Ordinaux et cardinaux

-

Le Barbuki 2

1ère édition

Florian Langlois

Rédigé entre mars 2024 et août 2024

Collection

Bienvenue dans ce livre ! C'est le deuxième d'une collection qui tente d'exposer et démontrer les mathématiques de niveau licence et master. Le nom BARBUKI est une référence au célèbre groupe BOURBAKI, dont la démarche de cette collection est inspirée.

1 – Théorie élémentaire des ensembles

2 – Ordinaux et cardinaux

Avant-propos

Cet ouvrage est là pour me permettre de coucher sur le papier les différentes mathématiques que j'ai apprises durant mes études supérieures : je le rédige principalement pour moi-même et il n'a pas pour but d'être pédagogique. Il va me permettre de conserver sur le long terme une trace de ces connaissances, mais aussi d'organiser celles-ci pour en avoir une vue d'ensemble.

Bien que ce livre reste assez personnel, il est possible qu'il vous soit utile. Afin de comprendre pleinement son contenu, il est nécessaire d'être au courant de ce dont parle le premier ouvrage, c'est-à-dire des bases de la théorie des ensembles, notamment à travers les différents axiomes de ZFC.

Il vous faut aussi savoir mener un raisonnement, ou tout du moins en suivre un, puisque c'est l'un des objets principaux de ce livre. Il est à noter que la construction de cette collection se fait sous la manière d'un escalier à gravir : nous n'utiliserons pas des résultats postérieurs pour démontrer des résultats antérieurs, les seules exceptions étant les exemples donnés pour illustrer, puisque ceux-ci ne sont là que pour aider à la lecture, et non permettre une quelconque démonstration, mais aussi certaines digressions abordant d'autres démonstrations que celles proposées.

Remerciements

Merci à Lyra, GrothenDitQue, Chæris, Cassis et Shika pour leur pinaillage.

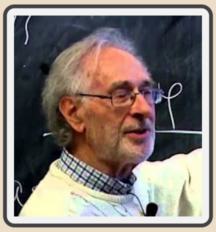
Les biographiques de mathématiciens sont en parties inspirées de Wikipédia ainsi que de l'excellent ouvrage *Des mathématiciens de A à Z* de Daniel Suratteau et Bertrand Hauchecorne, paru en 2008 aux éditions Ellipses.

Le contenu à proprement parlé est très fortement inspiré de l'incroyable ouvrage *The Foundations of Mathematics* de Kenneth Kunen dans son édition de 2007, ainsi que de *Théorie des ensembles* de Jean-Louis Krivine, paru aux éditions Cassini en 2007.

Pour la petite histoire

Kenneth Kunen (2 août 1943 – 14 août 2020) est un mathématicien américain, professeur émérite de mathématiques à l'université du Wisconsin à Madison qui travaillait en théorie des ensembles et à ses applications en topologie et en théorie de la mesure.

Pour la petite histoire



Jean-Louis Krivine (1939 –) est professeur à l'Université Paris7, spécialiste de géométrie algébrique réelle, d'analyse fonctionnelle, de logique et d'informatique théorique. Il a créé, en 1982, l'équipe de logique mathématique, qui est l'un des plus importants laboratoires au monde dans ce domaine. Lauréat de l'Académie des Sciences en 1994 et Prix du Rayonnement français en 2004, il est l'auteur de plusieurs ouvrages de référence en logique.

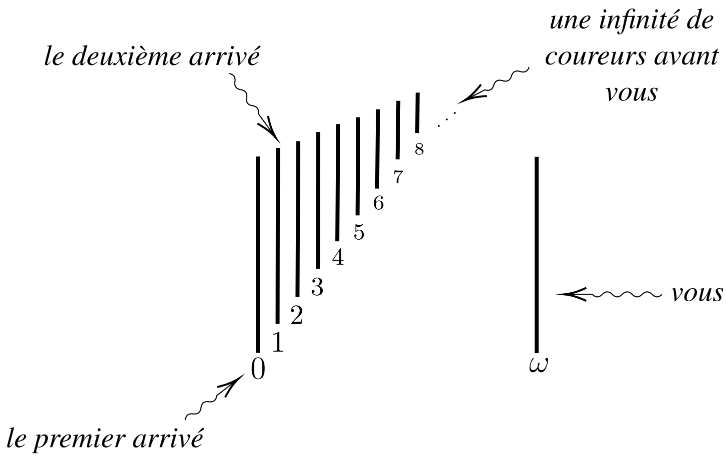
Table des matières

Chapitre 1

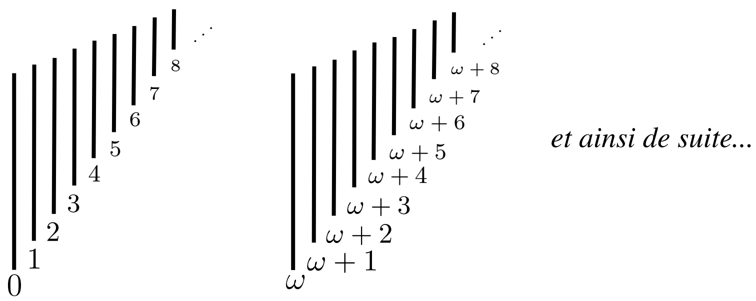
Ordinaux

Sommaire

Imaginez une course à laquelle vous concourez et à laquelle participe une infinité de coureurs. À la fin de la course, chaque participant se voit attribuer un nombre en fonction de l'ordre dans lequel il est arrivé : le premier arrivé reçoit le nombre 0, le deuxième le nombre 1, le troisième le nombre 2, et ainsi de suite pour chaque entier naturel. Et vous ? Vous arrivez après tous les coureurs ayant reçu un nombre entier naturel ! Quel nombre vous correspond-il ? Certainement pas un entier naturel, puisque ceux-ci ont déjà tous été attribués. Il faut donc introduire un nouveau nombre : on le note généralement ω.



Quel nombre attribuer alors à votre ami arrivé juste après vous ? Le nombre $\omega + 1$ naturellement ! Et $\omega + 2$ pour la personne juste après-lui, puis $\omega + 3$ et ainsi de suite pour les suivants !



Ces nouveaux nombres que nous venons d'introduire font partie de ce que l'on appelle les **nombres ordinaux**, catégorie dans laquelle se trouvent aussi les entiers naturels. L'objet de ce chapitre est justement de définir et développer les nombres ordinaux. Cela s'inscrit dans un contexte plus général qui est celui des **ensembles bien ordonnés**, pour lesquels chaque partie non vide admet un minimum, permettant de répondre notamment à la question « *quel élément vient juste après celui-ci ?* ». S'intéresser aux ordinaux présente différentes vertus :

- comme les nombres entiers naturels en font partie, nous aurons enfin l'occasion de les définir proprement.
- même si l'exemple de la course est un peu fantaisiste, des situations où l'on souhaite ordonner des choses avec l'une d'entre elle après une infinité d'autres peuvent se présenter à nous et les ordinaux représentent un outil de choix pour cela.
- enfin, les ordinaux constituent le cadre idéal pour compter le nombre d'éléments des ensembles, ce qui sera l'objet du chapitre 3.

1 Classes et assertions fonctionnelles

1.1 Assertions à paramètres

Dans le livre précédent, nous avons commencé par expliquer que les objets que nous manipulons sont tous considérés comme des ensembles, au point que la notion d'ensemble est en fait primitive. On ne donne pas de définition a priori de ce qu'est un ensemble, on impose juste des axiomes afin de mimer l'intuition d'ensemble.

Nous avons ensuite indiqué que ce ne sont pas les seuls choses manipulables : il y a aussi les assertions, qui sont des affirmations pouvant être vraies ou fausses. Il s'agit au fond d'une façon de structurer le discours à propos des ensembles. L'auteur de ce livre considère que le lecteur est au clair sur ces choses-là. Cependant, il estime aussi devoir préciser un certain nombre de nuances concernant les assertions. Certaines de ces définitions sont déjà évoquées dans le livre précédent, mais un rappel ne fait jamais de mal.

Définition 1 (Assertion à paramètres)

Une **assertion à paramètres** est une assertion qui nécessite un ou plusieurs paramètres pour être énoncée, et donc la vérité peut varier en fonction de ces paramètres éventuels. Un paramètre est toujours un ensemble.

Exemple :

1. L'assertion $P(n)$ définie par « n *est un entier pair* » dépend de qui est n. C'est en cela que l'on précise entre parenthèses la dépendance de P par rapport à n, pour insister sur ce point.
2. En revanche, l'assertion $Q(x)$ définie par « $x = x$ » est toujours vraie, quand bien même elle nécessite le paramètre x pour être énoncée.

1.2 Classes

La notion d'ensemble est née de l'idée de vouloir réunir et regrouper plusieurs objets différents : typiquement $\mathbb{Z}$ est l'ensemble qui contient tous les entiers relatifs. C'est justement le but du premier livre d'expliciter les règles que nous avons choisies ici pour régir les ensembles. Cependant afin d'éviter certains paradoxes et contradictions, nous avons dû restreindre la portée des ensembles : il n'est par exemple pas possible de définir l'ensemble de tous les ensembles, et si on le permettait on aboutirait au paradoxe de Russell. Nous verrons aussi plus tard, après avoir défini la notion d'ordinaux, qu'il est impossible d'avoir un ensemble contenant tous les ordinaux.

Cependant, nous aimerions bien pouvoir simplifier nos discours concernant "*tous les ensembles*" ou "*tous les ordinaux*", c'est-à-dire réunir différents objets sans pour autant craindre de former un ensemble paradoxal, ou même sans être freiné par les axiomes ensemblistes. C'est là qu'interviennent les **classes**. Heureusement, cela ne va pas nécessiter d'introduire autre chose que les ensembles ou que les assertions. En effet, nous allons définir la notion de classe comme étant la même que celle d'assertion à paramètres, le nouveau nom étant simplement associé à un nouvel usage. Il s'agit d'une approche similaire à celle que nous avons faite dans le premier livre concernant les familles : il n'y a à strictement parler pas de différence entre les familles et les applications, simplement un usage différent et des notations différentes.

L'intérêt des classes est comme nous l'avons dit de pouvoir regrouper différents objets, et donc beaucoup des notions associées aux classes sont inspirées de celles associées aux ensembles, notamment l'appartenance. Il n'est donc pas étonnant qu'on retrouve par exemple le symbole $\in$.

Définition 2 (Classe)

Soit C une assertion à paramètres.
Si C nécessite un seul paramètre pour être énoncée, on dit parfois que C est une **classe**.

Pour un ensemble x donné, on dit que x **appartient** à C si et seulement si $C(x)$ est vraie, auquel cas on note alors $x \in C$. On dit aussi que x est un **élément** de C.

Dans le cas contraire, c'est-à-dire si $C(x)$ est fausse, on dit que x n'appartient pas à C, ou que x n'est pas un élément de C, et on note $x \notin C$.

Ainsi, la notion de classe généralise celle d'ensemble. En effet, étant donné un ensemble E, on peut lui associer l'assertion à paramètres « $x \in E$ », qui est donc une classe. La définition qui suit précise cela.

Définition 3 (Classe propre)

Soient E un ensemble et C une classe.

1. On appelle classe **issue** de E la classe C_E définie pour tout ensemble x par
$$C_E(x) : « x \in E ».$$
Autrement dit, pour tout ensemble x on a l'équivalence $x \in C_E \iff x \in E$.
2. On dit que C est une classe **propre** si et seulement si C n'est pas issue d'un ensemble.

Remarque :
Si une classe C est issue d'un ensemble E, alors cet ensemble est unique. En effet, cela vient du fait que l'appartenance caractérise entièrement un ensemble. On commettra souvent l'abus de confondre une classe et l'ensemble dont elle est issue, si celui-ci existe.

Exemple :
Pour avoir des exemples de classes issues d'un ensemble, il suffit simplement de prendre un ensemble de son choix et de former sa classe associée. Voici en revanche quelques exemples de classes propres :

1. La classe U de tous les ensembles. Comme tout paramètre x est nécessairement un

ensemble, l'assertion $U(x)$ est toujours vraie. On peut par exemple définir $U(x)$ en posant simplement « $x = x$ ». Ainsi, pour tout ensemble x, on a $x \in U$.
D'après le paradoxe de Russell, une telle classe est nécessairement propre.

2. La classe ON des ordinaux, que nous aurons l'occasion d'aborder plus tard. Nous verrons via le paradoxe de Burali-Forti que cette classe est propre.

Notation

Soient C et D deux classes, E un ensemble et C_E la classe issue de E.

1. On note $C \subseteq D$ si et seulement si $\forall x, (x \in C \Rightarrow x \in D)$.
   En particulier on note $E \subseteq D$ si et seulement si $C_E \subseteq D$.
   Autrement dit, $E \subseteq D$ si et seulement si $\forall x, (x \in E \Rightarrow x \in D)$.
2. On note $C \cap D$ la classe définie pour tout ensemble x par

$$x \in C \cap D \iff (x \in C \text{ et } x \in D)$$

   En particulier on note $E \cap D$ la classe $C_E \cap D$.
   D'après l'axiome de compréhension que $E \cap D$ est une classe issue d'un ensemble.
   En effet, on a

$$E \cap D = \{x \in E \mid x \in D\} = \big\{x \in E \bigm| D(x)\big\}$$

   Comme indiqué précédemment on confondra souvent les deux.
3. On note $C \cup D$ la classe définie pour tout ensemble x par

$$x \in C \cup D \iff (x \in C \text{ ou } x \in D)$$

   En particulier on note $E \cup D$ la classe $C_E \cup D$.
4. On note $D \backslash C$ la définie pour tout ensemble x par

$$x \in D \backslash C \iff (x \in D \text{ et } x \notin C)$$

   En particulier on note $D \backslash E$ la classe $D \backslash C_E$.
5. On note $C \in D$ si et seulement si C est **issue d'un ensemble** F tel que $F \in D$.

1.3 Assertions fonctionnelles

Dans le livre précédent, nous nous sommes intéressés à des assertions à paramètres particulières : les assertions fonctionnelles. Comme le qualificatif *fonctionnelle* le laisse entendre, il s'agit d'une généralisation de la notion de fonction. Redonnons-en la définition.

Définition 4 (Assertion fonctionnelle)

Soit P une assertion à paramètres.
On dit que P est **fonctionnelle** si et seulement si elle nécessite deux paramètres pour être énoncée et pour tout ensembles x, y et y', on a l'implication

$$\Big(P(x,y) \text{ et } P(x,y')\Big) \implies y = y'$$

Ainsi pour un ensemble x donné, il y a au plus un ensemble y qui lui est associé par le biais de P. On dit alors que y est **l'image** de x par P et on note alors $P(x) := y$.

Exemple :

1. L'assertion P définie pour deux ensembles a et b par
$$P(a,b) \iff \text{« } a \textit{ est un entier naturel et } b = 2a \text{ »}$$
est une assertion fonctionnelle. Pour tout a entier naturel, on a alors $P(a) = 2a$.
2. Étant donnée une application f, on peut naturellement lui associer une assertion fonctionnelle P_f en posant pour tout ensembles x et y
$$P_f(x,y) \iff \text{« } x \in \operatorname{dom}(f) \textit{ et } y = f(x) \text{ »}$$
Pour tout $x \in \operatorname{dom}(f)$, on a alors $P_f(x) = f(x)$.

Comme l'indiquent ces exemples, la notion d'assertion fonctionnelle et la notion de fonctions sont très liées, du fait pour un ensemble x de n'associer qu'au plus un autre ensemble. On retrouve donc naturellement la notion d'image, et les notations $P(x)$ et $f(x)$ qui s'y réfèrent sont identiques. Il est important au passage pour une assertion fonctionnelle de ne pas confondre la notation $P(x,y)$ qui se réfère à l'assertion en elle-même et qui est donc soit vraie soit fausse en fonction des paramètres x et y, et la notation $P(x)$ qui désigne l'unique paramètre y tel que $P(x,y)$ soit vraie, à condition bien sûr que celui-ci existe.

Dans le cas d'une fonction f, on peut parler de son domaine $\operatorname{dom}(f)$ comme d'un ensemble, c'est-à-dire l'ensemble de tout ensemble qui admet une image par f. Il n'est pas toujours possible de faire de même pour une assertion fonctionnelle : par exemple l'assertion fonctionnelle « $x = y$ » aurait pour domaine l'ensemble de tous les ensembles, que nous savons n'existe pas. C'est là qu'interviennent les classes que nous avons introduites plus tôt : la classe de tous les ensembles existe bel et bien !

Définition 5 (Domaine et image d'une assertion fonctionnelle)

Soit P une assertion fonctionnelle.

1. On appelle **domaine** de P la classe notée $\operatorname{dom}(P)$ définie pour tout ensemble x par
$$x \in \operatorname{dom}(P) \iff \exists y, P(x,y)$$
2. On appelle **image** de P la classe notée $\operatorname{im}(P)$ définie pour tout ensemble y par
$$y \in \operatorname{im}(P) \iff \exists x, P(x,y)$$

Exemple :

1. L'assertion fonctionnelle P définie pour tout ensembles x et y par
$$P(x,y) \iff \text{« } x = y \text{ »}$$
a pour domaine U, la classe de tous les ensembles.
2. L'assertion fonctionnelle Q définie pour tout ensembles x et y par
$$Q(x,y) \iff \text{« } x \neq y \text{ »}$$
a pour domaine la classe issue de $\varnothing$. Comme dit précédemment, on commettra souvent l'abus de confondre un ensemble et la classe issue de celui-ci, si bien qu'on écrira $\mathrm{dom}(Q) = \varnothing$.
3. Soient f une application et F_f l'assertion fonctionnelle issue de f, c'est-à-dire
$$F_f(x,y) \iff \text{« } x \in \mathrm{dom}(f) \textit{ et } y = f(x) \text{ »}$$
On peut voir que $\mathrm{dom}(F_f)$ est tout simplement la classe issue de $\mathrm{dom}(f)$. Comme dit précédemment, on commettra souvent l'abus de confondre un ensemble et la classe issue de celui-ci, si bien qu'on écrira $\mathrm{dom}(F_f) = \mathrm{dom}(f)$.

Remarque :

1. A la manière des images directes et réciproques d'un ensemble par une fonction, on peut se donner une classe C et considérer son **image directe** par P, à savoir la classe notée $P^{\rightarrow}(C)$ définie pour tout ensemble y par
$$y \in P^{\rightarrow}(C) \iff \exists x \in C, P(x,y)$$
Nous avons vu dans le livre 1 via l'axiome de remplacement que si E est un ensemble tel que $E \subseteq \mathrm{dom}(P)$ alors $P^{\rightarrow}(E)$ est un ensemble que l'on a noté $\left\{ P(x) \mid x \in E \right\}$.
De même, on peut considère l'**image réciproque** de la classe C par P, à savoir la classe notée $P^{\leftarrow}(C)$ définie pour tout ensemble x par
$$x \in P^{\leftarrow}(C) \iff \exists y \in C, P(x,y)$$
2. Une façon intuitive de construire une assertion fonctionnelle est de se munir d'une **formule**. Autrement dit, étant donné un ensemble x, on construit $P(x)$ explicitement. Par exemple, on peut définir P en posant que pour tout ensembles x et y, on a
$$P(x,y) \iff y = \bigcup x$$
et dans ce cas-là on a naturellement $P(x) = \bigcup x$. C'est d'ailleurs par ce biais là des formules que l'on s'est déjà donné le moyen de construire des applications dans le précédent livre.
3. Soient P une assertion fonctionnelle et E un ensemble tel que $E \subseteq \mathrm{dom}(P)$. On a montré dans le précédent livre qu'il existe alors une unique application $f : E \longrightarrow ?$ telle que $\forall x \in E, f(x) = P(x)$, que l'on note généralement $\begin{pmatrix} E & \longrightarrow & ? \\ x & \longmapsto & P(x) \end{pmatrix}$.
En cela, on dira que f est la **restriction** de P à E, et on notera $P_{|E} := f$. Ainsi, même si P est une assertion fonctionnelle sans être une application, toute restriction de celle-ci à un ensemble est nécessairement une application.

Notation

Soient P une assertion fonctionnelle, C et D deux classes.

1. On notera $P : C \longrightarrow ?$ pour signifier $\mathrm{dom}(P) = C$.
2. On notera $P : C \longrightarrow D$ pour signifier $\mathrm{dom}(P) = C$ et $\mathrm{im}(P) \subseteq D$.

2 Bons ordres

Bien souvent en mathématique, nous aimerions étant donné un élément x pouvoir donner du sens à la question « *quel est l'élément qui vient juste après x ?* ». C'est là qu'intervient la notion de **bon ordre** : toute partie non vide de l'ensemble va admettre un élément minimum. De fait, l'élément qui suit directement x sera simplement le minimum des éléments strictement plus grands que x. Typiquement chez les entiers, $n+1$ est bien le minimum des entiers strictement plus grands que n.

Concentrons-nous quelques instants sur la notion d'élément minimal. Rappelons qu'un élément a de l'ensemble ordonné $(E, \preccurlyeq)$ est minimal si et seulement si pour tout $x \in E$ on a

$$x \preccurlyeq a \implies x = a$$

c'est-à-dire qu'il n'y a que a pour être plus petit ou égal à a.

Proposition 1 (Élément minimal et ordre strict)

Soient $(E, \preccurlyeq)$ un ensemble ordonné non vide, $\prec$ l'ordre strict associé à $\preccurlyeq$ et $a \in E$.

Alors a est minimal pour $(E, \preccurlyeq)$ si et seulement si $\forall x \in E, \text{non}(x \prec a)$.

Démonstration

Raisonnons par double implications.

$\boxed{\Rightarrow}$

Supposons que a est minimal pour $(E, \preccurlyeq)$.

Soit $x \in E$.

Supposons par l'absurde que $x \prec a$.

On a donc $x \preccurlyeq a$ et $x \neq a$.

Comme $x \preccurlyeq a$ et a est minimal pour $(E, \preccurlyeq)$, on a $x = a$.

Ainsi on a à la fois $x \neq a$ et $x = a$: c'est absurde.

Par l'absurde, on a donc montré que $\text{non}(x \prec a)$.

Donc $\forall x \in E, \text{non}(x \prec a)$.

Donc $\boxed{\text{si } a \text{ est minimal pour } (E, \preccurlyeq) \text{ alors } \forall x \in E, \text{non}(x \prec a)}$.

$\boxed{\Leftarrow}$

Supposons que $\forall x \in E, \text{non}(x \prec a)$.

Soit $x \in E$.

Supposons que $x \preccurlyeq a$.

On a donc $x \prec a$ ou $x = a$.

Or on a $\text{non}(x \prec a)$ par hypothèse donc nécessairement $x = a$.

Donc si $x \preccurlyeq a$ alors $x = a$.

Donc $\forall x \in E, \Big(x \preccurlyeq a \implies x = a\Big)$.

Donc a est minimal pour $(E, \preccurlyeq)$.

Donc si $\boxed{\forall x \in E, \mathrm{non}(x \prec a) \text{ alors } a \text{ est minimal pour } (E, \preccurlyeq)}$.

CQFD.

Nous l'avons dit dans l'introduction, nous allons dire qu'un ensemble est muni d'un bon ordre lorsque chacune de ses parties (non vides) admet un minimum. Une version plus faible de la notion de bon ordre est la notion d'ordre **bien fondé**, où l'on demande à chaque partie (non vide) d'admettre un élément minimal, mais qui n'est pas nécessairement le minimum de la partie.

Définition 6 (Ordre bien fondé et bon ordre)

Soit E un ensemble ordonné.

1. On dit que E est **bien fondé** si et seulement si toute partie non vide de E admet au moins un élément minimal.
2. On dit que E est **bien ordonné** si et seulement si toute partie non vide de E admet un minimum. On dit aussi que l'ordre sur E est un **bon ordre**.

Remarque :
Dans la suite de cet ouvrage, on va étendre les définitions qui concernent les ordres (larges) aux ordres stricts. Par exemple, considérons $(E, \preccurlyeq)$ un ensemble ordonné, $\prec$ l'ordre strict associé à $\preccurlyeq$ et $a \in E$.

- On dit que a est **minimal** pour $(E, \prec)$ si et seulement si a est minimal pour $(E, \preccurlyeq)$.
- On dit que a **le minimum** de $(E, \prec)$ si et seulement si a est le minimum de $(E, \preccurlyeq)$.
- On dit que $\prec$ est un **ordre strict bien fondé** sur E si et seulement si toute partie non vide de E admet un élément minimal pour $\prec$. Comme $\prec$ et $\preccurlyeq$ partagent les mêmes éléments minimaux d'après ce qui précède, $\prec$ est un ordre strict bien fondé sur E si et seulement si $\preccurlyeq$ est un ordre (large) bien fondé.
- On dit que $\prec$ est un **bon ordre strict** sur E, ou que $(E, \prec)$ est **strictement bien ordonné**, si et seulement si toute partie non vide de E admet un minimum pour $\prec$. Comme $\prec$ et $\preccurlyeq$ partagent le même minimum éventuel, $\prec$ est un bon ordre strict sur E si et seulement si $\preccurlyeq$ est un bon ordre (large) sur E.

On pourrait aussi parler d'éléments maximaux et de maximum, mais dans ce livre ce sont avant tout les minimaux et minimum qui vont nous intéresser, bien qu'à quelques endroits les maximaux et minimum reviendront nous voir.

Au premier abord la notion d'élément minimal et la notion d'élément minimum semble être la même chose. Ce n'est pas vrai, puisqu'un ensemble peut avoir plusieurs éléments minimaux. Pensons par exemple à $\mathbb{N}\backslash\{1\}$ muni de la relation de divisibilité : tous les nombres premiers sont des éléments minimaux sans qu'aucun ne soit un minimum. En réalité, pour qu'un élément minimal soit un minimum, il faut et il suffit qu'il soit comparable à tous les éléments de l'ensemble, ce qui explique pourquoi un bon ordre est nécessairement total.

Proposition 2 (Caractérisation des bons ordres)

Soit E un ensemble ordonné.
Les assertions suivantes sont équivalentes :

1. E est bien ordonné.
2. E est bien fondé et totalement ordonné.

Démonstration

Notons $\preccurlyeq$ l'ordre sur E.

Raisonnons par double implications.

$\boxed{1 \Rightarrow 2}$

Supposons que E est bien ordonné.

Alors toute partie non vide de E admet un minimum.

Or un minimum est un élément minimal (c'est alors le seul).

Donc toute partie non vide de E admet un élément minimal.

Donc $\boxed{E \text{ est bien fondé}}$.

Montrons que E est totalement ordonné.

> Soient x et y dans E.
>
> Alors $\{x, y\}$ est une partie non vide de E.
>
> Elle admet donc un minimum m.
>
> Si $m = x$ alors on a $x = m \preccurlyeq y$.
>
> Si $m = y$ alors on a $y = m \preccurlyeq x$.
>
> Dans les deux cas on a $x \preccurlyeq y$ ou $y \preccurlyeq x$.

Donc tous les éléments de E sont comparables : $\boxed{E \text{ est totalement ordonné}}$.

$\boxed{1 \Leftarrow 2}$

Supposons que E est bien fondé et totalement ordonné.

> Soit A une partie non vide de E.
>
> Comme E est bien fondé, A admet au moins un élément minimal m.
>
> Montrons que m est le minimum de A.
>
> > Supposons par l'absurde que m n'est pas le minimum de A.
> >
> > Il existe donc $a \in A$ tel que non$(m \preccurlyeq a)$.
> >
> > Or E est totalement ordonné par hypothèse.
> >
> > On a donc nécessairement $a \preccurlyeq m$.
> >
> > Or m est un élément minimal de A donc on a $a = m$.
> >
> > En particulier $m \preccurlyeq a$ par réflexivité de $\preccurlyeq$.
> >
> > C'est absurde par définition de a.

Donc m est le minimum de A.

Donc toute partie non vide de E admet un minimum.

Donc $\boxed{E \text{ est bien ordonné}}$.

CQFD.

Le fait pour un ensemble d'être muni d'un ordre bien fondé ou d'un bon ordre se transmet aux parties de cet ensemble, en considérant bien entendu que l'on conserve la même relation d'ordre au passage.

Proposition 3 (Partie d'un ensemble bien ordonné)

Soient E un ensemble ordonné et $A \subseteq E$.
On munit A de la même relation d'ordre que celle de E.

1. Si E est bien fondé alors A est bien fondé.
2. Si E est bien ordonné alors A est bien ordonné.

Démonstration

1. Supposons que E est bien fondé.

Soit B une partie non vide de A.

Comme $A \subseteq E$, B est aussi une partie non vide de E.

Or E est bien fondé par hypothèse.

Donc B admet au moins un élément minimal.

Donc toute partie non vide de A admet au moins un élément minimal.

Donc $\boxed{A \text{ est bien fondé}}$.

2. Supposons que E est bien ordonné.

Soit B une partie non vide de A.

Comme $A \subseteq E$, B est aussi une partie non vide de E.

Or E est bien ordonné par hypothèse.

Donc B admet un minimum.

Donc toute partie non vide de A admet un minimum.

Donc $\boxed{A \text{ est bien ordonné}}$.

CQFD.

Rappelons qu'étant donnés deux ensembles ordonnés $(E, \preccurlyeq)$ et $(F, \sqsubseteq)$, on peut munir $E \times F$ de l'ordre **lexicographique** associé, c'est-à-dire que pour x et y dans E et s et t dans F, on a

$$(x, s) \trianglelefteq (y, t) \iff \Big[x \prec y \text{ ou } (x = y \text{ et } s \sqsubseteq t) \Big]$$

où $\prec$ désigne l'ordre strict associé à $\preccurlyeq$. L'ordre lexicographique tire son nom du fait que les dictionnaires fonctionnement sur ce principe (par rapport à l'ordre alphabétique) : on compare d'abord les premières lettres de chaque mot, et éventuellement si ce sont les mêmes on compare les deuxième lettres et ainsi de suite. Ici il s'agit simplement de comparer des mots ayant chacun deux lettres.

Proposition 4 (Bons ordres et ordre lexicographique)

Soient $(E, \preccurlyeq)$ et $(F, \sqsubseteq)$ deux ensembles ordonnés.
Soit $\trianglelefteq$ l'ordre lexicographique associé sur $E \times F$.
Si $\preccurlyeq$ et $\sqsubseteq$ sont des bons ordres alors $\trianglelefteq$ est un bon ordre.

Démonstration

Notons $\prec$ l'ordre strict associé à $\preccurlyeq$.

Supposons que $\preccurlyeq$ et $\sqsubseteq$ sont des bons ordres.

Soit G une partie non vide de $E \times F$.

Considérons $A := \left\{x \in E \mid \exists y \in F, (x, y) \in G\right\}$.

Comme G est non vide, A est une partie non vide de E.

Or E est bien ordonné donc A admet un minimum a_0.

Considérons alors $B := \left\{y \in F \mid (a_0, y) \in G\right\}$.

Par définition on a $a_0 \in A$ donc il existe $y \in F$ tel que $(a_0, y) \in G$ et donc $y \in B$.

Donc B est une partie non vide de F.

Or F est bien ordonné donc B admet un minimum b_0.

Considérons alors $g_0 := (a_0, b_0)$ et montrons que g_0 est le minimum de G.

Soit $z = (x, y) \in G$.

Par définition de A on a $x \in A$.

Or a_0 est le minimum de A donc $a_0 \preccurlyeq x$.

On a donc $a_0 \prec x$ ou $a_0 = x$.

Si $a_0 \prec x$ alors par définition de $\trianglelefteq$ on a $(a_0, b_0) \trianglelefteq (x, y)$.

Supposons à présent que $a_0 = x$.

On a donc $(a_0, y) = (x, y) \in G$ donc $y \in B$ par définition de B.

Or b_0 est le minimum de B donc $b_0 \sqsubseteq y$.

On a donc $a_0 = x$ et $b_0 \sqsubseteq y$ donc $(a_0, b_0) \trianglelefteq (x, y)$ par définition de $\trianglelefteq$.

Dans les deux cas on a bien $g_0 \trianglelefteq z$.

Donc pour tout $z \in G$, on a $g_0 \trianglelefteq z$.

Donc g_0 est le minimum de G.

Donc toute partie non vide de $E \times F$ admet un minimum.

Donc $\boxed{E \times F \text{ est bien ordonné}}$.

CQFD.

Introduisons à présent la notion de **segment initial**. Une partie d'un ensemble ordonné est un segment initial si et seulement si pour chacun de ses éléments, elle contient aussi tous les éléments qui lui sont inférieurs.

Définition 7 (Segment initial)

Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.
On dit que A est un **segment initial** de E si et seulement si pour tout x et y dans E, on a

$$\big(y \preccurlyeq x \in A\big) \implies y \in A$$

Exemple :

1. Dans $\mathbb{R}$ muni de l'ordre usuel, $]-\infty, 2[$ est un segment initial. En revanche $]1;3]$ n'en est pas un car $2 \in]1;3]$ et $0 \leq 2$ alors que $0 \notin]1;3]$.
2. Dans $\mathbb{N}$ muni de la relation de divisibilité, $\{1,2,4,8\}$ est un segment initial. En revanche $\{1,2,6\}$ n'en est pas un car $6 \in \{1,2,6\}$ et $3|6$ alors que $3 \notin \{1,2,6\}$.

Remarque :
Soient $(E, \preccurlyeq)$ un ensemble ordonné, $\prec$ l'ordre strict associé et $x \in E$.
On rappelle que l'on a introduit la notation $x{\downarrow} = \{y \in E \mid y \prec x\}$.

Dans le cas des ensembles bien ordonnés, on a une caractérisation simple des segments initiaux propres. On rappelle au passage qu'une partie A d'un ensemble E est dite propre si et seulement si $A \neq E$.

Proposition 5 (Segments initiaux d'un ensemble bien ordonné)

Soient E un ensemble **bien ordonné** et A une partie de E.
Les assertions suivantes sont équivalentes :

1. A est un segment initial **propre** de E.
2. Il existe $x \in E$ tel que $A = x{\downarrow}$.

Démonstration

Soient $\preccurlyeq$ la relation d'ordre sur E et $\prec$ l'ordre strict associé à $\preccurlyeq$.

$\boxed{1 \Rightarrow 2}$

Supposons que A est un segment initial propre de E.

Comme A est une partie propre de E, on a $A \subsetneq E$ donc $E \backslash A \neq \varnothing$.

Or E est bien ordonné par définition donc $E \backslash A$ possède un minimum x.

Montrons que $A = x{\downarrow}$.

$\boxed{\subseteq}$

Soit $a \in A$.

Comme E est bien ordonné, E est totalement ordonné d'après la prop. 2 p. 11.

On a donc $x \preccurlyeq a$ ou $a \prec x$.

Supposons par l'absurde que $x \preccurlyeq a$.

On a donc $x \preccurlyeq a \in A$ et A est un segment initial de E par hypothèse.

Donc $x \in A$, ce qui est absurde car $x \in E \backslash A$.

Donc par l'absurde on a $a \prec x$, c'est-à-dire $a \in x{\downarrow}$.

On a donc $A \subseteq x{\downarrow}$.

$\boxed{\supseteq}$

Soit $y \in x{\downarrow}$.

On a alors $y \prec x$.

Or par définition x est le minimum de $E \backslash A$.

On a donc $y \notin E \backslash A$ et donc $y \in A$.

Donc $A \supseteq x{\downarrow}$ et donc $\boxed{A = x{\downarrow}}$.

$\boxed{1 \Leftarrow 2}$

Supposons qu'il existe $x \in E$ tel que $A = x{\downarrow}$.

Soient y et z dans E.

Supposons que $z \preccurlyeq y \in A$.

Par hypothèse on a $A = x{\downarrow}$ donc $y \in x{\downarrow}$ et donc $y < x$.

Comme $z \preccurlyeq y$ on a donc $z \prec x$ par transitivité et donc $z \in x{\downarrow} = A$.

Donc si $y \in A$ et $z \preccurlyeq y$ alors $z \in A$.

Donc $\boxed{A \text{ est un segment initial de } E}$.

De plus, on n'a pas $x \prec x$ par antiréflexivité donc $x \notin x{\downarrow} = A$.

Ainsi $x \in E$ et $x \notin A$, donc $E \neq A$ et donc $\boxed{A \text{ est une partie propre de } E}$.

CQFD.

3 Ordinaux

Lors du précédent livre, nous avons vu la notion d'**isomorphisme** entre deux ensembles ordonnés. C'est une façon de dire que ces deux ensembles ordonnés "*se comportent de la même manière*", pour peu que l'on ne s'intèresse qu'à leur structure d'ensembles ordonnés. Nous pouvons donc d'une certaine manière "*identifier*" deux ensembles ordonnés dès lors qu'il existe un isomorphisme entre les deux, et donc dire en ce sens-là qu'ils sont équivalents. Qui dit équivalence dit classe d'équivalence, c'est-à-dire rassembler en un seul endroit tous ces ensembles ordonnés qui sont isomorphes entre eux. Notons au passage que la notion de classe d'équivalence ici n'a pas besoin d'être un ensemble : nous avons justement introduit plus tôt le concept de classe (tout court) pour palier ce problème.

Se pose alors la question suivante : pour chacune de ces classes d'équivalences, peut-on se donner un représentant canonique, c'est-à-dire un ensemble ordonné qui représenterait toute la classe d'équivalence ? Si nous n'allons pas donner de réponse à cette question en toute généralité, nous allons le faire dans le cas particulier où les ensembles sont munis d'un bon ordre : c'est l'objectif derrière la construction des **ordinaux**, car nous verrons après les avoir définis qu'il en existera systématiquement un et un seul dans chacune des classes d'équivalence des ensembles bien ordonnés.

Pour choisir l'ensemble ordonné en question, il faut choisir en particulier sa relation d'ordre. Tout choix de relation pourrait sembler arbitraire, mais il en existe deux qui sortent naturellement du lot : $\in$ et $\subseteq$, car ce sont les relations les plus fondamentales qui existent chez les ensembles. Nous n'allons d'ailleurs pas avoir besoin de choisir entre les deux : nous allons faire en sorte que $\subseteq$ soit l'ordre (large) et $\in$ l'ordre strict associé.

Définition 8 (Ensemble transitif)

Soit E un ensemble.
On dit que E est **transitif** si et seulement si $\forall x \in E, x \subseteq E$.

Remarque :
Remarquons la chose suivante :

$$\begin{aligned} E \text{ est transitif} &\iff \forall y \in E, y \subseteq E \\ &\iff \forall y, \Big(y \in E \implies y \subseteq E\Big) \\ &\iff \forall x, \forall y, \Big(x \in y \in E \implies x \in E\Big) \end{aligned}$$

Ainsi, la transitivité de E signifie une certaine transitivité de $\in$.
Cette définition répond aussi au fait que nous allons faire de $\in$ un ordre strict sur E : en particulier $\in$ sera transitif, c'est-à-dire que pour x, y et z dans E, si $x \in y \in z$ alors $x \in z$. Le fait pour E d'être transitif va donc étendre légèrement cette propriété en se permettant en plus de remplacer z par E lui-même : si $x \in y \in E$ alors $x \in E$.

Définition 9 (Ordinaux)

Soit E un ensemble.
On dit que E est un **ordinal** si et seulement si

1. $\in$ est un bon ordre strict sur E.
2. E est transitif.

Remarque :
Ainsi, un ordinal est un ensemble E tel que :

1. $\in$ est antiréflexive sur E, c'est-à-dire $\forall x \in E, x \notin x$.
2. $\in$ est transitive sur E, c'est-à-dire $\forall x \in E, \forall y \in E, \forall z \in E, (x \in y \in z \Rightarrow x \in z)$.
3. Pour toute partie non vide F de E, F admet un minimum pour $\in$, c'est-à-dire qu'il existe $a \in F$ tel que $\forall x \in F, (x \neq a \Rightarrow a \in x)$.
4. E est transitif, c'est-à-dire que $\forall x, \forall y, (x \in y \in E \Rightarrow x \in E)$.

Pour la petite histoire

John von Neumann (28 décembre 1903 – 8 février 1957) est un mathématicien et physicien américano-hongrois. Il a apporté d'importantes contributions en mécanique quantique, en analyse fonctionnelle, en logique mathématique, en informatique théorique, en sciences économiques et dans beaucoup d'autres domaines des mathématiques et de la physique. Il a de plus participé aux programmes militaires américains comme le célèbre projet Manhatann.

C'est à lui que l'on doit cette définition d'ordinaux.

Exemple :

1. $\varnothing$ est un ordinal. En effet, par vérité creuse, on a les quatre points suivants :
   (a) On a $\forall x \in \varnothing, x \notin x$ donc $\in$ est antiréflexive sur $\varnothing$.
   (b) On a $\forall x \in \varnothing, \forall y \in \varnothing, \forall z \in \varnothing, (x \in y \in z \implies x \in z)$.
   Ainsi $\in$ est transitive sur $\varnothing$.
   (c) Comme aucune partie de $\varnothing$ n'est non vide, on a bien que toutes les parties non vides de $\varnothing$ admettent un minimum pour $\in$.
   (d) On a $\forall x \in \varnothing, x \subseteq \varnothing$ donc $\varnothing$ est transitif.

   Les points (a) et (b) font de $\in$ un ordre strict sur $\varnothing$.
   Combinés au point (c), on en conclut que $\in$ est un bon ordre strict sur $\varnothing$.
   Enfin, combinés au point (d) on en conclut que $\varnothing$ est un ordinal.

2. Nous verrons plus tard que tout entier naturel, et même $\mathbb{N}$ l'ensemble des entiers naturels lui-même, est un ordinal.

