b| \times |c|))$.
– S'il est égal à (0,1,1), on a $(a \times b) \times c = (1, |a| \times |b|) \times c = (0, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (0, |b| \times |c|) = (0, |a| \times (|b| \times |c|))$.
– S'il est égal à (1,0,0), on a $(a \times b) \times c = (1, |a| \times |b|) \times c = (1, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (0, |b| \times |c|) = (1, |a| \times (|b| \times |c|))$.
– S'il est égal à (1,0,1), on a $(a \times b) \times c = (1, |a| \times |b|) \times c = (0, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (1, |b| \times |c|) = (0, |a| \times (|b| \times |c|))$.
– S'il est égal à (1,1,0), on a $(a \times b) \times c = (0, |a| \times |b|) \times c = (0, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (1, |b| \times |c|) = (0, |a| \times (|b| \times |c|))$.
– S'il est égal à (1,1,1), on a $(a \times b) \times c = (0, |a| \times |b|) \times c = (1, (|a| \times |b|) \times |c|)$ et $a \times (b \times c) = a \times (0, |b| \times |c|) = (1, |a| \times (|b| \times |c|))$.

Notons que $(|a| \times |b|) \times |c| = |a| \times (|b| \times |c|)$ puisque la multiplication d'entiers naturels est associative, donc $(a \times b) \times c$ et $a \times (b \times c)$ sont égaux dans ces huit cas.

Dans tous les cas, on a bien $(a \times b) \times c = a \times (b \times c)$.

□

Lemme : La multiplication est distributive sur l'addition : pour tous éléments a, b et c de $\mathbb{Z}$, $a \times (b + c) = (a \times b) + (a \times c)$.

Démonstration :

- Si $\mathrm{sgn}(a) = \mathrm{sgn}(b) = \mathrm{sgn}(c) = 0$, alors $a \times (b + c) = a \times (0, |b| + |c|) = (0, |a| \times (|b| + |c|))$ et $(a \times b) + (a \times c) = (0, |a| \times |b|) + (0, |a| \times |c|) = (0, (|a| \times |b|) + (|a| \times |c|))$. Puisque, dans $\mathbb{N}$, la multiplication est distributive sur l'addition, on a $|a| \times (|b| + |c|) = (|a| \times |b|) + (|a| \times |c|)$, et donc $a \times (b + c) = (a \times b) + (a \times c)$.
- Si $\mathrm{sgn}(a) = \mathrm{sgn}(b) = \mathrm{sgn}(c) = 1$, alors $a \times (b + c) = a \times (1, |b| + |c|) = (0, |a| \times (|b| + |c|))$ et $(a \times b) + (a \times c) = (0, |a| \times |b|) + (0, |a| \times |c|) = (0, (|a| \times |b|) + (|a| \times |c|))$. Comme précédemment, on a donc $a \times (b + c) = (a \times b) + (a \times c)$.
- Si $a = (0,0)$, alors $a \times (b + c) = (0,0)$ et $(a \times b) + (a \times c) = 0 + 0 = 0$, donc $a \times (b + c) = (a \times b) + (a \times c)$.
- Si $b = (0,0)$, alors $a \times (b + c) = a \times c$ et $(a \times b) + (a \times c) = 0 + (a \times c) = a \times c$, donc $a \times (b + c) = (a \times b) + (a \times c)$.
- Si $c = (0,0)$, alors $a \times (b + c) = a \times b$ et $(a \times b) + (a \times c) = (a \times b) + 0 = a \times b$, donc $a \times (b + c) = (a \times b) + (a \times c)$.
- Si $\mathrm{sgn}(a) = 1$, $\mathrm{sgn}(b) = \mathrm{sgn}(c) = 0$, $b \neq 0$ et $c \neq 0$, alors $a \times (b + c) = a \times (0, |b| + |c|) = (1, |a| \times (|b| + |c|))$ et $(a \times b) + (a \times c) = (1, |a| \times |b|) + (1, |a| \times |c|) = (1, (|a| \times |b|) + (|a| \times |c|))$. Comme précédemment, on a donc $a \times (b + c) = (a \times b) + (a \times c)$.
- Si $\mathrm{sgn}(a) = 0$, $\mathrm{sgn}(b) = \mathrm{sgn}(c) = 1$ et $a \neq 0$, alors $a \times (b + c) = a \times (1, |b| + |c|) = (1, |a| \times (|b| + |c|))$ et $(a \times b) + (a \times c) = (1, |a| \times |b|) + (1, |a| \times |c|) = (1, (|a| \times |b|) + (|a| \times |c|))$. Comme précédemment, on a donc $a \times (b + c) = (a \times b) + (a \times c)$.
- Supposons $\mathrm{sgn}(a) = \mathrm{sgn}(c) = 0$, $\mathrm{sgn}(b) = 1$ et $a \neq 0$. Alors, $(a \times b) + (a \times c) = (1, |a| \times |b|) + (0, |a| \times |c|)$. Cette quantité est égale à $(1, |a| \times |b| - |a| \times |c|)$ si $|a| \times |b| > |a| \times |c|$, *i.e.*, si $|b| > |c|$, et à $(0, |a| \times |c| - |a| \times |b|)$ sinon. Par ailleurs, $b + c$ est égal à $(1, |b| - |c|)$ si $|b| > |c|$ et $(0, |c| - |b|)$ sinon. Donc, $a \times (b + c)$ est égal à $(1, |a|(|b| - |c|))$ dans le premier cas et à $(0, |a|(|c| - |b|))$ dans le second. Puisque $|a|(|b| - |c|) = |a||b| - |a||c|$ dans le premier cas et $|a|(|b| - |c|) = |a||c| - |a||b|$ dans le second, on en déduit $a \times (b + c) = (a \times b) + (a \times c)$.
- Supposons $\mathrm{sgn}(a) = \mathrm{sgn}(c) = 1$, $\mathrm{sgn}(b) = 0$ et $b \neq 0$. Alors, $(a \times b) + (a \times c) = (1, |a| \times |b|) + (0, |a| \times |c|)$. Cette quantité est égale à $(1, |a| \times |b| - |a| \times |c|)$ si $|a| \times |b| > |a| \times |c|$, *i.e.*, si $|b| > |c|$, et à $(0, |a| \times |c| - |a| \times |b|)$ sinon. Par ailleurs, $b + c$ est égal à $(0, |b| - |c|)$ si $|b| \geq |c|$ et $(1, |c| - |b|)$ sinon. Donc, $a \times (b + c)$ est égal à $(1, |a|(|b| - |c|))$ si $|b| > |c|$ et à $(0, |a|(|c| - |b|))$ sinon (y compris si $|b| = |c|$, puisqu'alors $(0, |c| - |b|) = (0,0)$). Puisque $|a|(|b| - |c|) = |a||b| - |a||c|$ dans le premier cas et $|a|(|c| - |b|) = |a||c| - |a||b|$ dans le second, on en déduit $a \times (b + c) = (a \times b) + (a \times c)$.
- Les deux derniers cas, où a et b sont de même signe et c de signe différent avec a, b et c non nuls, se ramènent aux deux cas précédents par commutativité de l'addition. En effet, ces derbiers montrent que $a \times (c + b) = (a \times c) + (a \times b)$, et donc, par commutativité de l'addition, $a \times (b + c) = (a \times b) + (a \times c)$.