Remarque :
Il est d'usage de désigner un ordinal par une lettre grecque minuscule.
Par exemple $\mathbb{N}$ sera aussi désigné par la lettre ω, qui lui sera alors réservée.

Notation :
On notera ON la classe de tous les ordinaux, c'est-à-dire que pour un ensemble x, on a l'équivalence $x \in ON \iff x$ est un ordinal.

Tentons de justifier le choix de la notion d'ordinal pour représenter une classe d'équivalence des ensembles bien ordonnés. Nous avons déjà justifié l'usage de $\in$ comme relation de bon ordre strict pour son côté naturel. Il reste donc simplement à justifier la transitivité de l'ensemble lui-même, c'est-à-dire le point 2 de la définition d'ordinal.

Pour cela, intéressons-nous au cas simple d'ensembles à deux éléments, pour la relation d'ordre strict $\in$. Comme on veut que $\in$ soit un bon ordre strict, on veut en particulier que tous les éléments distincts soient comparables pour l'appartenance, et donc que sur les deux éléments l'un appartienne à l'autre, ce qui impose au représentant α d'être de la forme $\alpha = \{x, E\}$ avec $x \in E$. Pour rendre le choix de α le plus naturel possible, on aimerait épurer au maximum le choix de x et de E : en particulier il semble naturel de demander $x = \varnothing$ pour ne pas s'encombrer avec d'éventuels éléments de x qui seraient nécessairement arbitraires. Pour la même raison, on aimerait que E ne contienne rien d'autre que x, ce qui impose naturellement $E = \{x\}$ et donc $\alpha = \big\{\varnothing, \{\varnothing\}\big\}$.

La transitivité va permettre de retirer les éventuels éléments encombrants : si x est un élément de l'ordinal α, alors par transitivité de α on a $x \subseteq \alpha$, c'est-à-dire que tous les éléments de x font aussi partis de α. Ainsi dans l'exemple $\alpha = \{x, E\}$, x ne peut rien contenir car tout élément éventuel de x se retrouverait en plus dans les éléments de α, et pour la même raison E ne peut rien contenir de plus que x.

Proposition 6 (Les éléments d'un ordinal sont des ordinaux)

Soient α un ordinal et x un ensemble.
Si $x \in \alpha$ alors x est un ordinal.

Démonstration

Supposons que $x \in \alpha$.

• Par définition α est un ordinal donc α est transitif et $(\alpha, \in)$ est strictement bien ordonné.

Comme $x \in \alpha$, on a donc $x \subseteq \alpha$ par définition de la transitivité.

Or on vient de dire que $(\alpha, \in)$ est strictement bien ordonné.

Donc $\boxed{(x, \in) \text{ est strictement bien ordonné}}$ d'après la proposition 3 page 12.

• Il reste donc à montrer que x est transitif.

Soit $y \in x$.

On a vu que $x \subseteq \alpha$ donc $y \in \alpha$ par définition de l'inclusion.

On a donc $y \subseteq \alpha$ car α est transitif.

Montrons que $y \subseteq x$.

Soit $z \in y$.

Comme $y \subseteq \alpha$, on a en particulier $z \in \alpha$ par définition de l'inclusion.

On a donc $z \in y \in x$, et tous les trois sont des éléments de α.

Or $(\alpha, \in)$ est strictement bien ordonné donc $\in$ est transitif sur α.

On a donc $z \in x$ par transitivité de $\in$.

Donc $\forall z \in y, z \in x$ et donc $y \subseteq x$ par définition de l'inclusion.

Donc $\forall y \in x, y \subseteq x$.

Ainsi $\boxed{x \text{ est transitif}}$.

Finalement, $(x, \in)$ est strictement bien ordonné et x est transitif.

Donc $\boxed{x \text{ est un ordinal}}$.

CQFD.

Proposition 7 (L'intersection de deux ordinaux est un ordinal)

Soient α et β deux ordinaux.
Alors $\alpha \cap \beta$ est un ordinal.

Démonstration

Comme α est un ordinal, $(\alpha, \in)$ est strictement bien ordonné.

Or $\alpha \cap \beta \subseteq \alpha$ donc $\boxed{(\alpha \cap \beta, \in) \text{ est strictement bien ordonné}}$ d'après la prop. 3 p. 12.

Il reste à montrer que $\alpha \cap \beta$ est transitif.

Soit $x \in \alpha \cap \beta$.

On a donc $x \in \alpha$ et $x \in \beta$.

Or α et β sont des ordinaux donc sont transitifs donc $x \subseteq \alpha$ et $x \subseteq \beta$.

On a donc $x \subseteq \alpha \cap \beta$.

Donc $\forall x \in \alpha \cap \beta, x \subseteq \alpha \cap \beta$.

Donc $\boxed{\alpha \cap \beta \text{ est transitif}}$.

Finalement $(\alpha \cap \beta, \in)$ est strictement bien ordonné et $\alpha \cap \beta$ est transitif.

On a donc $\boxed{\alpha \cap \beta \text{ est un ordinal}}$.

CQFD.

Nous l'avons annoncé quand nous avons introduit la notion d'ordinal : étant donné un ordinal, nous voulons faire de $\subseteq$ l'ordre (large) et de $\in$ l'ordre strict. Par définition d'un ordinal, $\in$ est le bon ordre strict concerné. La proposition suivante va nous montrer que $\subseteq$ est quant à lui l'ordre (large) associé à $\in$.

Proposition 8 (Ordre large sur les ordinaux)

Soient α et β deux ordinaux.
On a l'équivalence

$$\alpha \subseteq \beta \iff (\alpha \in \beta \text{ ou } \alpha = \beta)$$

Démonstration

Raisonnons par double implications.

$\boxed{\Rightarrow}$

Supposons que $\alpha \subseteq \beta$ et $\alpha \neq \beta$.

Montrons que $\alpha \in \beta$.

Posons $X := \beta \backslash \alpha$: par hypothèse on a $X \neq \varnothing$.

Or β est un ordinal donc $(\beta, \in)$ est strictement bien ordonné.

Donc comme $X \subseteq \beta$ et $X \neq \varnothing$, on en déduit que $(X, \in)$ admet un minimum ξ.

Comme $\xi \in X$ et $X \subseteq \beta$, on a $\xi \in \beta$ par définition de l'inclusion.

On peut donc montrer $\xi = \alpha$ pour conclure.

$\boxed{\subseteq}$

Soit $\mu \in \xi$.

On a alors $\mu \in \xi \in \beta$ et β est transitif (car ordinal) donc $\mu \in \beta$.

Comme $\mu \in \xi$ et que ξ est le minimum de $(X, \in)$, on a $\mu \notin X$.

On a donc $\mu \in \beta$ et $\mu \notin X$ donc $\mu \in \beta \backslash X = \alpha$.

Donc $\xi \subseteq \alpha$.

$\boxed{\supseteq}$

Supposons par l'absurde que $\xi \neq \alpha$, c'est-à-dire $\xi \subsetneq \alpha$ d'après ce qui précède.

On a donc $\alpha \backslash \xi \neq \varnothing$ donc il existe $\mu \in \alpha \backslash \xi$.

En particulier on a $\mu \in \alpha$.

Comme $\alpha \subseteq \beta$ par hypothèse, on a $\mu \in \beta$ par définition de l'inclusion.

Ainsi on a $\xi \in \beta$ et $\mu \in \beta$.

Or β est un ordinal donc $(\beta, \in)$ est strictement bien ordonné.

Donc $\in$ est un ordre strict total sur β d'après la proposition 2 page 11.

On a donc $\mu \in \xi$ ou $\xi \in \mu$ ou $\mu = \xi$.

- $\mu \in \xi$ est impossible.

En effet par définition on a $\mu \in \alpha \backslash \xi$ donc $\mu \notin \xi$.

- $\xi \in \mu$ est impossible.
  En effet on aurait $\xi \in \mu \in \alpha$ donc $\xi \in \alpha$ car α est transitif car ordinal.
  Or on a $\xi \in X = \beta \backslash \alpha$ donc $\xi \notin \alpha$.
- $\mu = \xi$ est impossible.
  En effet on a $\xi \in X = \beta \backslash \alpha$ donc $\xi \notin \alpha$ alors que $\mu \in \alpha \backslash \xi$ donc $\mu \in \alpha$.
  On a donc $\xi \notin \alpha$ et $\mu \in \alpha$ donc on ne peut pas avoir $\mu = \xi$.

On aboutit donc à une contradiction.

Par l'absurde, on a prouvé que $\xi = \alpha$.

Comme $\xi \in \beta$, on a donc $\alpha \in \beta$.

Donc $\big(\alpha \subseteq \beta$ et $\alpha \neq \beta\big) \implies \alpha \in \beta$.

Donc $\boxed{\alpha \subseteq \beta \implies \big(\alpha \in \beta \text{ ou } \alpha = \beta\big)}$.

$\boxed{\Leftarrow}$

Supposons que $\alpha \in \beta$ ou $\alpha = \beta$.

Si $\alpha \in \beta$ alors $\alpha \subseteq \beta$ car β est transitif car ordinal.

Si $\alpha = \beta$ alors en particulier $\alpha \subseteq \beta$.

Dans tous les cas on a $\alpha \subseteq \beta$.

Donc si $\boxed{\alpha \in \beta \text{ ou } \alpha = \beta \text{ alors } \alpha \subseteq \beta}$.

CQFD.

Remarque :
Désormais, on utilisera régulièrement le fait qu'étant donné un ordinal, il est naturellement muni de $\subseteq$ en tant que relation de bon ordre et que $\in$ est le bon ordre strict associé. En particulier pour deux ordinaux α et β, on a l'équivalence $\alpha \subsetneq \beta \iff \alpha \in \beta$.

Le fait d'avoir prouvé ces quelques propriétés générales sur les ordinaux nous permet d'entrevoir le magnifique théorème qui va suivre : celui-ci affirme qu'en fait c'est toute la classe ON qui se comporte comme un ordinal.

Théorème 1 (Bon ordre strict sur les ordinaux)

Soient α, β et γ trois ordinaux.

1. Si $\alpha \in \beta \in \gamma$ alors $\alpha \in \gamma$.
   Ainsi $\in$ est **transitif** sur ON.
2. On a $\alpha \notin \alpha$.
   Ainsi $\in$ est **antiréflexive** sur ON.

Ainsi par 1 et 2, $\in$ peut être vu comme un **ordre strict** sur ON.

3. On a $\alpha \in \beta$ ou $\beta \in \alpha$ ou $\alpha = \beta$.
   Autrement dit $\in$ est un ordre strict **total** sur ON.

4. Soit E un ensemble non vide dont les éléments sont tous des ordinaux.
Alors $(E, \in)$ possède un minimum.
Ainsi $\in$ est un **bon** ordre strict sur ON.

Ainsi, $\in$ est un **bon ordre strict** sur ON.

Démonstration

1. Supposons que $\alpha \in \beta \in \gamma$.

On a alors $\boxed{\alpha \in \gamma}$ car γ est transitif car ordinal.

2.

Supposons par l'absurde que $\alpha \in \alpha$.

En prenant $x := \alpha$, on a l'existence d'un $x \in \alpha$ tel que $x \in x$.

Or α est un ordinal donc $(\alpha, \in)$ est strictement bien ordonné donc $\in$ est antiréflexive sur α. En particulier $\forall x \in \alpha, x \notin x$, d'où l'absurdité.

Par l'absurde, on a donc $\boxed{\alpha \notin \alpha}$.

3. Considérons $\delta := \alpha \cap \beta$.

Alors δ est un ordinal d'après la proposition 7 page 19.

Or on a $\delta \subseteq \alpha$ donc ($\delta \in \alpha$ ou $\delta = \alpha$) d'après la proposition 8 page 20.

De même on a $\delta \subseteq \beta$ donc ($\delta \in \beta$ ou $\delta = \beta$) d'après la proposition 8 page 20.

- Si $\delta = \alpha$ alors comme on a ($\delta \in \beta$ ou $\delta = \beta$) on a $\boxed{\alpha \in \beta \text{ ou } \alpha = \beta}$.
- Si $\delta = \beta$ alors comme on a ($\delta \in \alpha$ ou $\delta = \alpha$) on a $\boxed{\beta \in \alpha \text{ ou } \beta = \alpha}$.
- Sinon si $\delta \neq \alpha$ et $\delta \neq \beta$ alors d'après ce qui précède on a $\delta \in \alpha$ et $\delta \in \beta$.
  On a donc $\delta \in \alpha \cap \beta$ par définition de l'intersection.
  Mais on a aussi $\delta = \alpha \cap \beta$ par définition de δ, donc $\delta \in \delta$, ce qui contredit 1.

Finalement, on a bien $\boxed{\alpha \in \beta \text{ ou } \beta \in \alpha \text{ ou } \alpha = \beta}$.

4. Comme E est non vide, il existe $\varepsilon \in E$.

Si ε est le minimum de $(E, \in)$ c'est bon.

Supposons donc que ε n'est pas le minimum de $(E, \in)$.

Il existe donc $\mu \in E$ tel que l'on n'a ni $\varepsilon \in \mu$ ni $\varepsilon = \mu$.

Or tous les éléments de E sont des ordinaux donc $\mu \in \varepsilon$ d'après 3.

Ainsi $\mu \in E$ et $\mu \in \varepsilon$ donc $\mu \in \varepsilon \cap E$ et donc $\varepsilon \cap E \neq \varnothing$.

Donc $\varepsilon \cap E$ est une partie non vide de ε.

Or $(\varepsilon, \in)$ est strictement bien ordonné car ε est un ordinal.

Donc $\varepsilon \cap E$ possède un minimum ξ.

Montrons que ξ est le minimum de E.

Soit $\nu \in E$.

Comme tous les éléments de E sont des ordinaux, on a $\nu \in \varepsilon$ ou $\varepsilon \in \nu$ ou $\nu = \varepsilon$ d'après 3.

- Si $\nu \in \varepsilon$ alors $\nu \in \varepsilon \cap E$ donc $\xi \in \nu$ car ξ est le minimum de $\varepsilon \cap E$.
- Si $\varepsilon \in \nu$, comme $\xi \in \varepsilon \cap E$ on a $\xi \in \varepsilon$ donc $\xi \in \varepsilon \in \nu$ et donc $\xi \in \nu$ d'après 1.
- Si $\nu = \varepsilon$, comme $\xi \in \varepsilon \cap E$ on a $\xi \in \varepsilon$ donc $\xi \in \nu$.

Dans tous les cas on a $\xi \in \nu$.

Donc ξ est le minimum de E.

Dans tous les cas, $\boxed{E \text{ admet un minimum}}$.

CQFD.

Remarque :

1. Ainsi on dira simplement que $(ON, \in)$ est une classe strictement bien ordonnée, et grâce à la proposition 8 page 20, nous savons que l'ordre associé est $\subseteq$, donc nous dirons aussi que $(ON, \subseteq)$ est une classe bien ordonné. Ces affirmations doivent être comprises comme étant un résumé du théorème qui précède.
2. Désormais pour α et β deux ordinaux, il va arriver fréquemment que nous notions $\alpha < \beta$ à la place de $\alpha \in \beta$ et $\alpha \leq \beta$ à la place de $\alpha \subseteq \beta$. **Ce ne sera pas toujours le cas**, mais quand nous le ferons ce sera pour insister sur le fait que c'est en tant que relation d'ordre strict et relation d'ordre (large) sur ON que nous employons ces objets mathématiques. Dans le cas où c'est véritablement l'idée d'appartenance et d'inclusion ensembliste qui nous intéressera, là nous resterons bel et bien avec les symboles $\in$ et $\subseteq$. À ce titre, nous aurons parfois l'occasion de jongler avec les deux types de symboles.
3. $\varnothing$ est le plus petit des ordinaux. En effet, on a déjà montré dans un exemple précédent que $\varnothing$ est un ordinal, et on sait déjà que pour tout ensemble E on a $\varnothing \subseteq E$. En particulier pour tout ordinal α on a $\varnothing \subseteq \alpha$ et donc $\varnothing \leq \alpha$.

Nous avons expliqué avant le théorème que la classe des ordinaux ON se comporte elle-même comme un ordinal, mais nous n'avons pas montré de propriété qui s'apparente à la transitivité d'un ordinal. En réalité si, c'est l'objet de la proposition 6 page 18 qui affirme que tout élément d'un ordinal est aussi un ordinal. Autrement dit, pour tout $\alpha \in ON$, tous les éléments de α sont des ordinaux et donc $\alpha \subseteq ON$.

Nous avons affirmé pour justifier de l'intérêt des classes qu'il n'existe pas d'ensemble de tous les ordinaux, si bien que ON est une classe qui n'est pas issue d'un ensemble (elle est donc une classe **propre**). Montrons-le enfin : c'est le fameux **paradoxe de Burali-Forti**.

Théorème 2 (Paradoxe de Burali-Forti)

Il n'existe pas d'ensemble contenant tous les ordinaux.

Démonstration

Supposons par l'absurde qu'il existe un ensemble E tel que tout ordinal en est un élément. Potentiellement il y a d'autres éléments dans E qui ne sont pas des ordinaux, mais on est cependant sûr que tout ordinal est un élément de E.
Considérons alors $X := \{x \in E \mid x \text{ est un ordinal}\}$.
X est donc par définition l'ensemble de tous les ordinaux.
Pour arriver à la contradiction, nous allons montrer qu'alors X est en fait lui-même un ordinal, si bien que $X \in X$, ce qui est impossible chez les ordinaux.

• Montrons X est transitif.
    Soit $\alpha \in X$.
    Par définition α est un ordinal.
        Soit $\beta \in \alpha$.
        Alors β est un ordinal d'après la proposition 6 page 18.
        On a donc $\beta \in E$ par définition de E et donc $\beta \in X$ par définition de X.
    Donc $\forall \beta \in \alpha, \beta \in X$ donc $\alpha \subseteq X$ par définition de l'inclusion.
Donc $\forall \alpha \in X, \alpha \subseteq X$ donc $\boxed{X \text{ est transitif}}$.

• D'après le théorème 1 page 21 $\boxed{(X, \in) \text{ est strictement bien ordonné}}$ car tous ses éléments sont des ordinaux.

Ainsi X est transitif et $(X, \in)$ est strictement bien ordonné.
Donc X est un ordinal donc $X \in E$ par définition de E donc $X \in X$ par définition de X.
C'est en contradiction avec l'antiréflexivité de $\in$ chez les ordinaux.
CQFD.

Pour la petite histoire

Cesare Burali-Forti (13 août 1861 – 21 janvier 1931) est un mathématicien italien.

Cesare Burali-Forti est assistant de Giuseppe Peano à Turin de 1894 à 1896. Bertrand Russell a nommé paradoxe de Burali-Forti, le paradoxe du plus grand ordinal en théorie des ensembles, en référence à un article de 1897 où le mathématicien italien, croyant démontrer que deux ordinaux ne sont pas toujours comparables, fait le raisonnement qui conduit au paradoxe décrit par Russell.

Ainsi, il n'existe pas d'ensemble contenant tous les ordinaux : ON n'est pas issue d'un ensemble, c'est donc une **classe propre**. De fait parmi toutes les sous-classes de ON, certaines sont propres (elle-même par exemple). Nous avons vu lors du théorème 1 page 21 que tout ensemble $X \subseteq ON$ possède un minimum. En fait, ce résultat reste vrai si on remplace X par une classe quelconque, pas forcément issue d'un ensemble.

Proposition 9 (Les sous-classes de ON possèdent un minimum)

Soit $C \subseteq ON$ une classe non vide.
Alors $(C, \leq)$ possède un ordinal minimum, c'est-à-dire $\exists \xi \in C, \forall \alpha \in C, \xi \leq \alpha$.

Démonstration

• Supposons que C est issue d'un ensemble X non vide.

En particulier $X \subseteq ON$ par définition de C.

D'après le théorème 1 page 21, X possède un ordinal minimum.

Donc $\boxed{C \text{ possède un ordinal minimum}}$.

• Supposons que C est propre.

En particulier elle n'est pas vide car pas issue de l'ensemble vide.

Il existe donc au moins un ordinal $\alpha \in C$.

Posons alors $X := \alpha \cap C = \{\beta \in \alpha \mid \beta \in C\} = \{\beta \in \alpha \mid C(\beta)\}$.

D'après l'axiome de compréhension, X est un ensemble.

► Supposons que X est vide.

Montrons que α est le minimum de C.

Soit $\beta \in C$.

Par définition de C on a $C \subseteq ON$.

Donc α et β sont des ordinaux.

On a donc $\alpha \leq \beta$ ou $\beta < \alpha$ d'après le théorème 1 page 21.

Supposons par l'absurde que $\beta < \alpha$.

On a donc $\beta \in \alpha$ par définition de $<$.

On a donc $\beta \in \alpha \cap C = X$.

Donc X est non vide.

C'est absurde puisqu'on a justement supposé que X est vide.

Par l'absurde on vient donc de montrer que $\alpha \leq \beta$.

Donc $\forall \beta \in C, \alpha \leq \beta$.

Donc α est le minimum de C.

► Supposons que X n'est pas vide.

Comme $X = \alpha \cap C$, on a $X \subseteq \alpha$.

Or α est un ordinal donc tous ses éléments sont des ordinaux.

Donc X est un ensemble non vide d'ordinaux.

Donc X possède un ordinal minimum ξ d'après le théorème 1 page 21.

Montrons que ξ est le minimum de C.

Comme $\xi \in X = \alpha \cap C$, on a déjà $\xi \in C$.

Soit $\beta \in C$.

Par définition de C on a $C \subseteq ON$.

Donc α et β sont des ordinaux.

On a donc $\alpha \leq \beta$ ou $\beta < \alpha$ d'après le théorème 1 page 21.

Supposons que $\alpha \leq \beta$, c'est-à-dire $\alpha \subseteq \beta$.

On a $\xi \in X = \alpha \cap C$ donc $\xi \in \alpha$.

On a donc $\xi \in \beta$ par définition de l'inclusion.

Donc $\xi \subseteq \beta$ car β est transitif car ordinal.

Supposons que $\beta < \alpha$, c'est-à-dire $\beta \in \alpha$.

Comme $\beta \in C$, on a $\beta \in \alpha \cap C = X$.

Or ξ est le minium de X donc $\xi \subseteq \beta$.

Donc $\forall \xi \in C, \xi \subseteq \beta$, et donc $\forall \xi \in C, \xi \leq \beta$.

Donc ξ est le minimum de C.

Dans tous les cas, $\boxed{C \text{ possède un ordinal minimum}}$.

CQFD.

Nous venons de voir que ON est une classe **propre**, et qu'elle se comporte *comme un ordinal*, c'est-à-dire :

1. ON est transitive, au sens où si $\beta \in \alpha \in ON$ alors $\beta \in ON$, puisque les éléments d'un ordinal sont eux aussi des ordinaux.
2. $(ON, \in)$ est strictement bien ordonné, d'après le théorème 1 page 21.

Il s'avère qu'en fait, il s'agit de la seule classe propre à vérifier ces deux propriétés, comme le montre la proposition suivante. En cela, ON est en quelque sorte l'ordinal ultime.

Proposition 10 (ON est la seule classe propre ordinale)

Soit C une classe propre.
Supposons que :

1. C est transitive, c'est-à-dire $\forall \alpha \in C, \alpha \subseteq C$.
2. $(C, \in)$ est strictement bien ordonné, c'est-à-dire :
   - $\in$ est antiréflexif sur C : $\forall \alpha \in C, \alpha \notin \alpha$
   - $\in$ est transitif sur C : $\forall \alpha \in C, \forall \beta \in C, \forall \gamma \in C, (\alpha \in \beta \in \gamma \implies \alpha \in \gamma)$.
   - Tout ensemble non vide $X \subseteq C$ possède un minimum pour $\in$.

Alors $C = ON$.

Démonstration

• Commençons par montrer que $C \subseteq ON$.

Autremen dit, montrons que tous les éléments de C sont des ordinaux.

Soit $\alpha \in C$.

Montrons que α est un ordinal.

► Montrons que α est transitif.

Par hypothèse C est transitive donc $\alpha \subseteq C$.

Soit $\beta \in \alpha$.

Comme $\alpha \subseteq C$, on a $\beta \in C$ par définition de l'inclusion.

Donc $\beta \subseteq C$ par transitivité de C.

Soit $\gamma \in \beta$.

Comme $\beta \subseteq C$, on a $\gamma \in C$ par définition de l'inclusion.

Ainsi on a $\gamma \in \beta \in \alpha$ et tous trois sont éléments de C.

Or $\in$ est transitive sur C par hypothèse donc $\gamma \in \alpha$.

Donc $\forall \gamma \in \beta, \gamma \in \alpha$ donc $\beta \subseteq \alpha$ par définition de l'inclusion.

Donc $\forall \beta \in \alpha, \beta \subseteq \alpha$ donc α est transitif.

► Montrons que $(\alpha, \in)$ est strictement bien ordonné.

Soient β, γ et δ dans α.

Supposons que $\beta \in \gamma \in \delta$.

On a dit que $\alpha \subseteq C$ donc β, γ et δ sont dans C.

Or $\in$ est transitive sur C donc $\beta \in \delta$.

Donc si $\beta \in \gamma \in \delta$ alors $\beta \in \delta$.

Donc $\in$ est transitive sur α.

Soit $\beta \in \alpha$.

On a dit que $\alpha \subseteq C$ donc $\beta \in C$ par définition de l'inclusion.

Donc $\beta \notin \beta$ par antiréflexivité de $\in$ sur C.

Donc $\forall \beta \in \alpha, \beta \notin \beta$.

Donc $\in$ est antiréflexive sur α.

Ainsi $(\alpha, \in)$ est strictement ordonné.

Soit X une partie non vide de α.

On a dit que $\alpha \subseteq C$ donc $X \subseteq C$ par transitivité de l'inclusion.

Ainsi X est un ensemble non vide inclus dans C.

Donc X possède un minimum pour $\in$ par hypothèse.

Donc toutes les parties non vides de α possède un minimum pour $\in$.

On en conclut que $(\alpha, \in)$ est strictement bien ordonné.

Ainsi α est transitif et $(\alpha, \in)$ est strictement bien ordonné.

Donc α est un ordinal.

Donc tout élément de C est un ordinal, et donc $\boxed{C \subseteq ON}$.

- Montrons que $C = ON$.

Supposons par l'absurde que $C \neq ON$.

On a donc $C \subsetneq ON$ par ce qui précède.

Considérons alors $D := ON \backslash C$, qui est donc une classe non vide.

Alors $(D, \in)$ possède un ordinal minimum δ d'après la proposition 9 page 25.

Montrons que $\delta = C$.

$\boxed{\subseteq}$

Soit $\alpha \in \delta$.

Comme δ est le minimum de $(D, \in)$, on a $\alpha \notin D$.

Or $\delta \in D = ON \backslash C$ donc $\delta \in ON$.

Donc α est un ordinal comme élément de l'ordinal δ.

Ainsi on a $\alpha \in ON$ et $\alpha \notin D$ donc $\alpha \in ON \backslash D = C$.

Donc $\forall \alpha \in \delta, \alpha \in C$ donc $\delta \subseteq C$ par définition de l'inclusion.

$\boxed{\supseteq}$

Soit $\alpha \in C$.

D'après ce qui précède, $C \subseteq ON$ donc $\alpha \in ON$.

Or on a aussi $\delta \in ON$.

On a donc $\alpha \in \delta$ ou $\alpha = \delta$ ou $\delta \in \alpha$ car $(ON, \in)$ est strictement bien ordonné.

▶ Plaçons-nous dans le cas où $\alpha = \delta$.

Comme $\alpha \in C$, on a alors $\delta \in C$.

- Plaçons-nous dans le cas où $\delta \in \alpha$.
  On a donc $\delta \in \alpha \in C$ et C est transitive par hypothèse.
  On a donc $\alpha \subseteq C$ et donc $\delta \in C$ par définition de l'inclusion.

Donc si $\alpha = \delta$ ou $\delta \in \alpha$ alors $\delta \in C$.
C'est absurde puisque $\delta \in D = ON \backslash C$ donc $\delta \notin C$.
On en déduit que $\alpha \in \delta$.

Ainsi $\forall \alpha \in C, \alpha \in \delta$ donc $C \subseteq \delta$ par définition de l'inclusion.
On en déduit donc que $C = \delta$ par ce qui précède.
Ainsi C est un ordinal : en particulier C est un ensemble.
C'est absurde puisque par définition C est une classe propre.

Par l'absurde, on a donc montré que nécessairement $\boxed{C = ON}$.
CQFD.

Cette propriété que nous venons de voir fait donc de ON en quelque sorte l'unique classe propre à pouvoir prétendre généraliser la notion d'ordinaux. Nous aurons l'occasion de la revoir quand nous aurons besoin d'étendre une définition qui initialement ne porte que sur les ordinaux : il semblera légitime de ne l'étendre qu'à ON.

Nous avons vu lors de la proposition 7 page 19 que l'intersection de deux ordinaux est aussi un ordinal. Il en va en fait de même pour l'union de deux ordinaux, et plus généralement pour l'intersection et la réunion d'ensembles d'ordinaux. Cela nous fournit au passage une expression explicite de la borne supérieure et du minimum d'un ensemble d'ordinaux.

Proposition 11 (Union et intersection d'ordinaux)

Soient α et β deux ordinaux.

1. $\alpha \cup \beta$ est un ordinal et $\alpha \cup \beta = \max(\alpha, \beta)$.
2. $\alpha \cap \beta$ est un ordinal et $\alpha \cap \beta = \min(\alpha, \beta)$.

Soit X un ensemble dont tous les éléments sont des ordinaux.

3. $\bigcup X$ est un ordinal et $\bigcup X = \sup(X)$.
   La notion de borne supérieure est à comprendre ici "*parmi les ordinaux*".
4. Si $X \neq \varnothing$ alors $\bigcap X$ est un ordinal et $\bigcap X = \min(X)$.

Démonstration

On a $\alpha \leq \beta$ ou $\beta < \alpha$ d'après le théorème 1 page 21.

1.

- Si $\alpha \leq \beta$ alors $\beta = \max(\alpha, \beta)$ par définition du maximum.

Or on a $\alpha \subseteq \beta$ par définition de $\leq$, donc $\alpha \cup \beta = \beta$.

En particulier $\alpha \cup \beta$ est un ordinal, et par ce qui précède $\alpha \cup \beta = \max(\alpha, \beta)$.

- ▶ Si $\beta < \alpha$ on a $\alpha = \max(\alpha, \beta)$ par définition du maximum.

  On a en particulier $\beta \leq \alpha$ puisque c'est l'ordre large associé.

  On a donc $\beta \subseteq \alpha$ par définition de $\leq$ et donc $\alpha \cup \beta = \alpha$.

  En particulier $\alpha \cup \beta$ est un ordinal, et par ce qui précède $\alpha \cup \beta = \max(\alpha, \beta)$.

Dans tous les cas $\boxed{\alpha \cup \beta \text{ est un ordinal et } \alpha \cup \beta = \max(\alpha, \beta)}$.

2. On a déjà vu lors de la proposition 7 page 19 que $\boxed{\alpha \cap \beta \text{ est un ordinal}}$.

- ▶ Si $\alpha \leq \beta$ alors $\alpha = \min(\alpha, \beta)$ par définition du minimum.

  Or on a $\alpha \subseteq \beta$ par définition de $\leq$ donc $\alpha \cap \beta = \alpha$.

  On a donc $\alpha \cap \beta = \min(\alpha, \beta)$.

- ▶ Si $\beta < \alpha$ alors on a $\beta = \min(\alpha, \beta)$ par définition du minimum.

  En particulier on a $\beta \leq \alpha$ puisque c'est l'ordre large associé.

  On a donc $\beta \subseteq \alpha$ par définition de $\leq$.

  On a donc $\alpha \cap \beta = \beta$ et donc $\alpha \cap \beta = \min(\alpha, \beta)$ par ce qui précède.

Dans tous les cas on a $\boxed{\alpha \cap \beta = \min(\alpha, \beta)}$.

3. Commençons par montrer que $\bigcup X$ est un ordinal.

• Montrons que $\bigcup X$ est transitif.

Soit $x \in \bigcup X$.

Par définition de la réunion, il existe $\alpha \in X$ tel que $x \in \alpha$.

Comme X est un ensemble d'ordinaux, α est un ordinal.

Donc α est transitif et donc $x \subseteq \alpha$.

Comme $\alpha \in X$, on a $\alpha \subseteq \bigcup X$ donc $x \subseteq \bigcup X$ par transitivité de l'inclusion.

Donc $\forall x \in \bigcup X, x \subseteq \bigcup X$ donc $\boxed{\bigcup X \text{ est transitif}}$.

• Montrons que $\in$ est un bon ordre strict sur $\bigcup X$.

- ▶ $\in$ est antiréflexive sur $\bigcup X$.

  Soit $x \in \bigcup X$.

  Par définition de la réunion, il existe $\alpha \in X$ tel que $x \in \alpha$.

  Comme X est un ensemble d'ordinaux, α est un ordinal.

  Donc x est un ordinal d'après la proposition 6 page 18.

  En particulier $x \notin x$ par antiréflexivité de $\in$ sur ON.

Donc $\forall x \in \bigcup X, x \notin x$ donc $\in$ est antiréflexive sur $\bigcup X$.

▶ $\in$ est transitive sur $\bigcup X$.

Soient x, y et z dans $\bigcup X$.

Il existe α, β et γ dans X tels que $x \in \alpha$, $y \in \beta$ et $z \in \gamma$.

Or tous les éléments de X sont des ordinaux donc α, β et γ sont des ordinaux.

En particulier d'après 1 $\alpha \cup \beta \cup \gamma$ est un ordinal, dont x, y et z sont des éléments.

Supposons que $x \in y \in z$.

On vient de dire que $\alpha \cup \beta \cup \gamma$ est un ordinal.

Donc $(\alpha \cup \beta \cup \gamma, \in)$ est strictement bien ordonné.

Donc $\in$ est transitive sur $\alpha \cup \beta \cup \gamma$.

On a donc $x \in z$ par transitivité.

Donc si $x \in y \in z$ alors $x \in z$.

Donc $\in$ est transitive sur $\bigcup X$.

Ainsi $\in$ est un ordre strict sur $\bigcup X$.

▶ $\in$ est un bon ordre strict sur $\bigcup X$.

Soit A une partie non vide de $\bigcup X$.

Soit $a \in A$.

Comme $A \subseteq \bigcup X$ on a $a \in \bigcup X$ par définition de l'inclusion.

Par définition de la réunion, il existe $\alpha \in X$ tel que $a \in \alpha$.

Or tous les éléments X sont des ordinaux donc α est un ordinal.

Donc a est un ordinal d'après la proposition 6 page 18.

Donc tous les éléments de A sont des ordinaux.

Comme A est non vide, il possède un minimum d'après le théorème 1 page 21.

Donc toutes les parties non vides de $\bigcup X$ possèdent un minimum.

Donc $\in$ est un bon ordre strict sur $\bigcup X$.

Donc $\boxed{\bigcup X \text{ est un ordinal}}$.

• Montrons que $\bigcup X = \sup(X)$.

Pour tout $\alpha \in X$, on a $\alpha \subseteq \bigcup X$ par définition de la réunion.

En particulier $\bigcup X$ est un majorant de X dans $(ON, \subseteq)$.

Soit β un majorant de X dans $(ON, \subseteq)$.

On a donc pour tout $\alpha \in X$, on a $\alpha \subseteq \beta$.

On a donc $\bigcup X \subseteq \beta$ par minimalité de la réunion pour l'inclusion.

Donc tout ordinal majorant de X dans $(ON, \subseteq)$ est plus grand que ou égal à $\bigcup X$.

Ainsi, $\bigcup X$ est le plus petit ordinal majorant de X dans $(ON, \subseteq)$.

Donc $\boxed{\sup(X) = \bigcup X}$.

4. Supposons que X est non vide.

Commençons par montrer que $\bigcap X$ est un ordinal.

• $\bigcap X$ est transitif.

En effet, soit $x \in \bigcap X$.

Pour tout $\alpha \in X$, on a $x \in \alpha$.

Or tous les éléments de X sont des ordinaux donc sont transitifs..

Donc pour tout $\alpha \in X$, on a $x \subseteq \alpha$.

Donc $x \subseteq \bigcap X$ par maximalité de l'intersection pour l'inclusion.

Donc $\forall x \in \bigcap X, x \subseteq \bigcap X$.

Donc $\bigcap X$ est transitif.

• Comme X est non vide, il existe $\alpha \in X$.

On a alors $\bigcap X \subseteq \alpha$.

Or tous les éléments de X sont des ordinaux donc α est un ordinal.

Donc $(\alpha, \in)$ est strictement bien ordonné.

Donc $\left(\bigcap X, \in\right)$ est strictement bien ordonné d'après la proposition 3 page 12.

On en conclut que $\boxed{\bigcap X \text{ est un ordinal}}$.

• Montrons que $\bigcap X = \min(X)$.

Par définition X est un ensemble non vide d'ordinaux.

Donc X admet un minimum ξ d'après le théorème 1 page 21.

Ainsi $\forall \alpha \in X, \xi \leq \alpha$ par définition du minimum.

Donc $\forall \alpha \in X, \xi \subseteq \alpha$ par définition de $\leq$.

Donc $\xi \subseteq \bigcap X$ par maximalité de l'intersection pour l'inclusion.

Or on a $\xi \in X$ puisque ξ est le minimum de X.

On a donc $\bigcap X \subseteq \xi$ par définition de l'intersection.

On a donc $\bigcap X = \xi$ par antisymétrie de l'inclusion.

Or par définition $\xi = \min(X)$ donc $\boxed{\bigcap X = \min(X)}$.

CQFD.

4 Ordinaux successeurs, limites et entiers naturels

Ce qui nous a motivé à introduire la notion de bon ordre est le fait qu'étant donné un élément x, il est possible de répondre à la question « *quel élément suit directement x ?* ». En effet, nous avons dit que dans ce cas-là, il suffit de prendre l'ensemble des éléments strictement plus grands que x, et de considérer alors son minimum. On parle alors du **successeur** de x. Dans le cas particulier des ordinaux, ce successeur a une expression simple (que l'on peut quand-même définir en toute généralité).

Définition 10 (Successeur d'un ensemble)

Soit x un ensemble.
On appelle **successeur** de x l'ensemble $S(x) := x \cup \{x\}$.

Exemple :
Il est temps de définir nos premiers entiers naturels.
On pose $0 := \varnothing$ et $1 := S(0)$.
Plus précisément, on a $1 = S(0) = S(\varnothing) = \varnothing \cup \{\varnothing\} = \{\varnothing\} = \{0\}$.
Nous verrons un peu plus tard comment définir tous les autres entiers naturels.
Quand nous aurons défini les entiers naturels, nous verrons que $n + 1$ sera défini comme étant $S(n)$, ce qui correspond bien à l'intuition de l'entier naturel qui suit directement n.

Nous avons défini la notion de successeur d'un ensemble en toute généralité, mais cette notion devient intéressante dans le cas des ordinaux puisqu'elle répond bien à la question de l'ordinal qui suit directement.

Proposition 12 (Successeur d'un ordinal)

Soient α et β deux ordinaux.

1. $S(\alpha)$ est un ordinal tel que $\alpha < S(\alpha)$.
   Ainsi $S(\alpha)$ est un ordinal strictement plus grand que α.
   Ou encore, α est un ordinal strictement plus petit que $S(\alpha)$.
2. On a l'équivalence $\alpha < \beta \iff S(\alpha) \leq \beta$.
   Ainsi $S(\alpha)$ est le plus petit des ordinaux strictement plus grands qu'α.
3. On a l'équivalence $\beta < S(\alpha) \iff \beta \leq \alpha$.
   Ainsi α est le plus grand des ordinaux strictement plus petits que $S(\alpha)$.

Ainsi $S(\alpha)$ porte bien son nom : c'est l'ordinal qui vient « *juste après* » α.

4. On a l'implication $S(\alpha) = S(\beta) \implies \alpha = \beta$.
   Ainsi le passage au successeur est injectif.

Démonstration

1. Commençons par montrer que $S(\alpha)$ est un ordinal.

Pour cela, montrons que $S(\alpha)$ est transitif.

Soit $x \in S(\alpha)$.

On a donc $x \in \alpha \cup \{\alpha\}$ par définition du successeur.

On a donc $x \in \alpha$ ou $x \in \{\alpha\}$.

- Plaçons-nous dans le cas où $x \in \alpha$.
  On a alors $x \subseteq \alpha$ car α est transitif car ordinal.
- Plaçons-nous dans le cas où $x = \alpha$.
  On a alors $x \subseteq \alpha$ par réflexivité de l'inclusion.

Dans les deux cas on a donc $x \subseteq \alpha$.

En particulier on a $x \subseteq \alpha \cup \{\alpha\}$ et donc $x \subseteq S(\alpha)$.

Donc pour tout $x \in S(\alpha)$, on a $x \subseteq S(\alpha)$.

Donc $S(\alpha)$ est transitif.

Montrons que $\big(S(\alpha), \in\big)$ est strictement bien ordonné.

On a $S(\alpha) = \alpha \cup \{\alpha\}$.

Donc chaque élément de $S(\alpha)$ est soit un élément de α, soit α lui-même.

Or α est un ordinal.

Donc tous les éléments de α sont des ordinaux d'après la prop. 6 p. 18.

Donc tous les éléments de $S(\alpha)$ sont des ordinaux.

Donc $\in$ est transitive et antiréflexive sur $S(\alpha)$ d'après le théorème 1 page 21.

De même, toute partie non vide de $S(\alpha)$ est alors un ensemble non vide d'ordinaux.