□

1.5.7 Puissance

Puissance d'entiers relatifs : Soit E l'ensemble des fonctions de $\mathbb{Z}$ dans $\mathbb{Z}$. On définit la suite Exp d'éléments de E par récurrence de la manière suivante :

- Pour tout élément m de $\mathbb{Z}$, $\text{Exp}(0)(m) = (0,1)$ (cela définit Exp(0)).
- Pour tout élément n de $\mathbb{N}$, pour tout élément m de $\mathbb{Z}$, $\text{Exp}(n+1)(m) = \text{Exp}(n)(m) \times m$ (cela définit $\text{Exp}(n+1)$ à partir de $\text{Exp}(n)$).

Notons que, pour tout élément m de $\mathbb{Z}$, on a $\text{Exp}(1)(m) = m$. Dans la suite, pour tous éléments n et m de $\mathbb{Z}$, on notera l'entier $\text{Exp}(n)(m)$ par m^n. Pour tous éléments n et m de $\mathbb{Z}$, on a donc $m^0 = 1$, $m^1 = m$ et $m^{n+1} = m^n \times m$. L'exponentiation est prioritaire sur la multiplication et l'addition. Par exemple, si a, b et c sont trois éléments de $\mathbb{Z}$, $a^b \times c$ est équivalent à $(a^b) \times c$ et $a^b + c$ est équivalent à $(a^b) + c$.

Lemme : Soit n et m deux entiers naturels. Alors, $(0,m)^n = (0,m^n)$.

Démonstration : On procède par récurrence sur n. Pour $n = 0$, on a $(0,m)^n = (0,1)$ et $(0,m^n) = (0,1)$, donc $(0,m)^n = (0,m^n)$. Soit n un entier naturel tel que $(0,m)^n = (0,m^n)$. Alors, $(0,m)^{n+1} = (0,m)^n \times (0,m) = (0,m^n) \times (0,m) = (0,\, m^n \times m) = (0,\, m^{n+1})$. Donc, $(0,m)^{n+1} = (0,m^{n+1})$. Par récurence, on en déduit que le résultat est vrai pour tout entier narurel n.