Donc toute partie non vide de $S(\alpha)$ admet un minimum d'après ce même théorème.

On en conclut que $\in$ est un bon ordre strict sur $S(\alpha)$.

Ainsi, $S(\alpha)$ est transitif et $\in$ est un bon ordre strict sur $S(\alpha)$.

Donc $\boxed{S(\alpha) \text{ est un ordinal}}$.

Par définition on a $\alpha \in \{\alpha\}$.

On a donc $\alpha \in \alpha \cup \{\alpha\}$.

On a donc $\alpha \in S(\alpha)$ par définition du successeur.

Autrement dit on a $\boxed{\alpha < S(\alpha)}$.

2. Raisonnons par double implications.

$\boxed{\Rightarrow}$

Supposons que $\alpha < \beta$.
En particulier on a $\alpha \leq \beta$ donc $\alpha \subseteq \beta$.
De plus comme $\alpha < \beta$, on a $\alpha \in \beta$ et donc $\{\alpha\} \subseteq \beta$.
Comme $\alpha \subseteq \beta$ et $\{\alpha\} \subseteq \beta$, on a $S(\alpha) = \alpha \cup \{\alpha\} \subseteq \beta$.
On a donc $S(\alpha) \leq \beta$.

Donc si $\alpha < \beta$ alors $S(\alpha) \leq \beta$.

$\boxed{\Leftarrow}$

Supposons que $S(\alpha) \leq \beta$.
On a donc $S(\alpha) \subseteq \beta$ et donc $\alpha \cup \{\alpha\} \subseteq \beta$.
En particulier $\{\alpha\} \subseteq \beta$ donc $\alpha \in \beta$ et donc $\alpha < \beta$.

Donc si $S(\alpha) \leq \beta$ alors $\alpha < \beta$.

Finalement, $\boxed{\alpha < \beta \iff S(\alpha) \leq \beta}$.

3. On a les équivalences suivantes

$$\begin{aligned}
\beta < S(\alpha) &\iff \beta \in S(\alpha)\\
&\iff \beta \in \alpha \cup \{\alpha\}\\
&\iff \beta \in \alpha \text{ ou } \beta \in \{\alpha\}\\
&\iff \beta \in \alpha \text{ ou } \beta = \alpha\\
&\iff \beta \subseteq \alpha \text{ d'après la prop. 8 p. 20}\\
&\iff \beta \leq \alpha
\end{aligned}$$

On a donc bien l'équivalence $\boxed{\beta < S(\alpha) \iff \beta \leq \alpha}$.

4. Supposons que $S(\alpha) = S(\beta)$.
D'après 1 on a $\beta < S(\beta)$ donc $\beta < S(\alpha)$ et donc $\beta \leq \alpha$ d'après 3.
De même, on a $\alpha < S(\alpha)$ donc $\alpha < S(\beta)$ et donc $\alpha \leq \beta$ d'après 3.
On a donc bien $\boxed{\alpha = \beta}$ par antisymétrie de $\leq$.
CQFD.

Remarque :
Comme on a défini 0 comme étant égal à $\varnothing$, on a déjà vu que 0 est le plus petit des ordinaux. En particulier il n'est le successeur d'aucun ordinal puisque sinon celui-ci serait strictement plus petit que 0.

Nous allons enfin définir la notion d'**entiers naturels** : il s'agit des premiers ordinaux. En effet 0 est le plus petit des ordinaux, 1 est son successeur, 2 est le successeur de 1 et ainsi de suite.

On pourrait penser qu'en partant de 0 et en enchaînant l'opération de successeur suffisamment de fois, on finirait par avoir parcouru tous les ordinaux. Il n'en est rien : il existe des ordinaux qui ne seront jamais atteints de cette manière. Le plus petit de ces ordinaux est noté ω : oui, il s'agit tout simplement de l'ensemble des entiers naturels, aussi noté $\mathbb{N}$. Tout ordinal plus petit que lui va donc lui appartenir, et donc être un entier naturel. Il n'a donc pas de prédécesseur direct : en effet si $\alpha < \omega$ alors $\alpha \in \omega$ donc α est un entier naturel par définition donc $S(\alpha) = \alpha + 1$ est aussi un entier naturel donc n'est pas ω (puisque sinon $\omega \in \omega$, ce qui est impossible chez les ordinaux).

Ainsi il existe des ordinaux qui ne sont successeurs d'aucun ordinal : il y a 0 bien sûr, mais aussi ω comme nous venons de le voir. Nous allons les appeler ordinaux **limites**, car il y a en quelque sorte une limite à franchir pour les atteindre, on ne peut pas simplement partir d'un ordinal et enchaîner des opérations de successeurs.

Définition 11 (Ordinaux successeurs, limites et entiers naturels)

Soit β un ordinal.

1. On dit que β est **successeur** si et seulement s'il existe un ordinal α tel que $\beta = S(\alpha)$.
2. On dit que β est **limite** si et seulement si β n'est pas successeur.
3. On dit que β est un **entier naturel** si et seulement si pour tout ordinal $\alpha \leq \beta$,
   - ou bien $\alpha = 0$
   - ou bien α est un ordinal successeur.

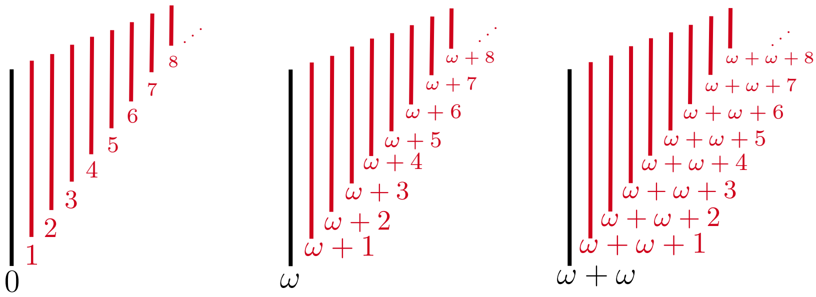
   On dit aussi que β est **fini**. Dans le cas contraire on dit que β est **transfini**.

Exemple :

1. Comme $0 = \varnothing$, on a déjà vu que 0 est un ordinal.
   1 en tant que successeur de 0 est aussi un ordinal.
   1 est un successeur (de 0 donc) et 0 est limite car non successeur car vide.
   0 et 1 sont tous les deux des entiers naturels.
2. Quand nous l'aurons défini, nous verrons que $\mathbb{N} = \omega$ l'ensemble des entiers naturel est un ordinal limite.
3. De même, nous définirons plus tard l'ordinal $\omega+1 = S(\omega)$, qui est lui bien successeur de ω donc n'est pas limite, mais n'est pas entier naturel non plus puisque $\omega \leq \omega + 1$ alors que ω n'est ni 0 ni successeur.

Remarque :
La plupart des ouvrages sur le sujet considère que 0 n'est pas un ordinal limite. En effet, dans ce cas-là il n'y a pas eu de limite à franchir pour l'atteindre. Pour des soucis de simplification d'énoncés, nous considérons ici bien qu'il l'est : au contraire l'exclure demande souvent de l'exclure artificiellement de beaucoup d'énoncés de résultats sur les ordinaux limites.

Pour aider à visualiser tout cela, on peut proposer l'illustration suivante :



Une représentation visuelle des ordinaux.

Il faut ici voir la disposition des bâtons comme s'étendant à l'infini à l'horizon, l'ordre des bâtons étant rangés de la gauche vers la droite : au début on a un bâton pour chaque entier naturel, puis après tous les entiers naturels vient le bâton associé à ω. Ensuite vient le bâton associé à $\omega+1$, puis $\omega+2$ et ainsi de suite pour tous les ordinaux de la forme $\omega+n$ où n est un entier naturel, donc une infinité de bâtons sont disposés après celui de ω. Mais après tous ceux-là se trouve un bâton associé à l'ordinal $\omega+\omega$, et ainsi de suite. Nous aurons bien entendu tout le temps de définir proprement chacun de ces ordinaux, l'idée est ici simplement de comprendre intuitivement ce que nous sommes en train de construire. Gardons bien en tête que la taille des bâtons n'a aucune importante, seul leur agencement horizontal importe. Le fait de représenter des bâtons de plus en plus petits est seulement une astuce pour en faire tenir une infinité.

On peut voir sur l'illustration que les ordinaux limites sont les bâtons qui n'ont pas de prédécesseur direct : nous les avons représentés en **noir**. En **rouge** sont représentés les ordinaux successeurs.

Proposition 13 (Successeur et ordinal limite)

Soit α un ordinal.
Les assertions suivantes sont équivalentes :

1. α est un ordinal limite.
2. Pour tout ordinal $\beta < \alpha$ on a $S(\beta) < \alpha$.

Autrement dit, un ordinal est limite si et seulement si partant d'un ordinal strictement plus petit, on reste strictement plus petit même en passant au successeur.

Démonstration

$\boxed{1 \Rightarrow 2}$

Supposons que α est un ordinal limite.

Soit β un ordinal tel que $\beta < \alpha$.

On a alors $S(\beta) \leq \alpha$ d'après la proposition 12 page 33.

On a donc $S(\beta) < \alpha$ ou $S(\beta) = \alpha$.

Or $S(\beta) = \alpha$ est impossible car par définition α est un ordinal limite.

On a donc nécessairement $S(\beta) < \alpha$.

Donc pour tout ordinal $\beta < \alpha$ on a $S(\beta) < \alpha$.

Donc $\boxed{\text{si } \alpha \text{ est un ordinal limite alors pour tout ordinal } \beta < \alpha, \text{ on a } S(\beta) < \alpha}$.

$\boxed{2 \Rightarrow 1}$

Supposons que pour tout ordinal $\beta < \alpha$ on a $S(\beta) < \alpha$.

Supposons par l'absurde que α n'est pas limite.

Par définition, α est donc successeur.

Il existe donc un ordinal β tel que $\alpha = S(\beta)$.

Or on a $\beta < S(\beta)$ d'après la proposition 12 page 33 donc $\beta < \alpha$.

On a donc $S(\beta) < \alpha$ par l'hypothèse.

Or on a dit que $\alpha = S(\beta)$, si bien que $\alpha < \alpha$.

C'est absurde par antiréflexivité de $<$.

Par l'absurde, on vient de montrer que α est limite.

Donc $\boxed{\text{si pour tout ordinal } \beta < \alpha \text{ on a } S(\beta) < \alpha \text{ alors } \alpha \text{ est limite}}$.

CQFD.

Proposition 14 (Successeur d'un entier naturel)

Soit n un entier naturel.

1. $S(n)$ est un entier naturel.
2. Tout ordinal $\alpha \leq n$ est aussi un entier naturel.

Démonstration

1. Par définition n est un entier naturel donc est un ordinal.

Donc $S(n)$ est un ordinal d'après la proposition 12 page 33.

Soit un ordinal $\alpha \leq S(n)$.

On a donc ou bien $\alpha < S(n)$ ou bien $\alpha = S(n)$.

- Supposons que $\alpha < S(n)$.

  On a alors $\alpha \leq n$ d'après la proposition 12 page 33.

  Or n est un entier naturel.

  Donc ou bien $\alpha = 0$, ou bien α est un successeur.

- Supposons que $\alpha = S(n)$. Comme n est un entier naturel, n est un ordinal.

  Donc $\alpha = S(n)$ est un successeur.

Dans les deux cas, ou bien $\alpha = 0$ ou bien α est un successeur.

Donc tous les ordinaux plus petit que $S(n)$ sont ou 0 ou bien un successeur.

Comme $S(n)$ est un ordinal, c'est donc par définition $\boxed{\text{un entier naturel}}$.

2. Soit un ordinal $\alpha \leq n$.

Soit un ordinal $\beta \leq \alpha$.

On a donc $\beta \leq n$ par transitivité de $\leq$.

Or n est un entier naturel et β un ordinal.

Donc ou bien $\beta = 0$ ou bien β est un successeur.

Donc tous les ordinaux plus petits que α sont ou bien 0 ou bien un successeur.

Comme α est un ordinal, par définition $\boxed{\alpha \text{ est un entier naturel}}$.

CQFD.

Bien souvent en mathématiques nous sommes amenés à mener un **raisonnement par récurrence** afin de prouver qu'une assertion P à paramètres est vraie pour tout entier naturel n. Pour cela on raisonne en deux étapes :

1. On prouve que $P(0)$ est vraie : c'est l'étape d'**initialisation**.
2. On prouve que pour tout entier naturel n, si $P(n)$ est vraie alors $P(n+1)$ est aussi vraie. C'est l'étape d'**hérédité**.

Grâce à ces deux étapes, on en conclut que $P(n)$ est vraie pour tout entier naturel n. Qu'est-ce qui justifie la validité de ce raisonnement ? La réponse se cache dans le théorème suivant.

Théorème 3 (Principe d'induction chez les entiers naturels)

Soit X un ensemble tel que :

1. $0 \in X$
2. Pour tout $x \in X$ on a $S(x) \in X$.

Alors X contient tous les entiers naturels.

Démonstration

Voici rapidement l'idée de la preuve : on suppose par l'absurde que X ne contient pas un entier naturel donné n. On regarde alors l'ensemble Y des entiers naturels plus petits que n qui ne sont pas dans X. En particulier n est dedans donc Y n'est pas vide : il va avoir un plus petit entier naturel k. Le soucis vient alors du fait que k est le plus petit entier naturel à ne pas être dans X, et donc $k-1$ va être dans X, ce qui contredit l'hypothèse 2 selon laquelle X est stable par passage au successeur.

Soit n un entier naturel.

Supposons par l'absurde que $n \notin X$.

Considérons $Y := S(n) \backslash X$.

Comme n est un entier naturel, $S(n)$ est un entier naturel d'après la prop. 14 p. 38.

Donc tous les éléments de $S(n)$ sont des entiers naturels d'après la prop. 14 p. 38.

Or $Y = S(n)\backslash X$ donc $Y \subseteq S(n)$.

Donc tous les éléments de Y sont des entiers naturels.

On a $n < S(n)$ d'après la proposition 12 page 33.

On a donc $n \in S(n)$ par définition de $<$, et $n \notin X$ par hypothèse.

On a donc $n \in Y$ puisque $Y = S(n)\backslash X$.

Donc Y est un ensemble non vide d'entiers naturels.

Il possède donc un entier naturel minimum k d'après le théorème 1 page 21.

On a $k \leq k$ par réflexivité de $\leq$.

Donc k est un ordinal plus petit qu'un entier naturel (lui-même).

Donc k est ou bien 0 ou bien un successeur par définition.

Or $k \in Y = S(n)\backslash X$ donc $k \notin X$. Comme $0 \in X$ par hypothèse, on a donc $k \neq 0$.

Donc k est un successeur : il existe un ordinal i tel que $k = S(i)$.

Or on a $i < S(i)$ d'après la proposition 12 page 33 donc $i < k$.

Donc $i \notin Y$ car k est le minimum de Y.

Mais comme $n \in Y$, on a aussi $k \leq n$, toujours par minimalité de k.

Ainsi on a $i < k \leq n < S(n)$ donc $i < S(n)$ par transitivité.

On a donc $i \in S(n)$ par définition de $<$.

Ainsi $i \notin Y$ et $i \in S(n)$ donc $i \in S(n)\backslash Y = X$.

Or par hypothèse X est stable par successeur donc $S(i) \in X$ et donc $k \in X$.

C'est absurde puisque $k \in Y$ et $Y = S(n)\backslash X$ donc $k \notin X$.

Donc par l'absurde on vient donc de montrer $\boxed{n \in X}$.

CQFD.

Nous pouvons donc justifier la validité du raisonnement par récurrence : imaginons avoir démontré l'étape d'initialisation et l'étape d'hérédité. On peut alors considérer l'ensemble $X := \{n \in \mathbb{N} \mid P(n)\}$ qui répond alors aux hypothèses du théorème ci-dessus : il contient tous les entiers naturels, ce qui prouve donc bien que $P(n)$ est vraie pour tout entier naturel.

En vérité, il manque quelque chose pour valider ce que nous venons d'affirmer : l'existence de $\mathbb{N}$ lui-même. En effet on affirme depuis le début que $\mathbb{N}$, l'ensemble de tous les entiers naturels existe, et on l'a même aussi noté ω en affirmant qu'il s'agit d'un ordinal. Malheureusement, on ne peut le faire sans un axiome, que l'on va donc rajouter aux différents axiomes de ZFC du précédent livre : l'**axiome de l'infini**.

Axiome 1 (de l'infini)

Il existe au moins un ensemble X tel que

1. $0 \in X$
2. Pour tout $x \in X$ on a $S(x) \in X$.

Nous sommes à présents armés pour définir proprement $\mathbb{N}$.

Proposition 15 (Ensemble des entiers naturels)

Il existe un unique ensemble $\mathbb{N}$ tel que pour tout ensemble n, on a l'équivalence

$$n \in \mathbb{N} \iff n \text{ est un entier naturel}$$

On dit donc que $\mathbb{N}$ est l'**ensemble des entiers naturels**, et on le note aussi parfois ω.

Démonstration

Existence :

D'après l'**axiome de l'infini**, il existe un ensemble X tel que

1. $0 \in X$
2. Pour tout $x \in X$ on a $S(x) \in X$.

Posons alors $\mathbb{N} := \{x \in X \mid x \text{ est un entier naturel}\}$.

Montrons que $\mathbb{N}$ ainsi défini vérifie l'équivalence de l'énoncé.

Soit n un ensemble.

$\boxed{\Rightarrow}$ Si $n \in \mathbb{N}$ alors par définition n est un entier naturel.

$\boxed{\Leftarrow}$

Supposons que n est un entier naturel.

Alors $n \in X$ d'après le principe d'induction chez les entiers naturels.

Donc $n \in X$ et n est un entier naturel.

Donc $n \in \mathbb{N}$ par définition de $n \in \mathbb{N}$.

Donc si n est un entier naturel alors $\mathbb{N}$.

Ainsi pour tout ensemble n, on a bien l'équivalence $\boxed{n \in \mathbb{N} \iff n \text{ est un entier naturel}}$.

Unicité :

L'unicité est garantie par le fait que cette équivalence caractérise l'appartenance à $\mathbb{N}$.

CQFD.

Avant de prouver que $\mathbb{N}$ est un ordinal, intéressons-nous aux segments initiaux de ON.

Proposition 16 (Segment initiaux des ordinaux)

Soit X un ensemble.

Les assertions suivantes sont équivalentes :

1. X est un ordinal.

2. Tous les éléments de X sont des ordinaux et X est transitif.
3. X est un segment initial de ON.

Démonstration

Nous allons montrer 1⇔2⇔3.

$\boxed{1\Rightarrow 2}$

Supposons que X est un ordinal.

En particulier X est transitif par définition.

De plus, tous les éléments de X sont des ordinaux d'après la proposition 6 page 18.

$\boxed{1\Leftarrow 2}$

Supposons que tous les éléments de X sont des ordinaux et que X est transitif.

Comme X est un ensemble d'ordinaux, $(X, \in)$ est strictement bien ordonné d'après le théorème 1 page 21. Comme X est transitif, on en conclut que $\boxed{X \text{ est un ordinal}}$.

$\boxed{2\Rightarrow 3}$

Supposons que tous les éléments de X sont des ordinaux et que X est transitif.

En particulier on sait déjà que $X \subseteq ON$ par définition de ON.

Soient α et β deux ordinaux.

Supposons que $\alpha \leq \beta \in X$.

Comme $\alpha \leq \beta$, on a $(\alpha < \beta$ ou $\alpha = \beta)$.

- Plaçons-nous dans le cas où $\alpha < \beta$.
  Par définition cela veut dire que $\alpha \in \beta$.
  Ainsi on a $\alpha \in \beta \in X$.
  Or X est transitif, donc par définition $\alpha \in X$.
- Plaçons-nous dans le cas où $\alpha = \beta$.
  Par hypothèse on a $\beta \in X$ donc $\alpha \in X$.

Donc dans les deux cas on a $\alpha \in X$.

Donc si $\alpha \leq \beta \in X$ alors $\alpha \in X$.

Donc $\boxed{X \text{ est un segment initial de } ON}$.

$\boxed{2\Leftarrow 3}$

Supposons que X est un segment initial de ON.

Par définition on a alors $X \subseteq ON$.

Autrement dit, tous les éléments de X sont des ordinaux.

Soit $\beta \in X$.

Comme on vient de le dire, tous les éléments de X sont des ordinaux.

Donc β est un ordinal.

Soit $\alpha \in \beta$.

Alors α est un ordinal en tant qu'élément d'un ordinal.

Comme $\alpha \in \beta$ on a $\alpha < \beta$ et en particulier $\alpha \leq \beta$.

Ainsi α et β sont deux ordinaux tels que $\alpha \leq \beta \in X$.

On a donc $\alpha \in X$ puisque X est un segment initial de ON.

Donc $\forall \alpha \in \beta, \alpha \in X$ et donc $\beta \subseteq X$ par définition de l'inclusion.

Donc $\forall \beta \in X, \beta \subseteq X$ et donc $\boxed{X \text{ est transitif}}$.

CQFD.

Remarque :
On a vu grâce au théorème 1 page 21 que les ordinaux sont munis d'un bon ordre.
X est un segment initial des ordinaux est donc équivalent à l'existence d'un ordinal ξ tel que $X = \xi\downarrow$ d'après la proposition 5 page 14. Ici ξ est tout trouvé : c'est X lui-même d'après cette proposition. C'est d'ailleurs assez logique puisque la relation d'ordre strict sur les ordinaux est l'appartenance et donc $X = \{\alpha \mid \alpha \in X\} = \{\alpha \mid \alpha < X\} = X\downarrow$.

Nous pouvons désormais prouver que ω, autre nom donné à $\mathbb{N}$, est un ordinal. Comme nous l'avons dit plus tôt, c'est même un ordinal limite, c'est-à-dire qu'il n'est pas un successeur. Mieux, c'est même le plus petit des ordinaux limites non nuls, c'est-à-dire le tout premier après 0 !

Proposition 17 (omega est le plus petit ordinal limite non nul)

1. ω est un ordinal limite.
2. ω est le plus petit des ordinaux limites non nuls.
   Autrement dit pour tout ordinal limite non nul α, on a $\omega \leq \alpha$.

Démonstration

1.

• Montrons que ω est un ordinal.

D'après la proposition 16 page 41, il suffit de montrer que ω est un segment initial de ON.

ω ne contient que des entiers naturels (et les contient tous) par définition.

En particulier ω est un ensemble d'ordinaux : on sait déjà que $\omega \subseteq ON$.

Soient n et m deux ordinaux.

Supposons que $n \leq m \in \omega$.

On a $m \in \omega$ donc m est un entier naturel par définition.

On a $n \leq m$ donc n est un entier naturel d'après la proposition 14 page 38.

On a donc $n \in \omega$ par définition.

Donc si $n \leq m \in \omega$ alors $n \in \omega$.

Donc pour tout n et m dans ON, si $n \leq m \in \omega$ alors $n \in \omega$.

Donc ω est un segment initial de ON.

Donc $\boxed{\omega \text{ est un ordinal}}$ d'après la proposition 16 page 41.

• Montrons que ω est un ordinal limite.

Supposons par l'absurde que ω est successeur.

Il existe donc un ordinal α tel que $\omega = S(\alpha)$.

On a $\alpha < S(\alpha)$ d'après la proposition 12 page 33.

On a donc $\alpha < \omega$, c'est-à-dire $\alpha \in \omega$ par définition de $<$.

Donc α est un entier naturel par définition de ω.

Donc $S(\alpha)$ est un entier naturel d'après la proposition 14 page 38.

Donc $S(\alpha) \in \omega$ par définition de ω, c'est-à-dire $\omega \in \omega$.

On a donc $\omega < \omega$: c'est absurde par antiréflexivité de $<$.

Donc ω n'est pas un successeur et donc $\boxed{\omega \text{ est limite}}$.

2. Montrons que ω est plus petit que tout ordinal limite non nul.

Soit α un ordinal limite non nul.

Soit n un ordinal tel que $n < \omega$.

On a donc $n \in \omega$ par définition de $<$.

Donc n est un entier naturel par définition de ω.

Or on a $n \leq n$ par réflexivité de $\leq$.

Donc n est un ordinal plus petit qu'un entier naturel (lui-même).

Donc $n = 0$ ou n est un successeur par définition des entiers naturels.

Donc tout ordinal strictement plus petit que ω est ou bien nul ou bien successeur.

Or α est limite non nul donc n'est ni nul ni successeur.

Donc α n'est pas strictement plus petit que ω.

On a donc $\boxed{\omega \leq \alpha}$ puisque $\leq$ est total chez les ordinaux.

CQFD.

Nous l'avons dit quand nous avons évoqué le paradoxe de Burali-Forti : il n'est pas possible d'encapsuler tous les ordinaux dans un seul ensemble. En fait le résultat est même plus fort : tout ensemble d'ordinaux est majoré par d'autres ordinaux qui ne sont pas dans l'ensemble. En particulier parmi tous ces majorants stricts se cache un plus petit majorant strict.

Proposition 18 (Plus petit majorant strict d'ordinaux)

Soit X un ensemble d'ordinaux.
Alors il existe un unique ordinal α tel que

1. α est un majorant strict de X.
   Autrement dit $\forall \xi \in X, \xi < \alpha$.
2. α est plus petit que tout majorant strict de X.
   Autrement dit pour tout ordinal β, si $\forall \xi \in X, \xi < \beta$ alors $\alpha \leq \beta$.

Autrement dit α est le plus petit de tous les majorants stricts de X.

Démonstration

D'après la proposition 11 page 29, $\bigcup X$ est un ordinal.

Le plus petit des majorants stricts de X va dépendre de si $\bigcup X$ appartient à X ou non.

Posons alors $\alpha := \begin{cases} \bigcup X & \text{si } \bigcup X \notin X \\ S(\bigcup X) & \text{si } \bigcup X \in X \end{cases}$.

1.

On a vu lors de la proposition 11 page 29 que $\bigcup X = \sup(X)$.

En particulier $\bigcup X$ est un majorant de X.

- Plaçons-nous dans le cas où $\bigcup X \notin X$.
  Alors $\bigcup X$ est un majorant strict de X puisqu'il n'en est pas un élément.
  Or dans ce cas-là on a $\alpha = \bigcup X$ donc α est un majorant strict de X.
- Supposons à présent que $\bigcup X \in X$.
  On a donc $\alpha = S(\bigcup X)$.
  Or $\bigcup X$ est un majorant de X donc $\forall \xi \in X, \xi \leq \bigcup X$.
  Donc $\forall \xi \in X, \xi < S(\bigcup X)$ d'après la proposition 12 page 33.
  On a donc $\forall \xi \in X, \xi < \alpha$ et donc α est un majorant strict de X.

Dans les deux cas, $\boxed{\alpha \text{ est un majorant strict de } X}$.

2. Soit β un ordinal majorant strict de X.

Comme α et β sont deux ordinaux, on a $\beta < \alpha$ ou $\alpha \leq \beta$.

Supposons par l'absurde que $\beta < \alpha$.

- Plaçons-nous dans le cas où $\bigcup X \notin X$.
  Par définition de α on a alors $\alpha = \bigcup X$ donc $\beta < \bigcup X$.
  Autrement dit on a $\beta \in \bigcup X$ par définition de $<$.
  Par définition de la réunion, il existe donc $\xi \in X$ tel que $\beta \in \xi$.
  Autrement dit il existe $\xi \in X$ tel que $\beta < \xi$ par définition de $<$.

Donc β n'est pas un majorant de X, ce qui est absurde.

- Plaçons-nous dans le cas où $\bigcup X \in X$.
  Par définition de α on a alors $\alpha = S(\bigcup X)$ donc $\beta \in S(\bigcup X)$.
  On a donc $\beta < S(\bigcup X)$ par définition de $<$.
  Donc $\beta \leq \bigcup X$ d'après la proposition 12 page 33.
  Or $\bigcup X \in X$ par hypothèse donc β n'est pas un majorant strict de X.
  C'est absurde.

Dans les deux cas on aboutit à une absurdité.
Donc par l'absurde on a montré que l'on n'a pas $\beta < \alpha$, et donc $\boxed{\alpha \leq \beta}$.
CQFD.

Dans la preuve qui précède, nous avons discuté du fait que pour un ensemble d'ordinaux X, sa borne supérieure $\sup(X) = \bigcup X$ est un élément de X ou non. Si ce n'est pas le cas, on est en fait assuré que $\sup(X)$ est un ordinal limite.

Proposition 19 (Borne supérieure qui n'est pas un maximum)

Soit X un ensemble d'ordinaux.
Si $\sup(X) \notin X$ alors $\sup(X)$ est un ordinal limite.

Démonstration

Montrons le résultat par contraposition.
Supposons que $\sup(X)$ n'est pas un ordinal limite.
Donc $\sup(X)$ est un successeur par définition.
Il existe donc un ordinal α tel que $\sup(X) = S(\alpha)$.
Par définition $\sup(X)$ est un majorant de X.
Donc $S(\alpha)$ est un majorant de X : on a $\forall \xi \in X, \xi \leq S(\alpha)$.
Supposons par l'absurde que $\sup(X) \notin X$.
On a donc $S(\alpha) \notin X$ donc $\forall \xi \in X, \xi \neq S(\alpha)$.
Donc $\forall \xi \in X, \xi < S(\alpha)$ d'après ce qui précède.
On a donc $\forall \xi \in X, \xi \leq \alpha$ d'après la proposition 10 page 33.
Donc α est un majorant de X.
Or on a $\alpha < S(\alpha)$ d'après la proposition 10 page 33.
Donc $S(\alpha)$ n'est pas le plus petit des majorants de X.
C'est absurde : cela veut dire que $S(\alpha)$ n'est pas la borne supérieure de X.
Par l'absurde, on vient de montrer que $\sup(X) \in X$.
Donc si $\sup(X)$ n'est pas limite alors $\sup(X) \in X$.

Par contraposition, on a $\boxed{\text{si } \sup(X) \in X \text{ alors } \sup(X) \text{ est limite}}$.

CQFD.

Dans le cas où X est lui-même un ordinal, cette proposition se précise. Cela nous fournit même une autre caractérisation d'être un ordinal limite, en plus de celle donnée par la proposition 13 page 37.

Proposition 20 (Ordinal limite et borne supérieure)

Soit α un ordinal.
Les assertions suivantes sont équivalentes :

1. α est un ordinal limite.
2. $\sup(\alpha) = \alpha$

Démonstration

$\boxed{1 \Rightarrow 2}$ Supposons que α est un ordinal limite.

On a donc $\forall \beta \in \alpha, S(\beta) < \alpha$ d'après la proposition 13 page 37.

Notons $(\star)$ cette affirmation.

Par définition de $<$ on a $\forall \beta \in \alpha, \beta < \alpha$.

En particulier $\forall \beta \in \alpha, \beta \leq \alpha$ donc α est un majorant de lui-même.

On a donc $\sup(\alpha) \leq \alpha$ par minimalité de la borne supérieure.

Supposons par l'absurde que $\sup(\alpha) \neq \alpha$.

On a donc $\sup(\alpha) < \alpha$ par ce qui précède.

On a donc $S\big(\sup(\alpha)\big) < \alpha$ d'après $(\star)$, donc $S\big(\sup(\alpha)\big) \in \alpha$ par définition de $<$.

Or on a $\sup(\alpha) < S\big(\sup(\alpha)\big)$ d'après la proposition 12 page 33.

Donc $\sup(\alpha)$ n'est pas un majorant de α.

C'est absurde par définition de la borne supérieure.

Par l'absurde, on vient de montrer que $\boxed{\sup(\alpha) = \alpha}$.

$\boxed{2 \Rightarrow 1}$ Supposons que $\sup(\alpha) = \alpha$.

On n'a pas $\alpha < \alpha$ par antiréflexivité de $<$.

On n'a donc pas $\sup(\alpha) < \alpha$ par hypothèse, et donc $\sup(\alpha) \notin \alpha$ par définition de $<$.

Donc $\sup(\alpha)$ est un ordinal limite d'après la proposition 19 page 46.

Donc comme $\sup(\alpha) = \alpha$, on en déduit que $\boxed{\alpha \text{ est un ordinal limite}}$.

CQFD.

5 Isomorphisme avec les ordinaux

Jusqu'à présent, nous avons définis, construits et étudiés les ordinaux pour eux-mêmes. Or à la base nous les avons introduits dans l'optique d'en faire des représentants de classes d'isomorphie. Il est donc temps d'étudier d'un peu plus près les isomorphismes. Commençons par constater quelques propriétés de base que conservent les isomorphismes : c'est en cela que l'on peut dire que si deux ensembles ordonnés sont isomorphes, alors ils représentent en fait la même structure d'ensemble ordonné.

Proposition 21 (Isomorphismes et propriétés conservées)

Soient E et F deux ensembles ordonnées.
Soient $f : E \longrightarrow F$ un isomorphisme d'ordre,$A \subseteq E$ et $x \in E$.

Majorants et minorants

1. x est un majorant de A si et seulement si $f(x)$ est un majorant de $f^{\to}(A)$.
   En particulier, A est majorée si et seulement si $f^{\to}(A)$ est majorée.
2. x est un minorant de A si et seulement si $f(x)$ est un minorant de $f^{\to}(A)$.
   En particulier, A est minorée si et seulement si $f^{\to}(A)$ est minorée.

Maximum et minimum

3. A admet un maximum si et seulement si $f^{\to}(A)$ admet un maximum.
   Dans ce cas-là on a $f\big(\max(A)\big) = \max\big(f^{\to}(A)\big)$.
4. A admet un minimum si et seulement si $f^{\to}(A)$ admet un minimum.
   Dans ce cas-là on a $f\big(\min(A)\big) = \min\big(f^{\to}(A)\big)$.

Bornes supérieure et inférieure

5. A admet une borne supérieure si et seulement si $f^{\to}(A)$ admet une borne supérieure.
   Dans ce cas-là on a $f\big(\sup(A)\big) = \sup\big(f^{\to}(A)\big)$.
6. A admet une borne inférieure si et seulement si $f^{\to}(A)$ admet une borne inférieure.
   Dans ce cas-là on a $f\big(\inf(A)\big) = \inf\big(f^{\to}(A)\big)$.

Maximal et minimal

7. x est un élément maximal de A si et seulement si $f(x)$ est un élément maximal de $f^{\to}(A)$. En particulier, A admet un élément maximal si et seulement si $f^{\to}(A)$ admet un élément maximal.
8. x est un élément minimal de A si et seulement si $f(x)$ est un élément minimal de $f^{\to}(A)$. En particulier, A admet un élément minimal si et seulement si $f^{\to}(A)$ admet un élément minimal.

Ordre total, ordre bien fondé et bon ordre

9. E est totalement ordonné si et seulement si F est totalement ordonné.
10. L'ordre sur E est bien fondé si et seulement si l'ordre sur F est bien fondé.
11. E est bien ordonné si et seulement si F est bien ordonné.

Démonstration

Notons $\preccurlyeq$ l'ordre sur E et $\sqsubseteq$ l'ordre sur F.

1. On a les équivalences suivantes :

$$\begin{aligned} x \text{ majore } A &\iff \forall a \in A, a \preccurlyeq x \\ &\iff \forall a \in A, f(a) \sqsubseteq f(x) \text{ car } f \text{ est un isomorphisme d'ordres} \\ &\iff \forall y \in f^{\rightarrow}(A), y \sqsubseteq f(x) \\ &\iff f(x) \text{ majore } f^{\rightarrow}(A) \end{aligned}$$

De cela, on montre en particulier :

$\boxed{\Rightarrow}$

Supposons que A est majorée.

Elle admet donc un majorant $m \in E$.

D'après ce qui précède $f(m)$ est un majorant de $f^{\rightarrow}(A)$.

Donc $f^{\rightarrow}(A)$ est majorée.

Donc si A est majorée alors $f^{\rightarrow}(A)$ est majorée.

$\boxed{\Leftarrow}$

Supposons que $f^{\rightarrow}(A)$ est majorée.

Elle admet donc un majorant $M \in F$.

Or f est un isomorphisme d'ordres donc en particulier f est surjectif dans F.

Il existe donc $m \in E$ tel que $M = f(m)$.

Ainsi $f(m)$ est un majorant de $f^{\rightarrow}(A)$.

Donc m est un majorant de A d'après ce qui précède, et donc A est majorée.

Donc si $f^{\rightarrow}(A)$ est majorée alors A est majorée.

2. Cela se montre exactement de la même manière.

3. $\boxed{\Rightarrow}$

Supposons que A admet un maximum.

Par définition $\max(A)$ est un majorant de A.

Donc $f\big(\max(A)\big)$ est un majorant de $f^{\rightarrow}(A)$ d'après 1.

De plus $\max(A) \in A$ par définition donc $f\big(\max(A)\big) \in f^{\rightarrow}(A)$.

Ainsi $f\big(\max(A)\big)$ est un majorant de $f^{\rightarrow}(A)$ et en est un élément.

Donc $f^{\rightarrow}(A)$ admet pour maximum $f\big(\max(A)\big)$.

Donc si A admet un maximum alors $f^{\rightarrow}(A)$ admet un maximum.

Dans ce cas-là, on vient de montrer que $\max\big(f^{\rightarrow}(A)\big) = f\big(\max(A)\big)$.

$\boxed{\Leftarrow}$

Supposons que $f^{\rightarrow}(A)$ admet un maximum M.

Par définition on a $M \in f^{\rightarrow}(A)$ donc il existe $m \in A$ tel que $M = f(m)$.

Par définition M est un majorant de $f^{\rightarrow}(A)$ donc m est un majorant de A d'après 1.

Ainsi m est un majorant de A et en est un élément.

Donc A admet pour maximum m.

Donc si $f^{\rightarrow}(A)$ admet un maximum alors A admet un maximum.

4. Cela se montre de la même manière.

5. $\boxed{\Rightarrow}$

Supposons que A admet une borne supérieure.

Par définition $\sup(A)$ est un majorant de A.

Donc $f\big(\sup(A)\big)$ est un majorant de $f^{\rightarrow}(A)$ d'après 1.

Soit M un majorant de $f^{\rightarrow}(A)$.

Comme f est un isomorphisme d'ordres, f est en particulier inversible.

Considérons $m := f^{-1}(M)$.

Alors m est un majorant de $(f^{-1})^{\rightarrow}\big(f^{\rightarrow}(A)\big) = A$ d'après 1.

Donc $\sup(A) \preccurlyeq m$ par minimalité de la borne supérieure.

Donc $f\big(\sup(A)\big) \sqsubseteq f(m)$ car f est un isomorphisme d'ordre.

Autrement dit on a $f\big(\sup(A)\big) \sqsubseteq M$.

Donc $f\big(\sup(A)\big)$ est le plus petit des majorants de $f^{\rightarrow}(A)$.

Donc $f^{\rightarrow}(A)$ admet pour borne supérieure $f\big(\sup(A)\big)$.

Donc si A admet une borne supérieure alors $f^{\rightarrow}(A)$ admet une borne supérieure.

Dans ce cas-là on vient de voir que $\sup\big(f^{\rightarrow}(A)\big) = f\big(\sup(A)\big)$.

$\boxed{\Leftarrow}$

Supposons que $f^{\rightarrow}(A)$ admet une borne supérieure S.

Comme f est un isomorphisme d'ordres, f est en particulier inversible.

Considérons $s := f^{-1}(S)$.

Par définition S est un majorant de $f^{\rightarrow}(A)$.

Donc s est un majorant de $(f^{-1})^{\rightarrow}\big(f^{\rightarrow}(A)\big) = A$ d'après 1.

Soit m un majorant de A.

Alors $f(m)$ est un majorant de $f^{\rightarrow}(A)$ d'après 1.

Donc $S \sqsubseteq f(m)$ par minimalité de la borne supérieure.

Autrement dit on a $f(s) \sqsubseteq f(m)$.

Donc $s \preccurlyeq m$ car f est un isomorphisme d'ordres.

Donc s est le plus petit des majorants de A.

Donc A admet pour borne supérieure s.

Donc si $f^{\rightarrow}(A)$ admet une borne supérieure alors A admet une borne supérieure.

6. Cela se montre exactement de la même manière.

7. $\boxed{\Rightarrow}$

Supposons que x est un élément maximal de A.

En particulier $x \in A$ par définition, et donc $f(x) \in f^{\rightarrow}(A)$.

Soit $y \in f^{\rightarrow}(A)$.

Par définition, il existe $a \in A$ tel que $y = f(a)$.

Supposons que $f(x) \sqsubseteq y$.

On a donc $f(x) \sqsubseteq f(a)$.

Donc $x \preccurlyeq a$ car f est un isomorphisme d'ordres.

Or x est un élément maximal de A.

Donc $x = a$ par définition.

Donc $f(x) = f(a) = y$.

Donc si $f(x) \sqsubseteq y$ alors $f(x) = y$.

Donc pour tout $y \in f^{\rightarrow}(A)$, si $f(x) \sqsubseteq y$ alors $f(x) = y$.

Comme $f(x) \in f^{\rightarrow}(A)$, on en conclut que $f(x)$ est un élément maximal de $f^{\rightarrow}(A)$.

Donc si x est un élément maximal de A alors $f(x)$ est un élément maximal de $f^{\rightarrow}(A)$.

$\boxed{\Leftarrow}$

Supposons que $f(x)$ est un élément maximal de $f^{\rightarrow}(A)$.

En particulier $f(x) \in f^{\rightarrow}(A)$: il existe $a \in A$ tel que $f(x) = f(a)$.

Or f est un isomorphisme d'ordres donc en particulier f est injectif.