□

Lemme : Soit n un entier naturel et m un entier naturel non nul. Alors, $(1,m)^{2n} = (0,m^{2n})$ et $(1,m)^{2n+1} = (1,m^{2n+1})$.

Démonstration : On procède par récurrence sur n. Pour $n = 0$, on a $(1,m)^{2n} = (1,m)^0 = (0,1) = (0,m^0) = (0,m^{2n})$ et $(1,m)^{2n+1} = (1,m)^{2n} \times (1,m) = (0,1) \times (1,m) = (1,m) = (1,m^1) = (1,m^{2n+1})$. Donc, $(1,m)^{2n} = (0,m^{2n})$ et $(1,m)^{2n+1} = (1,m^{2n+1})$.

Soit n un entier naurel tel que $(1,m)^{2n} = (0,m^{2n})$ et $(1,m)^{2n+1} = (1,m^{2n+1})$. Alors, $(1,m)^{2(n+1)} = (1,m)^{2n+2} = (1,m)^{(2n+1)+1} = (1,m)^{2n+1} \times (1,m) = (1,\, m^{2n+1}) \times (1,m) = (0,m^{2n+1} \times m) = (0,\, m^{2n+1+1}) = (0,\, m^{2(n+1)})$ et $(1,m)^{2(n+1)+1} = (1,m)^{2(n+1)} \times (1,m) = (0,\, m^{2(n+1)}) \times (1,m) = (1,m^{2(n+1)} \times m) = (1,\, m^{2(n+1)+1})$. Donc, $(1,m)^{2(n+1)} = (0,\, m^{2(n+1)})$ et $(1,m)^{2(n+1)+1} = (1,\, m^{2(n+1)+1})$. Par récurrence, le résultat attendu est vrai pour tout entier naturel n.

□

1.5.8 Factoriel

Définition : Soit n un entier relatif. Si $n \geq 0$, alors on peut choisir un entier naturel m tel que $n = (0,m)$. On pose alors $n! = m!$. Sinon, on pose $n! = 0$.

1.5.9 Fonctions min et max

On définit les deux fonctions min et max sur $\mathbb{Z}^2$ de la manière suivante : si a et b sont deux entiers naturels, alors

$$\min(a,b) = \begin{cases} a & \text{si } a \leq b \\ b & \text{si } a > b \end{cases}, \qquad \max(a,b) = \begin{cases} a & \text{si } a \geq b \\ b & \text{si } a < b \end{cases}.$$

Lemme : Soit a, b et c trois éléments de $\mathbb{Z}$. Alors,

- Si $c \leq \min(a,b)$, alors $c \leq a$ et $c \leq b$.
- Si $c < \min(a,b)$, alors $c < a$ et $c < b$.
- Si $c \geq \max(a,b)$, alors $c \geq a$ et $c \geq b$.
- Si $c > \max(a,b)$, alors $c > a$ et $c > b$.

Démonstration : Considérons le cas où $a \leq b$. Si $b < a$, on se ramène à ce cas en échangeant les rôles de a et b (puisqu'on a alors $b \leq a$), le résultat étant symétrique par échange de ces deux nombres. On a alors $\min(a,\, b) = a$ et $\max(a,\, b) = b$.

- Si $c \leq \min(a,b)$, alors $c \leq a$. Puisque $a \leq b$, cela donne $c \leq b$.
- Si $c < \min(a,b)$, alors $c < a$. Puisque $a \leq b$, cela donne $c < b$.
- Si $c \geq \max(a,b)$, alors $c \geq b$. Puisque $b \geq a$, cela donne $c \geq a$.
- Si $c > \max(a,b)$, alors $c > b$. Puisque $b \geq a$, cela donne $c > a$.

□

Appendice A : Jeux avec les entiers

A.1 Liste des premiers nombres premiers

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163
167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331
337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503
509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691
701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887
907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063
1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229
1231 1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409
1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553
1559 1567 1571 1579 1583 1597 1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697 1699 1709
1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879
1889 1901 1907 1913 1931 1933 1949 1951 1973 1979 1987 1993 1997 1999 2003 2011 2017 2027 2029 2039 2053 2063
2069 2081 2083 2087 2089 2099 2111 2113 2129 2131 2137 2141 2143 2153 2161 2179 2203 2207 2213 2221 2237 2239
2243 2251 2267 2269 2273 2281 2287 2293 2297 2309 2311 2333 2339 2341 2347 2351 2357 2371 2377 2381 2383 2389
2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477 2503 2521 2531 2539 2543 2549 2551 2557 2579 2591
2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683 2687 2689 2693 2699 2707 2711 2713 2719 2729 2731
2741 2749 2753 2767 2777 2789 2791 2797 2801 2803 2819 2833 2837 2843 2851 2857 2861 2879 2887 2897 2903 2909
2917 2927 2939 2953 2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041 3049 3061 3067 3079 3083 3089 3109
3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221 3229 3251 3253 3257 3259 3271 3299 3301 3307
3313 3319 3323 3329 3331 3343 3347 3359 3361 3371 3373 3389 3391 3407 3413 3433 3449 3457 3461 3463 3467 3469
3491 3499 3511 3517 3527 3529 3533 3539 3541 3547 3557 3559 3571 3581 3583 3593 3607 3613 3617 3623 3631 3637
3643 3659 3671 3673 3677 3691 3697 3701 3709 3719 3727 3733 3739 3761 3767 3769 3779 3793 3797 3803 3821 3823
3833 3847 3851 3853 3863 3877 3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001 4003 4007
4013 4019 4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133 4139 4153 4157 4159 4177 4201
4211 4217 4219 4229 4231 4241 4243 4253 4259 4261 4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373
4391 4397 4409 4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547 4549 4561 4567
4583 4591 4597 4603 4621 4637 4639 4643 4649 4651 4657 4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759
4783 4787 4789 4793 4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937 4943 4951 4957
4967 4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059 5077 5081 5087 5099 5101 5107 5113 5119
5147 5153 5167 5171 5179 5189 5197 5209 5227 5231 5233 5237 5261 5273 5279 5281 5297 5303 5309 5323 5333 5347
5351 5381 5387 5393 5399 5407 5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501 5503 5507 5519
5521 5527 5531 5557 5563 5569 5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669 5683 5689 5693 5701
5711 5717 5737 5741 5743 5749 5779 5783 5791 5801 5807 5813 5821 5827 5839 5843 5849 5851 5857 5861 5867 5869
5879 5881 5897 5903 5923 5927 5939 5953 5981 5987 6007 6011 6029 6037 6043 6047 6053 6067 6073 6079 6089 6091
6101 6113 6121 6131 6133 6143 6151 6163 6173 6197 6199 6203 6211 6217 6221 6229 6247 6257 6263 6269 6271 6277
6287 6299 6301 6311 6317 6323 6329 6337 6343 6353 6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469
6473 6481 6491 6521 6529 6547 6551 6553 6563 6569 6571 6577 6581 6599 6607 6619 6637 6653 6659 6661 6673 6679
6689 6691 6701 6703 6709 6719 6733 6737 6761 6763 6779 6781 6791 6793 6803 6823 6827 6829 6833 6841 6857 6863
6869 6871 6883 6899 6907 6911 6917 6947 6949 6959 6961 6967 6971 6977 6983 6991 6997 7001 7013 7019 7027 7039
7043 7057 7069 7079 7103 7109 7121 7127 7129 7151 7159 7177 7187 7193 7207 7211 7213 7219 7229 7237 7243 7247
7253 7283 7297 7307 7309 7321 7331 7333 7349 7351 7369 7393 7411 7417 7433 7451 7457 7459 7477 7481 7487 7489
7499 7507 7517 7523 7529 7537 7541 7547 7549 7559 7561 7573 7577 7583 7589 7591 7603 7607 7621 7639 7643 7649
7669 7673 7681 7687 7691 7699 7703 7717 7723 7727 7741 7753 7757 7759 7789 7793 7817 7823 7829 7841 7853 7867
7873 7877 7879 7883 7901 7907 7919 7927 7933 7937 7949 7951 7963 7993 8009 8011 8017 8039 8053 8059 8069 8081
8087 8089 8093 8101 8111 8117 8123 8147 8161 8167 8171 8179 8191 8209 8219 8221 8231 8233 8237 8243 8263 8269
8273 8287 8291 8293 8297 8311 8317 8329 8353 8363 8369 8377 8387 8389 8419 8423 8429 8431 8443 8447 8461 8467
8501 8513 8521 8527 8537 8539 8543 8563 8573 8581 8597 8599 8609 8623 8627 8629 8641 8647 8663 8669 8677 8681
8689 8693 8699 8707 8713 8719 8731 8737 8741 8747 8753 8761 8779 8783 8803 8807 8819 8821 8831 8837 8839 8849
8861 8863 8867 8887 8893 8923 8929 8933 8941 8951 8963 8969 8971 8999 9001 9007 9011 9013 9029 9041 9043 9049
9059 9067 9091 9103 9109 9127 9133 9137 9151 9157 9161 9173 9181 9187 9199 9203 9209 9221 9227 9239 9241 9257
9277 9281 9283 9293 9311 9319 9323 9337 9341 9343 9349 9371 9377 9391 9397 9403 9413 9419 9421 9431 9433 9437