Donc $x = a$ et donc $x \in A$.

Soit $b \in A$.

Par définition on a $f(b) \in f^{\rightarrow}(A)$.

Supposons que $x \preccurlyeq b$.

Alors $f(x) \sqsubseteq f(b)$ car f est un isomorphisme d'ordres.

Or $f(b) \in f^{\rightarrow}(A)$ et $f(x)$ est un élément maximal de $f^{\rightarrow}(A)$.

Donc $f(x) = f(b)$ par définition.

Donc $x = b$ car f est un isomorphisme d'ordres donc est injectif.

Donc si $x \preccurlyeq b$ alors $x = b$.

Donc pour tout $b \in A$, si $x \preccurlyeq b$ alors $x = b$.

Donc x est un élément maximal de A.

Donc si $f(x)$ est un élément maximal de $f^{\rightarrow}(A)$ alors x est un élément maximal de A.

Cela permet de démontrer les implications qui suivent :

$\boxed{\Rightarrow}$

Supposons que A admet un élément maximal m.

Alors $f(m)$ est un élément maximal de $f^{\rightarrow}(A)$ d'après ce qui précède.

Donc si A admet un élément maximal alors $f^{\rightarrow}(A)$ admet un élément maximal.

$\boxed{\Leftarrow}$

Supposons que $f^{\rightarrow}(A)$ admet un élément maximal M.

Par définition il existe $a \in A$ tel que $M = f(a)$.

Comme $f(a)$ est un élément maximal de $f^{\rightarrow}(A)$, a est un élément maximal de A d'après ce qui précède.

Donc si $f^{\rightarrow}(A)$ admet un élément maximal alors A admet un élément maximal.

8. Cela se montre exactement de la même manière.

9. $\boxed{\Rightarrow}$

Supposons que E est totalement ordonné.

Soient y_1 et y_2 dans F.

Par définition f est un isomorphismes d'ordres.

En particulier f est surjective dans F.

Il existe donc x_1 et x_2 dans E tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.

Or E est totalement ordonné donc $x_1 \preccurlyeq x_2$ ou $x_2 \preccurlyeq x_1$.

On a donc $f(x_1) \sqsubseteq f(x_2)$ ou $f(x_2) \sqsubseteq f(x_1)$ car f est un isomorphisme d'ordres. On a donc $y_1 \sqsubseteq y_2$ ou $y_2 \sqsubseteq y_1$.

Donc F est totalement ordonné.

Donc si E est totalement ordonné alors F est totalement ordonné.

$\boxed{\Leftarrow}$

Supposons que F est totalement ordonné.

Par définition $f : E \longrightarrow F$ est un isomorphisme d'ordres.

Donc f est inversible et $f^{-1} : F \longrightarrow E$ est un isomorphisme d'ordres.

Donc E est totalement ordonné d'après le sens $\boxed{\Rightarrow}$.

Donc si F est totalement ordonné alors E est totalement ordonné.

10. $\boxed{\Rightarrow}$

Supposons que l'ordre sur E est bien fondé.

Soit B une partie non vide de F.

Considérons $A := f^{\leftarrow}(B)$.

Comme f est un isomorphisme d'ordres, A est une partie non vide de E.

Or l'ordre sur E est bien fondé donc A admet un élément minimal a_0.

Donc $f(a_0)$ est un élément minimal de $f^{\rightarrow}(A)$.

Or f est un isomorphisme d'ordre, donc en particulier

$$f^{\rightarrow}(A) = f^{\rightarrow}\big(f^{\leftarrow}(B)\big) = B$$

Donc B admet un élément minimal.

Donc toute partie non vide de F admet un élément minimal.

Donc l'ordre sur F est bien fondé.

Donc si l'ordre sur E est bien fondé alors l'ordre sur F est bien fondé.

$\boxed{\Leftarrow}$

Supposons que l'ordre sur F est bien fondé.

Par définition $f : E \longrightarrow F$ est un isomorphisme d'ordres.

Donc f est inversible et $f^{-1} : F \longrightarrow E$ est un isomorphisme d'ordres.

Donc l'ordre sur F est bien fondé d'après le sens $\boxed{\Rightarrow}$.

Donc si l'ordre sur F est bien fondé alors l'ordre sur E est bien fondé.

11. On a les équivalences suivantes :

E est bien ordonné $\iff$ L'ordre sur E est total et bien fondé d'après la prop. 2 p. 11

$\iff$ L'ordre sur F est total et bien fondé d'après 9. et 10.

F est bien ordonné d'après la prop. 2 p. 11

D'où l'équivalence recherchée.

CQFD.

Ceci étant fait, rentrons plutôt dans le coeur de ce qui nous intéresse : constatons qu'un ensemble bien ordonné est toujours isomorphe à l'ensemble de ses segments initiaux propres. Ce n'est pas étonnant dans la mesure où l'on a dit que tout segment propre d'un ensemble bien ordonné est de la forme $x\downarrow$ lors de la proposition 5 page 14.

Proposition 22 (Ensemble des segments initiaux)

Soit E un ensemble **bien ordonné**.
Soit $X := \big\{A \subseteq E \;\big|\; A \text{ est un segment initial propre de } E\big\}$.
On munit X de la relation d'ordre $\subseteq$.

Soit $f := \begin{pmatrix} E & \longrightarrow & X \\ x & \longmapsto & x\downarrow \end{pmatrix}$.

On a alors :

1. f est un isomorphisme d'ordre de E vers X.
2. Si de plus E est un ordinal alors $f = \mathrm{id}_E$ et en particulier $E = X$.

Démonstration

Soient $\preccurlyeq$ la relation d'ordre sur E et $\prec$ l'ordre strict associé.

1.

• Montrons que f est strictement croissante.

Soient x et y dans E.

Supposons que $x \prec y$.

On a alors $x \in y\downarrow$ par définition.

Or on n'a pas $x \prec x$ par antiréflexivité de $\prec$ donc $x \notin x\downarrow$.

Comme $x \in y\downarrow$ et $x \notin x\downarrow$ on a $x\downarrow \neq y\downarrow$.

Soit $z \in x\downarrow$.

On a alors $z \prec x$ par définition.

Donc $z \prec y$ par transitivité de $\prec$.

Donc $z \in y\downarrow$ par définition.

Donc $x\downarrow \subseteq y\downarrow$ par définition de l'inclusion.

Comme $x\downarrow \neq y\downarrow$, on a donc $x\downarrow \subsetneq y\downarrow$

Ainsi on a $f(x) \subsetneq f(y)$ par définition de f.

Donc si $x \prec y$ alors $f(x) \subsetneq f(y)$.

Donc f est strictement croissante.

En particulier $\boxed{f \text{ est croissante et injective}}$.

• Montrons que f est surjective dans X.

Par définition de f on sait déjà que $\mathrm{im}(f) \subseteq X$.

Soit $A \in X$.

Alors A est un segment initial propre de E par définition de X.

Or E est bien ordonné donc il existe $x \in E$ tel que $A = x\downarrow$ d'après la prop. 5 p. 14.

On a donc $A = f(x)$ et donc $A \in \mathrm{im}(f)$.

Donc $\mathrm{im}(f) \supseteq X$ et donc $\mathrm{im}(f) = X$.

Ainsi $\boxed{f \text{ est surjective dans } X}$.

• Ainsi f est croissante, injective et surjective dans X.

Or E est bien ordonné donc est totalement ordonné d'après la proposition 2 page 11.

Donc $\boxed{f \text{ est un isomorphisme de } E \text{ vers } X}$.

2. Supposons que E est un ordinal.

Dans ce cas particulier, l'ordre strict $\prec$ est l'appartenance $\in$.

Ainsi pour tout $\alpha \in E$ on a $\alpha{\downarrow} = \{\beta \in E \mid \beta \prec \alpha\} = \{\beta \in E \mid \beta \in \alpha\} = E \cap \alpha$.

Remarquons pour commencer que f et id_E ont le même domaine E.

Soit $\alpha \in E$.

Comme E est ordinal, E est transitif donc $\alpha \subseteq E$ et donc $E \cap \alpha = \alpha$.

Or on a vu que $\alpha{\downarrow} = E \cap \alpha$ donc $\alpha{\downarrow} = \alpha$.

En particulier $f(\alpha) = \alpha{\downarrow} = \alpha = \mathrm{id}_E(\alpha)$.

Donc $\forall \alpha \in E, f(\alpha) = \mathrm{id}_E(\alpha)$.

Donc $\boxed{f = \mathrm{id}_E}$.

En particulier $\boxed{E = \mathrm{im}(\mathrm{id}_E) = \mathrm{im}(f) = X}$.

CQFD.

Remarque :

1. On peut remarquer que $g := \begin{pmatrix} X & \longrightarrow & E \\ A & \longmapsto & \min(E \backslash A) \end{pmatrix}$ est la réciproque de f.
2. Le cas où E est un ordinal n'est pas non plus étonnant : on a déjà vu lors de la proposition 16 page 41 que les ordinaux sont eux-mêmes les segments initiaux de ON.

Quand nous avons dit que les ordinaux fournissaient un représentant de chaque classe d'isomorphie pour les bons ordres, nous avons aussi affirmé qu'il n'y en avait qu'un seul par classe. Autrement dit, si deux ordinaux sont isomorphes, alors nécessairement il s'agit d'un même ordinal.

Proposition 23 (Isomorphisme entre ordinaux)

Soient α et β deux ordinaux et $f : \alpha \longrightarrow \beta$.
Si f est un isomorphisme de α vers β alors $f = \mathrm{id}_\alpha$ et donc $\alpha = \beta$.

Démonstration

Supposons que f est un isomorphisme de α vers β.

En particulier f est injective, surjective sur β et croissante.

Étant injective et croissante, f est strictement croissante.

Remarquons que comme α est un ordinal, α est transitif.

Donc pour tout $\xi \in \alpha$, on aussi $\xi \subseteq \alpha$.

Autrement dit tout élément de α est aussi une partie de α.

Donc pour tout $\xi \in \alpha$, on peut s'intéresser à la fois à $f(\xi)$ et $f^{\rightarrow}(\xi)$.

- Montrons que pour tout $\xi \in \alpha$, on a $f(\xi) = f^{\rightarrow}(\xi)$.

Soit $\xi \in \alpha$.

Montrons que $f(\xi) = f^{\rightarrow}(\xi)$.

$\boxed{\subseteq}$

Soit $\gamma \in f(\xi)$.

Comme f est surjective sur β on a $\mathrm{im}(f) = \beta$ donc $f(\xi) \in \beta$.

Comme β est un ordinal, β est transitif donc $f(\xi) \subseteq \beta$.

On a donc $\gamma \in \beta$ par définition de l'inclusion.

Comme $\mathrm{im}(f) = \beta$ on a $\gamma \in \mathrm{im}(f)$ donc il existe $\mu \in \alpha$ tel que $\gamma = f(\mu)$.

Comme α est un ordinal, μ et ξ sont des ordinaux d'après la prop. 6 p. 18.

On a donc $\mu < \xi$ ou $\mu = \xi$ ou $\xi < \mu$ d'après le théorème 1 page 21.

- ▶ Si $\mu = \xi$ alors $\gamma = f(\mu) = f(\xi)$.
  Or par définition on a $\gamma \in f(\xi)$, donc $\gamma \in \gamma$ et donc $\gamma < \gamma$.
- ▶ Si $\xi < \mu$ alors $f(\xi) < f(\mu)$ par stricte croissance de f.
  Comme $f(\mu) = \gamma$ par définition de μ, on a donc $f(\xi) < \gamma$.
  Or par définition on a $\gamma \in f(\xi)$ donc $\gamma < f(\xi)$.
  On a donc $\gamma < \gamma$ par transitivité de $<$.

Dans ces deux cas-là on a donc nécessairement $\gamma < \gamma$.

C'est absurde par antiréflexivité de $<$.

On a donc nécessairement le troisième cas $\mu < \xi$.

On a donc $\mu \in \xi$ par définition de $<$.

Donc $f(\mu) \in f^{\rightarrow}(\xi)$ par définition de l'image directe.

Comme $\gamma = f(\mu)$, on a donc $\gamma \in f^{\rightarrow}(\xi)$.

Donc $f(\xi) \subseteq f^{\rightarrow}(\xi)$.

$\boxed{\supseteq}$

Soit $\gamma \in f^{\rightarrow}(\xi)$.

Il existe donc $\mu \in \xi$ tel que $\gamma = f(\mu)$.

Comme $\mu \in \xi$, on a $\mu < \xi$ par définition de $<$.

On a donc $f(\mu) < f(\xi)$ par stricte croissance de f.

Or $\gamma = f(\mu)$ donc $\gamma < f(\xi)$.

On a donc $\gamma \in f(\xi)$ par définition de $<$.

Donc $f(\xi) \supseteq f^{\rightarrow}(\xi)$.

Finalement on a bien $f(\xi) = f^{\rightarrow}(\xi)$.

Donc $\boxed{\text{pour tout } \xi \in \alpha, \text{ on a } f(\xi) = f^{\rightarrow}(\xi)}$ $(\star)$.

• On veut montrer que $f = \mathrm{id}_\alpha$.

Comme elles ont le même domaine α, cela revient à montrer que $\forall \xi \in \alpha, f(\xi) = \xi$.

Pour cela, considérons $X := \{\xi \in \alpha \mid f(\xi) \neq \xi\}$ et montrons que $X = \varnothing$.

Supposons par l'absurde que X est non vide.

Par définition X est donc une partie non vide de l'ordinal α.

Or tous les éléments de α sont des ordinaux d'après la proposition 6 page 18.

Donc X est un ensemble non vide dont les éléments sont tous des ordinaux.

Il possède donc un ordinal minimum ξ d'après le théorème 1 page 21.

Soit $\mu \in \xi$.

On a donc $\mu < \xi$ par définition de $<$.

Comme ξ est minimum de X, on a $\mu \notin X$.

Or $\xi \in X$ et $X \subseteq \alpha$ par définitions, donc $\xi \in \alpha$ par définition de l'inclusion.

On a donc $\xi < \alpha$ par définition de $<$.

Ainsi on a $\mu < \xi < \alpha$ donc $\mu < \alpha$ par transitivité de $<$.

On a donc $\mu \in \alpha$ par définition de $<$, et on a vu que $\mu \notin X$.

On a donc $f(\mu) = \mu$ par définition de X.

Donc $\forall \mu \in \xi, f(\mu) = \mu$.

Donc $f(\xi) \underset{(\star)}{=} f^{\rightarrow}(\xi) = \{f(\mu) \mid \mu \in \xi\} = \{\mu \mid \mu \in \xi\} = \xi$.

Donc $f(\xi) = \xi$ donc $\xi \notin X$ par définition de X : c'est absurde.

Par l'absurde, on vient de montrer que X est vide.

Donc $\forall \xi \in \alpha, f(\xi) = \xi$ par définition de X.

Finalement, on a donc $\boxed{f = \mathrm{id}_\alpha}$.

On a en particulier $\alpha = \mathrm{im}(\mathrm{id}_\alpha) = \mathrm{im}(f) = \beta$ par surjectivité de f sur β.

CQFD.

Ainsi, on vient de montrer qu'au sein d'une classe d'isomorphie, il ne peut y avoir au maximum qu'un seul ordinal. Précisions ce que l'on entend par là.

Proposition 24 (Au plus un ordinal associé à un bon ordre)

Soit $(E, \preccurlyeq)$ un ensemble ordonné.
Supposons qu'il existe au moins un ordinal α tel que $(E, \preccurlyeq)$ et $(\alpha, \leq)$ sont isomorphes.
Alors un tel α est unique, et l'isomorphisme de $(E, \preccurlyeq)$ vers $(\alpha, \leq)$ est unique.

Démonstration

• **Unicité de l'ordinal**

Soit $f : E \longrightarrow \alpha$ un isomorphisme.

Soit β un ordinal tel que $(E, \preccurlyeq)$ et $(\beta, \leq)$ sont isomorphes.

Il existe donc un isomorphisme $g : E \longrightarrow \beta$.

Comme $f : E \longrightarrow \alpha$ un isomorphisme, $f^{-1} : \alpha \longrightarrow E$ est un isomorphisme.

Donc $g \circ f^{-1} : \alpha \longrightarrow \beta$ est un isomorphisme.

Donc $\alpha = \beta$ d'après la proposition 23 page 55.

On a donc $\boxed{\text{unicité de l'ordinal } \alpha \text{ isomorphe à } E}$.

• **Unicité de l'isomorphisme**.

Soit $g : E \longrightarrow \alpha$ un isomorphisme.

Alors $g^{-1} : \alpha \longrightarrow E$ est un isomorphisme.

Donc $f \circ g^{-1} : \alpha \longrightarrow \alpha$ est un isomorphisme.

Donc $f \circ g^{-1} = \mathrm{id}_\alpha$ d'après la proposition 23 page 55.

Donc $f = f \circ \mathrm{id}_E = f \circ g^{-1} \circ g = \mathrm{id}_\alpha \circ g = g$.

On a donc $\boxed{\text{unicité de l'isomorphisme de } E \text{ vers } \alpha}$.

CQFD.

Venons-en finalement à ce qui nous intéressait depuis le début : utiliser les ordinaux pour représenter n'importe quel bon ordre, à isomorphisme près. On vient déjà de voir l'unicité, mais formulons quand-même complètement un théorème digne de ce nom !

Pour le démontrer, nous allons utiliser l'idée proposée par la proposition 22 page 53, qui affirme qu'à isomorphisme près, un ensemble bien ordonné se comporte comme l'ensemble de ses segments initiaux propres. Autrement dit, on peut tout à fait raisonner sur les segments initiaux propres plutôt que sur l'ensemble directement.

Théorème 4 (Unique ordinal associé à un bon ordre)

Soit $(E, \preccurlyeq)$ un ensemble bien ordonné.
Alors il existe un unique ordinal α tel que $(E, \preccurlyeq)$ et $(\alpha, \leq)$ sont isomorphes.
On dit alors que α est le **type** de $(E, \preccurlyeq)$ et on note $\mathrm{type}(E, \preccurlyeq) := \alpha$.

Démonstration

• Soit $\prec$ l'ordre strict sur E associé à $\preccurlyeq$.

Soit $x \in E$.

Rappelons-nous que $x\!\downarrow = \{y \in E \mid y \prec x\}$.

Ainsi $x\!\downarrow$ est une partie de E et $(E, \preccurlyeq)$ est bien ordonné.

Donc $(x\!\downarrow, \preccurlyeq)$ est bien ordonné d'après la prop. 3 p. 12.

Pour la suite de cette démonstration, on dira que x est **bon** si et seulement s'il existe au moins un ordinal ξ tel que $(x\downarrow, \preccurlyeq)$ est isomorphe à $(\xi, \leq)$.

Dans ce cas-là, un tel ordinal ξ est unique d'après la proposition 24 page 57.

Notons noterons par la suite $f(x) := \xi$ cet unique ordinal.

Posons $G := \{x \in E \mid x \text{ est bon } \}$.

On a donc l'application $f : G \longrightarrow ?$ qui à $x \in G$ associe l'unique ordinal $f(x)$ tel que $(x\downarrow, \preccurlyeq)$ est isomorphe à $\big(f(x), \leq\big)$.

Pour tout $x \in G$, l'isomorphisme de $(x\downarrow, \preccurlyeq)$ vers $\big(f(x), \leq\big)$ est unique d'après la proposition 24 page 57 : on le notera h_x. Ainsi on a $h_x : x\downarrow \longrightarrow f(x)$.

Avant d'avancer, remarquons que par définition pour tout $x \in G$, son image $f(x)$ est un ordinal. En particulier $\mathrm{im}(f)$ est un ensemble d'ordinaux et est donc naturellement muni de l'ordre induit $\leq$.

Voici à présent les différentes étapes de la preuve :

1. On prouve que G est un segment initial de E.
2. On montre que f est un isomorphisme de $(G, \preccurlyeq)$ dans $\big(\mathrm{im}(f), \leq\big)$.
3. On montre que $\mathrm{im}(f)$ est un ordinal : G est donc lui-même isomorphe à un ordinal.
4. On montre qu'en fait $G = E$, ce qui permet de conclure.

1. Montrons que G est un segment initial de E.

Autrement dit, montrons que pour tout x et y dans E, si $y \prec x \in G$ alors $y \in G$.

Montrons aussi au passage que dans ce cas-là on a $f(y) = h_x(y)$.

Soient x et y dans E tels que $y \prec x \in G$.

Alors pour tout $z \in y\downarrow$, on a $z \prec y$ donc $z \prec x$ par transitivité de $\prec$ et donc $z \in x\downarrow$.

Ainsi $y\downarrow \subseteq x\downarrow$ donc on peut considérer la restriction de h_x à $y\downarrow$.

Nous allons montrer que $(h_x)_{|(y\downarrow)}$ est un isomorphisme de $y\downarrow$ vers $h_x(y)$.

Par définition on sait déjà que $(h_x)_{|(y\downarrow)}$ a pour domaine $y\downarrow$.

Par définition h_x est un isomorphisme d'ordre, donc est injectif et croissant.

On en déduit déjà que $(h_x)_{|(y\downarrow)}$ est lui aussi injectif et croissant.

De plus, on en déduit aussi que h_x est strictement croissant.

Montrons que $(h_x)_{|(y\downarrow)}$ est surjectif sur $h_x(y)$, c'est-à-dire $\mathrm{im}\big((h_x)_{|(y\downarrow)}\big) = h_x(y)$.

$\boxed{\subseteq}$

Soit $u \in \mathrm{im}\big((h_x)_{|(y\downarrow)}\big)$.

Il existe donc $z \in y\downarrow$ tel que $u = (h_x)_{|(y\downarrow)}(z) = h_x(z)$.

Comme $z \in y\downarrow$, on a $z \prec y$ donc $h_x(z) < h_x(y)$ par stricte croissance de h_x.

Ainsi on a $h_x(z) \in h_x(y)$ par définition de $<$, et donc $u \in h_x(y)$.

Donc $\operatorname{im}\big((h_x)_{|(y\downarrow)}\big) \subseteq h_x(y)$.

$\boxed{\supseteq}$

Soit $\beta \in h_x(y)$.

Comme $h_x : x\downarrow \longrightarrow f(x)$ on a $h_x(y) \in f(x)$.

Ainsi on a $\beta \in h_x(y) \in f(x)$.

Or $f(x)$ est un ordinal par définition de f donc $f(x)$ est transitif.

On en déduit donc que $\beta \in f(x)$.

Or par définition h_x est surjectif dans $f(x)$.

Il existe donc $b \in x\downarrow$ tel que $h_x(b) = \beta$.

Or $(E, \preccurlyeq)$ est bien ordonné par définition.

Donc $(E, \preccurlyeq)$ est totalement ordonné d'après la proposition 2 page 11.

On a donc $b \prec y$ ou $y \preccurlyeq b$.

Supposons par l'absurde que $y \preccurlyeq b$.

On a alors $h_x(y) \leq h_x(b)$ par croissance de h_x.

Comme $h_x(b) = \beta$ par définition de b, on a $h_x(y) \leq \beta$.

Or on a $\beta \in h_x(y)$ par définition de β, c'est-à-dire $\beta < h_x(y)$.

On vient donc de montrer $\beta < h_x(y) \leq \beta$, ce qui est absurde.

On a donc nécessairement l'autre option $b \prec y$ c'est-à-dire $b \in y\downarrow$.

Comme $\beta = h_x(b)$, on a donc $\beta \in h_x{}^{\rightarrow}\big(y\downarrow\big)$.

Autrement dit, on a $\beta \in \operatorname{im}\big((h_x)_{|(y\downarrow)}\big)$.

On a donc $\operatorname{im}\big((h_x)_{|(y\downarrow)}\big) \supseteq h_x(y)$ et donc $\operatorname{im}\big((h_x)_{|(y\downarrow)}\big) = h_x(y)$.

Ainsi $(h_x)_{|(y\downarrow)}$ est surjective sur $h_x(y)$.

On a donc $(h_x)_{|(y\downarrow)}$ est croissante, injective et surjective sur $h_x(y)$.

Or on a dit que $\preccurlyeq$ est total sur E.

Donc $(h_x)_{|(y\downarrow)}$ est un isomorphisme de $y\downarrow$ vers $h_x(y)$.

Ainsi $y\downarrow$ et $h_x(y)$ sont isomorphes.

Or on a dit que $h_x(y)$ est un ordinal puisqu'élément de $f(x)$.

Donc $y\downarrow$ est isomorphe à un ordinal, et donc $y \in G$.

On note au passage que par unicité de l'ordinal on a $f(y) = h_x(y)$.

Donc $\boxed{\text{pour tout } x \text{ et } y \text{ dans } E, \text{ si } y \prec x \in G \text{ alors } y \in G \text{ avec } f(y) = h_x(y)}$ $(\star)$.

2. Montrons que f est un isomorphisme de $(G, \preccurlyeq)$ dans $\big(\operatorname{im}(f), \leq\big)$.

Pour cela, montrons que f est strictement croissante.

Soient x et y dans G.

Supposons que $y \prec x$.

D'après $(\star)$ on a alors $f(y) = h_x(y)$.

Or par définition h_x est à valeurs dans $f(x)$.

On a donc $h_x(y) \in f(x)$ et donc $f(y) \in f(x)$.

On a donc $f(y) < f(x)$ par définition de $<$.

Donc si $y \prec x$ alors $f(y) < f(x)$.

Donc f est strictement croissante.

En particulier f est croissante et injective, donc f est croissante et bijective sur $\mathrm{im}(f)$.

Or on a dit que $\preccurlyeq$ est total sur E donc $\preccurlyeq$ est total sur G puisque $G \subseteq E$.

Donc $\boxed{f \text{ est un isomorphisme de } (G, \preccurlyeq) \text{ dans } \big(\mathrm{im}(f), \leq\big)}$.

3. Montrons que $\mathrm{im}(f)$ est un ordinal.

► Montrons que $\mathrm{im}(f)$ est transitif.

Soit $a \in \mathrm{im}(f)$.

Il existe donc $x \in G$ tel que $a = f(x)$.

Soit $b \in a$.

Par définition h_x est un isomorphisme d'ordres de $x\downarrow$ dans $f(x)$.

En particulier h_x es surjectif sur $f(x)$.

Comme $a = f(x)$, on en déduit que h_x est surjectif sur a.

On a donc $\mathrm{im}(h_x) = a$ et donc $b \in \mathrm{im}(h_x)$.

Il existe donc $y \in x\downarrow$ tel que $b = h_x(y)$.

Comme $y \in x\downarrow$ on a $y \prec x$ et donc $h_x(y) = f(y)$ d'après $(\star)$.

Donc $b = f(y)$ et donc $b \in \mathrm{im}(f)$.

Donc $a \subseteq \mathrm{im}(f)$ par définition de l'inclusion.

Donc $\forall a \in \mathrm{im}(f), a \subseteq \mathrm{im}(f)$.

Donc $\mathrm{im}(f)$ est transitif.

► Par définition de f, tous les éléments de $\mathrm{im}(f)$ sont des ordinaux.

Donc $\in$ est un bon ordre strict sur $\mathrm{im}(f)$ d'après le théorème 1 page 21.

Ainsi, $\mathrm{im}(f)$ est transitif et $\in$ est un bon ordre strict sur $\mathrm{im}(f)$.

Donc $\boxed{\mathrm{im}(f) \text{ est un ordinal}}$.

4. Ainsi f est un isomorphisme de G vers l'ordinal $\mathrm{im}(f)$.

Il ne reste plus qu'à prouver que $G = E$ pour conclure.

Supposons par l'absurde que $G \subsetneq E$.

Alors $E \backslash G$ est une partie non vide de l'ensemble bien ordonné E.

Elle admet donc un minimum e.

Montrons que $e\downarrow = G$.

$\boxed{\subseteq}$

Soit $x \in e\downarrow$.

Par définition on a $x \prec e$ donc $x \notin E \backslash G$ car e en est minimum.

On a donc $x \in G$.

Donc $e\downarrow \subseteq G$ par définition de l'inclusion.

$\boxed{\supseteq}$

Soit $x \in G$.

On a dit que $\preccurlyeq$ est total sur E donc $x \prec e$ ou $x = e$ ou $e \prec x$.

- Si $x = e$ alors $e \in G$ puisque $x \in G$.
- Si $e \prec x$ alors $e \in G$ d'après $(\star)$.

Dans ces deux cas-là on a donc $e \in G$ ce qui est absurde puisque $e \in E \backslash G$.

On a donc nécessairement $x < e$ et donc $x \in e\downarrow$.

Donc $e\downarrow \supseteq G$ et donc $e\downarrow = G$.

Or G est isomorphe à l'ordinal $\mathrm{im}(f)$ d'après ce qui précède.

Donc $e\downarrow$ est isomorphe à l'ordinal $\mathrm{im}(f)$.

Donc $e \in G$ par définition de G, ce qui est absurde puisque $e \in E \backslash G$.

On a donc $E = G$.

Or G est isomorphe à l'ordinal $\mathrm{im}(f)$ d'après ce qui précède.

Donc $\boxed{E \text{ est isomorphe à l'ordinal } \mathrm{im}(f)}$.

L'unicité est garantie par la proposition 24 page 57.

CQFD.

Remarque :

1. Ainsi on note $\mathrm{type}(E, \preccurlyeq)$ l'unique ordinal isomorphe à l'ensemble bien ordonné $(E, \preccurlyeq)$. Comme nous avons déjà eu l'occasion de le faire, on omet parfois d'écrire $\preccurlyeq$ car l'ordre est sous-entendu, afin de simplifier et fluidifier le discours. On notera très donc très souvent $\mathrm{type}(E)$.
2. Soit α un ordinal : comme α est nécessairement isomorphe à lui-même, on a donc $\mathrm{type}(\alpha) = \alpha$.

Pour la proposition qui suit, rappelons qu'une partie d'un ensemble bien ordonné est elle aussi bien ordonnée en vertue de la proposition 3 page 12.

Proposition 25 (Ordinal associé et inclusion)

Soient $(A, \preccurlyeq)$ un ensemble bien ordonné et X une partie de A.
On a $\operatorname{type}\big(X, \preccurlyeq\big) \leq \operatorname{type}\big(A, \preccurlyeq\big)$.

Démonstration

• Commençons par supposer que A est un ordinal : la relation $\preccurlyeq$ est donc $\leq$.

Ainsi tous les éléments de A sont des ordinaux d'après la proposition 6 page 18.

Or X est une partie de A donc X est un ensemble d'ordinaux.

Posons alors $\delta := \operatorname{type}(X, \leq)$ et $f : X \longrightarrow \delta$ l'isomorphisme associé.

Rappelons que δ étant un ordinal, X et δ sont munis tous de $\leq$.

En particulier les éléments de X et les éléments de δ sont comparables pour $\leq$.

En particulier pour tout $\xi \in X$, $f(\xi)$ et ξ sont comparables pour $\leq$.

Montrons que $\forall \xi \in X, f(\xi) \leq \xi$.

Pour cela posons $E := \big\{\xi \in X \mid f(\xi) \leq \xi\big\}$ et montrons que $E = X$.

> Supposons par l'absurde que $E \subsetneq X$.
>
> Alors $X \backslash E$ est un ensemble non vide d'ordinaux.
>
> Il admet donc un minimum ξ d'après le théorème 1 page 21.
>
> Comme $\xi \in X \backslash E$, on a $\xi \notin E$ et donc $f(\xi) \nleq \xi$ par définition de E.
>
> Or $\leq$ est total chez les ordinaux donc on a $\xi < f(\xi)$.
>
> Or $\operatorname{im}(f) = \delta$ par définition de f donc $f(\xi) \in \delta$ et donc $f(\xi) < \delta$.
>
> Ainsi $\xi < f(\xi) < \delta$ donc $\xi < \delta$ par transitivité de $<$.
>
> Comme $\operatorname{im}(f) = \delta$ on a donc $\xi < \operatorname{im}(f)$ et donc $\xi \in \operatorname{im}(f)$.
>
> Il existe donc $\gamma \in E$ tel que $\xi = f(\gamma)$.
>
> Comme $\xi < f(\xi)$ on a donc $f(\gamma) < f(\xi)$.
>
> Comme f est un isomorphisme d'ordres, on a donc $\gamma < \xi$.
>
> Comme ξ est le minimum de $X \backslash E$, on a donc $\gamma \notin X \backslash E$ donc $\gamma \in E$.
>
> On a donc $f(\gamma) \leq \gamma$ par définition de E, c'est-à-dire $\xi \leq \gamma$ par définition de γ.
>
> C'est absurde puisque l'on a dit que $\gamma < \xi$.

Par l'absurde, on a donc montré que $E = X$.

Ainsi, $\boxed{\forall \xi \in X, f(\xi) \leq \xi}$ $\quad (\star_1)$.

Montrons que $\delta \leq A$.

> Soit $\varepsilon \in \delta$.

Par définition de f on a $\mathrm{im}(f) = \delta$ donc $\varepsilon \in \mathrm{im}(f)$.

Il existe donc $\xi \in X$ tel que $\varepsilon = f(\xi)$.

D'après $(\star_1)$ on a $f(\xi) \leq \xi$ donc $\varepsilon \leq \xi$.

Or on a $\xi \in X \subseteq A$ donc $\xi \in A$ par définition de l'inclusion.

On a donc $\xi < A$ par définition de $<$, donc $\varepsilon \leq \xi < A$ et donc $\varepsilon < A$ par transitivité.

Ainsi on a $\varepsilon \in A$.

Donc $\delta \subseteq A$ par définition de l'inclusion, et donc $\delta \leq A$.

Or par définition $\delta = \mathrm{type}\big(X, \leq\big)$ donc $\mathrm{type}\big(X, \leq\big) \leq A$.

Or A est un ordinal donc en particulier est l'unique ordinal isomorphe à lui-même.

Autrement dit on a $A = \mathrm{type}\big(A, \leq\big)$.

On a donc bien $\boxed{\mathrm{type}\big(X, \leq\big) \leq \mathrm{type}\big(A, \leq\big)}$ $(\star_2)$.

• Plus généralement on ne suppose plus spécialement que A est un ordinal.

Soient alors $\alpha := \mathrm{type}(A, \preccurlyeq)$ et $g : A \longrightarrow \alpha$ l'isomorphisme associé.

Considérons $Y := g^{\rightarrow}(X)$, de telle que sorte que Y est une partie de α.

On se retrouve dans la situation précédente : d'après $(\star_2)$ on a $\mathrm{type}\big(Y, \leq\big) \leq \mathrm{type}\big(\alpha, \leq\big)$.

Or g est un isomorphisme d'ordres.

Donc en particulier g est croissant et injectif.

Donc $g_{|X}$ est croissant et injectif.

Donc $g_{|X}$ est croissant et une bijection de X dans $g^{\rightarrow}(X) = Y$.

Or X est bien ordonné donc en particulier est totalement ordonné d'après la proposition 2 page 11. Donc $g_{|X}$ est un isomorphisme d'ordres de X dans Y.

En particulier X et Y sont isomorphes.

Donc X et $\mathrm{type}(Y, \leq)$ sont isomorphes par transitivité de l'isomorphie.

Donc $\mathrm{type}(X, \preccurlyeq) = \mathrm{type}(Y, \leq)$ par unicité de l'ordinal associé.

On a donc $\boxed{\mathrm{type}\big(X, \preccurlyeq\big) \leq \mathrm{type}\big(A, \preccurlyeq\big)}$.

CQFD.

6 Récurrence : induction et récursion

Au lycée, nous découvrons la notion de récurrence. On la retrouve notamment à travers le **raisonnement par récurrence** qui, comme nous l'avons déjà explicité, permet de prouver qu'une propriété est vraie pour tous les entiers naturels :

$$\text{Supposons } \begin{cases} P(0) \\ \forall n \in \mathbb{N}, \Big(P(n) \implies P(n+1)\Big) \end{cases}$$

Alors on a $\forall n \in \mathbb{N}, P(n)$.

Dans le même temps, on retrouve aussi la récurrence à travers les **définitions par récurrence**, qui permettent de définir une suite à partir d'une donnée initiale et d'une règle pour passer d'un entier au suivant :

$$\begin{cases} u_0 := a \\ \forall n \in \mathbb{N}, u_{n+1} := f(u_n) \end{cases}$$

Ces deux incarnations de la récurrence portent chacune un nom : le raisonnement par récurrence est aussi appelé **induction**, et la définition par récurrence est aussi appelée **récursion**.

6.1 Induction

L'induction chez les ordinaux est donc une généralisation de l'induction chez les nombres entiers : le principe est le même que pour le raisonnement par récurrence classique, c'est-à-dire prouver qu'une assertion est vraie à un certain ordinal et qu'elle se transmet de proche en proche par opération de successeur :

$$\text{Supposons } \begin{cases} P(0) \\ \forall \alpha \in ON, \Big(P(\alpha) \implies P\big(S(\alpha)\big)\Big) \end{cases}$$

Alors on a $\forall \alpha \in ON, P(\alpha)$.

Cependant, nous l'avons dit : certains ordinaux ne sont le successeur de personne et donc il est impossible que l'assertion leur parvienne de cette façon (sauf pour 0 qui est déjà atteint au début). Autrement dit, la formulation qui précède n'est pas correcte.

Pour palier ce problème, on peut commencer par reformuler le raisonnement par récurrence sur les entiers naturels d'une autre manière. Pour démontrer qu'une assertion à paramètres P est vraie pour tout entier naturel n, on peut plutôt montrer :

$$\text{Supposons } \begin{cases} P(0) \\ \forall n \in \mathbb{N}, \Big(\forall m < n, P(m)\Big) \implies P(n) \end{cases}$$

Alors on a $\forall n \in \mathbb{N}, P(n)$.

On retrouve ce que l'on appelle usuellement le raisonnement par récurrence **forte**. En réalité, il ne s'agit pas d'un raisonnement plus fort que le raisonnement par récurrence classique. Pour s'en convaincre, il suffit de poser $Q(n)$:« $\forall m < n, P(m)$ ». On peut alors remarquer que faire l'hypothèse de $Q(n)$, c'est faire l'hypothèse que P est vraie pour tout entier de 0 à $n-1$, et dire que cela implique alors $P(n)$ signifie désormais que P est vraie pour un entier de plus, c'est-à-dire pour tout entier précédent $n+1$, et donc que $Q(n+1)$ est vraie. Il s'agit donc tout simplement de l'implication $Q(n) \implies Q(n+1)$. C'est donc bel et bien une hérédité classique.

Remarquons au passage qu'on peut enfouir l'initialisation $P(0)$ dans l'implication $\Big(\forall m < 0, P(m)\Big) \implies P(0)$ puisque la prémisse étant toujours vraie, cette implication est équivalente à $P(0)$. Autrement dit, on peut reformuler le raisonnement par récurrence sur les entiers de la façon suivante :

Supposons $\forall n \in \mathbb{N}, \Big(\forall m < n, P(m)\Big) \implies P(n)$.
Alors on a $\forall n \in \mathbb{N}, P(n)$.

Or cette fois-ci il n'est pas question de successeur : cette formulation se généralise très bien aux ordinaux ! C'est l'objet du théorème qui suit.

Théorème 5 (Principe d'induction transfinie)

Soit P une assertion à paramètres.
Supposons que pour tout ordinal α, on a

$$\Big(\forall \beta < \alpha, P(\beta)\Big) \implies P(\alpha)$$

Alors pour tout ordinal α, on a $P(\alpha)$.

Démonstration

Supposons que pour tout ordinal α, on a $\Big(\forall \beta < \alpha, P(\beta)\Big) \implies P(\alpha)$.

Supposons par l'absurde qu'il existe au moins un ordinal α tel que l'on n'a pas $P(\alpha)$.

Soit X l'ensemble des ordinaux plus petit ou égaux à α et qui ne vérifient pas P.

Par définition on a $\alpha \in X$ donc X est un ensemble non vide d'ordinaux.

Il admet donc un ordinal minimum ξ d'après le théorème 1 page 21.

Soit μ un ordinal tel que $\mu < \xi$.

Alors $\mu \notin X$ car ξ est minimum de X.

Or $\xi \in X$ donc $\xi \leq \alpha$ et donc $\mu < \xi \leq \alpha$.

On a donc $\mu \leq \alpha$ par transitivité.

Ainsi on a $\mu \notin X$ alors que $\mu \leq \alpha$.

Donc nécessairement on a $P(\mu)$ par définition de X.

Donc $\forall \mu < \xi, P(\mu)$.

On a donc $P(\xi)$ par hypothèse du théorème.

C'est absurde puisque $\xi \in X$ et donc $P(\xi)$ est faux.

Donc par l'absurde on a montré que $\boxed{\text{pour tout ordinal } \alpha \text{ on a } P(\alpha)}$.

CQFD.

On est cependant en droit de se demander : la formulation classique avec le passage de n à $n+1$ a-t-elle une généralisation chez les ordinaux ? La réponse est oui, à condition de traiter séparément le cas des ordinaux limites puisqu'ils ne sont pas successeurs. C'est donc au fond un mélange des deux formulations. À la manière de la récurrence classique et de la récurrence forte chez les entiers naturels, c'est une formulation équivalente à la précédente, on ne dit au fond rien de moins même si naïvement on peut en avoir l'impression.

Proposition 26 (Principe faible d'induction transfinie)

Soit P une assertion à paramètres.
Supposons que :

1. On a $P(0)$.
2. Pour tout ordinal α, si $P(\alpha)$ alors $P\big(S(\alpha)\big)$.
3. Pour tout ordinal limite α, si $\forall \beta < \alpha, P(\beta)$ alors $P(\alpha)$.

Alors pour tout ordinal α on a $P(\alpha)$.

Démonstration

Appliquons le théorème 5 page 66.

Soit α un ordinal.

Supposons que $\forall \beta < \alpha, P(\beta) \ \ (\star)$.

- Si $\alpha = 0$, alors d'après l'hypothèse 1 on a $P(\alpha)$.
- Supposons que α est un successeur.
  Par définition il existe un ordinal β tel que $\alpha = S(\beta)$.
  Alors $\beta < \alpha$ d'après la proposition 12 page 33.
  On a donc $P(\beta)$ d'après l'hypothèse $(\star)$.
  On a donc $P\big(\alpha\big)$ d'après l'hypothèse 2.
- Supposons que α est un ordinal limite.
  On alors $P(\alpha)$ d'après les hypothèses $(\star)$ et 3.

Dans tous les cas on a donc $P(\alpha)$.

Donc si $\forall \beta < \alpha, P(\beta)$ alors $P(\alpha)$.

Donc pour tout ordinal α, on l'implication $\Big(\forall \beta < \alpha, P(\beta)\Big) \implies P(\alpha)$.

Donc $\boxed{\text{pour tout ordinal } \alpha, \text{ on a } P(\alpha)}$ d'après le théorème 5 page 66.

CQFD.

Remarque :
0 étant un ordinal limite, il entre à la fois dans le cas 1 et le cas 3, mais comme $\forall \beta < 0, P(\beta)$ est nécessairement vraie, l'implication $\Big(\forall \beta < 0, P(\beta)\Big) \implies P(0)$ est équivalente à $P(0)$ et donc il y a seulement une redondance, pas de contradiction.

6.2 Récursion

Nous l'avons dit, la récursion chez les entiers naturels est aussi connue sous le nom de définition par récurrence, pour définir une suite : on définit la valeur de de cette suite en un entier puis l'on se donne une règle pour déterminer la valeur de la suite sur l'entier suivant à partir du précédent, ce qui permet de proche en proche de définir la suite sur chaque entier. Par exemple on pourrait être amenés à définir la suite suivante :

$$\begin{cases} u_0 := 1 \\ \forall n \in \mathbb{N}^*, u_n := 3u_{n-1} \end{cases}$$

qui va alors donner la suite des puissances de 3. On peut se retrouver dans le cas où l'étape de propagation nécessite en fait les deux termes précédents (auquel cas il faut déterminer la valeur de la suite sur deux entiers au début), comme c'est le cas avec **la suite de Fibonacci** :

$$\begin{cases} u_0 := 1 \\ u_1 := 1 \\ \forall n \geq 2, u_n := u_{n-1} + u_{n-2} \end{cases}$$

Plus généralement, on peut même vouloir définir un terme à partir de toutes les valeurs précédentes. La notion qui va permettre de donner une "*règle de construction*" en toute généralité pour se servir des valeurs précédentes est celle d'**assertion fonctionnelle** que nous avons rappelée au début de ce chapitre. Ainsi, si H est une assertion fonctionnelle, la forme la plus générale qu'on pourrait être amenés à utiliser pour définir une suite par récurrence sur les entiers est

$$\forall n \in \mathbb{N}, u_n := H\big(u_{|[\![0,n[\![}\big)$$

où $u_{|[\![0,n[\![}$ désigne la restriction de la suite u à tous les entiers de 0 à $n-1$. Ainsi, on tient bien compte des valeurs de u jusqu'à n (non compris). Remarquons bien que comme H est très générale, elle peut en particulier ne regarder que quelques valeurs parmi les précédentes et non toutes (par exemple seulement les deux précédentes comme dans le cas de Fibonacci), et aussi être constante en quelques entiers pour s'assurer d'avoir fixé les premières valeurs de la suite. Ainsi dans le cas de la suite de Fibonacci, H serait définie de telle sorte à avoir

$$\begin{cases} H\big(u_{|[\![0,n[\![}\big) := 1 & \text{si } n = 0 \\ H\big(u_{|[\![0,n[\![}\big) := 1 & \text{si } n = 1 \\ H\big(u_{|[\![0,n[\![}\big) := u_{n-1} + u_{n-2} & \text{sinon} \end{cases}$$

C'est ce cadre-là que nous allons désormais définir proprement pour le généraliser encore plus, c'est-à-dire à présent sur tous les ordinaux. Le principe va cependant rester le même : se donner une règle de propagation via les assertions fonctionnelles, et l'utiliser pour définir la valeur d'une suite à un ordinal à partir de la restriction de la suite aux ordinaux précédents.

On remarque que pour que u puisse être définie, il faut que ses restrictions respectives soient bien dans le domaine de H pour que l'étape de propagation ait du sens. C'est à travers la notion d'application inductive (une suite étant une application particulière) que nous allons faire cela.

Définition 12 (Application inductive)

Soient H une assertion fonctionnelle et u une application.
On dit que u est **H-inductive** si et seulement si :

1. $\mathrm{dom}(u)$ est un ordinal.
2. Pour tout $\beta \in \mathrm{dom}(u)$, on a $u_{|\beta} \in \mathrm{dom}(H)$ et $u(\beta) = H(u_{|\beta})$.

Ne perdons pas de vue qu'un ordinal est lui-même l'ensemble de tous les ordinaux qui le précèdent, autrement dit $u_{|\beta}$ est bien la restriction de u à tous les ordinaux qui viennent avant β, au même titre que $u_{|[\![0,n[\![}$ est la restriction de u à tous les entiers qui précèdent n. Nous verrons d'ailleurs quand nous nous attarderons en détails sur les entiers naturels que n sera justement égal à $[\![0, n[\![$, donc nous retomberons bien sur nos pieds avec la théorie plus générale des ordinaux.

À ce stade, nous avons déjà défini les notions utiles pour construire les différentes suites que nous avons évoquées : il suffit pour cela de bien choisir le H en question et les applications u qui sont H-inductives et concernées seront celles telles que $\mathrm{dom}(u) = \omega$ l'ensemble des entiers naturels.

Cependant nous avons exprimé le souhait d'aller au delà de ω à travers la théorie plus générale des ordinaux. On pourrait tout à fait se contenter pour cela de la définition que nous venons d'énoncer : si l'on souhaite se rendre jusqu'à un ordinal α, même très grand, il suffit de demander $\mathrm{dom}(u) = \alpha$ pour les applications H-inductives qui nous intéressent.

Il y a néanmoins des cas où nous ne voudrions pas particulièrement limiter l'ordinal jusqu'où construire l'application u. Typiquement, étant donnés deux ordinaux α et β, nous serons amenés à définir l'addition $\alpha + \beta$. Nous le ferons à l'aide d'une assertion fonctionnelle H bien choisie. En passant par une application u qui est H-inductive, on pourra faire en sorte que
$\forall \beta \in \mathrm{dom}(u), u(\beta) = \alpha + \beta$, en ayant fixé α au préalable. Le problème vient alors de savoir le sens à donner à $\alpha + \mathrm{dom}(u)$. En effet, $\mathrm{dom}(u)$ est lui-même un ordinal, que l'on devra en plus choisir arbitrairement. On peut se contenter de se limiter à $\mathrm{dom}(u)$ en l'ayant pris très grand, mais cela présente une inélégance que l'on peut corriger.

On aimerait pour cela ne pas limiter le domaine des applications : comment faire pour que le domaine soit ON la classe de tous les ordinaux ? En fait, il nous suffit de passer par la généralisation des applications dont nous avons déjà tant parlée : les assertions fonctionnelles. Ainsi, nous allons simplement étendre la définition précédente aux assertions fonctionnelles.

Définition 13 (Assertion fonctionnelle inductive)

Soient H et F deux assertions fonctionnelles.
On dit que F est **H-inductive** si et seulement si :

1. $\mathrm{dom}(F) \in ON$ ou $\mathrm{dom}(F) = ON$.
2. Pour tout $\beta \in \mathrm{dom}(F)$, on a $F_{|\beta} \in \mathrm{dom}(H)$ et $F(\beta) = H(F_{|\beta})$.

Le seul véritable cas nouveau est celui pour lequel $\mathrm{dom}(F) = ON$. En effet, si $\mathrm{dom}(F) \in ON$

alors $\mathrm{dom}(F)$ est un ordinal donc F est alors associée à une application et donc on confond sans problème les deux. On peut cependant se demander pourquoi le seul cas nouveau que l'on rajoute est celui où $\mathrm{dom}(F) = ON$. Au fond, tant qu'on est à généraliser, on pourrait demander plus largement $\mathrm{dom}(F) \subseteq ON$, non ? La réponse nous a déjà été fournie par la proposition 10 page 27 : ON est en quelque sorte la seule classe propre légitime à généraliser les ordinaux.

On peut remarquer la chose suivante : restreindre une assertion fonctionnelle (ou donc une application) qui est H-inductive à un ordinal de son domaine va nécessairement produire une application qui est encore H-inductive. En effet : *qui peut le plus peut le moins*.

Proposition 27 (Restriction d'une application inductive)

Soient H et F deux assertions fonctionnelles.
Si F est H-inductive alors pour tout $\beta \in \mathrm{dom}(u)$, l'application $F_{|\beta}$ est H-inductive.

Démonstration

Supposons que F est H-inductive.

Alors on a $\mathrm{dom}(F) \in ON$ ou $\mathrm{dom}(F) = ON$ par définition.

On a donc $\mathrm{dom}(F) \subseteq ON$ d'après la proposition 6 page 18.

Soit $\beta \in \mathrm{dom}(F)$.

Comme $\mathrm{dom}(F) \subseteq ON$, on en déduit que $\mathrm{dom}(F_{|\beta}) = \beta$ est un ordinal.

Soit $\gamma \in \beta$.

On a alors $\gamma \in \beta \in \mathrm{dom}(F)$ donc $\gamma \in \mathrm{dom}(F)$ par transitivité :

Si $\mathrm{dom}(F) \in ON$ alors c'est la transitivité de $\in$ sur ON qu'on applique.

Si $\mathrm{dom}(F) = ON$, c'est la transitivité de ON qu'on applique.

Or F est H-inductive par hypothèse.

Donc $F_{|\gamma}$ est dans le domaine de H et $F(\gamma) = H(F_{|\gamma})$.

Or $\gamma \in \beta$ donc $\gamma \subseteq \beta$ par transitivité.

Donc $(F_{|\beta})_{|\gamma} = F_{|\gamma}$ donc en particulier $(F_{|\beta})_{|\gamma}$ est dans le domaine de H.

De plus $F_{|\beta}(\gamma) = F(\gamma) = H(F_{|\gamma}) = H\Big((F_{|\beta})_{|\gamma}\Big)$.

Donc pour tout $\gamma \in \beta$, $(F_{|\beta})_{|\gamma}$ est dans le domaine de H et $F_{|\beta}(\gamma) = H\Big((F_{|\beta})_{|\gamma}\Big)$.

Donc $F_{|\beta}$ est H-inductive.

Donc $\boxed{\text{pour tout } \beta \in \mathrm{dom}(F),\ F_{|\beta} \text{ est } H\text{-inductive}}$.

CQFD.

Pour pouvoir dire qu'on souhaite définir une assertion fonctionnelle F par la relation

$$\forall \beta \in \mathrm{dom}(F), F(\beta) = H(F_{|\beta})$$

il faut s'assurer qu'une telle relation ne convient pas pour plusieurs assertions fonctionnelles : c'est l'objet de la proposition suivante.

Proposition 28 (Au plus une application inductive)

Soit H une assertion fonctionnelle.
Soit C une classe telle que $C \in ON$ ou $C = ON$.
Il existe au plus une assertion fonctionnelle de domaine C qui est H-inductive.

Démonstration

Soient F et G deux assertions fonctionnelles qui sont toutes deux H-inductives et telles que $\mathrm{dom}(F) = C = \mathrm{dom}(F)$.

Montrons que $F = G$ par l'absurde.

Supposons par l'absurde que $F \neq G$.

Comme elles ont le même domaine C, il existe $\alpha \in C$ tel que $F(\alpha) \neq G(\alpha)$.

Considérons alors $X := \{\beta \in C \mid F(\beta) \neq G(\beta)\}$.

Par définition on a $X \subseteq C$, et $\alpha \in X$ donc X est non vide.

Or on a ($C \in ON$ ou $C = ON$) par définition de C, donc $C \subseteq ON$ et donc $X \subseteq ON$.

Ainsi X est classe non vide telle que $X \subseteq ON$.

Donc X possède un ordinal minimum ξ d'après la proposition 9 page 25.

Remarquons que l'on a $\xi \in X$ et $X \subseteq C$ donc $\xi \in C$ par définition de l'inclusion.

Soit $\gamma \in \xi$.

On a dit que $\xi \in C$ donc $\gamma \in C$ par transitivité :

Si $C \in ON$ alors c'est la transitivité de $\in$ sur ON qu'on applique.

Si $C = ON$, c'est la transitivité de ON qu'on applique.

On a aussi $\gamma < \xi$ par définition de $<$.

Comme ξ est le minimum de X, on a donc $\gamma \notin X$.

Ainsi on a $\gamma \notin X$ alors que $\gamma \in C$.

Nécessairement on a donc $F(\gamma) = G(\gamma)$ par définition de X.

Donc $\forall \gamma \in \xi, F(\gamma) = G(\gamma)$ et donc $F_{|\xi} = G_{|\xi}$.

Or F et G sont H-inductives donc $F(\xi) = H(F_{|\xi}) = H(G_{|\xi}) = G(\xi)$.

C'est absurde puisque $\xi \in X$ donc $F(\xi) \neq G(\xi)$.

Donc par l'absurde on a $F = G$, $\boxed{\text{d'où l'unicité}}$.

CQFD.

Remarque :
En particulier si F est H-inductive, alors pour tout $\alpha \in \mathrm{dom}(F)$, l'application $F_{|\alpha}$ est l'unique application H-inductive de domaine α.

Nous venons de voir qu'à domaine fixé, il existe au plus une assertion fonctionnelle qui est H-inductive. Mais en existe-t-il au moins une ? La réponse est oui, mais à une certaine condition sur H. En fait l'idée est de construire notre assertion fonctionnelle de proche en proche, donc par récurrence (plus précisément par récursion), puisque la valeur en un ordinal est fonction des valeurs en les ordinaux précédents.

Imaginons que l'on ait défini notre application/assertion fonctionnelle jusqu'à l'ordinal α. Cela revient à dire que nous avons à notre disposition une application $v : \alpha \longrightarrow ?$ qui est H-inductive. Pour pouvoir poursuivre à nouveau la construction, et faire en sorte que v ne soit en fait que la restriction à α de notre assertion fonctionnelle finale, il faut simplement s'assurer que v elle-même est dans le domaine de H, et non pas seulement ses restrictions. C'est pour cela que dans le théorème suivant, on a rajouté cette condition.

Théorème 6 (Principe de récursion transfinie)

Soit H une assertion fonctionnelle.
Soit C une classe telle que $C \in ON$ ou $C = ON$.
Supposons que pour tout $\alpha \in C$ et toute application $v : \alpha \longrightarrow ?$ on a

si v est H-inductive alors v est dans le domaine de H

Alors il existe une unique assertion fonctionnelle de domaine C qui est H-inductive.

Démonstration

Unicité

C'est exactement l'objet de la proposition 28 page 71.

Existence

Considérons T la classe des $\alpha \in C$ tel qu'il existe une application $\alpha \longrightarrow ?$ qui est H-inductive et dans le domaine de H. Une telle application est alors unique d'après la proposition 28 page 71. Ainsi T représente en quelque sorte le domaine maximal auquel on peut construire notre assertion fonctionnelle. Notre but va donc simplement être de montrer que $T = C$: on peut en fait aller jusqu'au bout.

Voici les différentes étapes de notre preuve :

1. On montre que comme pour C, on a $T \in ON$ ou $T = ON$
   Autrement dit T est un ordinal ou est la généralisation d'un ordinal.
   On s'assure ainsi que le domaine est pertinent pour une construction par récursion.
   (a) Cela passe d'abord par montrer que T est transitive.
   (b) Puis on conclut avec le fait que $(T, \in)$ est strictement bien ordonné.
2. On construit l'assertion fonctionnelle $U_T : T \longrightarrow ?$ qui est H-inductive.
   La construction va se faire par récursion : c'est justement notre objectif.
3. On montre que l'existence de U_T implique nécessairement que $T = C$.

1.(a) Montrons que T est transitive.

Soit $\alpha \in T$.

Comme $\alpha \in T$, par définition de T il existe une application $u : \alpha \longrightarrow ?$ qui est H-inductive et dans le domaine de H.

Soit $\beta \in \alpha$.

Comme u est H-inductive, $u_{|\beta}$ est dans le domaine de H.

De plus $u_{|\beta} : \beta \longrightarrow ?$ est H-inductive d'après la proposition 27 page 70.

Ainsi il existe une application $\beta \longrightarrow ?$ qui est H-inductive et dans le domaine de H. Pour prouver que $\beta \in T$, il reste donc à prouver que $\beta \in C$.

Or on a $\beta \in \alpha \in C$ donc $\beta \in C$ par transitivité.

Si $C \in ON$ alors c'est la transitivité de $\in$ sur ON qu'on applique.

Si $C = ON$, c'est la transitivité de ON qu'on applique.

Donc $\beta \in T$ par définition de T.

Donc pour tout $\beta \in \alpha$, on a $\beta \in T$.

Donc $\alpha \subseteq T$ par définition de l'inclusion.

Ainsi $\forall \alpha \in T, \alpha \subseteq T$ donc $\boxed{T \text{ est transitive}}$.

1.(b) Montrons que $T \in ON$ ou $T = ON$.

On a $(C \in ON$ ou $C = ON)$ donc $C \subseteq ON$.

Comme $T \subseteq C$ on a donc $T \subseteq ON$.

Ainsi tous les éléments de T sont des ordinaux.

Donc $(T, \in)$ est strictement bien ordonnée d'après le théorème 1 page 21.

Or on vient de montrer que T est transitive.

- Si T est issue d'un ensemble alors T est un ordinal par définition d'être un ordinal.
- Si T est une classe propre, alors $T = ON$ d'après la proposition 10 page 27.

On a donc nécessairement $\boxed{T \in ON \text{ ou } T = ON}$.

2. Pour tout $\alpha \in T$, posons u_α l'unique application $\alpha \longrightarrow ?$ qui est H-inductive et dans le domaine de H. Construisons maintenant $U_T : T \longrightarrow ?$ l'unique assertion fonctionnelle qui est H-inductive.

Pour cela, on peut raisonner par analyse synthèse : imaginons qu'on ait déjà à notre disposition l'unique assertion fonctionnelle $U_T : T \longrightarrow ?$ qui est H-inductive.

Le fait qu'elle est H-inductive signifie en particulier que pour tout $\alpha \in T$, on a

$$U_T(\alpha) = H\big((U_T)_{|\alpha}\big)$$

Autrement dit, pour connaître la valeur de $U_T(\alpha)$, il nous faut connaître $(U_T)_{|\alpha}$.

Mais comme U_T est H-inductive, on a forcément que $(U_T)_{|\alpha} : \alpha \longrightarrow ?$ est elle-même H-inductive d'après la proposition 27 page 70. Or justement on sait qu'une telle application est nécessairement u_α par définition de u_α. Autrement dit, on a nécessairement $(U_T)_{|\alpha} = u_\alpha$ et donc on a nécessairement $U_T(\alpha) = H(u_\alpha)$. Ainsi, notre candidat pour U_T est donné par

$$U_T := \begin{pmatrix} T & \longrightarrow & ? \\ \alpha & \longmapsto & H(u_\alpha) \end{pmatrix}$$

Montrons que U_T ainsi définie est H-inductive.
On sait déjà que $\mathrm{dom}(U_T) = T$ est ou bien un ordinal ou bien ON toute entière.

Soit $\alpha \in T$.

Montrons que $(U_T)_{|\alpha} = u_\alpha$.

Soit $\beta \in \alpha$.

▶ On a alors $\beta \in \alpha \in T$ donc $\beta \in T$ par transitivité.

Si $T \in ON$ alors c'est la transitivité de $\in$ sur ON qu'on applique.

Si $T = ON$, c'est la transitivité de ON qu'on applique.

On a $(U_T)_{|\alpha}(\beta) = U_T(\beta)$ par définition d'une restriction.
Or $U_T(\beta) = H(u_\beta)$ par définition de U_T, donc $(U_T)_{|\alpha}(\beta) = H(u_\beta)$.

▶ D'un autre côté, on sait que u_α est par définition H-inductive.
Donc $u_\alpha(\beta) = H\Big((u_\alpha)_{|\beta}\Big)$ par définition de la H-inductivité.

▶ Enfin $(u_\alpha)_{|\beta}$ est H-inductive d'après la proposition 27 page 70.
Donc $(u_\alpha)_{|\beta} = u_\beta$ par unicité de l'application de domaine β qui est H-inductive.

On a donc montré que $\begin{cases} (U_T)_{|\alpha}(\beta) = H(u_\beta) \\ u_\alpha(\beta) = H\Big((u_\alpha)_{|\beta}\Big) \\ (u_\alpha)_{|\beta} = u_\beta \end{cases}$

Les deux dernières lignes nous disent que $u_\alpha(\beta) = H(u_\beta)$.
Combiné à la première ligne, on en déduit que $(U_T)_{|\alpha}(\beta) = u_\alpha(\beta)$.

Ainsi $\forall \beta \in \alpha, (U_T)_{|\alpha}(\beta) = u_\alpha(\beta)$.
Or $(U_T)_{|\alpha}$ et u_α ont le même domaine α donc $(U_T)_{|\alpha} = u_\alpha$.
Or par définitions u_α est dans le domaine de H et $U_T(\alpha) = H(u_\alpha)$.

Donc $(U_T)_{|\alpha}$ est dans le domaine de H et $U_T(\alpha) = H\Big((U_T)_{|\alpha}\Big)$.

Donc pour tout $\alpha \in T$, $(U_T)_{|\alpha}$ est dans le domaine de H et $U_T(\alpha) = H\Big((U_T)_{|\alpha}\Big)$.

Donc $\boxed{U_T \text{ est } H\text{-inductive}}$.

3. Enfin, montrons que $T = C$ pour conclure.

Supposons par l'absurde que $T \neq C$.

Par définition de T on a $T \subseteq C$ donc on a $T \subsetneq C$.

On a dit que $(T \in ON$ ou $T = ON)$ et $(C \in ON$ ou $C = ON)$.

- Si $T \in ON$ et $C \in ON$ alors $T \in C$ d'après la prop. 8 p. 20.
- Si $T \in ON$ et $C = ON$ alors immédiatement $T \in C$.
- Si $T = ON$ et $C \in ON$ c'est absurde puisque $T \subsetneq C$.
- Si $T = ON$ et $C = ON$ c'est absurde puisque $T \subsetneq C$.

On a donc nécessairement $T \in C$.

Comme $(C \in ON$ ou $C = ON)$ on a $C \subseteq ON$.

On a donc $T \in ON$ par définition de l'inclusion.

Donc T est un ordinal donc en particulier est un ensemble.

Donc U_T est une assertion fonctionnelle de domaine un ensemble.

Donc U_T est une application.

Ainsi U_T est une application H-inductive dont le domaine appartient à C.

Donc U_T est dans le domaine de H par hypothèse du théorème.

Ainsi T est un élément de C et le domaine d'une application H-inductive qui est elle-même dans le domaine de H.

Donc $T \in T$ par définition de T.

C'est absurde par antiréflexivité de $\in$ sur ON.

On a donc montré par l'absurde que $T = C$.

Or U_T est une assertion fonctionnelle de domaine T qui est H-inductive.

Donc $\boxed{U_T \text{ est une assertion fonctionnelle de domaine } C \text{ qui est } H\text{-inductive}}$.

CQFD.

Exemple :

Reprenons les exemples du début et éclairons-les de ce que l'on vient d'apprendre.

1. Si l'on souhaite définir proprement l'unique suite $(u_n)_{n\in\mathbb{N}}$ vérifiant

$$\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N}, u_{n+1} = 3u_n \end{cases}$$

il suffit de considérer l'assertion fonctionnelle H définie pour toute application f

telle que $\mathrm{dom}(f) \in \mathbb{N}$ par

$$\begin{cases} H(f) := 1 & \text{si } \mathrm{dom}(f) = 0 \\ H(f) := 3f(n) & \text{si } \mathrm{dom}(f) = n+1 \text{ avec } n \in \mathbb{N} \end{cases}$$

En effet, on considère alors $C = \mathbb{N}$, qui vérifie bien $C \in ON$ d'après la proposition 17 page 43. Prenons alors $n \in \mathbb{N}$ et $f : n \longrightarrow ?$ quelconque : par définition de H, f est nécessairement dans le domaine de H. Cela reste donc vrai si en particulier f est H-inductive. Ainsi H et C vérifient les hypothèses du théorème précédent : il existe une unique suite $u = (u_n)_{n\in\mathbb{N}}$ qui est H-inductive. Cette suite vérifie alors

$$\begin{cases} u_0 = u(0) = H(u_{|0}) = 1 \\ \forall n \in \mathbb{N}, u_{n+1} = u(n+1) = H(u_{|n+1}) = 3u(n) = u_n \end{cases}$$

2. Si l'on souhaite définir proprement l'unique suite $(u_n)_{n\in\mathbb{N}}$ vérifiant

$$\begin{cases} u_0 = 1 \\ u_1 = 1 \\ \forall n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n \end{cases}$$

il suffit de considérer l'assertion fonctionnelle H définie pour toute application f telle que $\mathrm{dom}(f) \in \mathbb{N}$ par

$$\begin{cases} H(f) := 1 & \text{si } \mathrm{dom}(f) = 0 \\ H(f) := 1 & \text{si } \mathrm{dom}(f) = 1 \\ H(f) := f(n+1) + f(n) & \text{si } \mathrm{dom}(f) = n+2 \text{ pour } n \in \mathbb{N} \end{cases}$$

On considère ici encore $C = \mathbb{N}$. Pour les mêmes raisons que l'exemple précédent, H et C vérifient les hypothèses du théorème précédent : il existe une unique suite $u = (u_n)_{n\in\mathbb{N}}$ qui est H-inductive. Cette suite vérifie alors

$$\begin{cases} u_0 = u(0) = H(u_{|0}) = 1 \\ u_1 = u(1) = H(u_{|1}) = 1 \\ \forall n \in \mathbb{N}, u_{n+2} = u(n+2) = H(u_{|n+2}) = u(n+1) + u(n) = u_{n+1} + u_n \end{cases}$$

C'est la célèbre **suite de Fibonacci**.

Pour la petite histoire

Leonardo Fibonacci ($\sim$1170 – $\sim$1250), de son vrai nom Léonard De Pise, est le fils d'un commerçant toscan. Ce dernier émigre avec toute sa famille à Béjaïa dans l'actuelle Algérie et Leonardo est encouragé à maîtriser les comptes pour l'aider. Par la suite, Fibonacci parcourt l'Égypte, la Sicile, la Grèce et la Syrie. Il entre ainsi en contact avec les mathématiques arabes et grecques.

Convaincu de la supériorité du système d'écriture des nombres par les chiffres arabes, il écrit *Liber abaci* à son retour en Europe en 1202, ce qui les introduira en occident. Dans cet ouvrage, il explique la notation de position, les méthodes de calcul des opérations élémentaires, et des méthodes de résolutions d'équations.

Si la suite de Fibonacci était déjà connue au moins depuis 200 avant JC en Inde, c'est Fibonacci qui la rendra célèbre en occident dans *Liber abaci*.

6.3 Suites

Les exemples précédents parlent de suites, mais nous n'avons pas encore eu l'occasion de définir proprement ce que c'est. Intuitivement, une suite est une liste d'objets mathématiques, un pour chaque entier naturel. Autrement dit, c'est simplement une application $\mathbb{N} \longrightarrow ?$.

Définition 14 (Suite)

On appelle **suite** toute application $u : \mathbb{N} \longrightarrow ?$.
Pour tout ensemble E, on appelle suite **à valeurs dans** E toute suite $u : \mathbb{N} \longrightarrow E$.

Remarque :

1. Nous avons vu dans le livre précédent que les familles ne sont qu'un autre nom donné aux applications, mais qu'il est associé à d'autres notations et usages. Les suites rentrent plutôt dans le cadre des familles : c'est pourquoi une suite u est souvent notée $(u_n)_{n\in\mathbb{N}}$.
2. L'ensemble des suites à valeurs dans E étant l'ensemble $\mathcal{F}(\mathbb{N} \longrightarrow E)$ des applications de $\mathbb{N}$ dans E, il est aussi souvent noté $E^{\mathbb{N}}$.
3. Pour la fin de ce chapitre, notons $n+1$ à la place de $S(n)$, puisque c'est de toute manière l'intuition qui se cache derrière $S(n)$. Bien heureusement, au prochain chapitre nous définirons proprement l'addition, et nous verrons que l'on a bien $n+1 = S(n)$.

Dans les exemples précédents nous avons défini des suites par récurrence, plus précisément par récursion. Pour cela, nous avons invoqué une assertion fonctionnelle particulière et utilisé le théorème 6 page 72. Nous aimerions ne plus avoir à passer par une assertion fonctionnelle à chaque fois et pouvoir directement définir la suite en question. La proposition suivante se propose simplement de le faire une bonne fois pour toute.

Proposition 29 (Suites définies par récurrence)

Soient E un ensemble, $a \in E$ et $f : E \longrightarrow E$.
Alors il existe une unique suite $(u_n)_{n\in\mathbb{N}}$ à valeurs dans E telle que

$$\begin{cases} u_0 = a \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$$

Démonstration

Pour tout $m \in \mathbb{N}$ et tout $g : m \longrightarrow E$, posons

$$\begin{cases} H(g) = a & \text{si } m = 0 \\ H(g) = f\big(g(n)\big) & \text{si } m = n+1 \text{ avec } n \in \mathbb{N} \end{cases}$$

On vient ainsi de définir une assertion fonctionnelle H. Par définition, un ensemble g est dans le domaine de H si et seulement s'il existe $m \in \mathbb{N}$ tel que $g : m \longrightarrow E$.

Nous allons utiliser le théorème 6 page 72 avec $C := \mathbb{N}$. On sait déjà que C est un ordinal d'après la proposition 17 page 43, donc vérifie $C \in ON$. Il reste donc à montrer que H et C vérifie l'hypothèse du théorème.

Soient $m \in \mathbb{N}$ et $g : m \longrightarrow ?$ qui est H-inductive.

Montrons que $g : m \longrightarrow E$, c'est-à-dire $\mathrm{im}(g) \subseteq E$.

Soit $y \in \mathrm{im}(g)$.
Par définition il existe $n \in \mathrm{dom}(g)$ tel que $y = g(n)$.
Or g est H-inductive par définition.

On a donc $g_{|n} \in \mathrm{dom}(H)$ et $y = g(n) = H(g_{|n})$.
Remarquons deux choses : tout d'abord $g_{|n} \in \mathrm{dom}(H)$ donc $g_{|n} : n \longrightarrow E$ par définition de H, si bien que pour tout $p < n$, on a $g_{|n}(p) \in \mathrm{dom}(f)$ puisque $f : E \longrightarrow E$ par définition, si bien que l'on peut tout à fait parler de $f\big(g_{|n}(p)\big)$.
Deuxièmement, $n \in \mathrm{dom}(g)$ et $g : m \longrightarrow ?$ donc $n \in m$, c'est-à-dire $n < m$ par définition de $<$. Comme $m \in \mathbb{N}$, on a $n \in \mathbb{N}$ d'après la proposition 14 page 38. Donc n est ou bien 0, ou bien le successeur d'un entier naturel p par définition d'être un entier naturel.

- Plaçons-nous dans le cas où $n = 0$.
  Alors $\mathrm{dom}(g_{|n}) = 0$ donc $y = H(g_{|0}) = a$ par définition de H.

Comme $a \in E$ par définition, on a $y \in E$.

- Plaçons-nous dans le cas où $n = p+1$ avec $p \in \mathbb{N}$. Alors $\mathrm{dom}(g_{|n}) = p+1$ donc $y = H(g_{|n}) = f\big(g_{|n}(p)\big)$ par définition de H. Or par définition on a $f : E \longrightarrow E$ donc $\mathrm{im}(f) \subseteq E$ et donc $y \in E$.

Dans les deux cas on a $y \in E$.

Ainsi on a $\mathrm{im}(g) \subseteq E$ par définition de l'inclusion, et donc $g : m \longrightarrow E$.

Donc pour tout $m \in \mathbb{N}$ et toute application $g : m \longrightarrow ?$, si g est H-inductive alors $g : m \longrightarrow E$ et donc g est dans le domaine de H.

Ainsi $C = \mathbb{N}$ et H vérifient les hypothèses du théorème 6 page 72.
Il existe donc une unique application $u : \mathbb{N} \longrightarrow ?$ qui est H-inductive.
En particulier u vérifie

$$\begin{cases} u_0 = u(0) = H(u_{|0}) = a \\ \forall n \in \mathbb{N}, u_{n+1} = u(n+1) = H(u_{|n+1}) = f\big(u(n)\big) = f(u_n) \end{cases}$$

CQFD.

Remarque :
Dans la proposition précédente, nous avons explicité le cas où la valeur de u en un entier ne dépend que de la valeur de u à l'entier précédent, nous permettant de ne plus avoir à passer par une assertion fonctionnelle à chaque fois qu'une suite est définie par une récurrence. Cependant, nous n'avons pas décrit le cas où la valeur de u en un entier dépend des valeurs de u aux deux, trois, voire tous les entiers précédents.

Nous n'allons évidemment pas le faire : tenter de traiter tous les cas possibles reviendrait précisément à réénoncer le théorème 6 page 72. Autrement dit, nous allons désormais simplement considérer que le lecteur comprend comment le faire en toute généralité. Nous avons par exemple déjà donné la recette de cuisine pour la suite de Fibonacci.

Remarquons que cela nous permet par exemple de définir des suites vérifiant $u_{n+1} = \sum\limits_{k=0}^{n} u_n$ (en ayant fixée la valeur en 0) puisque l'on a dit qu'on peut utiliser toutes les valeurs aux entiers précédents !

En tant qu'ordinal, $\mathbb{N} = \omega$ est muni d'une relation d'ordre. À ce titre, pour tout ensemble ordonné E, on a déjà donné du sens dans le livre précédent à la notion de suite (strictement) croissante, (strictement) décroissante et constante. Rajoutons une petite dernière : celle de stationnarité.

Définition 15 (Suite stationnaire)

Soient E un ensemble et $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs dans E.
On dit que $(u_n)_{n\in\mathbb{N}}$ est **stationnaire** si et seulement s'il existe $n_0 \in \mathbb{N}$ tel que

$$\forall n \geq n_0, u_n = u_{n_0}$$

Remarque :
Une suite constante est un cas particulier de suite stationnaire : elle l'est simplement depuis le début, c'est-à-dire qu'on peut prendre $n_0 = 0$.

La notion de successeurs chez les ordinaux et donc chez les entiers naturels offre une caractérisation intéressante de ces propriétés dont on a parlé juste avant : il suffit qu'elles soient vérifié entre un entier et le suivant pour se propager en fait à tous les entiers. C'est l'objet de la proposition suivante. On utilise ici la notation $n+1$ pour désigner $S(n)$, bien que nous verrons qu'elle coïncide bien avec l'addition quand nous l'aurons définie dans le prochain chapitre.

Proposition 30 (Suites croissantes, décroissantes, constantes)

Soient $(E, \preccurlyeq)$ un ensemble ordonné et $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs dans E.
Soit $\prec$ l'ordre strict associé à $\preccurlyeq$.

1. $(u_n)_{n\in\mathbb{N}}$ est croissante si et seulement si $\forall n \in \mathbb{N}, u_n \preccurlyeq u_{n+1}$.
2. $(u_n)_{n\in\mathbb{N}}$ est strictement croissante si et seulement si $\forall n \in \mathbb{N}, u_n \prec u_{n+1}$.
3. $(u_n)_{n\in\mathbb{N}}$ est décroissante si et seulement si $\forall n \in \mathbb{N}, u_{n+1} \preccurlyeq u_n$.
4. $(u_n)_{n\in\mathbb{N}}$ est strictement décroissante si et seulement si $\forall n \in \mathbb{N}, u_{n+1} \prec u_n$.
5. $(u_n)_{n\in\mathbb{N}}$ est constante si et seulement si $\forall n \in \mathbb{N}, u_n = u_{n+1}$.
6. $(u_n)_{n\in\mathbb{N}}$ est stationnaire si et seulement si $\exists n_0 \in \mathbb{N}, \forall n \geq n_0, u_n = u_{n+1}$.

Démonstration

1. $\boxed{\Rightarrow}$

Supposons que $(u_n)_{n\in\mathbb{N}}$ est croissante.

Soit $n \in \mathbb{N}$.

On sait que $n < n+1$ d'après la proposition 12 page 33.

En particulier on a $n \leq n+1$.

On a donc $u_n \preccurlyeq u_{n+1}$ par croissance de u.

Donc $\boxed{\forall n \in \mathbb{N}, u_n \preccurlyeq u_{n+1}}$.

$\boxed{\Leftarrow}$

Supposons que $\forall n \in \mathbb{N}, u_n \preccurlyeq u_{n+1}$.

Soit $m \in \mathbb{N}$.

Pour tout $n \in \mathbb{N}$, posons $P(n)$ l'assertion $m \leq n \implies u_m \preccurlyeq u_n$.

Montrons par récurrence que pour tout $n \in \mathbb{N}$, on a $P(n)$.

Initialisation

- Plaçons-nous dans le cas où $m = 0$.
  Dans ce cas-là on a $u_m = u_0$ donc $u_m \preccurlyeq u_0$ par réflexivité de $\preccurlyeq$.
  L'implication $m \leq 0 \implies u_m \preccurlyeq u_0$ est donc vraie.
- Plaçons-nous dans le cas où $m \neq 0$.
  L'implication $m \leq 0 \implies u_m \preccurlyeq u_0$ est alors vraie car sa prémisse est fausse.

Dans les deux cas, on a $P(0)$.

Hérédité

Soit $n \in \mathbb{N}$ tel que $P(n)$.

Supposons que $m \leq n + 1$.

On a donc $m < n + 1$ ou $m = n + 1$.

- Plaçons-nous dans le cas où $m < n + 1$.
  On a alors $m \leq n$ d'après la proposition 12 page 33.
  On a donc $u_m \preccurlyeq u_n$ par $P(n)$.
  Or on a $u_n \preccurlyeq u_{n+1}$ par hypothèse.
  On a donc $u_m \preccurlyeq u_{n+1}$ par transitivité de $\preccurlyeq$.
- Plaçons-nous dans le cas où $m = n + 1$.
  On a alors $u_m = u_{n+1}$ donc $u_m \preccurlyeq u_{n+1}$ par réflexivité de $\preccurlyeq$.

Dans les deux cas on a $u_m \preccurlyeq u_{n+1}$.

Donc si $m \leq n + 1$ alors $u_m \preccurlyeq u_{n+1}$.

On a donc $P(n + 1)$.

Donc pour tout $n \in \mathbb{N}$, on a $P(n) \implies P(n + 1)$.

D'après le principe d'induction sur les entiers naturels, on a donc $\forall n \in \mathbb{N}, P(n)$.

Autrement dit, $\forall n \in \mathbb{N}, (m \leq n \Rightarrow u_m \preccurlyeq u_n)$.

Donc $\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, (m \leq n \Rightarrow u_m \preccurlyeq u_n)$.

Donc $\boxed{(u_n)_{n \in \mathbb{N}} \text{ est croissante}}$.

2. $\boxed{\Rightarrow}$

Supposons que $(u_n)_{n \in \mathbb{N}}$ est strictement croissante.

Soit $n \in \mathbb{N}$.

On sait que $n < n + 1$ d'après la proposition 12 page 33.

On a donc $u_n \prec u_{n+1}$ par stricte croissance de u.

Donc $\boxed{\forall n \in \mathbb{N}, u_n \prec u_{n+1}}$.

$\boxed{\Leftarrow}$

Supposons que $\forall n \in \mathbb{N}, u_n \prec u_{n+1}$.

Soit $m \in \mathbb{N}$.

Pour tout $n \in \mathbb{N}$, posons $P(n)$ l'assertion $m < n \implies u_m \prec u_n$.

Montrons par récurrence que pour tout $n \in \mathbb{N}$, on a $P(n)$.

Initialisation

L'implication $m < 0 \implies u_m \prec u_0$ est vraie car sa prémisse est fausse.

On a donc $P(0)$.

Hérédité

Soit $n \in \mathbb{N}$ tel qu'on a $P(n)$.

Supposons que $m < n + 1$.

On a donc $m \leq n$ d'après la proposition 12 page 33.

On a donc $m < n$ ou $m = n$.

- Plaçons-nous dans le cas où $m < n$.

  On a alors $u_m \prec u_n$ d'après $P(n)$.

  Or on a $u_n \prec u_{n+1}$ par hypothèse.

  On a donc $u_m \prec u_{n+1}$ par transitivité de $\prec$.

- Plaçons-nous dans le cas où $m = n$.

  On a donc $u_m = u_n$.

  Or on a $u_n \prec u_{n+1}$ par hypothèse.

  On a donc $u_m \prec u_{n+1}$.

Dans les deux cas on a $u_m \prec u_{n+1}$.

Donc si $m < n + 1$ alors $u_m \prec u_{n+1}$.

On a donc $P(n + 1)$.

Donc pour tout $n \in \mathbb{N}$, on a $P(n) \implies P(n + 1)$.

D'après le principe d'induction sur les entiers naturels, on a donc $\forall n \in \mathbb{N}, P(n)$.