A.2 Décomposition des premiers entiers en produits de facteurs premiers

$2 = 2^1$
$3 = 3^1$
$4 = 2^2$
$5 = 5^1$
$6 = 2^1 \times 3^1$
$7 = 7^1$
$8 = 2^3$
$9 = 3^2$
$10 = 2^1 \times 5^1$
$11 = 11^1$
$12 = 2^2 \times 3^1$
$13 = 13^1$
$14 = 2^1 \times 7^1$
$15 = 3^1 \times 5^1$
$16 = 2^4$
$17 = 17^1$
$18 = 2^1 \times 3^2$
$19 = 19^1$
$20 = 2^2 \times 5^1$
$21 = 3^1 \times 7^1$
$22 = 2^1 \times 11^1$
$23 = 23^1$
$24 = 2^3 \times 3^1$
$25 = 5^2$
$26 = 2^1 \times 13^1$
$27 = 3^3$
$28 = 2^2 \times 7^1$
$29 = 29^1$
$30 = 2^1 \times 3^1 \times 5^1$
$31 = 31^1$
$32 = 2^5$
$33 = 3^1 \times 11^1$
$34 = 2^1 \times 17^1$
$35 = 5^1 \times 7^1$
$36 = 2^2 \times 3^2$
$37 = 37^1$
$38 = 2^1 \times 19^1$
$39 = 3^1 \times 13^1$
$40 = 2^3 \times 5^1$
$41 = 41^1$
$42 = 2^1 \times 3^1 \times 7^1$
$43 = 43^1$
$44 = 2^2 \times 11^1$
$45 = 3^2 \times 5^1$
$46 = 2^1 \times 23^1$
$47 = 47^1$
$48 = 2^4 \times 3^1$
$49 = 7^2$
$50 = 2^1 \times 5^2$
$51 = 3^1 \times 17^1$
$52 = 2^2 \times 13^1$
$53 = 53^1$
$54 = 2^1 \times 3^3$
$55 = 5^1 \times 11^1$
$56 = 2^3 \times 7^1$
$57 = 3^1 \times 19^1$
$58 = 2^1 \times 29^1$
$59 = 59^1$
$60 = 2^2 \times 3^1 \times 5^1$
$61 = 61^1$
$62 = 2^1 \times 31^1$
$63 = 3^2 \times 7^1$
$64 = 2^6$
$65 = 5^1 \times 13^1$
$66 = 2^1 \times 3^1 \times 11^1$
$67 = 67^1$
$68 = 2^2 \times 17^1$
$69 = 3^1 \times 23^1$
$70 = 2^1 \times 5^1 \times 7^1$
$71 = 71^1$
$72 = 2^3 \times 3^2$
$73 = 73^1$
$74 = 2^1 \times 37^1$
$75 = 3^1 \times 5^2$
$76 = 2^2 \times 19^1$
$77 = 7^1 \times 11^1$
$78 = 2^1 \times 3^1 \times 13^1$
$79 = 79^1$
$80 = 2^4 \times 5^1$
$81 = 3^4$
$82 = 2^1 \times 41^1$
$83 = 83^1$
$84 = 2^2 \times 3^1 \times 7^1$
$85 = 5^1 \times 17^1$
$86 = 2^1 \times 43^1$
$87 = 3^1 \times 29^1$
$88 = 2^3 \times 11^1$
$89 = 89^1$
$90 = 2^1 \times 3^2 \times 5^1$
$91 = 7^1 \times 13^1$
$92 = 2^2 \times 23^1$
$93 = 3^1 \times 31^1$
$94 = 2^1 \times 47^1$
$95 = 5^1 \times 19^1$
$96 = 2^5 \times 3^1$
$97 = 97^1$
$98 = 2^1 \times 7^2$
$99 = 3^2 \times 11^1$
$100 = 2^2 \times 5^2$
$101 = 101^1$
$102 = 2^1 \times 3^1 \times 17^1$
$103 = 103^1$
$104 = 2^3 \times 13^1$
$105 = 3^1 \times 5^1 \times 7^1$
$106 = 2^1 \times 53^1$
$107 = 107^1$
$108 = 2^2 \times 3^3$
$109 = 109^1$
$110 = 2^1 \times 5^1 \times 11^1$
$111 = 3^1 \times 37^1$
$112 = 2^4 \times 7^1$
$113 = 113^1$
$114 = 2^1 \times 3^1 \times 19^1$
$115 = 5^1 \times 23^1$
$116 = 2^2 \times 29^1$
$117 = 3^2 \times 13^1$
$118 = 2^1 \times 59^1$
$119 = 7^1 \times 17^1$
$120 = 2^3 \times 3^1 \times 5^1$
$121 = 11^2$
$122 = 2^1 \times 61^1$
$123 = 3^1 \times 41^1$
$124 = 2^2 \times 31^1$
$125 = 5^3$
$126 = 2^1 \times 3^2 \times 7^1$
$127 = 127^1$
$128 = 2^7$
$129 = 3^1 \times 43^1$
$130 = 2^1 \times 5^1 \times 13^1$
$131 = 131^1$
$132 = 2^2 \times 3^1 \times 11^1$
$133 = 7^1 \times 19^1$
$134 = 2^1 \times 67^1$
$135 = 3^3 \times 5^1$
$136 = 2^3 \times 17^1$
$137 = 137^1$
$138 = 2^1 \times 3^1 \times 23^1$
$139 = 139^1$
$140 = 2^2 \times 5^1 \times 7^1$
$141 = 3^1 \times 47^1$
$142 = 2^1 \times 71^1$
$143 = 11^1 \times 13^1$
$144 = 2^4 \times 3^2$
$145 = 5^1 \times 29^1$
$146 = 2^1 \times 73^1$
$147 = 3^1 \times 7^2$
$148 = 2^2 \times 37^1$
$149 = 149^1$
$150 = 2^1 \times 3^1 \times 5^2$
$151 = 151^1$
$152 = 2^3 \times 19^1$
$153 = 3^2 \times 17^1$
$154 = 2^1 \times 7^1 \times 11^1$
$155 = 5^1 \times 31^1$
$156 = 2^2 \times 3^1 \times 13^1$
$157 = 157^1$
$158 = 2^1 \times 79^1$
$159 = 3^1 \times 53^1$
$160 = 2^5 \times 5^1$
$161 = 7^1 \times 23^1$
$162 = 2^1 \times 3^4$
$163 = 163^1$
$164 = 2^2 \times 41^1$
$165 = 3^1 \times 5^1 \times 11^1$
$166 = 2^1 \times 83^1$
$167 = 167^1$
$168 = 2^3 \times 3^1 \times 7^1$
$169 = 13^2$
$170 = 2^1 \times 5^1 \times 17^1$
$171 = 3^2 \times 19^1$
$172 = 2^2 \times 43^1$
$173 = 173^1$
$174 = 2^1 \times 3^1 \times 29^1$
$175 = 5^2 \times 7^1$
$176 = 2^4 \times 11^1$
$177 = 3^1 \times 59^1$
$178 = 2^1 \times 89^1$
$179 = 179^1$
$180 = 2^2 \times 3^2 \times 5^1$
$181 = 181^1$
$182 = 2^1 \times 7^1 \times 13^1$
$183 = 3^1 \times 61^1$
$184 = 2^3 \times 23^1$
$185 = 5^1 \times 37^1$
$186 = 2^1 \times 3^1 \times 31^1$
$187 = 11^1 \times 17^1$
$188 = 2^2 \times 47^1$
$189 = 3^3 \times 7^1$
$190 = 2^1 \times 5^1 \times 19^1$
$191 = 191^1$
$192 = 2^6 \times 3^1$
$193 = 193^1$
$194 = 2^1 \times 97^1$
$195 = 3^1 \times 5^1 \times 13^1$
$196 = 2^2 \times 7^2$
$197 = 197^1$
$198 = 2^1 \times 3^2 \times 11^1$
$199 = 199^1$
$200 = 2^3 \times 5^2$
$201 = 3^1 \times 67^1$
$202 = 2^1 \times 101^1$
$203 = 7^1 \times 29^1$
$204 = 2^2 \times 3^1 \times 17^1$
$205 = 5^1 \times 41^1$
$206 = 2^1 \times 103^1$
$207 = 3^2 \times 23^1$
$208 = 2^4 \times 13^1$
$209 = 11^1 \times 19^1$
$210 = 2^1 \times 3^1 \times 5^1 \times 7^1$
$211 = 211^1$
$212 = 2^2 \times 53^1$
$213 = 3^1 \times 71^1$
$214 = 2^1 \times 107^1$
$215 = 5^1 \times 43^1$
$216 = 2^3 \times 3^3$
$217 = 7^1 \times 31^1$
$218 = 2^1 \times 109^1$
$219 = 3^1 \times 73^1$
$220 = 2^2 \times 5^1 \times 11^1$
$221 = 13^1 \times 17^1$
$222 = 2^1 \times 3^1 \times 37^1$
$223 = 223^1$
$224 = 2^5 \times 7^1$
$225 = 3^2 \times 5^2$
$226 = 2^1 \times 113^1$
$227 = 227^1$
$228 = 2^2 \times 3^1 \times 19^1$
$229 = 229^1$
$230 = 2^1 \times 5^1 \times 23^1$
$231 = 3^1 \times 7^1 \times 11^1$
$232 = 2^3 \times 29^1$
$233 = 233^1$
$234 = 2^1 \times 3^2 \times 13^1$
$235 = 5^1 \times 47^1$
$236 = 2^2 \times 59^1$
$237 = 3^1 \times 79^1$
$238 = 2^1 \times 7^1 \times 17^1$
$239 = 239^1$
$240 = 2^4 \times 3^1 \times 5^1$
$241 = 241^1$
$242 = 2^1 \times 11^2$
$243 = 3^5$
$244 = 2^2 \times 61^1$
$245 = 5^1 \times 7^2$
$246 = 2^1 \times 3^1 \times 41^1$
$247 = 13^1 \times 19^1$
$248 = 2^3 \times 31^1$
$249 = 3^1 \times 83^1$
$250 = 2^1 \times 5^3$
$251 = 251^1$