Autrement dit $\forall n \in \mathbb{N}, (m < n \Rightarrow u_m \prec u_n)$.

Donc $\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, (m < n \Rightarrow u_m \prec u_n)$.

Donc $\boxed{(u_n)_{n \in \mathbb{N}} \text{ est strictement croissante}}$.

3. Considérons la relation $\succcurlyeq$ symétrique de $\preccurlyeq$, c'est-à-dire que pour tout x et y dans E, on a

$$x \succcurlyeq y \iff y \preccurlyeq x$$

On peut montrer que $\succcurlyeq$ est une relation d'ordre sur E.
On a alors les équivalences :

$$\begin{aligned}
(u_n)_{n\in\mathbb{N}} \text{ est décroissante pour } \preccurlyeq &\iff \forall m \in \mathbb{N}, \forall n \in \mathbb{N}, (m \leq n \Rightarrow u_n \preccurlyeq u_m) \\
&\iff \forall m \in \mathbb{N}, \forall n \in \mathbb{N}, (m \leq n \Rightarrow u_m \succcurlyeq u_n) \\
&\iff (u_n)_{n\in\mathbb{N}} \text{ est croissante pour } \succcurlyeq \\
&\iff \forall n \in \mathbb{N}, u_n \succcurlyeq u_{n+1} \text{ d'après 1.} \\
&\iff \forall n \in \mathbb{N}, u_{n+1} \preccurlyeq u_n
\end{aligned}$$

D'où $\boxed{(u_n)_{n\in\mathbb{N}} \text{ est décroissante si et seulement si } \forall n \in \mathbb{N}, u_{n+1} \preccurlyeq u_n}$.

4. Considérons la relation $\succ$ symétrique de $\prec$, c'est-à-dire que pour tout x et y dans E, on a

$$x \succ y \iff y \prec x$$

On peut montrer que $\succ$ est une relation d'ordre strict sur E.
On a alors les équivalences :

$$\begin{aligned}
(u_n)_{n\in\mathbb{N}} \text{ est strictement décroissante pour } \prec &\iff \forall m \in \mathbb{N}, \forall n \in \mathbb{N}, (m < n \Rightarrow u_n \prec u_m) \\
&\iff \forall m \in \mathbb{N}, \forall n \in \mathbb{N}, (m < n \Rightarrow u_m \succ u_n) \\
&\iff (u_n)_{n\in\mathbb{N}} \text{ est strictement croissante pour } \succ \\
&\iff \forall n \in \mathbb{N}, u_n \succ u_{n+1} \text{ d'après 2.} \\
&\iff \forall n \in \mathbb{N}, u_{n+1} \prec u_n
\end{aligned}$$

D'où $\boxed{(u_n)_{n\in\mathbb{N}} \text{ est strictement décroissante si et seulement si } \forall n \in \mathbb{N}, u_{n+1} \prec u_n}$.

5. On a les équivalences suivantes :

$$\begin{aligned}
(u_n)_{n\in\mathbb{N}} \text{ est constante} &\iff (u_n)_{n\in\mathbb{N}} \text{ est croissante et décroissante} \\
&\iff (\forall n \in \mathbb{N}, u_n \preccurlyeq u_{n+1}) \text{ et } (\forall n \in \mathbb{N}, u_{n+1} \preccurlyeq u_n) \text{ d'après 1. et 3.} \\
&\iff \forall n \in \mathbb{N}, (u_n \preccurlyeq u_{n+1} \text{ et } u_{n+1} \preccurlyeq u_n) \\
&\iff \forall n \in \mathbb{N}, u_n = u_{n+1} \text{ par antisymétrie et réflexivité de } \preccurlyeq
\end{aligned}$$

D'où $\boxed{(u_n)_{n\in\mathbb{N}} \text{ est constante si et seulement si } \forall n \in \mathbb{N}, u_n = u_{n+1}}$.

6. $\boxed{\Rightarrow}$
Supposons que $(u_n)_{n\in\mathbb{N}}$ est stationnaire.

Il existe donc $n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0, u_n = u_{n_0}$.

Soit $n \geq n_0$.

On a donc $u_{n_0} = u_n$ par hypothèse.

Comme $n_0 \leq n$ on a aussi $n_0 < n+1$ d'après la proposition 12 page 33.

En particulier $n_0 \leq n+1$ donc $u_{n_0} = u_{n+1}$ par hypothèse.

On a donc $u_n = u_{n+1}$.

Donc $\boxed{\forall n \geq n_0, u_n = u_{n+1}}$.

$\boxed{\Leftarrow}$

Supposons qu'il existe $n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0, u_n = u_{n+1}$.

Pour tout $n \in \mathbb{N}$, posons $P(n)$ l'assertion $n_0 \leq n \implies u_{n_0} = u_n$.

Montrons par récurrence que pour tout $n \in \mathbb{N}$ on a $P(n)$.

Initialisation

Supposons que $n_0 \leq 0$.

On a donc $n_0 \subseteq 0$ par définition de $\leq$.

On a donc $n_0 = 0$ puisque par définition $0 = \varnothing$.

Donc $u_{n_0} = u_0$.

On a donc $n_0 \leq 0 \implies u_{n_0} = u_0$, c'est-à-dire $P(0)$.

Hérédité

Soit $n \in \mathbb{N}$ tel que $P(n)$.

Supposons que $n_0 \leq n+1$.

On a donc $n_0 < n+1$ ou $n_0 = n+1$.

- Plaçons-nous dans le cas où $n_0 < n+1$.

  On a donc $n_0 \leq n$ d'après la proposition 12 page 33.

  On a donc $u_{n_0} = u_n$ d'après $P(n)$.

  Or on a $u_n = u_{n+1}$ par hypothèse.

  Donc $u_{n_0} = u_{n+1}$.

- Plaçons-nous dans le cas où $n_0 = n+1$.

  On donc $u_{n_0} = u_{n+1}$.

Dans les deux cas, on a donc $u_{n_0} = u_{n+1}$.

Donc si $n_0 \leq n+1$ alors $u_{n_0} = u_{n+1}$, donc on a $P(n+1)$.

Donc pour tout $n \in \mathbb{N}$, si $P(n)$ alors $P(n+1)$.

D'après le principe d'induction chez les entiers, on a donc $\forall n \in \mathbb{N}, P(n)$.

Autrement dit $\forall n \in \mathbb{N}, (n_0 \leq n \Rightarrow u_n = u_{n_0})$.

Dit encore autrement, $\forall n \geq n_0, u_n = u_{n_0}$.

Donc $\boxed{(u_n)_{n\in\mathbb{N}} \text{ est stationnaire}}$.

CQFD.

Observons à présent un phénomène qui peut parfois se produire : pour certains ensembles ordonnés, une suite décroissante est forcément stationnaire. Autrement dit, c'est comme si toute suite décroissante était forcée de s'arrêter à un moment. On parle de la **condition de la chaîne descendante**.

Définition 16 (Condition de la chaîne descendante)

Soit E un ensemble ordonné.
On dit que E vérifie la **condition de la chaîne descendante** si et seulement si pour toute suite $(u_n)_{n\in\mathbb{N}}$ à valeurs dans E, si $(u_n)_{n\in\mathbb{N}}$ est décroissante alors $(u_n)_{n\in\mathbb{N}}$ est stationnaire.

Venons-en à une caractérisation très puissante des ensembles bien ordonnés : parmi les ensembles totalement ordonnés, ce sont précisément ceux qui vérifient la condition de la chaîne descendante.

Proposition 31 (Cond. de la chaîne descendante et bon ordre)

Soit E un ensemble ordonné.
Les assertions suivantes sont équivalentes :

1. E est bien ordonné.
2. E est totalement ordonné et vérifie la condition de la chaîne descendante.

Démonstration

Notons $\preccurlyeq$ la relation d'ordre sur E et $\prec$ l'ordre strict associé.

$\boxed{\Rightarrow}$

Supposons que E est bien ordonné.

On sait déjà que E est totalement ordonné d'après la proposition 2 page 11.

Montrons que E vérifie la condition de la chaîne descendante.

Soit $(u_n)_{n\in\mathbb{N}}$ une suite à valeurs dans E.

Supposons que $(u_n)_{n\in\mathbb{N}}$ est décroissante.

Considérons $X := \{u_n \mid n \in \mathbb{N}\}$, qui est donc une partie non vide de E.

Or E est **bien ordonné** par hypothèse.

Donc X admet un minimum x : on a donc $\forall n \in \mathbb{N}, x \preccurlyeq u_n$.

Mais on sait aussi que $x \in X$ donc il existe $m \in \mathbb{N}$ tel que $x = u_m$.

Ainsi pour tout $n \geq m$, on a donc $u_m \preccurlyeq u_n$ par ce qui précède.

Mais on sait aussi que $(u_n)_{n\in\mathbb{N}}$ est décroissante.

Donc pour tout $n \geq m$, on a $u_n \preccurlyeq u_m$ et donc $u_n = u_m$ par antisymétrie de $\preccurlyeq$.

Ainsi $(u_n)_{n\in\mathbb{N}}$ est stationnaire.

Donc si $(u_n)_{n\in\mathbb{N}}$ est décroissante alors $(u_n)_{n\in\mathbb{N}}$ est stationnaire.

Donc $\boxed{E \text{ vérifie la condition de la chaîne descendante}}$.

$\boxed{\Leftarrow}$

Supposons que E est totalement ordonné et vérifie la condition de la chaîne descendante.

Supposons par l'absurde que E n'est pas bien ordonné.

Il existe donc une partie X de E qui est non vide mais n'admet pas de minimum.

Pour tout $x \in X$, posons $X_{\prec x}$ l'ensemble $\{y \in X \mid y \prec x\}$.

Supposons par l'absurde qu'il existe $x \in X$ tel que $X_{\prec x}$ est vide.

Autrement dit pour tout $y \in X$, on n'a pas $y \prec x$.

Or E est **totalement ordonné** par hypothèse donc pour tout $y \in X$ on a $x \preccurlyeq y$.

Autrement dit x est le minimum de X, ce qui est absurde car X n'en a pas.

Ainsi pour tout $x \in X$, on a $X_{\prec x} \neq \varnothing$.

D'après l'**axiome du choix**, il existe une application $g : \mathscr{P}(X)\backslash\{\varnothing\} \longrightarrow ?$ telle que $\forall A \in \mathscr{P}(X)\backslash\{\varnothing\}, g(A) \in A$.

En particulier pour tout $x \in X$, on a $g(X_{\prec x}) \in X_{\prec x}$ donc $g(X_{\prec x}) \prec x$.

Pour tout $x \in X$, posons $f(x) := g(X_{\prec x})$ de sorte que $f(x) \prec x$.

On a dit que X est non vide : soit $a \in X$.

Considérons alors la suite $(u_n)_{n\in\mathbb{N}}$ définie par récurrence par

$$\begin{cases} u_0 := a \\ \forall n \in \mathbb{N}, u_{n+1} := f(u_n) \end{cases}$$

Ainsi $(u_n)_{n\in\mathbb{N}}$ est une suite à valeurs dans X donc dans E car $X \subseteq E$.

De plus on a $\forall n \in \mathbb{N}, u_{n+1} = f(u_n) \prec u_n$ donc $(u_n)_{n\in\mathbb{N}}$ est strictement décroissante.

En particulier $(u_n)_{n\in\mathbb{N}}$ est décroissante.

Or E vérifie **la condition de la chaîne descendante** donc $(u_n)_{n\in\mathbb{N}}$ est stationnaire.

C'est absurde puisqu'on vient de dire qu'elle est strictement décroissante.

Par l'absurde, on vient de montrer que $\boxed{E \text{ est bien ordonné}}$.

CQFD.

Pour la petite histoire

Emmy Noether (23 mars 1882 – 14 avril 1935) est une mathématicienne allemande spécialiste d'algèbre abstraite et de physique théorique. Considérée par Albert Einstein comme «*le génie mathématique créatif le plus considérable produit depuis que les femmes ont eu accès aux études supérieures*», elle a révolutionné les théories des anneaux, des corps et des algèbres, notamment en développant la notion d'idéal. En physique, le théorème de Noether explique le lien fondamental entre la symétrie et les lois de conservation et est considéré comme aussi important que la théorie de la relativité.

Noether introduit la condition de la chaîne descendante dans son article de 1921 *Idealtheorie in Ringbereichen* mais précise que ce concept avait déjà été introduit précédemment par Dedekind (dans le cas des corps de nombres) et par Lasker (dans le cas des polynômes). Elle est la première à l'introduire dans le cadre général de son article : celui des anneaux commutatifs dont chaque idéal est finiment engendré.

Chapitre 2

Opérations sur les ordinaux

Note de l'auteur

Nous avons défini et étudié les ordinaux lors du chapitre précédent, en se munissant de toute une batterie d'outils pour cela. Il est temps maintenant d'agir sur ceux-ci via l'introduction d'opérations entre ordinaux. Nous allons voir comment les additionner, les multiplier et les élever à une puissance. L'outil de récursion développé à la fin du chapitre précédent nous sera pour cela d'une grande aide.

Sommaire

1 Généralités

Si nous avons déployé l'artillerie lourde avec la notion d'assertion fonctionnelle inductive, c'est pour avoir les mains libres au moment de la définition de trois opérations importantes chez les ordinaux : l'addition, la multiplication et l'exponentiation. Prenons pour exemple l'addition des ordinaux : nous aimerions donner du sens à l'addition $\alpha + \beta$ pour α et β deux ordinaux. On peut pour cela s'inspirer de l'addition chez les entiers naturels.

Comment allons-nous définir l'addition $2+7$ par exemple ? On considère que $2+6$ a déjà été définie et on pose alors $2+7 := (2+6)+1$. Ainsi on est en train de poser $2+(6+1) := (2+6)+1$ et en le réécrivant avec la notation de successeur, cela donne $2 + S(6) := S(2 + 6)$. Pour définir l'addition de 2 par tous les entiers, on le fait simplement de la manière suivante en initialisant la valeur en 0 :

$$\begin{cases} 2+0 := 2 \\ 2+S(m) := S(2+m) \text{ pour tout entier naturel } m \end{cases}$$

Pour donner du sens à $2 + S(m)$, on considère que $2 + m$ a déjà du sens : c'est bien là une récursion. Quel sens donner alors à $2 + \omega$? On va simplement dire que c'est l'ordinal qui vient après tous les $2 + n$ avec $n \in \omega$. Autrement dit, on va dire que $2 + \omega$ est la borne supérieure de l'ensemble $\{2 + n \mid n \in \omega\}$. Plus généralement, on va poser

$$\begin{cases} 2+0 := 2 \\ 2+S(\beta) := S(2+\beta) \text{ pour tout ordinal } \beta \\ 2+\gamma := \sup\limits_{\delta\in\gamma}(2+\delta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

Encore plus généralement, pour α un ordinal quelconque fixé à l'avance, on va poser

$$\begin{cases} \alpha+0 := \alpha \\ \alpha+S(\beta) := S(\alpha+\beta) \text{ pour tout ordinal } \beta \\ \alpha+\gamma := \sup\limits_{\delta\in\gamma}(\alpha+\delta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

Comment allons-nous procéder pour s'assurer qu'il s'agit d'une définition rigoureuse ? On souhaite en fait définir par récursion une assertion fonctionnelle F_α vérifiant :

$$\begin{cases} F_\alpha(0) := \alpha \\ F_\alpha\big(S(\beta)\big) := S\big(F_\alpha(\beta)\big) \text{ pour tout ordinal } \beta \\ F_\alpha(\gamma) := \sup\limits_{\delta\in\gamma} F_\alpha(\delta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

et on pose alors $\alpha + \beta := F_\alpha(\beta)$. Pour pouvoir justifier proprement qu'une telle construction est possible, et pouvoir de même définir la multiplication et l'exponentiation, énonçant la proposition suivante. L'ordinal μ_0 joue le rôle du résultat de l'initialisation, et l'assertion fonctionnelle G est là pour généraliser S.

Proposition 32 (Justification des opérations sur les ordinaux)

Soient μ_0 un ordinal et $G : ON \longrightarrow ON$ une assertion fonctionnelle.
Alors il existe une unique assertion fonctionnelle $F : ON \longrightarrow ON$ telle que

$$\begin{cases} F(0) = \mu_0 \\ F\big(S(\beta)\big) = G\big(F(\beta)\big) \text{ pour tout ordinal } \beta \\ F_\alpha(\gamma) := \sup\limits_{\delta\in\gamma} F_\alpha(\delta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

Démonstration

Existence

Pour toute application f telle que $\operatorname{dom}(f)$ est un ordinal et tel que $\operatorname{im}(f) \subseteq ON$, on pose

$$\begin{cases} H(f) := \mu_0 & \text{si } \operatorname{dom}(f) = 0 \\ H(f) := G\big(f(\beta)\big) & \text{si } \operatorname{dom}(f) = S(\beta) \text{ avec } \beta \text{ un ordinal} \\ H(f) := \sup\limits_{\delta\in\gamma} f(\delta) & \text{si } \operatorname{dom}(f) = \gamma \text{ est un ordinal limite non nul} \end{cases}$$

On obtient alors H une assertion fonctionnelle.

• Montrons que $\operatorname{im}(H) \subseteq ON$.

Soit $y \in \operatorname{im}(H)$.

Il existe donc $f \in \operatorname{dom}(H)$ tel que $y = H(f)$.

Par définition de H, f est une application telle que $\operatorname{dom}(f) \in ON$ et $\operatorname{im}(f) \subseteq ON$.

- ▶ Si $\operatorname{dom}(f) = 0$ alors $y = H(f) = \mu_0 \in ON$.
- ▶ Si $\operatorname{dom}(f) = S(\beta)$ avec β un ordinal, alors $y = H(f) = G\big(f(\beta)\big) \in \operatorname{im}(G)$.
  Or par définition $G : ON \longrightarrow ON$ donc $\operatorname{im}(G) \subseteq ON$ et donc $y \in ON$.
- ▶ Si $\operatorname{dom}(f)$ est un ordinal limite non nul γ alors $y = H(f) = \sup\limits_{\delta\in\gamma} f(\delta)$.
  Or $\operatorname{im}(f) \subseteq ON$ donc $\operatorname{im}(f) = \big\{f(\delta) \;\big|\; \delta \in \gamma\big\}$ est un ensemble d'ordinaux.
  Donc y sa borne supérieure est un ordinal.

Dans tous les cas, on a bien $y \in ON$.

Donc $\forall y \in \operatorname{im}(H), y \in ON$, si bien que $\operatorname{im}(H) \subseteq ON$.

• Montrons que H vérifie l'hypothèse du théorème 6 page 72.

Soient α un ordinal et $f : \alpha \longrightarrow ?$ une application H-inductive.

On sait déjà que $\operatorname{dom}(f) = \alpha$ est un ordinal.

Il suffit donc de montrer que $\operatorname{im}(f) \subseteq ON$.

Soit $y \in \mathrm{im}(f)$.
Il existe donc $\beta \in \alpha$ tel que $y = f(\beta)$.
Or f est H-inductive par définition.
On a donc $f_{|\beta} \in \mathrm{dom}(H)$ et $y = f(\beta) = H(f_{|\beta}) \in \mathrm{im}(H)$.
Or on a dit que $\mathrm{im}(H) \subseteq ON$ donc $y \in ON$.
On a donc $\forall y \in \mathrm{im}(f), y \in ON$ donc $\mathrm{im}(f) \subseteq ON$.
Ainsi on a $\mathrm{dom}(f) \in ON$ et $\mathrm{im}(f) \subseteq ON$ donc $f \in \mathrm{dom}(H)$.
Ainsi pour tout $\alpha \in ON$ et toute application $f : \alpha \longrightarrow ?$, si f est H-inductive alors $f \in \mathrm{dom}(H)$. Donc H et $C = ON$ vérifient l'hypothèse du théorème 6 page 72.

• Il existe donc une unique assertion fonctionnelle $F : ON \longrightarrow ?$ qui est H-inductive.
Par définition de la H-inductivité et par définition de H, on a alors

$$\begin{cases} F(0) = H(F_{|0}) = \mu_0 \\ F\big(S(\beta)\big) = H(F_{|S(\beta)}) = G\big(F_{|S(\beta)}(\beta)\big) = G\big(F(\beta)\big) \text{ pour tout ordinal } \beta \\ F(\gamma) = H(F_{|\gamma}) = \sup\limits_{\beta\in\gamma} F_{|\gamma}(\beta) = \sup\limits_{\delta\in\gamma} F(\delta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

Ainsi $\boxed{F \text{ vérifie les conditions de l'énoncé}}$.
Remarquons que comme $\mathrm{im}(H) \subseteq ON$ et comme par définition on a $\mathrm{im}(F) \subseteq \mathrm{im}(H)$, on a donc $\mathrm{im}(F) \subseteq ON$ et donc on a bien $F : ON \longrightarrow ON$.

Unicité
Soit $F' : ON \longrightarrow ON$ une assertion fonctionnelle vérifiant les conditions de l'énoncé.
Montrons par induction transfinie que $F = F'$.
Considérons alors l'assertion à paramètres P définie pour tout ordinal α par

$$P(\beta) \iff F(\beta) = F'(\beta)$$

▶ *Initialisation*
On a $F(0) = \mu_0 = F'(0)$ donc $P(0)$ est vraie.

▶ *Hérédité*
Soit α un ordinal tel que $P(\alpha)$.
On a donc $F(\alpha) = F'(\alpha)$.
Donc $F\big(S(\alpha)\big) = G\big(F(\alpha)\big) = G\big(F'(\alpha)\big) = F'\big(S(\alpha)\big)$.
On a donc $P\big(S(\alpha)\big)$.
Donc pour tout ordinal α, on a $P(\alpha) \implies P\big(S(\alpha)\big)$.

▶ *Hérédité limite*

Soit α un ordinal limite non nul tel que $\forall \beta \in \alpha, P(\beta)$.

On a donc $\forall \beta \in \alpha, F(\beta) = F'(\beta)$.

Donc $F(\alpha) = \sup\limits_{\beta \in \alpha} F(\beta) = \sup\limits_{\beta \in \alpha} F'(\beta) = F'(\alpha)$.

On a donc $P(\alpha)$.

Donc pour tout ordinal limite non nul α, on a $\Big(\forall \beta \in \alpha, P(\beta)\Big) \implies P(\alpha)$.

Ainsi P vérifie les trois hypothèses du principe faible d'induction transfinie.

Donc pour tout ordinal α, on a $P(\alpha)$, c'est-à-dire $F(\alpha) = F'(\alpha)$.

Ainsi on a $F = F'$, $\boxed{\text{d'où l'unicité}}$.

CQFD.

2 Addition d'ordinaux

2.1 Définition et propriétés

Nous pouvons enfin définir l'addition sur les ordinaux.

Définition 17 (Addition d'ordinaux)

Soit α un ordinal.
On pose

$$\begin{cases} \alpha + 0 := \alpha \\ \alpha + S(\beta) := S(\alpha + \beta) \text{ pour tout ordinal } \beta \\ \alpha + \gamma := \sup\limits_{\beta \in \gamma}(\alpha + \beta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

Remarque :
Pour justifier proprement que cette définition a du sens, on utilise simplement la proposition 32 page 91 qui précède, en posant $\mu_0 := \alpha$ et $G(\xi) := S(\xi)$ pour tout ordinal ξ. La proposition nous donne alors une assertion fonctionnelle F_α telle que

$$\begin{cases} F_\alpha(0) := \alpha \\ F_\alpha\big(S(\beta)\big) := S\big(F_\alpha(\beta)\big) \text{ pour tout ordinal } \beta \\ F_\alpha(\gamma) := \sup\limits_{\beta \in \gamma} F_\alpha(\beta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

et on pose alors $\alpha + \beta := F_\alpha(\beta)$ pour tout ordinal β.

Nous affirmons depuis des pages et des pages que pour un entier naturel n, on va définir $n+1$ comme étant $S(n)$. En fait comme n et 1 sont des cas particuliers d'ordinaux, on a déjà donné du sens à $n+1$, et on retombe bien sur $S(n)$. Plus généralement, on a la proposition suivante.

Proposition 33 (Successeur et plus un)

Soit α un ordinal.
On a $S(\alpha) = \alpha + 1$.

Démonstration

Remarquons que par définition de l'addition, on a $\alpha + 0 = \alpha$.

On a donc les égalités suivantes :

$$\alpha + 1 = \alpha + S(0) \text{ par définition de } 1$$

$$= S(\alpha + 0) \text{ par définition de l'addition}$$
$$= S(\alpha) \text{ puisque } \alpha + 0 = \alpha$$

On a donc $\boxed{\alpha + 1 = S(\alpha)}$
CQFD.

Proposition 34 (0 est neutre pour l'addition des ordinaux)

Pour tout ordinal α, on a $\alpha + 0 = \alpha = 0 + \alpha$.
On dit que 0 est **neutre** pour l'addition des ordinaux.

Démonstration

Par définition de l'addition, on sait déjà que pour tout ordinal α on a $\alpha + 0 = \alpha$.

Montrons l'autre égalité par induction.

Considérons P l'assertion à paramètre définie pour tout ordinal α par

$$P(\alpha) \iff 0 + \alpha = \alpha$$

▶ *Initialisation*

Par définition de l'addition on a $0 + 0 = 0$ donc on a $P(0)$.

▶ *Hérédité*

Soit α un ordinal tel que $P(\alpha)$.

Autrement dit on a $0 + \alpha = \alpha$.

On a alors par définition de l'addition $0 + S(\alpha) = S(0 + \alpha) = S(\alpha)$.

On a donc $P\big(S(\alpha)\big)$.

Donc pour tout ordinal α, si $P(\alpha)$ alors $P\big(S(\alpha)\big)$.

▶ *Hérédité limite*

Soit α un ordinal limite non nul tel que $\forall \beta \in \alpha, P(\beta)$.

Autrement dit pour tout $\beta \in \alpha$, on a $0 + \beta = \beta$.

On a alors par définition de l'addition $0 + \alpha = \sup\limits_{\beta \in \alpha}(0 + \beta) = \sup\limits_{\beta \in \alpha} \beta$.

Or α est un ordinal limite donc $\sup\limits_{\beta \in \alpha} \beta = \sup(\alpha) = \alpha$ d'après la prop. 20 p. 47.

On a donc $0 + \alpha = \alpha$ et donc $P(\alpha)$.

Donc pour tout ordinal limite non nul α, si $\forall \beta \in \alpha, P(\beta)$ alors $P(\alpha)$.

Ainsi P vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal α on a $P(\alpha)$.

Autrement dit pour tout ordinal α on a $\boxed{0 + \alpha = \alpha}$.

CQFD.

Proposition 35 (Addition de deux entiers naturels)

Pour tout entiers naturels n et m, l'ordinal $n + m$ est un entier naturel.
On dit que $\mathbb{N} = \omega$ est **stable par addition**.

Démonstration

Fixons n un entier naturel.

Soit P l'assertion à paramètre définie pour tout entier naturel m par

$$P(m) \iff n + m \in \mathbb{N}$$

Raisonnons par induction sur les entiers naturels.

► *Initialisation*

Par définition de l'addition on a $n + 0 = n$.

Or n est un entier naturel par définition.

Donc $n + 0$ est un entier naturel.

On a donc $P(0)$.

► *Hérédité*

Soit m un entier naturel tel que $P(m)$.

Autrement dit $n + m$ est un entier naturel.

Donc $S(n + m)$ est un entier naturel d'après la proposition 14 page 38.

Or $n + S(m) = S(n + m)$ par définition de l'addition.

Donc $n + S(m)$ est un entier naturel.

Autrement dit on a $P\big(S(m)\big)$.

Donc pour tout entier naturel m, si $P(m)$ alors $P\big(S(m)\big)$.

Ainsi P vérifie les deux conditions de l'induction chez les entiers naturels.

Donc pour tout entier naturel m, on a $P(m)$.

Autrement dit, $\boxed{\text{pour tout entier naturel } m,\ n + m \text{ est un entier naturel}}$.

CQFD.

Proposition 36 (Croissance de l'addition des ordinaux)

Soient α, β et γ trois ordinaux.

1. Si $\beta \in \gamma$ alors $\alpha + \beta \in \alpha + \gamma$.
   On dit que l'addition à gauche est **strictement croissante**.
2. Si $\beta \subseteq \gamma$ alors $\alpha + \beta \subseteq \alpha + \gamma$.
   On dit que l'addition à gauche est **croissante**.
3. Si $\beta \subseteq \gamma$ alors $\beta + \alpha \subseteq \gamma + \alpha$.
   On dit que l'addition à droite est **croissante**.

Démonstration

1. Fixons α et β.

Posons $P_{\alpha,\beta}$ l'assertion à paramètre définie pour tout ordinal γ par

$$P_{\alpha,\beta}(\gamma) \iff \Big(\beta \in \gamma \Rightarrow \alpha + \beta \in \alpha + \gamma\Big)$$

Montrons le résultat par le principe faible d'induction.

► *Initialisation*

La prémisse $\beta \in 0$ étant fausse, on a l'implication $\beta \in 0 \Rightarrow \alpha + \beta \in \alpha + 0$.

Ainsi on a $P_{\alpha,\beta}(0)$.

► *Hérédité*

Soit γ un ordinal tel que $P_{\alpha,\beta}(\gamma)$.

Ainsi on a $\beta \in \gamma \Rightarrow \alpha + \beta \in \alpha + \gamma$.

Supposons que $\beta \in S(\gamma)$.

On a alors $\beta \subseteq \gamma$ d'après la proposition 12 page 33.

On a donc $\beta \in \gamma$ ou $\beta = \gamma$ d'après la proposition 8 page 20.

- Plaçons-nous dans le cas où $\beta \in \gamma$.
  On a alors $\alpha + \beta \in \alpha + \gamma$ d'après $P_{\alpha,\beta}(\gamma)$.
  Or on a $\alpha + \gamma \in S(\alpha + \gamma)$ d'après la proposition 12 page 33.
  On a donc $\alpha + \beta \in S(\alpha + \gamma)$ par transitivité de $\in$ sur ON.
- Plaçons-nous dans le cas où $\beta = \gamma$.
  On a donc $\alpha + \beta = \alpha + \gamma$.
  Or on a $\alpha + \gamma \in S(\alpha + \gamma)$ d'après la proposition 12 page 33.
  On a donc $\alpha + \beta \in S(\alpha + \gamma)$.

Ainsi dans les deux cas on a $\alpha + \beta \in S(\alpha + \gamma)$.

Or par définition de l'addition on a $S(\alpha + \gamma) = \alpha + S(\gamma)$.

On a donc $\alpha + \beta \in \alpha + S(\gamma)$.

Donc si $\beta \in S(\gamma)$ alors $\alpha + \beta \in \alpha + S(\gamma)$.

Ainsi on a $P_{\alpha,\beta}\big(S(\gamma)\big)$.

Donc pour tout ordinal γ on a $P_{\alpha,\beta}(\gamma) \implies P_{\alpha,\beta}\big(S(\gamma)\big)$.

▶ *Hérédité limite*

Soit γ un ordinal limite non nul tel que $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$.

Supposons que $\beta \in \gamma$.

On a alors $S(\beta) \in \gamma$ d'après la proposition 13 page 37.

Or par hypothèse on a $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$ donc $P_{\alpha,\beta}\big(S(\beta)\big)$.

Autrement dit on a $\beta \in S(\beta) \implies \alpha + \beta \in \alpha + S(\beta)$.

Or on a $\beta \in S(\beta)$ d'après la proposition 12 page 33.

On a donc $\alpha + \beta \in \alpha + S(\beta)$ par modus ponens.

Or on a $S(\beta) \in \gamma$ donc $\alpha + S(\beta) \in \{\alpha + \delta \mid \delta \in \gamma\}$.

Donc $\alpha + S(\beta) \subseteq \sup\limits_{\delta \in \gamma}(\alpha + \delta)$ par définition de la borne supérieure.

Comme $\alpha + \beta \in \alpha + S(\beta)$ on a $\alpha + \beta \in \sup\limits_{\delta \in \gamma}(\alpha + \delta)$ par transitivité.

Or γ est un ordinal limite non nul donc $\alpha + \gamma = \sup\limits_{\delta \in \gamma}(\alpha + \delta)$ par définition de l'addition. On a donc $\alpha + \beta \in \alpha + \gamma$.

Donc si $\beta \in \gamma$ alors $\alpha + \beta \in \alpha + \gamma$.

Autrement dit on a $P_{\alpha,\beta}(\gamma)$.

Donc pour tout ordinal limite non nul γ, si $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$ alors $P_{\alpha,\beta}(\gamma)$.

Ainsi $P_{\alpha,\beta}$ vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal γ on a $P_{\alpha,\beta}(\gamma)$.

Autrement dit, $\boxed{\text{pour tout ordinal } \gamma \text{ on a } \beta \in \gamma \Rightarrow \alpha + \beta \in \alpha + \gamma}$.

2. Supposons que $\beta \subseteq \gamma$.

On a donc $\beta \in \gamma$ ou $\beta = \gamma$ d'après la proposition 8 page 20.

- ▶ Plaçons-nous dans le cas où $\beta \in \gamma$.

  On a donc $\alpha + \beta \in \alpha + \gamma$ d'après 1.

  On a en particulier $\alpha + \beta \subseteq \alpha + \gamma$ d'après la proposition 8 page 20.

- ▶ Plaçons-nous dans le cas où $\beta = \gamma$.

  On a alors $\alpha + \beta = \alpha + \gamma$.

  En particulier on a $\alpha + \beta \subseteq \alpha + \gamma$.

Dans les deux cas on a donc $\boxed{\alpha + \beta \subseteq \alpha + \gamma}$.

3. Fixons β et γ.

Posons $Q_{\beta,\gamma}$ l'assertion à paramètre définie pour tout ordinal α par

$$Q_{\beta,\gamma}(\alpha) \iff \Big(\beta \subseteq \gamma \Rightarrow \beta + \alpha \subseteq \gamma + \alpha\Big)$$

Montrons le résultat par le principe faible d'induction.

► *Initialisation*

On a $\beta + 0 = \beta$ et $\gamma + 0 = \gamma$ par définition de l'addition.

On a donc l'implication $\beta \subseteq \gamma \implies \beta + 0 \subseteq \gamma + 0$.

Autrement dit on a $Q_{\beta,\gamma}(0)$.

► *Hérédité*

Soit α un ordinal tel que $Q_{\beta,\gamma}(\alpha)$.

Autrement dit on a l'implication $\beta \subseteq \gamma \Rightarrow \beta + \alpha \subseteq \gamma + \alpha$.

Supposons que $\beta \subseteq \gamma$.

Par modus ponens on a donc $\beta + \alpha \subseteq \gamma + \alpha$ par ce qui précède.

On a donc $\beta + \alpha \in \gamma + \alpha$ ou $\beta + \alpha = \gamma + \alpha$ d'après la prop. 8 p. 20.

- Plaçons-nous dans le cas où $\beta + \alpha \in \gamma + \alpha$.
  On a donc $S(\beta + \alpha) \subseteq \gamma + \alpha$ d'après la proposition 12 page 33.
  Or on a $\gamma + \alpha \in S(\gamma + \alpha)$ toujours d'après cette même proposition.
  On a donc $S(\beta + \alpha) \in S(\gamma + \alpha)$ par transitivité chez les ordinaux.
  En particulier on a $S(\beta + \alpha) \subseteq S(\gamma + \alpha)$ d'après la prop. 8 p. 20.

- Plaçons-nous dans le cas où $\beta + \alpha = \gamma + \alpha$.
  On a donc $S(\beta + \alpha) = S(\gamma + \alpha)$.
  En particulier on a $S(\beta + \alpha) \subseteq S(\gamma + \alpha)$.

Dans les deux cas on a $S(\beta + \alpha) \subseteq S(\gamma + \alpha)$.

Or on a $S(\beta + \alpha) = \beta + S(\alpha)$ et $S(\gamma + \alpha) = \gamma + S(\alpha)$ par définition de l'addition. On a donc $\beta + S(\alpha) \subseteq \gamma + S(\alpha)$.

Donc si $\beta \subseteq \gamma$ alors $\beta + S(\alpha) \subseteq \gamma + S(\alpha)$.

Autrement dit on a $Q_{\beta,\gamma}\big(S(\alpha)\big)$.

Donc pour tout ordinal α, si $Q_{\beta,\gamma}(\alpha)$ alors $Q_{\beta,\gamma}\big(S(\alpha)\big)$.

► *Hérédité limite*

Soit α un ordinal limite non nul tel que $\forall \delta \in \alpha, Q_{\beta,\gamma}(\delta)$.

Autrement dit pour tout $\delta \in \alpha$ on a $\beta \subseteq \gamma \Rightarrow \beta + \delta \subseteq \gamma + \delta$.

Supposons que $\beta \subseteq \gamma$.

Par modus ponens pour tout $\delta \in \alpha$ on a $\beta + \delta \subseteq \gamma + \delta$.

Soit $\delta \in \alpha$.

D'après ce qui précède on a $\beta + \delta \subseteq \gamma + \delta$.

Or $\gamma + \delta \in \{\gamma + \varepsilon \mid \varepsilon \in \alpha\}$.

Donc $\gamma + \delta \subseteq \sup\limits_{\varepsilon \in \alpha}(\gamma + \varepsilon)$ par définition de la borne supérieure.

Or on a $\gamma + \alpha = \sup\limits_{\varepsilon \in \alpha}(\gamma + \varepsilon)$ par définition de l'addition.

On a donc $\gamma + \delta \subseteq \gamma + \alpha$.

On a donc $\beta + \delta \subseteq \gamma + \alpha$ par transitivité de l'inclusion.

Donc pour tout $\delta \in \alpha$ on a $\beta + \delta \subseteq \gamma + \alpha$.

Ainsi $\gamma + \alpha$ est un majorant de $\{\beta + \delta \mid \delta \in \alpha\}$.

On a donc $\sup\limits_{\delta \in \alpha}(\beta + \delta) \subseteq \gamma + \alpha$ par minimalité de la borne supérieure.

Or on a $\beta + \alpha = \sup\limits_{\delta \in \alpha}(\beta + \delta)$ par définition de l'addition.

On a donc $\beta + \alpha \subseteq \gamma + \alpha$.

Donc si $\beta \subseteq \gamma$ alors $\beta + \alpha \subseteq \gamma + \alpha$.

Autrement dit, on a $Q_{\beta,\gamma}(\alpha)$.

Donc pour tout ordinal limite non nul α, si $\forall \delta \in \alpha, Q_{\beta,\gamma}(\delta)$ alors $Q_{\beta,\gamma}(\alpha)$.

Ainsi $Q_{\beta,\gamma}$ vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal α on a $Q_{\beta,\gamma}(\alpha)$.

Autrement dit pour tout ordinal α on a $\boxed{\beta \subseteq \gamma \implies \beta + \alpha \subseteq \gamma + \alpha}$.

CQFD.

Remarque :

1. En particulier si $\beta \subseteq \gamma$ alors $\beta + 1 \subseteq \gamma + 1$ donc $S(\beta) \subseteq S(\gamma)$ d'après la proposition 33 page 94.
2. Soit $n \in \omega$.
   Pour tout $m \in \omega$, on a $n + m \in \omega$ par stabilité de ω pour l'addition.
   On a donc $\sup\limits_{m \in \omega}(n + m) \subseteq \omega$ par minimalité de la borne supérieure.
   On a donc :

$$\begin{aligned} \omega &= 0 + \omega \text{ par neutralité de } 0 \text{ pour l'addition} \\ &\subseteq n + \omega \text{ par croissance de l'addition} \\ &= \sup_{m \in \omega}(n + m) \text{ par définition de l'addition} \\ &\subseteq \omega \text{ par ce qui précède} \end{aligned}$$

   Ainsi on a $\omega \subseteq n + \omega \subseteq \omega$ et donc $n + \omega = \omega$.
   En particulier si n est non nul, on a $0 \in n$ et donc $\omega = \omega + 0 \in \omega + n$ par stricte croissance de l'addition à gauche. Cela implique que $\omega \neq \omega + n$, et donc $n + \omega \neq \omega + n$.
   Surprise, l'addition des ordinaux n'est pas commutative !
   Heureusement, nous verrons plus tard qu'elle l'est chez les entiers naturels !

Le fait que par exemple $1+\omega=\omega$ ne doit pas nous surprendre pour autant ! En effet, $1+\omega$ est défini comme la borne supérieure de l'ensemble $\{1+0;1+1;1+2;\ldots\}=\{1;2;3;\}$ et c'est bien de ω dont il s'agit. La même idée peut être appliquer pour expliquer que $n+\omega=\omega$.

Proposition 37 (Régularité de l'addition des ordinaux)

Soient α, β et γ trois ordinaux.
Si $\alpha+\beta=\alpha+\gamma$ alors $\beta=\gamma$.
On dit que l'addition à gauche des ordinaux est **régulière**.

Démonstration

Montrons-le par contraposition.

Supposons que $\beta\neq\gamma$.

On a donc $\beta\in\gamma$ ou $\gamma\in\beta$ d'après le théorème 1 page 21.

Si $\beta\in\gamma$ alors $\alpha+\beta\in\alpha+\gamma$ d'après la proposition 36 page 97.

Si $\gamma\in\beta$ alors $\alpha+\gamma\in\alpha+\beta$ d'après la proposition 36 page 97.

Dans les deux cas on a $\alpha+\beta\neq\alpha+\gamma$.

Donc si $\beta\neq\gamma$ alors $\alpha+\beta\neq\alpha+\gamma$.

Par contraposition $\boxed{\text{si } \alpha+\beta=\alpha+\gamma \text{ alors } \beta=\gamma}$.