Cette décomposition est utile pour calculer le nombre de diviseurs $\varphi(n)$ d'un entier naturel non nul n : $\varphi(1) = 1$ et, pour tour entier naturel n strictement supérieur à 1, $\varphi(n)$ est égal au produit des puissances apparaissant dans la décomposition de n augmentées de 1. Cela est représenté figure A.1 et figure A.2. (Le code utilisé dans cette section se trouve dans le fichier **decomposition_prime_factors.rs**.)

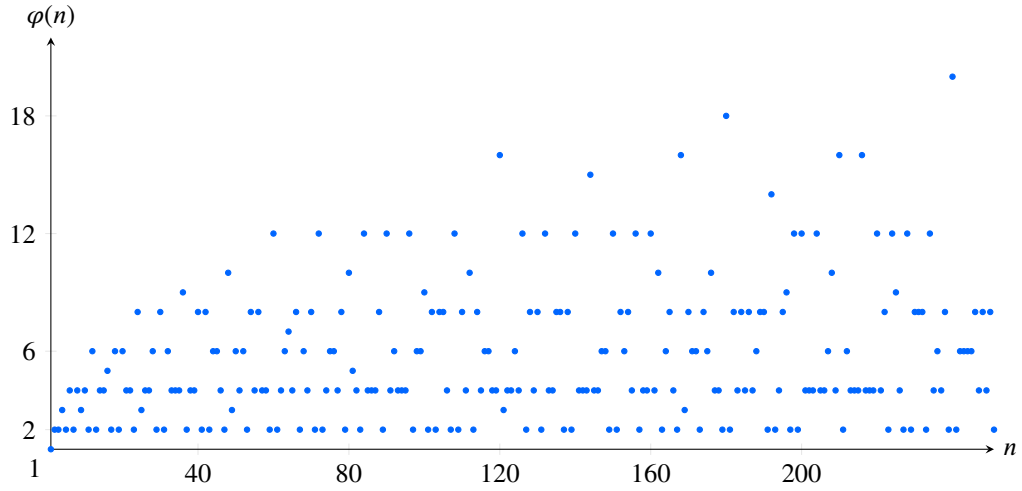


Figure A.1 Nombre de diviseurs d'un entier naturel non nul n, noté $\varphi(n)$, en fonction de n pour n allant de 1 à 251. Notons que $\varphi(1) = 1$ et, pour tout entier naturel non nul n, $\varphi(n) = 2$ si et seulement si n est premier.