CQFD.

Remarque :
Malheureusement l'addition à droite n'est pas régulière.
En effet on a montré lors d'une précédente remarque que $1+\omega=\omega=2+\omega$, alors que l'on n'a pas $1=2$.

Dans la définition de l'addition, si γ est un ordinal limite non nul alors $\alpha+\gamma=\sup\limits_{\delta\in\gamma}(\alpha+\delta)$. Or un ordinal limite est lui-même sa propre borne supérieure $\gamma=\sup\limits_{\delta\in\gamma}\delta$ d'après la proposition 20 page 47, si bien que l'on a en fait $\alpha+\sup\limits_{\delta\in\gamma}\delta=\sup\limits_{\delta\in\gamma}(\alpha+\delta)$. Ainsi l'addition à gauche commute avec la borne supérieure. Nous verrons que c'est vrai même pour la borne supérieure d'un ensemble qui n'est pas lui-même un ordinal. Pour l'heure, généralisons ce concept avec la définition qui suit.

Définition 18 (Assertion fonctionnelle croissante continue)

Soit $F:ON\longrightarrow ON$ une assertion fonctionnelle.

1. On dit que F est **croissante** si et seulement si pour tout ordinaux α et β,

$$\alpha\subseteq\beta\implies F(\alpha)\subseteq F(\beta)$$

2. Supposons que F est croissante.
   On dit que F est **continue** si et seulement si pour tout ensemble d'ordinaux non vide X,
$$F\big(\sup(X)\big) = \sup\big(F^{\rightarrow}(X)\big)$$

Le point 2 de cette définition est bien une généralisation de ce que nous avons vu juste avant : cela dit que $F\left(\sup\limits_{\xi \in X} \xi\right) = \sup\limits_{\xi \in X} F(\xi)$.

Pourquoi cette propriété s'appelle-t-elle *continuité* ? Parce qu'elle rappelle ce qu'il se passe dans le cadre de l'analyse : par exemple pour $f : \mathbb{R} \longrightarrow \mathbb{R}$ une application croissante, f est *continue* (à gauche) en $a \in \mathbb{R}$ si et seulement si $f\left(\lim\limits_{x<a} x\right) = \lim\limits_{x<a} f(x)$.

Il s'avère qu'en fait on peut affaiblir cette condition et quand-même retrouver la continuité en question : en la demandant seulement sur les ordinaux limites, on la retrouve partout.

Proposition 38 (Caractérisation de continuité)

Soit $F : ON \longrightarrow ON$ une assertion fonctionnelle **croissante**.
Les assertions suivantes sont équivalentes :

1. F est continue.
2. Pour tout ordinal limite non nul γ, on a $F(\gamma) = \sup\limits_{\delta \in \gamma} F(\delta)$.

Démonstration

$\boxed{1 \Rightarrow 2}$

Supposons que F est continue.

Par définition pour tout ensemble non vide d'ordinaux X, on a $F\left(\sup\limits_{\xi \in X} \xi\right) = \sup\limits_{\xi \in X} F(\xi)$.

Soit γ un ordinal limite non nul.

On a donc $F\left(\sup\limits_{\delta \in \gamma} \delta\right) = \sup\limits_{\delta \in \gamma} F(\delta)$.

Or γ est un ordinal limite.

On a donc $\sup\limits_{\delta \in \gamma} \delta = \sup(\gamma) = \gamma$ d'après la proposition 20 page 47.

On a donc $F(\gamma) = \sup\limits_{\delta \in \gamma} F(\delta)$.

Donc $\boxed{\text{pour tout ordinal limite non nul } \gamma, \text{ on a } F(\gamma) = \sup\limits_{\delta \in \gamma} F(\delta)}$.

$\boxed{1 \Leftarrow 2}$

Supposons que pour tout ordinal limite non nul γ on a $F(\gamma) = \sup\limits_{\delta \in \gamma} F(\delta)$.

Soit X un ensemble non vide d'ordinaux.

Montrons que $F\big(\sup(X)\big) = \sup\big(F^{\rightarrow}(X)\big)$.

Rappelons-nous la chose suivante : comme X est un ensemble, $F^{\rightarrow}(X) = \big\{F(\xi) \,\big|\, \xi \in X\big\}$ est aussi un ensemble d'après le schéma d'axiome de remplacement.

C'est bien un ensemble d'ordinaux car F est à valeurs dans ON.

Raisonnons par double inclusions.

$\boxed{\subseteq}$

• Plaçons-nous dans le cas où $\sup(X) \in X$.

Alors $F\big(\sup(X)\big) \in F^{\rightarrow}(X)$ par définition de l'image directe.

On a donc $F\big(\sup(X)\big) \subseteq \sup\big(F^{\rightarrow}(X)\big)$ car la borne supérieure est un majorant.

• Plaçons-nous dans le cas où $\sup(X) \notin X$.

Alors $\sup(X)$ est un ordinal limite d'après la proposition 19 page 46.

Supposons par l'absurde que $\sup(X) = 0$.

Comme $\sup(X)$ est un majorant de X, on a $\forall \xi \in X, \xi \subseteq \sup(X)$.

Comme $\sup(X) = 0 = \varnothing$, on a $\forall \xi \in X, \xi = \sup(X)$.

Comme X est non vide, on a donc $X = \big\{\sup(X)\big\}$ et donc $\sup(X) \in X$.

C'est absurde puisqu'on a supposé que $\sup(X) \notin X$.

Donc $\sup(X)$ est un ordinal limite non nul.

Donc par hypothèse on a $F\big(\sup(X)\big) = \sup\limits_{\delta \in \sup(X)} F(\delta)$.

Montrons donc que $\sup\limits_{\delta \in \sup(X)} F(\delta) \subseteq \sup\big(F^{\rightarrow}(X)\big)$.

Soit $\delta \in \sup(X)$.

Par définition $\sup(X)$ est le plus petit majorant de X.

Donc δ n'est pas un majorant de X.

Il existe donc $\xi \in X$ tel que $\delta \subseteq \xi$.

Par croissance de F on a donc $F(\delta) \subseteq F(\xi)$.

Or $\xi \in X$ donc $F(\xi) \in F^{\rightarrow}(X)$ et donc $F(\xi) \subseteq \sup\big(F^{\rightarrow}(X)\big)$.

Par transitivité de l'inclusion on a donc $F(\delta) \subseteq \sup\big(F^{\rightarrow}(X)\big)$.

Donc $\forall \delta \in \sup(X), F(\delta) \subseteq \sup\big(F^{\rightarrow}(X)\big)$.

Donc $\sup\limits_{\delta \in \sup(X)} F(\delta) \subseteq \sup\big(F^{\rightarrow}(X)\big)$ par minimalité de la borne supérieure.

On a donc $F\big(\sup(X)\big) \subseteq \sup\big(F^{\rightarrow}(X)\big)$ d'après ce qui précède.

Ainsi dans les deux cas on a $\boxed{F\big(\sup(X)\big) \subseteq \sup\big(F^{\rightarrow}(X)\big)}$.

$\boxed{\supseteq}$

Soit $\mu \in F^{\rightarrow}(X)$.

Par définition il existe $\xi \in X$ tel que $\mu = F(\xi)$.

On a $\xi \subseteq \sup(X)$ car la borne supérieure est un majorant.

On a donc $F(\xi) \subseteq F\big(\sup(X)\big)$ par croissance de F.

On a donc $\mu \subseteq F\big(\sup(X)\big)$ par définition de ξ.

Donc pour tout $\mu \in F^{\rightarrow}(X)$, on a $\mu \subseteq F\big(\sup(X)\big)$.

Donc $\boxed{\sup(F^{\rightarrow}(X)) \subseteq F\big(\sup(X)\big)}$ par minimalité de la borne supérieure.

Finalement on a bien $\boxed{F\big(\sup(X)\big) = \sup\big(F^{\rightarrow}(X)\big)}$.

CQFD.

Ce que l'on vient de dire s'applique en particulier à l'addition qui vérifie bien la condition sur les ordinaux limites non vides. Ainsi l'addition à gauche est continue.

Proposition 39 (Continuité de l'addition des ordinaux)

Soient α un ordinal et X un ensemble non vide d'ordinaux.
On a $\sup_{\xi \in X}(\alpha + \xi) = \alpha + \sup_{\xi \in X} \xi$.
Autrement dit l'addition à gauche est continue.

Démonstration

Par définition de l'addition, pour tout ordinal limite non nul γ, on a

$$\alpha + \gamma = \sup_{\delta \in \gamma}(\alpha + \delta)$$

On peut alors appliquer la proposition 38 page 102 pour conclure.

CQFD.

Remarque :
Malheureusement l'addition à droite n'est pas continue.
En effet, prenons $X = \omega = \alpha$.
On sait que ω est un ordinal limite d'après la proposition 17 page 43.
On a donc $\sup_{n \in \omega} n = \omega$ d'après la proposition 20 page 47.
Or on a montré que pour tout $n \in \omega$, on a $n + \omega = \omega$.
On a donc $\sup_{n \in \omega}(n + \omega) = \sup_{n \in \omega} \omega = \omega$ tandis que $\left(\sup_{n \in \omega} n\right) + \omega = \omega + \omega$.
Or $\omega \underset{12\text{ p. }33}{\in} S(\omega) \underset{33\text{ p. }94}{=} \omega + 1 \subseteq \sup_{n \in \omega}(\omega + n) = \omega + \omega$.
On a donc $\omega \neq \omega + \omega$ et donc $\sup_{n \in \omega}(n + \omega) \neq \left(\sup_{n \in \omega} n\right) + \omega$.

Proposition 40 (Associativité de l'addition des ordinaux)

Pour tout ordinaux α, β et γ, on a l'égalité

$$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$$

On dit que l'addition des ordinaux est **associative**.

Démonstration

Montrons-le à l'aide du principe faible d'induction transfinie.

Fixons α et β deux ordinaux.

Posons $P_{\alpha,\beta}$ l'assertion à paramètre définie pour tout ordinal γ par

$$P_{\alpha,\beta}(\gamma) \iff (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$$

► *Initialisation*

Par définition de l'addition on a $(\alpha+\beta)+0=\alpha+\beta$.

De même, par définition de l'addition on a $\beta+0=\beta$ donc $\alpha+(\beta+0)=\alpha+\beta$.

On a donc $(\alpha+\beta)+0=\alpha+(\beta+0)$.

On a donc $P_{\alpha,\beta}(0)$.

► *Hérédité*

Soit γ un ordinal tel que $P_{\alpha,\beta}(\gamma)$.

On a donc $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$.

On a alors

$$\begin{aligned}(\alpha+\beta)+S(\gamma) &= S\big((\alpha+\beta)+\gamma\big) \text{ par définition de l'addition}\\ &= S\big(\alpha+(\beta+\gamma)\big) \text{ puisqu'on a } P_{\alpha,\beta}(\gamma)\\ &= \alpha+S(\beta+\gamma) \text{ par définition de l'addition}\\ &= \alpha+\big(\beta+S(\gamma)\big) \text{ par définition de l'addition}\end{aligned}$$

Ainsi on a $(\alpha+\beta)+S(\gamma)=\alpha+\big(\beta+S(\gamma)\big)$, c'est-à-dire $P_{\alpha,\beta}\big(S(\gamma)\big)$.

Donc pour tout ordinal γ, on a $P_{\alpha,\beta}(\gamma) \implies P_{\alpha,\beta}\big(S(\gamma)\big)$.

► *Hérédité limite*

Soit γ un ordinal limite non nul tel que $\forall\delta\in\gamma, P_{\alpha,\beta}(\delta)$.

Posons $X:=\{\beta+\delta \mid \delta\in\gamma\}$.

On a alors $\big\{\alpha+(\beta+\delta) \bigm| \delta\in\gamma\big\}=\{\alpha+\xi \mid \xi\in X\}$.

En particulier $\sup\big\{\alpha+(\beta+\delta) \bigm| \delta\in\gamma\big\}=\sup\{\alpha+\xi \mid \xi\in X\} \quad (\star)$.

On en déduit donc que :

$$\begin{aligned}
(\alpha+\beta)+\gamma &= \sup_{\delta\in\gamma}\Big((\alpha+\beta)+\delta\Big) \text{ par définition de l'addition}\\
&= \sup_{\delta\in\gamma}\Big(\alpha+(\beta+\delta)\Big) \text{ puisque } \forall\delta\in\gamma, P_{\alpha,\beta}(\delta)\\
&= \sup_{\xi\in X}(\alpha+\xi) \text{ par } (\star)\\
&= \alpha+\sup_{\xi\in X}\xi \text{ par continuité de l'addition à gauche}\\
&= \alpha+\sup_{\delta\in\gamma}(\beta+\delta) \text{ par définition de } X\\
&= \alpha+(\beta+\gamma) \text{ par définition de l'addition}
\end{aligned}$$

On a donc $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$.

Autrement dit on a $P_{\alpha,\beta}(\gamma)$.

Ainsi pour tout ordinal limite non nul γ, on a $\Big(\forall\delta\in\gamma, P_{\alpha,\beta}(\delta)\Big) \implies P_{\alpha,\beta}(\gamma)$.

Ainsi $P_{\alpha,\beta}$ vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal γ, on a $P_{\alpha,\beta}(\gamma)$.

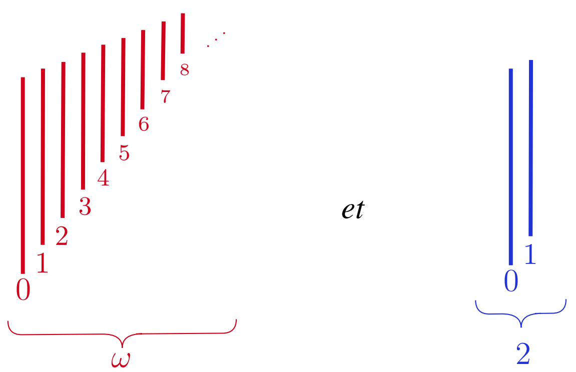
Autrement dit pour tout ordinal γ on a $\boxed{(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)}$.

CQFD.

Remarque :
Désormais pour α, β et γ trois ordinaux, on notera $\alpha+\beta+\gamma$ pour désigner indifféremment $(\alpha+\beta)+\gamma$ et $\alpha+(\beta+\gamma)$, puisqu'il y a égalité.

2.2 Interprétation graphique : la concaténation

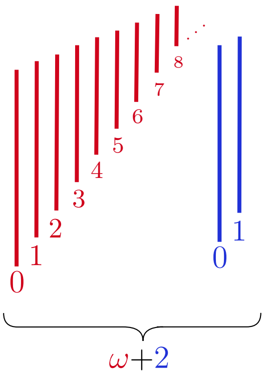
L'addition des ordinaux a une interprétation graphique : visualisons par exemple l'addition des ordinaux ω et 2. Commençons par les représenter tous les deux avec des bâtons indépendemment l'un de l'autre, ω et ses éléments étant en **rouge** et 2 et ses éléments étant en **bleu** :



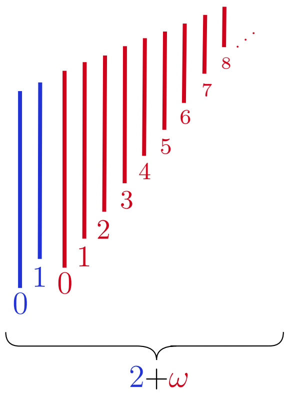
Rappelons qu'ici la taille des bâtons n'a aucune importante, seul leur agencement horizontal importe. Le fait de représenter des bâtons de plus en plus petits est seulement une astuce pour en faire tenir une infinité.

L'interprétation visuelle consiste alors à concaténer les deux ordinaux à additionner, c'est-à-dire à les placer l'un derrière l'autre. Ainsi, on peut les disposer de deux manières :

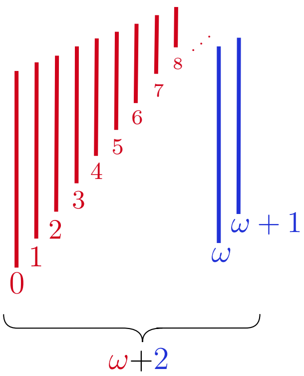
- d'abord ω puis 2 à sa droite, ce qui donne la représentation graphique de $\omega + 2$
- d'abord 2 puis ω à sa droite, ce qui donne la représentation graphique de $2 + \omega$



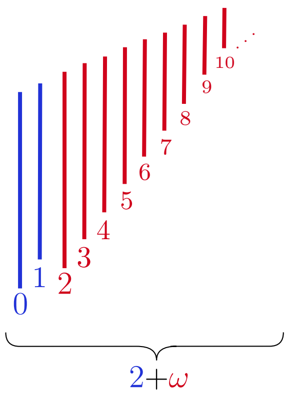
ou alors



On renumérote alors les bâtons en fonction de l'ordre dans lequel ils arrivent, de la gauche vers la droite,



ou alors



ce qui permet ainsi de voir que

- $\omega + 2$ est égal à $\{0, 1, 2, \dots, \omega, \omega + 1\}$ donc est l'ordinal qui vient juste après $\omega + 1$, c'est-à-dire son successeur.
- $2 + \omega$ est égal à $\{0, 1, 2, 3, \dots\}$, c'est-à-dire tout simplement ω lui-même.

On retrouve bien le fait démontré précédemment que $2 + \omega = \omega$ et que $2 + \omega \neq \omega + 2$.

Pour l'heure, cette illustration est là pour nous faire comprendre l'intuition derrière l'addition des ordinaux : cette idée de concaténation va se traduire formellement par la notion d'**union disjointe**.

Définition 19 (Union disjointe de deux ensembles)

Soient A et B deux ensembles.
On appelle **union disjointe** de A et B l'ensemble

$$A \amalg B := \big(\{0\} \times A\big) \cup \big(\{1\} \times B\big)$$

Ainsi les éléments de $A \amalg B$ sont des couples dont la première composante est un élément de $\{0, 1\}$ et la deuxième un élément de $A \cup B$, si bien que $A \amalg B$ est une partie de $\{0, 1\} \times (A \cup B)$. Cependant, on a en plus l'information qu'une première composante égale à 0 correspond à une deuxième composante dans A, et on a le même lien entre 1 et B. De cette manière, les éléments de A « viennent avant » les éléments de B, ce qui traduit bien l'idée intuitive de concaténation que nous avons pu voir illustrée.

Dans le cas où A et B sont munit d'un ordre, voyons comment s'en servir pour construire un ordre sur $A \amalg B$.

Définition 20 (Ordre sur l'union disjointe de deux ensembles)

Soient $(A, \leq)$ et $(B, \preceq)$ deux ensembles ordonnés.
On appelle **ordre de concaténation** sur $A \amalg B$ la relation binaire $\trianglelefteq$ définie pour tout (i, x) et (j, y) dans $A \amalg B$ par

$$(i, x) \trianglelefteq (j, y) \iff \begin{cases} i = 0 \text{ et } j = 1 \\ \text{ou} \\ i = 0 = j \text{ et } x \leq y \\ \text{ou} \\ i = 1 = j \text{ et } x \preceq y \end{cases}$$

Au fond la construction formelle et ensembliste de $A \amalg B$ et son ordre de concaténation associé importe peu. Ce qui nous importe, ce sont les propriétés qu'ils vérifient, au sens où l'intuition qu'on a de la concaténation est respectée. C'est justement l'objet de la proposition qui suit.

Proposition 41 (Caractérisation de la concaténation)

Soient $(A, \leq)$ et $(B, \preceq)$ deux ensembles ordonnés.
Soit $\trianglelefteq$ l'ordre de concaténation associé sur $A \amalg B$.

1. $\trianglelefteq$ est une relation d'ordre sur $A \amalg B$.

Soient $f := \begin{pmatrix} A & \longrightarrow & A \amalg B \\ a & \longmapsto & (0, a) \end{pmatrix}$ et $g := \begin{pmatrix} B & \longrightarrow & A \amalg B \\ b & \longmapsto & (1, b) \end{pmatrix}$.

2. $\mathrm{im}(f) \cup \mathrm{im}(g) = A \amalg B$ et $\mathrm{im}(f) \cap \mathrm{im}(g) = \varnothing$.
3. f et g sont des isomorphismes d'ordre sur leurs images respectives.
4. Pour tout $u \in \mathrm{im}(f)$ et $v \in \mathrm{im}(g)$, on a $u \trianglelefteq v$.
5. $\trianglelefteq$ est l'unique relation d'ordre sur $A \amalg B$ vérifiant simultanément 3 et 4.

Démonstration

1. **Réflexivité**

Soit $(i, x) \in A \amalg B$.

- Supposons que $i = 0$.
  Par définition de $A \amalg B$, on a alors $x \in A$.
  Par réflexivité de $\leq$ sur A, on a $x \leq x$.
  Ainsi ($i = 0 = i$ et $x \leq x$) donc $(i, x) \trianglelefteq (i, x)$ par définition de $\trianglelefteq$.
- On raisonne de la même manière si $i = 1$.

On a donc $(i, x) \trianglelefteq (i, x)$.

Donc $\trianglelefteq$ est réflexive sur $A \amalg B$.

Antisymétrie

Soient (i, x) et (j, y) dans $A \amalg B$.

Supposons que $(i, x) \trianglelefteq (j, y)$ et $(j, y) \trianglelefteq (i, x)$.

- Plaçons-nous dans le cas où $i = 0$ et $j = 1$.
  C'est impossible puisqu'on a $(j, y) \trianglelefteq (i, x)$.
- Plaçons-nous dans le cas où $i = 1$ et $j = 0$.
  C'est impossible puisqu'on a $(i, x) \trianglelefteq (j, y)$.
- Plaçons-nous dans le cas où $i = 0 = j$.
  Par définition de $A \amalg B$, on a alors $x \in A$ et $y \in A$.
  Comme $(i, x) \trianglelefteq (j, y)$, on a $x \leq y$.
  Comme $(j, y) \trianglelefteq (i, x)$, on a $y \leq x$.
  On a donc $x = y$ par antisymétrie de $\leq$.
  Ainsi $i = j$ et $x = y$ donc $(i, x) = (j, y)$.
- Le cas $i = 1 = j$ se traite de la même manière.

Ainsi dans les deux cas possibles on a $(i, x) = (j, y)$.

Donc si $(i, x) \trianglelefteq (j, y)$ et $(j, y) \trianglelefteq (i, x)$ alors $(i, x) = (j, y)$.

Donc $\trianglelefteq$ est antisymétrique.

Transitivité

Soient (i, x), (j, y) et (k, z) dans $A \amalg B$.

Supposons que $(i, x) \trianglelefteq (j, y)$ et $(j, y) \trianglelefteq (k, z)$.

- Plaçons-nous dans le cas où $i = j = k = 0$.
  Par définition de $A \amalg B$, on a alors $x \in A$, $y \in A$ et $z \in A$.
  Comme $(i, x) \trianglelefteq (j, y)$ et $(j, y) \trianglelefteq (k, z)$, on a $x \leq y$ et $y \leq z$.

On a donc $x \leq z$ par transitivité de $\leq$.

Comme $i = 0 = k$ et $x \leq z$, on a $(i, x) \trianglelefteq (k, z)$.

- Le cas $i = j = k = 1$ se traite de la même manière.
- Si $i = 0 = j$ et $k = 1$ alors on a automatiquement $(i, x) \trianglelefteq (k, z)$.
- Si $i = 0$ et $j = 1 = k$ alors on a automatiquement $(i, x) \trianglelefteq (k, z)$.
- Les autres cas sur les valeurs de i, j et k sont impossibles puisque l'on a $(i, x) \trianglelefteq (j, y)$ et $(j, y) \trianglelefteq (k, z)$.

Dans tous les cas, on a nécessairement $(i, x) \trianglelefteq (k, z)$.

Donc si $(i, x) \trianglelefteq (j, y)$ et $(j, y) \trianglelefteq (k, z)$ alors $(i, x) \trianglelefteq (k, z)$.

Donc $\trianglelefteq$ est transitive.

Ainsi $\trianglelefteq$ est réflexive sur $A \amalg B$, est antisymétrique et transitive.

Donc $\boxed{\trianglelefteq \text{ est une relation d'ordre sur } A \amalg B}$.

2. Montrons que $\mathrm{im}(f) \cup \mathrm{im}(g) = A \amalg B$

$\boxed{\subseteq}$

Par définition de f et de g, on a $\mathrm{im}(f) \subseteq A \amalg B$ et $\mathrm{im}(g) \subseteq A \amalg B$.

On a donc $\mathrm{im}(f) \cup \mathrm{im}(g) \subseteq A \amalg B$.

$\boxed{\supseteq}$

Soit $(i, x) \in A \amalg B$.

Par définition de $A \amalg B$, on a $i = 0$ ou $i = 1$.

- Supposons que $i = 0$.
  Par définition de $A \amalg B$, on a alors $x \in A$.
  Alors $(i, x) = f(x) \in \mathrm{im}(f)$ donc $(i, x) \in \mathrm{im}(f) \cup \mathrm{im}(g)$.
- Supposons que $i = 1$.
  Par définition de $A \amalg B$, on a alors $x \in B$.
  Alors $(i, x) = g(x) \in \mathrm{im}(g)$ donc $(i, x) \in \mathrm{im}(f) \cup \mathrm{im}(g)$.

Dans les deux cas, on a $(i, x) \in \mathrm{im}(f) \cup \mathrm{im}(g)$.

Ainsi $\mathrm{im}(f) \cup \mathrm{im}(g) \supseteq A \amalg B$ et donc $\boxed{\mathrm{im}(f) \cup \mathrm{im}(g) = A \amalg B}$.

Montrons que $\mathrm{im}(f) \cap \mathrm{im}(g) = \varnothing$.

Supposons par l'absurde que $\mathrm{im}(f) \cap \mathrm{im}(g) \neq \varnothing$.

Il existe donc $(i, x) \in \mathrm{im}(f) \cap \mathrm{im}(g)$.

Comme $(i, x) \in \mathrm{im}(f)$, il existe $a \in A$ tel que $(i, x) = f(a)$.

Par définition de f, on a $i = 0$.

De même, comme $(i, x) \in \operatorname{im}(g)$, il existe $b \in B$ tel que $(i, x) = g(b)$.

Par définition de g, on a $i = 1$.

Ainsi on a $i = 0$ et $i = 1$, ce qui est absurde.

Par l'absurde, on vient de montrer que $\boxed{\operatorname{im}(f) \cap \operatorname{im}(g) = \varnothing}$.

3. Montrons que f injective.

Soient a et a' dans A.

Supposons que $f(a) = f(a')$.

Par définition de f on a donc $f(a) = (0, a)$ et $f(a') = (0, a')$.

Ainsi on a $(0, a) = (0, a')$ et donc $a = a'$.

Donc si $f(a) = f(a')$ alors $a = a'$.

Donc f est injective.

L'injectivité de g se montre de la même manière.

Montrons que f est croissante.

Soient a et a' dans A.

Supposons que $a \leq a'$.

Ainsi $0 = 0$ et $a \leq a'$ donc $(0, a) \trianglelefteq (0, a')$ par définition de $\trianglelefteq$.

Or $f(a) = (0, a)$ et $f(a') = (0, a')$ par définition de f.

Donc $f(a) \trianglelefteq f(a')$.

Donc si $a \leq a'$ alors $f(a) \trianglelefteq f(a')$.

Donc f est croissante.

La croissance de g se montre de la même manière.

Comme f est injective, $f^{-1} : \operatorname{im}(f) \longrightarrow A$ est bien définie.

Montrons que f^{-1} est croissante.

Soient (i, x) et (j, y) dans $\operatorname{im}(f)$.

Il existe donc a et a' tels que $(i, x) = f(a)$ et $(j, y) = f(a')$.

Par définition de f on a donc $x = a$ et $y = a'$ donc $x \in A$ et $y \in A$.

Par définition de f on a aussi $i = 0 = j$.

Par définition de f^{-1}, on a alors $f^{-1}(i, x) = a = x$ et $f^{-1}(j, y) = a' = y$.

Supposons que $(i, x) \trianglelefteq (j, y)$.

Comme $i = 0 = j$, on a $x \leq y$ par définition de $\trianglelefteq$.

Or on a dit que $f^{-1}(i, x) = x$ et $f^{-1}(j, y) = y$.

On a donc $f^{-1}(i, x) \leq f^{-1}(j, y)$.

Donc si $(i, x) \trianglelefteq (j, y)$ alors $f^{-1}(i, x) \leq f^{-1}(j, y)$.

Donc f^{-1} est croissante.

La croissance de g^{-1} se montre de la même manière.

Ainsi f est injective, f et f^{-1} sont croissantes.
Donc $\boxed{f \text{ est un isomorphisme d'ordre de } \operatorname{dom}(f) \text{ dans } \operatorname{im}(f)}$.
L'isomorphie d'ordre de g de $\operatorname{dom}(g)$ dans $\operatorname{im}(g)$ se montre de la même manière.

4. Soient $u \in \operatorname{im}(f)$ et $v \in \operatorname{im}(g)$.
Il existe alors $a \in A$ et $b \in B$ tels que $u = f(a)$ et $v = g(b)$.
Par définition de f et de g, on a $f(a) = (0, a)$ et $g(b) = (1, b)$.
On a donc $u = (0, a)$ et $v = (1, b)$.
Or on a $(0, a) \trianglelefteq (1, b)$ par définition de $\trianglelefteq$.
On a donc $\boxed{u \trianglelefteq v}$.

5. Soit $\preccurlyeq$ une relation d'ordre sur $A \amalg B$ vérifiant simultanément 3 et 4.
Montrons que pour tout u et v dans $A \amalg B$, on a l'équivalence $u \preccurlyeq v \iff u \trianglelefteq v$.

Soient (i, x) et (j, y) dans $A \amalg B$.

- Plaçons-nous dans le cas où $i = 0 = j$.
  Par définition de $A \amalg B$, on a alors $x \in A$ et $y \in A$.
  Par définition de f, on a alors $(i, x) = f(x)$ et $(j, y) = f(y)$.
  On a donc les équivalences suivantes :

$$\begin{aligned}
(i,x) \preccurlyeq (j,y) &\iff f(x) \preccurlyeq f(y) \\
&\iff x \leq y \text{ car } f \text{ est un isomorphisme d'ordre} \\
&\iff (0,x) \trianglelefteq (0,y) \text{ par définition de } \trianglelefteq \\
&\iff (i,x) \trianglelefteq (j,y) \text{ puisque } i = 0 = j
\end{aligned}$$

  Donc $(i, x) \preccurlyeq (j, y) \iff (i, x) \trianglelefteq (j, y)$.

- Le cas $i = 1 = j$ se traite de la même manière.

- Plaçons-nous dans le cas où $i = 0$ et $j = 1$.
  Par définition de $A \amalg B$ on a alors $x \in A$ et $y \in B$.
  Par définitions de f et g on a alors $f(x) = (i, x)$ et $g(y) = (j, y)$.
  En particulier on a $(i, x) \in \operatorname{im}(f)$ et $(j, y) \in \operatorname{im}(g)$.
  On a donc $(i, x) \trianglelefteq (j, y)$ d'après 4.
  De même, on a $(i, x) \preccurlyeq (j, y)$ puisque $\preccurlyeq$ vérifie 4.
  En particulier on a l'équivalence $(i, x) \preccurlyeq (j, y) \iff (i, x) \trianglelefteq (j, y)$.

- Plaçons-nous dans le cas où $i = 1$ et $j = 0$.

Par définition de $A \amalg B$ on a alors $x \in B$ et $y \in A$.

Par définitions de f et g on a alors $g(x) = (i, x)$ et $f(y) = (j, y)$.

En particulier on a $(j, y) \trianglelefteq (i, x)$ d'après 4.

De même on a $(j, y) \preccurlyeq (i, x)$ puisque $\preccurlyeq$ vérifie 4.

On a donc les équivalences suivantes

$$\begin{aligned}
(i,x) \preccurlyeq (j,y) &\iff (i,x) \preccurlyeq (j,y) \text{ et } (j,y) \preccurlyeq (i,x) \text{ d'après ce qui précède} \\
&\iff (i,x) = (j,y) \text{ par antisymétrie} \\
&\iff (i,x) \trianglelefteq (j,y) \text{ et } (j,y) \trianglelefteq (i,x) \\
&\iff (i,x) \trianglelefteq (j,y) \text{ d'après ce qui précède}
\end{aligned}$$

On a donc bien l'équivalence $(i, x) \preccurlyeq (j, y) \iff (i, x) \trianglelefteq (j, y)$.

Dans tous les cas, on a l'équivalence $(i, x) \preccurlyeq (j, y) \iff (i, x) \trianglelefteq (j, y)$.

Ainsi pour tout u et v dans $A \amalg B$, on a l'équivalence $u \preccurlyeq v \iff u \trianglelefteq v$.

Donc $\preccurlyeq$ et $\trianglelefteq$ sont en fait la même relation d'ordre, $\boxed{\text{d'où l'unicité}}$.

CQFD.

Nous avons formalisé ce qu'était l'opération de concaténation de deux ensembles ordonnés : passer par leur union disjointe et associer à celle-ci l'ordre de concaténation. Il s'avère que si les deux ensembles en question sont bien ordonnés, il en va de même pour leur union disjointe. Heureusement d'ailleurs, puisque notre objectif est d'en tirer un ordinal à la fin (n'oublions pas que l'on s'intéresse à l'addition d'ordinaux !)

Proposition 42 (Concaténation de bons ordres)

Soient $(A, \leq)$ et $(B, \preceq)$ deux ensembles ordonnés.
Soit $\trianglelefteq$ l'ordre de concaténation associé sur $A \amalg B$.

Si $(A, \leq)$ et $(B, \preceq)$ sont bien ordonnés alors $(A \amalg B, \trianglelefteq)$ est bien ordonné.

Démonstration

Supposons que $(A, \leq)$ et $(B, \preceq)$ sont bien ordonnés.

Montrons que toute partie non vide de $A \amalg B$ admet un minimum.

Soit C une partie non vide $A \amalg B$.

- Supposons dans un premier temps qu'il existe $a \in A$ tel que $(0, a) \in C$.

  Considérons alors $E := \{a \in A \mid (0, a) \in C\}$.

  Alors E est donc une partie non vide de A.

  Comme A est bien ordonné, E admet un minimum a_0.

Ainsi on a $(0, a_0) \in C$ par définition de E.

Montrons que $(0, a_0)$ est le minimum de C.

Soit $(i, x) \in C$.

- Plaçons-nous dans le cas où $i = 0$.
  Dans ce cas-là $x \in A$ par définition de $A \amalg B$.
  Donc $x \in A$ est tel que $(0, x) = (i, x) \in C$.
  Alors $x \in E$ par définition de E.
  Donc $a_0 \leq x$ car a_0 est le minimum de E.
  Ainsi ($i = 0$ et $a_0 \leq x$) donc $(0, a_0) \trianglelefteq (i, x)$ par définition de $\trianglelefteq$.
- Plaçons-nous dans le cas où $i = 1$.
  Ainsi $0 = 0$ et $i = 1$ donc $(0, a_0) \trianglelefteq (i, x)$ par définition de $\trianglelefteq$.

Dans tous les cas on a $(0, a_0) \trianglelefteq (i, x)$.

Donc $(0, a_0)$ est le minimum de C.

► Supposons à présent qu'il n'existe pas de $a \in A$ tel que $(0, a) \in C$.

Donc pour tout $(i, x) \in C$, on a $i = 1$ et $x \in B$ par définition de $A \amalg B$.

Posons alors $F := \left\{b \in B \;\middle|\; (1, b) \in C\right\}$.

Comme C est non vide, F est une partie non vide de B.

Or B est bien ordonné donc F admet un minimum b_0.

Ainsi on a $(1, b_0) \in C$ par définition de F.

Montrons que $(1, b_0)$ est le minimum de C.

Soit $(i, x) \in C$.

D'après ce qui précède, on a nécessairement $i = 1$ et $x \in B$.

Ainsi $x \in B$ est tel que $(1, x) = (i, x) \in C$.

Donc $x \in F$ par définition de F.

Donc $b_0 \preceq x$ car b_0 est le minimum de F.

Ainsi ($i = 1$ et $b_0 \preceq x$) donc $(1, b_0) \trianglelefteq (i, x)$ par définition de $\trianglelefteq$.

Donc $(1, b_0)$ est le minimum de C.

Dans les deux cas C admet un minimum.

Donc toute partie non vide de $A \amalg B$ admet un minimum.

Donc $\boxed{A \amalg B \text{ est bien ordonné}}$.

CQFD.

Notation :
Soient E et F deux ensembles ordonnés.
On note $E \cong F$ si et seulement si E et F sont isomorphes.

Proposition 43 (Union disjointe et isomorphismes)

1. Soient A_0, A_1, B_0 et B_1 quatre ensembles ordonnés.
   Si $A_0 \cong B_0$ et $A_1 \cong B_1$ alors $A_0 \amalg A_1 \cong B_0 \amalg B_1$.
2. Soient α et β deux ordinaux.
   Si $\beta \subseteq \alpha$ alors $\alpha \cong \beta \amalg (\alpha \backslash \beta)$.

Démonstration

1. Supposons que $A_0 \cong B_0$ et $A_1 \cong B_1$.
Pour tout $i \in \{0, 1\}$, il existe donc $f_i : A_i \longrightarrow B_i$ un isomorphisme d'ordre.
Considérons alors $\varphi := \begin{pmatrix} A_0 \amalg A_1 & \longrightarrow & B_0 \amalg B_1 \\ (i, x) & \longmapsto & \big(i, f_i(x)\big) \end{pmatrix}$.
Montrons que φ est un isomorphisme d'ordre de $A_0 \amalg A_1$ vers $B_0 \amalg B_1$.

• Montrons que φ est bijective de $A_0 \amalg A_1$ vers $B_0 \amalg B_1$.
Pour tout $i \in \{0, 1\}$, f_i est un isomorphisme d'ordre de A_i vers B_i.
Donc tout $i \in \{0, 1\}$, f_i est inversible, avec $f_i^{-1} : B_i \longrightarrow A_i$.
Considérons alors $\psi := \begin{pmatrix} B_0 \amalg B_1 & \longrightarrow & A_0 \amalg A_1 \\ (j, y) & \longmapsto & \big(j, f_j^{-1}(y)\big) \end{pmatrix}$.
Montrons que φ et ψ sont réciproques l'une de l'autre.
En effet, pour tout $(i, x) \in A_0 \amalg A_1$ on a

$$\begin{aligned}(\psi \circ \varphi)(i, x) &= \psi\big(\varphi(i, x)\big) = \psi\big(i, f_i(x)\big) = \Big(i, f_i^{-1}\big(f_i(x)\big)\Big) = (i, x) \\ &= \mathrm{id}_{A_0 \amalg A_1}(i, x)\end{aligned}$$

si bien que $\psi \circ \varphi = \mathrm{id}_{A_0 \amalg A_1}$.
De même pour tout $(j, y) \in B_0 \amalg B_1$ on a

$$\begin{aligned}(\varphi \circ \psi)(j, y) &= \varphi\big(\psi(j, y)\big) = \varphi\big(j, f_j^{-1}(y)\big) = \Big(y, f_y\big(f_y^{-1}(y)\big)\Big) = (j, y) \\ &= \mathrm{id}_{B_0 \amalg B_1}(j, y)\end{aligned}$$

si bien que $\varphi \circ \psi = \mathrm{id}_{B_0 \amalg B_1}$.
Ainsi φ et ψ sont réciproques l'une de l'autre.
En particulier φ est bijective de $A_0 \amalg A_1$ vers $B_0 \amalg B_1$.

• Montrons que φ est croissante.
Pour tout $i \in \{0, 1\}$, f_i est un isomorphisme de A_i vers B_i.

Donc pour tout $i \in \{0,1\}$, f_i est croissante.

Pour tout $i \in \{0,1\}$, notons $\leq_i$ l'ordre sur A_i et $\preceq_i$ l'ordre sur B_i.

Notons $\trianglelefteq_A$ et $\trianglelefteq_B$ les ordres de concaténation associés sur $A_0 \amalg A_1$ et $B_0 \amalg B_1$.

Soient (i,x) et (j,y) dans $A_0 \amalg A_1$.

Supposons que $(i,x) \trianglelefteq_A (j,y)$.

- Plaçons-nous dans le cas où $i = j$.
  On a $(i,x) \trianglelefteq_A (i,y)$.
  On a donc $x \leq_i y$ par définition de $\trianglelefteq_A$.
  Donc $f_i(x) \preceq_i f_i(y)$ par croissance de f_i.
  Donc $\big(i, f_i(x)\big) \trianglelefteq_B \big(i, f_i(y)\big)$ par définition de $\trianglelefteq_B$.
  Donc $\varphi(i,x) \trianglelefteq_B \varphi(i,y)$ par définition de φ.
  On a donc $\varphi(i,x) \trianglelefteq_B \varphi(j,y)$ puisque $i = j$.
- Plaçons-nous dans le cas où $i = 0$ et $j = 1$.
  On a $\big(0, f_0(x)\big) \trianglelefteq_B \big(1, f_1(y)\big)$ par définition de $\trianglelefteq_B$.
  Donc $\varphi(0,x) \trianglelefteq_B \varphi(1,y)$ par définition de φ.
  On a donc $\varphi(i,x) \trianglelefteq_B \varphi(j,y)$ puisque $i = 0$ et $j = 1$.
- Plaçons-nous dans le cas où $i = 1$ et $j = 0$.
  On a $(0,y) \trianglelefteq_A (1,x)$ par définition de $\trianglelefteq_A$.
  On a donc $(j,y) \trianglelefteq_A (i,x)$ puisque $i = 1$ et $j = 0$.
  On a donc $(i,x) = (j,y)$ par antisymétrie de $\trianglelefteq_A$.
  C'est absurde puisque $i \neq j$.