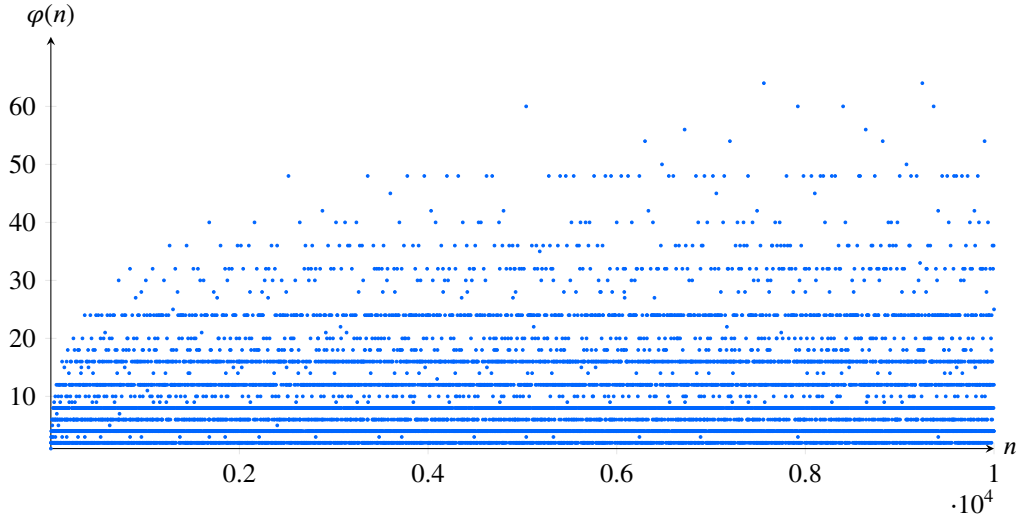


Figure A.2 Même plot que sur la figure A.1 pour n allant de 1 à 10000.

A.3 Une séquence de nombres pseudo-aléatoire

La séquence de nombres suivante sera (avec une très haute probabilité) différent à chaque compilation de ce document. (Il y a 10^{4278} possibilités différentes.)

```
75982879416627564179161569685791345375166700811838048768317482230845726294995198361658014325163372652372241815034866978239078769384758683299315173649569918884494247825191402019948957822009276790677464581824608181199092126082963830409120143320968634058336143124948507810555392345025487550894976527351495156139855018286082379104470842657936705152289811769067898007498212869124351111264337854237285918118058675400937210592717430372370913651693865188784635972552990962609037402527115413686870146929054546052389692258090749480466662506403905028734975232183074141267833860964839248170533884969888825934935283013404551140554293587543221843133687884558898076517136982582286765743387813260460651323669621929654009671367822602534229645679141634547703858512300108617859207556790759499199591932335506439730023951933834216400698937079815884949720047321333065637776636649403728246569520172666680569036148314984538109151812370203406475275378287202475288263607792757468863058398218268204388087377575086237900877383324346495857422937650292865057688041480939572619479028157264519997262952101070754576860216067095393446509006494657156170171808575686601640968345960866064597645773271344781712334026809005362239349312162751240616901564504326562764907198154267141094828261203378527110774323656651804444998517712311055474850400713699446757089511502248920605713188718979047988601620847933811857742206221181557699013135565284732937232126994585393843494162012196825288470156817593281049696666533338809319482437227502799615831836181029596153134431236473057383690807790457817044360727936823836782224493212687766006459604251470962099951035749455782644710577971073679805915493712547290551840773101794223021128163001534685954285671199918164807273293928062158896038310726899386801581303455386537630656494962148790423564269059736312616826042936534912177679433951805605663922894817959055448016585621359577998398855690071558252787945209243681419155037366578537088528773546244841948257478201130745691935709051075670027669742677222966705477316818124364587072510194126098320936821133633716263971285870871552340010052599393761529244751901646263803116797594127985762326785487804382479586894383286447510808788482915673454818704376242299015622115462132597679658454821210503635841874522299457477324592183874139095459958154966031188082556638217867449481501635936922795648955608204602687436274958574294750666671542523417209774984835506740966119813128545863364379119855146364497289444378999491625869921235125041080338709282107403951255437772905944464258840962688391211248287685803899624743804212702471047510055956291195032921117643868442235282594216506741051419085244465131724168288472318950785232620157126268748970259505907965197267567333575671520649872175655896917544844394195360624792161924281917699296046137261357662747729033682091077861916828690988766132115855542767108461601807475210681509436727918105977062096355809069431359756424454906493782619594453989481176302706246582487375006102307863512599990759969482720532310560908978139827379672844919913253359425020797844473528312629777422037453210460046052670141878710835681008637674879647016445512102995516164821504261138775205435718060697355882220590570926179814759876136406503551010801933395133089671330731138918541286035952495889472726967256946756985119272524132951489652286447602883430280635222767343982888529823310285208779660026779512285401975328207436176454707849625980935824840357001355982647673671861183424602532385346082288532156838733456733907624637364836962761216670277484735320863324656410383930786440963592100202752991322634230758183205038034244020856871633091786294663798044900105594780262909104057480317451958467783896371091209857508220891568355471440103078083343073373560894565028911652781043403445106036516559576824842217990661831586635345906600490969892411511178270799109791855865014342383002851371017535899979594653635332348037416544304967029151733695421279359574970245475351075003922443585238819733307708082985029577936358771464847815304381376966947613505828161279722802364771012085742836561870719265756428994502219371869800876031916350755262129043523939929016647744520610789246953352419715743662244159378816982405567311957561558341871464145181785873373604363947668689485780659536333404502425709436333403013732683812119670026715892867475950373586865188888079471206424790596609116870433836534446830749610946941369059306492274328246785103360470095476678153652354378513884058050572988839035771
```

Index

Index des symboles