Donc dans tous les cas possibles, on a $\varphi(i,x) \trianglelefteq_B \varphi(j,y)$.

Donc si $(i,x) \trianglelefteq_A (j,y)$ alors $\varphi(i,x) \trianglelefteq_B \varphi(j,y)$.

Donc φ est croissante.

On montre de la même manière que ψ est croissante.

• Ainsi φ est bijective de $A_0 \amalg A_1$ vers $B_0 \amalg B_1$.

φ et sa réciproque ψ sont croissantes.

Donc φ est un isomorphisme d'ordre de $A_0 \amalg A_1$ vers $B_0 \amalg B_1$.

Donc $\boxed{A_0 \amalg A_1 \cong B_0 \amalg B_1}$.

2. Supposons que $\beta \subseteq \alpha$.

Pour tout $\gamma \in \beta$, on a donc $\gamma \in \alpha$.

De même on a $\alpha \backslash \beta \subseteq \alpha$ donc pour tout $\gamma \in \alpha \backslash \beta$ on a $\gamma \in \alpha$.

On peut donc définir $\varphi := \begin{pmatrix} \beta \amalg (\alpha \backslash \beta) & \longrightarrow & \alpha \\ (i,\gamma) & \longmapsto & \gamma \end{pmatrix}$.

• Montrons que φ est injective.

Soient (i,γ) et (j,δ) dans $\beta \amalg (\alpha\backslash\beta)$ tels que $\varphi(i,\gamma)=\varphi(j,\delta)$.

Par définition de φ on a alors $\gamma=\delta$.

En particulier on a à la fois $(i,\gamma)\in\beta \amalg (\alpha\backslash\beta)$ et à la fois $(j,\gamma)\in\beta \amalg (\alpha\backslash\beta)$.

Supposons par l'absurde que $i\neq j$.

On vient de voir que $(i,\gamma)\in\beta \amalg (\alpha\backslash\beta)$ et $(j,\gamma)\in\beta \amalg (\alpha\backslash\beta)$.

Donc $\gamma\in\beta$ et $\gamma\in\alpha\backslash\beta$ par définition de $\beta \amalg (\alpha\backslash\beta)$.

On a donc $\gamma\in\beta\cap(\alpha\backslash\beta)$ et donc $\beta\cap(\alpha\backslash\beta)\neq\varnothing$.

C'est absurde.

Par l'absurde on vient de montrer que $i=j$.

Comme $\gamma=\delta$ on a donc $(i,\gamma)=(j,\delta)$.

Donc pour tout (i,γ) et (j,δ) dans $\beta \amalg (\alpha\backslash\beta)$, si $\varphi(i,\gamma)=\varphi(j,\delta)$ alors $(i,\gamma)=(j,\delta)$.

Donc φ est injective.

• Montrons que φ est surjective dans α.

Soit $\gamma\in\alpha$.

Comme $\beta\subseteq\alpha$, on a $\alpha=\beta\cup(\alpha\backslash\beta)$.

On a donc $\gamma\in\beta\cup(\alpha\backslash\beta)$ et donc ($\gamma\in\beta$ ou $\gamma\in\alpha\backslash\beta$).

Si $\gamma\in\beta$ alors $\gamma=\varphi(0,\gamma)$ et si $\gamma\in\alpha\backslash\beta$ alors $\gamma=\varphi(1,\gamma)$ par définition de φ.

Dans les deux cas on a $\gamma\in\mathrm{im}(\varphi)$.

On a donc $\alpha\subseteq\mathrm{im}(\varphi)$.

Or par définition de φ on a $\alpha\supseteq\mathrm{im}(\varphi)$, et donc $\alpha=\mathrm{im}(\varphi)$.

Ainsi φ est surjective dans α.

On en conclut donc que φ est bijective de $\beta \amalg (\alpha\backslash\beta)$ vers α.

• Montrons que φ est croissante.

Considérons $\trianglelefteq$ l'ordre de concaténation associé sur $\beta \amalg (\alpha\backslash\beta)$.

Soient (i,γ) et (j,δ) dans $\beta \amalg (\alpha\backslash\beta)$.

Supposons que $(i,\gamma)\trianglelefteq(j,\delta)$.

▶ Plaçons-nous dans le cas où $i=j$.

On a donc $\gamma\subseteq\delta$ par définition de $\trianglelefteq$.

▶ Plaçons-nous dans le cas où $i=0$ et $j=1$.

On a donc $\gamma\in\beta$ et $\delta\in\alpha\backslash\beta$ par définition de $\beta \amalg (\alpha\backslash\beta)$.

Comme $\delta\in\alpha\backslash\beta$, on a $\delta\notin\beta$ donc $\beta\subseteq\delta$ d'après le théorème 1 page 21.

Comme $\gamma\in\beta$, on en déduit donc que $\gamma\in\delta$ par transitivité sur ON.

En particulier on a $\gamma\subseteq\delta$ d'après la proposition 8 page 20.

► Plaçons-nous dans le cas où $i = 1$ et $j = 0$.

On a donc $(j, \delta) \trianglelefteq (i, \gamma)$ par définition de $\trianglelefteq$.

On a donc $(i, \gamma) = (j, \delta)$ par antisymétrie de $\trianglelefteq$.

C'est absurde puisqu'on a $i = 1$ et $j = 0$ donc $i \neq j$.

Donc dans les seuls cas possibles, on a nécessairement $\gamma \subseteq \delta$.

Or on a $\varphi(i, \gamma) = \gamma$ et $\varphi(j, \delta) = \delta$ par définition de φ.

On a donc $\varphi(i, \gamma) \subseteq \varphi(j, \delta)$.

Donc si $(i, \gamma) \trianglelefteq (j, \delta)$ alors $\varphi(i, \gamma) \subseteq \varphi(j, \delta)$.

Donc φ est croissante.

Ainsi φ est bijective de $\beta \amalg (\alpha \backslash \beta)$ vers α et est croissante.

Or β et $\alpha \backslash \beta$ sont bien ordonnés d'après le théorème 1 page 21.

Donc $\beta \amalg (\alpha \backslash \beta)$ est bien ordonné d'après la proposition 42 page 113.

En particulier $\beta \amalg (\alpha \backslash \beta)$ est totalement ordonné d'après la proposition 2 page 11.

Donc φ est un isomorphisme d'ordre $\beta \amalg (\alpha \backslash \beta)$ vers α.

En particulier on a $\boxed{\alpha \cong \beta \amalg (\alpha \backslash \beta)}$.

CQFD.

Nous y voilà ! Prenons deux ordinaux α et β : ils sont bien ordonnés par $\subseteq$ donc $\alpha \amalg \beta$ est aussi bien ordonné par l'ordre de concaténation associé. Donc d'après le théorème 4 page 58, il existe un unique ordinal isomorphe à $\alpha \amalg \beta$, que l'on a noté $\mathrm{type}(\alpha \amalg \beta)$. L'intuition est confirmée par le théorème suivant : cet unique ordinal est en fait $\alpha + \beta$!

Au passage, remarquons que le fait de passer de $\alpha \amalg \beta$ à $\mathrm{type}(\alpha \amalg \beta)$ correspond à la renumérotation que l'on a fait dans l'exemple visuel de $2 + \omega$: c'était une étape nécessaire pour s'assurer d'avoir un ordinal à la fin.

Théorème 7 (Addition d'ordinaux et concaténation)

Soient α et β deux ordinaux.
On munit $\alpha \amalg \beta$ de l'ordre de concaténation associé.

Alors $\alpha + \beta = \mathrm{type}(\alpha \amalg \beta)$.

Démonstration

Notons $\trianglelefteq$ l'ordre de concaténation associé à $\alpha \amalg \beta$.

Construisons un isomorphisme d'ordre entre $\alpha \amalg \beta$ et $\alpha + \beta$.

• Construction de l'application.

Remarquons que pour tout $(i, \gamma) \in \alpha \amalg \beta$, on a :

► Plaçons-nous dans le cas où $i = 0$.
Alors par définition de $\alpha \amalg \beta$ on a $\gamma \in \alpha$.
On sait que $0 \subseteq \beta$ car le vide est inclus dans tout ensemble.
Donc $\alpha + 0 \subseteq \alpha + \beta$ par croissance de l'addition à gauche.
Or $\alpha = \alpha + 0$ par définition de l'addition donc $\alpha \subseteq \alpha + \beta$.
On a donc $\gamma \in \alpha + \beta$ par définition de l'inclusion.

► Plaçons-nous dans le cas où $i = 1$.
Alors par définition de $\alpha \amalg \beta$ on a $\gamma \in \beta$.
Alors $\alpha + \gamma \in \alpha + \beta$ par croissance de l'addition à gauche.

Ainsi, on peut poser $\varphi_\beta := \left(\begin{array}{ccc} \alpha \amalg \beta & \longrightarrow & \alpha + \beta \\ (i, \gamma) & \longmapsto & \begin{cases} \gamma & \text{si } i = 0 \\ \alpha + \gamma & \text{si } i = 1 \end{cases} \end{array} \right)$.

Le fait d'avoir mis β en indice va répondre à un besoin ultérieur où l'on fera une induction sur β.

• Montrons que φ_β est croissante.
Soient (i, γ) et (j, δ) dans $\alpha \amalg \beta$.
Supposons que $(i, \gamma) \trianglelefteq (j, \delta)$.

► Plaçons-nous dans le cas où $i = 0 = j$.
Alors on a $\varphi_\beta(i, \gamma) = \gamma$ et $\varphi_\beta(j, \delta) = \delta$ par définition de φ_β.
Comme $(i, \gamma) \trianglelefteq (j, \delta)$ on a $\gamma \subseteq \delta$ par définition de $\trianglelefteq$.
On a donc $\varphi_\beta(i, \gamma) \subseteq \varphi_\beta(j, \delta)$.

► Plaçons-nous dans le cas où $i = 1 = j$.
Alors $\varphi_\beta(i, \gamma) = \alpha + \gamma$ et $\varphi_\beta(j, \delta) = \alpha + \delta$ par définition de φ_β.
Comme $(i, \gamma) \trianglelefteq (j, \delta)$ on a $\gamma \subseteq \delta$ par définition de $\trianglelefteq$.
On a donc $\alpha + \gamma \subseteq \alpha + \delta$ par croissance de l'addition.
On a donc $\varphi_\beta(i, \gamma) \subseteq \varphi_\beta(j, \delta)$.

► Plaçons-nous dans le cas où $i = 0$ et $j = 1$.
Alors $\gamma \in \alpha$ (et $\delta \in \beta$) par définition de $\alpha \amalg \beta$.
De plus $\varphi_\beta(i, \gamma) = \gamma$ et $\varphi_\beta(j, \delta) = \alpha + \delta$ par définition de φ_β.
On a $\gamma \in \alpha = \alpha + 0 \subseteq \alpha + \delta$ par croissance de l'addition.
On a donc $\gamma \subseteq \alpha + \delta$ par transitivité chez les ordinaux.
On a donc $\varphi_\beta(i, \gamma) \subseteq \varphi_\beta(j, \delta)$.

► Plaçons-nous dans le cas où $i = 1$ et $j = 0$.
On a alors $(j, \delta) \trianglelefteq (i, \gamma)$ par définition de $\trianglelefteq$.

On a donc $(i,\gamma)=(j,\delta)$ par antisymétrie de $\trianglelefteq$.

On a donc $i=j$, c'est qui est absurde puisque $i=1$ et $j=0$.

Dans tous les cas possibles on a $\varphi_\beta(i,\gamma)\subseteq\varphi_\beta(j,\delta)$.

Donc si $(i,\gamma)\trianglelefteq(j,\delta)$ alors $\varphi_\beta(i,\gamma)\subseteq\varphi_\beta(j,\delta)$.

Donc $\boxed{\varphi_\beta \text{ est croissante}}$.

• Montrons que φ_β est injective.

Soit (i,γ) et (j,δ) dans $\alpha \amalg \beta$.

Supposons que $\varphi_\beta(i,\gamma)=\varphi_\beta(j,\delta)$.

▶ Plaçons-nous dans le cas où $i=0=j$.
On a alors $\varphi_\beta(i,\gamma)=\gamma$ et $\varphi_\beta(j,\delta)=\delta$ par définition de φ_β.
Comme $\varphi_\beta(i,\gamma)=\varphi_\beta(j,\delta)$ on a donc $\gamma=\delta$.
Comme $i=j$ et $\gamma=\delta$ on a $(i,\gamma)=(j,\delta)$.

▶ Plaçons-nous dans le cas où $i=1=j$.
On a alors $\varphi_\beta(i,\gamma)=\alpha+\gamma$ et $\varphi_\beta(j,\delta)=\alpha+\delta$ par définition de φ_β.
Comme $\varphi_\beta(i,\gamma)=\varphi_\beta(j,\delta)$ on a donc $\alpha+\gamma=\alpha+\delta$.
On en déduit que $\gamma=\delta$ par régularité de l'addition à gauche.
Comme $i=j$ et $\gamma=\delta$ on a $(i,\gamma)=(j,\delta)$.

▶ Plaçons-nous dans le cas où $i=0$ et $j=1$.
On a alors $\gamma\in\alpha$ et $\delta\in\beta$ par définition de $\alpha \amalg \beta$.
On a aussi $\varphi_\beta(i,\gamma)=\gamma$ et $\varphi_\beta(j,\delta)=\alpha+\delta$ par définition de φ_β.
Or on a $\gamma\in\alpha=\alpha+0\subseteq\alpha+\delta$.
On a donc $\gamma\in\alpha+\delta$ par transitivité chez les ordinaux.
On a donc $\varphi_\beta(i,\gamma)\in\varphi_\beta(j,\delta)$.
Or on a fait l'hypothèse que $\varphi_\beta(i,\gamma)=\varphi_\beta(j,\delta)$.
C'est absurde par antiréflexivité de $\in$ sur ON.

▶ Le cas où $i=1$ et $j=0$ est absurde pour la même raison.

Les deux seuls cas possibles conduisent alors à $(i,\gamma)=(j,\delta)$.

Donc si $\varphi_\beta(i,\gamma)=\varphi_\beta(j,\delta)$ alors $(i,\gamma)=(j,\delta)$.

Donc $\boxed{\varphi_\beta \text{ est injective}}$.

• Montrons que φ_β est surjective sur $\alpha+\beta$.

On sait déjà par définition de φ_β que $\mathrm{im}(\varphi_\beta)\subseteq\alpha+\beta$.

Fixons un ordinal α et posons P l'assertion à paramètre définie pour tout ordinal β par

$$P(\beta) \iff \mathrm{im}(\varphi_\beta)=\alpha+\beta$$

Remarquons la chose suivante : soient β et β' deux ordinaux tels que $\beta \subseteq \beta'$.
On a alors $\big(\{1\} \times \beta\big) \subseteq \big(\{1\} \times \beta'\big)$ donc $\alpha \amalg \beta \subseteq \alpha \amalg \beta'$.
Or pour tout $(i, \gamma) \in \alpha \amalg \beta$ on a $\varphi_\beta(i, \gamma) = \varphi_{\beta'}(i, \gamma)$ par définition de φ_β et $\varphi_{\beta'}$.
Autrement dit on a alors $\varphi_\beta = (\varphi_{\beta'})_{|\alpha \amalg \beta}$.

► *Initialisation*

On a alors $\alpha + 0 = \alpha$ par définition de l'addition.
Montrons que $\mathrm{im}(\varphi_0) \supseteq \alpha$.
Soit $\gamma \in \alpha$.
On a alors $\varphi_0(0, \gamma) = \gamma$ par définition de φ_0.
Donc $\gamma \in \mathrm{im}(\varphi_0)$.
On a donc $\mathrm{im}(\varphi_0) \supseteq \alpha$ et donc $\mathrm{im}(\varphi_0) = \alpha$.
Ainsi on a $\mathrm{im}(\varphi_0) = \alpha + 0$ et donc on a $P(0)$.

► *Hérédité*

Soit β un ordinal tel que $P(\beta)$.
On a donc $\mathrm{im}(\varphi_\beta) = \alpha + \beta$.
On a $\alpha + S(\beta) = S(\alpha + \beta)$ par définition de l'addition.
Montrons que $\mathrm{im}\big(\varphi_{S(\beta)}\big) \supseteq S(\alpha + \beta)$.
Soit $\gamma \in S(\alpha + \beta)$.
On a donc $\gamma \subseteq \alpha + \beta$ d'après la proposition 12 page 33.
On a donc $\gamma \in \alpha + \beta$ ou $\gamma = \alpha + \beta$ d'après la proposition 8 page 20.

Plaçons-nous dans le cas où $\gamma \in \alpha + \beta$.
Par hypothèse on a $\mathrm{im}(\varphi_\beta) = \alpha + \beta$ donc on a $\gamma \in \mathrm{im}(\varphi_\beta)$.
Or $\beta \in S(\beta)$ d'après la proposition 12 page 33 donc $\beta \subseteq S(\beta)$.
On a donc $\varphi_\beta = \big(\varphi_{S(\beta)}\big)_{|\alpha \amalg \beta}$ donc $\mathrm{im}(\varphi_\beta) \subseteq \mathrm{im}\big(\varphi_{S(\beta)}\big)$.
Ainsi on a $\gamma \in \mathrm{im}\big(\varphi_{S(\beta)}\big)$ par définition de l'inclusion.

Plaçons-nous dans le cas où $\gamma = \alpha + \beta$.
On a $\beta \in S(\beta)$ d'après la proposition 12 page 33.
Ainsi $\gamma = \alpha + \beta = \varphi_{S(\beta)}(1, \beta)$ par définition de $\varphi_{S(\beta)}$.
On a donc $\gamma \in \mathrm{im}\big(\varphi_{S(\beta)}\big)$.

Ainsi dans les deux cas on a $\gamma \in \mathrm{im}\big(\varphi_{S(\beta)}\big)$.
On a donc $\mathrm{im}\big(\varphi_{S(\beta)}\big) \supseteq S(\alpha + \beta)$ et donc $\mathrm{im}\big(\varphi_{S(\beta)}\big) = S(\alpha + \beta)$.
Autrement dit on a $P\big(S(\beta)\big)$.

Donc pour tout ordinal β, si $P(\beta)$ alors $P\big(S(\beta)\big)$.

▶ *Hérédité limite*

Soit β un ordinal limite non nul tel que $\forall \delta \in \beta, P(\delta)$.

Montrons que $\mathrm{im}(\varphi_\beta) \supseteq \alpha + \beta$.

Soit $\gamma \in \alpha + \beta$.

On sait que β est un ordinal limite non nul.

Donc $\alpha + \beta = \sup\limits_{\delta \in \beta}(\alpha + \beta) = \bigcup\limits_{\delta \in \beta}(\alpha + \delta)$ par définition de l'addition.

On a donc $\gamma \in \bigcup\limits_{\delta \in \beta}(\alpha + \delta)$.

Il existe donc $\delta \in \beta$ tel que $\gamma \in \alpha + \delta$.

Or par hypothèse on a $P(\delta)$ donc $\alpha + \delta = \mathrm{im}(\varphi_\delta)$.

Or $\delta \in \beta$ donc $\delta \subseteq \beta$ donc $\varphi_\delta = (\varphi_\beta)_{|\alpha \amalg \delta}$.

On a donc $\mathrm{im}(\varphi_\delta) \subseteq \mathrm{im}(\varphi_\beta)$.

On a donc $\gamma \in \mathrm{im}(\varphi_\beta)$ par définition de l'inclusion.

On a donc $\mathrm{im}(\varphi_\beta) \supseteq \alpha + \beta$ et donc $\mathrm{im}(\varphi_\beta) = \alpha + \beta$.

Autrement dit on a $P(\beta)$.

Donc pour tout ordinal limite non nul β, si $\forall \delta \in \beta, P(\delta)$ alors $P(\beta)$.

Ainsi P vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal β on a $P(\beta)$.

Autrement dit pour tout ordinal β on a $\mathrm{im}(\varphi_\beta) = \alpha + \beta$.

Autrement dit pour tout ordinal β, $\boxed{\varphi_\beta \text{ est surjective dans } \alpha + \beta}$.

• Conclusion.

Fixons à nouveau un ordinal β.

Alors l'application $\varphi_\beta : \alpha \amalg \beta \longrightarrow \alpha + \beta$ est croissante, injective et surjective dans $\alpha + \beta$.

Or α et β sont bien ordonnés d'après le théorème 1 page 21.

Donc $\alpha \amalg \beta$ est bien ordonné d'après la proposition 42 page 113.

Donc $\alpha \amalg \beta$ est totalement ordonné d'après la proposition 2 page 11.

Ainis $\mathrm{dom}(\varphi_\beta)$ est totalement ordonné.

Donc φ_β est un isomorphisme d'ordres de $\alpha \amalg \beta$ dans $\alpha + \beta$.

Or $\alpha + \beta$ est un ordinal par définition.

Donc $\boxed{\mathrm{type}(\alpha \amalg \beta) = \alpha + \beta}$ par définition du type d'un ensemble bien ordonné.

CQFD.

À l'école primaire, après l'addition vient rapidement la soustraction. Nous apprenons à cet âge-là qu'il n'est pas possible de soustraire un nombre par un nombre plus grand : la raison est simplement que cela produit un nombre négatif, notion qui n'est à ce moment-là pas abordée.

C'est un peu le cas ici : il n'est pas encore temps de définir les nombres négatifs, et donc nous nous contenterons de ne pouvoir soustraire que les ordinaux plus grands par des ordinaux plus petits.

Proposition 44 (Soustraction d'ordinaux)

Soient α et β deux ordinaux.
Les assertions suivantes sont équivalentes :

1. $\beta \subseteq \alpha$
2. Il existe un ordinal γ tel que $\alpha = \beta + \gamma$.

Dans ce cas-là, un tel ordinal γ est unique.
On le note $\alpha - \beta$, si bien que $\alpha = \beta + (\alpha - \beta)$.

On a en fait $\alpha - \beta = \mathrm{type}(\alpha \backslash \beta)$.
Autrement dit on a $\alpha = \beta + \mathrm{type}(\alpha \backslash \beta)$.

Démonstration

• Commençons par montrer l'équivalence.

$\boxed{1 \Rightarrow 2}$

Supposons que $\beta \subseteq \alpha$.

On a donc $\beta \in S(\alpha)$ d'après la proposition 12 page 33.

On munit $\beta \amalg S(\alpha)$ de $\trianglelefteq$ l'ordre de concaténation associé.

Soit $\varphi := \left(\begin{array}{ccc} \beta \amalg S(\alpha) & \longrightarrow & \beta + S(\alpha) \\ (i,\gamma) & \longmapsto & \begin{cases} \gamma & \text{si } i = 0 \\ \beta + \gamma & \text{si } i = 1 \end{cases} \end{array} \right)$.

On a montré lors de la preuve du théorème 7 page 118 que φ est surjective dans $\beta + S(\alpha)$.

Autrement dit on a $\mathrm{im}(\varphi) = \beta + S(\alpha)$.

Or on a $\alpha \underset{12 \text{ p. } 33}{\in} S(\alpha) \underset{34 \text{ p. } 95}{=} 0 + S(\alpha) \underset{36 \text{ p. } 97}{\subseteq} \beta + S(\alpha)$.

On a donc $\alpha \in \beta + S(\alpha)$ donc $\alpha \in \mathrm{im}(\varphi)$.

Il existe donc $(i,\gamma) \in \beta \amalg S(\alpha)$ tel que $\alpha = \varphi(i,\gamma)$.

> Supposons par l'absurde que $i = 0$.
>
> On a alors $\varphi(i,\gamma) = \gamma$ par définition de φ.
>
> On a aussi $\gamma \in \beta$ par définition de $\beta \amalg S(\alpha)$.
>
> Comme $\alpha = \varphi(i,\gamma)$ on a donc $\alpha = \gamma$ et donc $\alpha \in \beta$.
>
> C'est absurde puisque par hypothèse on a $\beta \subseteq \alpha$.

Par l'absurde, on vient donc de montrer que $i = 1$.

On a donc $\varphi(i,\gamma) = \beta + \gamma$ par définition de φ.

Comme $\alpha = \varphi(i,\gamma)$ on a donc $\boxed{\alpha = \beta + \gamma}$.

$\boxed{1 \Leftarrow 2}$

Supposons qu'il existe un ordinal γ tel que $\alpha = \beta + \gamma$.

Or on a $\beta = \beta + 0 \subseteq \beta + \gamma$ par définition de l'addition et croissance de l'addition à gauche.

On a donc $\boxed{\beta \subseteq \alpha}$.

• On se place à présent dans le cas où effectivement $\beta \subseteq \alpha$.

Montrons qu'un tel γ est alors unique.

> Soit γ' un ordinal tel que $\alpha = \beta + \gamma'$.
>
> On a $\gamma \in \gamma'$ ou $\gamma' \in \gamma$ ou $\gamma = \gamma'$ d'après le théorème 1 page 21.
>
> Si $\gamma \in \gamma'$ alors $\beta + \gamma \in \beta + \gamma'$ par stricte croissance de l'addition à gauche.
>
> De même si $\gamma' \in \gamma$ alors $\beta + \gamma' \in \beta + \gamma$.
>
> Dans ces deux cas on a donc $\alpha \in \alpha$, ce qui est absurde par antiréflexivité de $\in$.
>
> On a donc nécessairement $\gamma = \gamma'$.

On a donc $\boxed{\text{unicité d'un tel ordinal } \gamma}$.

• Montrons que $\gamma = \mathrm{type}(\alpha \backslash \beta)$.

Par définition du type on a $\alpha \backslash \beta \cong \mathrm{type}(\alpha \backslash \beta)$.

On a aussi $\beta \cong \beta$ par réflexivité de l'isomorphie d'ordres.

On a donc $\beta \amalg (\alpha \backslash \beta) \cong \beta \amalg \mathrm{type}(\alpha \backslash \beta)$ d'après la proposition 43 page 115.

On a donc les isormophies d'ordres suivantes :

$$\begin{aligned} \alpha &\cong \beta \amalg (\alpha \backslash \beta) \text{ d'après la prop. 43 p. 115} \\ &\cong \beta \amalg \mathrm{type}(\alpha \backslash \beta) \text{ par ce qui précède} \\ &\cong \mathrm{type}\Big(\beta \amalg \mathrm{type}(\alpha \backslash \beta)\Big) \text{ par définition du type} \\ &\cong \beta + \mathrm{type}(\alpha \backslash \beta) \text{ d'après le théorème 7 page 118} \end{aligned}$$

Ainsi $\boxed{\alpha \cong \beta + \mathrm{type}(\alpha \backslash \beta)}$ par transitivité de l'isomorphie d'ordres.

Autrement dit on a $\boxed{\alpha - \beta = \gamma = \mathrm{type}(\alpha \backslash \beta)}$ par l'unicité prouvée plus tôt.

CQFD.

3 Multiplication d'ordinaux

3.1 Définition et propriétés

Pour définir la multiplication chez les ordinaux, on peut à nouveau s'inspirer de la multiplication chez les entiers naturels. Comment définir 5×3 ? Intuitivement il s'agit de $5+5+5$, c'est-à-dire une répétition d'additions de 5, où le nombre 5 est répété 3 fois. Ce n'est cependant pas une définition très pratique ici, car on n'a pas particulièrement donné de sens à "*répéter* 3 *fois une addition*". Il nous faudrait plutôt une définition par récursion, puisqu'on a développé tous les outils pour cela précédemment. On peut remarquer que $5 \times 2 = 5 + 5$, si bien que $5 \times 3 = 5+5+5 = (5+5)+5 = (5 \times 2)+5$. En voilà une définition par récursion !

Ainsi, pour définir 5×3 on considère que 5×2 est déjà défini, puis on pose $5\times3 := (5\times2)+5$. Autrement dit, on a posé $5 \times S(2) := (5 \times 2) + 2$. Cela nous guide donc vers la définition suivante.

Définition 21 (Multiplication d'ordinaux)

Soit α un ordinal.
On pose

$$\begin{cases} \alpha \cdot 0 := 0 \\ \alpha \cdot S(\beta) := (\alpha \cdot \beta) + \alpha \text{ pour tout ordinal } \beta \\ \alpha \cdot \gamma := \sup\limits_{\delta \in \gamma}(\alpha \cdot \delta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

Remarque :

1. Comme on peut le voir dans la définition, pour deux ordinaux α et β on note généralement $\alpha \cdot \beta$ plutôt que $\alpha \times \beta$. Cela évitera au passage la confusion avec le produit cartésien, même si nous verrons qu'il y a un lien entre les deux.
2. Afin de simplifier les expressions, on considère désormais que la multiplication des ordinaux est prioritaire sur l'addition des ordinaux. Ainsi, l'expression $\alpha \cdot \beta + \gamma$ désigne $(\alpha \cdot \beta) + \gamma$ et non $\alpha \cdot (\beta + \gamma)$.
3. Pour justifier proprement cette définition, on utilise simplement la proposition 32 page 91, en posant $\mu_0 := 0$, et $G(\xi) := \xi + \alpha$ pour tout ordinal ξ. La proposition nous donne alors une unique assertion fonctionnelle F_α telle que

$$\begin{cases} F_\alpha(0) = 0 \\ F_\alpha\big(S(\beta)\big) = F_\alpha(\beta) + \alpha \text{ pour tout ordinal } \beta \\ F_\alpha(\gamma) = \sup\limits_{\delta \in \gamma} F_\alpha(\delta) \text{ pour tout ordinal limite non nul } \gamma \end{cases}$$

et on pose alors $\alpha \cdot \beta := F_\alpha(\beta)$ pour tout ordinal β.

Proposition 45 (0 est absorbant pour la multiplication)

Pour tout ordinal α, on a $\alpha \cdot 0 = 0 = 0 \cdot \alpha$.
On dit que 0 est **absorbant** pour la multiplication des ordinaux.

Démonstration

On sait déjà que pour tout ordinal α, on a $\alpha \cdot 0 = \alpha$ par définition de la multiplication.

Montrons l'autre égalité par induction.

Considérons P l'assertion à paramètres définie pour tout ordinal α par

$$P(\alpha) \iff 0 \cdot \alpha = 0$$

► *Initialisation*

On a $0 \cdot 0 = 0$ par définition de la multiplication.

On a donc $P(0)$.

► *Hérédité*

Soit α un ordinal tel que $P(\alpha)$.

Autrement dit on a $0 \cdot \alpha = 0$.

On a donc

$$\begin{aligned} 0 \cdot S(\alpha) &= 0 \cdot \alpha + 0 \text{ par définition de la multiplication} \\ &= 0 \cdot \alpha \text{ par neutralité de } 0 \text{ pour l'addition} \\ &= 0 \text{ puisqu'on a } P(\alpha) \end{aligned}$$

Ainsi on a $0 \cdot S(\alpha) = 0$ et donc $P\big(S(\alpha)\big)$.

Ainsi pour tout ordinal α, si $P(\alpha)$ alors $P\big(S(\alpha)\big)$.

► *Hérédité limite*

Soit α un ordinal limite non nul tel que $\forall \beta \in \alpha, P(\beta)$.

Autrement dit pour tout $\beta \in \alpha$, on a $0 \cdot \beta = 0$.

Par définition de la multiplication on a donc $0 \cdot \alpha = \sup\limits_{\beta \in \alpha}(0 \cdot \beta) = \sup\limits_{\beta \in \alpha} 0 = 0$.

Autrement dit on a $P(\alpha)$.

Ainsi pour tout ordinal limite non nul α, si $\forall \beta \in \alpha, P(\beta)$ alors $P(\alpha)$.

Ainsi P vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal α, on a $P(\alpha)$.

Autrement dit $\boxed{\text{pour tout ordinal } \alpha \text{ on a } 0 \cdot \alpha = 0}$.
CQFD.

Proposition 46 (1 est neutre pour la multiplication)

Pour tout ordinal α, on a $\alpha \cdot 1 = \alpha = 1 \cdot \alpha$.
On dit que 1 est **neutre** pour la multiplication des ordinaux.

Démonstration

Pour tout ordinal α on a

$$\begin{aligned}\alpha \cdot 1 &= \alpha \cdot S(0) \text{ par définition de } 1\\ &= \alpha \cdot 0 + \alpha \text{ par définition de la multiplication}\\ &= 0 + \alpha \text{ par définition de la multiplication}\\ &= \alpha \text{ par neutralité de } 0 \text{ pour l'addition}\end{aligned}$$

Ainsi on sait déjà que $\boxed{\text{pour tout ordinal } \alpha \text{ on a } \alpha \cdot 1 = \alpha}$.

Montrons l'autre égalité par induction.
Considérons P l'assertion à paramètre définie pour tout ordinal α par

$$P(\alpha) \iff 1 \cdot \alpha = \alpha$$

▶ *Initialisation*
On a $1 \cdot 0 = 0$ par définition de la multiplication.
Autrement dit on a $P(0)$.

▶ *Hérédité*
Soit α un ordinal tel que $P(\alpha)$.
Autrement dit on a $1 \cdot \alpha = \alpha$.
On a alors

$$\begin{aligned}1 \cdot S(\alpha) &= 1 \cdot \alpha + 1 \text{ par définition de l'addition}\\ &= \alpha + 1 \text{ puisque l'on a } P(\alpha)\\ &= S(\alpha) \text{ d'après la prop. 33 p. 94}\end{aligned}$$

Ainsi on a $1 \cdot S(\alpha) = S(\alpha)$.
Autrement dit on a $P\big(S(\alpha)\big)$.

Ainsi pour tout ordinal α, si $P(\alpha)$ alors $P\big(S(\alpha)\big)$.

► *Hérédité limite*

Soit α un ordinal limite non nul tel que $\forall\beta \in \alpha, P(\beta)$.

Autrement dit pour tout $\beta \in \alpha$ on a $1 \cdot \beta = \beta$.

Comme α est un ordinal limite, on a $\sup\limits_{\beta\in\alpha} \beta = \alpha$ d'après la proposition 20 page 47.

Par définition de la multiplication on a donc $1 \cdot \alpha = \sup\limits_{\beta\in\alpha}(1 \cdot \beta) = \sup\limits_{\beta\in\alpha} \beta = \alpha$.

Ainsi on a $1 \cdot \alpha = \alpha$.

Autrement dit on a $P(\alpha)$.

Donc pour tout ordinal limite non nul α, si $\forall\beta \in \alpha, P(\beta)$ alors $P(\alpha)$.

Ainsi P vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal α, on a $P(\alpha)$.

Autrement dit $\boxed{\text{pour tout ordinal } \alpha \text{ on a } 1 \cdot \alpha = \alpha}$.

CQFD.

Proposition 47 (Multiplication de deux entiers naturels)

Pour tout entiers naturels n et m, l'ordinal $n \cdot m$ est un entier naturel.
On dit que $\mathbb{N} = \omega$ est **stable** par multiplication.

Démonstration

Fixons n un entier naturel.

Soit P l'assertion à paramètre définie pour tout entier naturel m par

$$P(m) \iff n \cdot m \in \mathbb{N}$$

Raisonnons par induction sur les entiers naturels.

► *Initialisation*

On a $n \cdot 0 = 0$ par définition de la multiplication.

Or 0 est un entier naturel donc $n \cdot 0$ est un entier naturel.

Autrement dit on a $P(0)$.

► *Hérédité*

Soit m un entier naturel tel que $P(m)$.

Autrement dit $n \cdot m$ est un entier naturel.

Donc $n \cdot m + n$ est un entier naturel d'après la proposition 35 page 96.

Or on a $n \cdot S(m) = n \cdot m + n$ par définition de la multiplication.

Donc $n \cdot S(m)$ est un entier naturel.

Autrement dit on a $P\big(S(m)\big)$.

Donc pour tout entier naturel m, si $P(m)$ alors $P\big(S(m)\big)$.

Ainsi P vérifie les deux conditions du principe d'induction chez les entiers naturels.

Donc pour tout entier naturel m on a $P(m)$.

Autrement dit $\boxed{\text{pour tout entier naturel } m\text{, l'ordinal } n \cdot m \text{ est un entier naturel}}$.

CQFD.

Proposition 48 (Croissance de la multiplication des ordinaux)

Soient α, β et γ trois ordinaux.

1. Supposons que α est **non nul**.
   Si $\beta \in \gamma$ alors $\alpha \cdot \beta \in \alpha \cdot \gamma$.
   On dit que la multiplication est **strictement croissante à droite**.
2. Si $\beta \subseteq \gamma$ alors $\alpha \cdot \beta \subseteq \alpha \cdot \gamma$.
   On dit que la multiplication est **croissante à droite**.
3. Si $\beta \subseteq \gamma$ alors $\beta \cdot \alpha \subseteq \gamma \cdot \alpha$.
   On dit que la multiplication est **croissante à gauche**.

Démonstration

1. Fixons deux ordinaux α et β, avec α non nul.

Posons $P_{\alpha,\beta}$ l'assertion à paramètre définie pour tout ordinal γ par

$$P_{\alpha,\beta}(\gamma) \iff \big(\beta \in \gamma \Rightarrow \alpha \cdot \beta \in \alpha \cdot \gamma\big)$$

Montrons le résultat par le principe faible d'induction.

► *Initialisation*

La prémisse $\beta \in 0$ étant fausse, on a l'implication $\beta \in 0 \Rightarrow \alpha \cdot \beta \in \alpha \cdot 0$.

Autrement dit on a $P_{\alpha,\beta}(0)$.

► *Hérédité*

Soit γ un ordinal tel que $P_{\alpha,\beta}(\gamma)$.

Autrement dit on a l'implication $\beta \in \gamma \Rightarrow \alpha \cdot \beta \in \alpha \cdot \gamma$.

Supposons que $\beta \in S(\gamma)$.

On a alors $\beta \subseteq \gamma$ d'après la proposition 12 page 33.

On a donc $\beta \in \gamma$ ou $\beta = \gamma$ d'après la proposition 8 page 20.

Commençons par remarquer que l'on a :

$$\begin{aligned}\alpha \cdot \gamma &= \alpha \cdot \gamma + 0 \text{ car } 0 \text{ est neutre pour l'addition}\\ &\in \alpha \cdot \gamma + \alpha \text{ par stricte croissance à droite de l'addition et } \alpha \neq 0\\ &= \alpha \cdot S(\gamma) \text{ par définition de la multiplication}\end{aligned}$$

Ainsi on a $\alpha \cdot \gamma \in \alpha \cdot S(\gamma)$.

- Plaçons-nous dans le cas où $\beta \in \gamma$.
  On a alors $\alpha \cdot \beta \in \alpha \cdot \gamma$ d'après $P_{\alpha,\beta}(\gamma)$.
  Or on a dit que $\alpha \cdot \gamma \in \alpha \cdot S(\gamma)$.
  On a donc $\alpha \cdot \beta \in \alpha \cdot S(\gamma)$ par transitivité de $\in$ chez ON.
- Plaçons-nous dans le cas où $\beta = \gamma$.
  On a donc $\alpha \cdot \beta = \alpha \cdot \gamma$.
  Or on a dit que $\alpha \cdot \gamma \in \alpha \cdot S(\gamma)$.
  On a donc $\alpha \cdot \beta \in \alpha \cdot S(\gamma)$.

Dans les deux cas on a $\alpha \cdot \beta \in \alpha \cdot S(\gamma)$.
Donc si $\beta \in S(\gamma)$ alors $\alpha \cdot \beta \in \alpha \cdot S(\gamma)$.
Autrement dit on a $P_{\alpha,\beta}\big(S(\gamma)\big)$.
Donc pour tout ordinal γ, si $P_{\alpha,\beta}(\gamma)$ alors $P_{\alpha,\beta}\big(S(\gamma)\big)$.

► *Hérédité limite*

Soit γ un ordinal limite non nul tel que $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$.
Supposons que $\beta \in \gamma$.
On a donc $S(\beta) \in \gamma$ d'après la proposition 13 page 37.
Donc comme $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$, on a en particulier $P_{\alpha,\beta}\big(S(\beta)\big)$.
Autrement dit on a $\beta \in S(\beta) \Rightarrow \alpha \cdot \beta \in \alpha \cdot S(\beta)$.
Or on a $\beta \in S(\beta)$ d'après la proposition 12 page 33.
On a donc $\alpha \cdot \beta \in \alpha \cdot S(\beta)$ par modus ponens.
Or on a dit que $S(\beta) \in \gamma$ donc $\alpha \cdot S(\beta) \in \{\alpha \cdot \delta \mid \delta \in \gamma\}$.
Donc $\alpha \cdot S(\beta) \subseteq \sup\limits_{\delta \in \gamma}(\alpha \cdot \delta)$ car la borne supérieure est un majorant.
On a donc $\alpha \cdot \beta \in \sup\limits_{\delta \in \gamma}(\alpha \cdot \delta)$ par définition de l'inclusion.
Or $\alpha \cdot \gamma = \sup\limits_{\delta \in \gamma}(\alpha \cdot \delta)$ par définition de la multiplication.
On a donc $\alpha \cdot \beta \in \alpha \cdot \gamma$.
Donc si $\beta \in \gamma$ alors $\alpha \cdot \beta \in \alpha \cdot \gamma$.
Autrement dit on a $P_{\alpha,\beta}(\gamma)$.
Donc pour tout ordinal limite non nul γ, si $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$ alors $P_{\alpha,\beta}(\gamma)$.

Ainsi $P_{\alpha,\beta}$ vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal γ, on a $P_{\alpha,\beta}(\gamma)$.

Autrement dit $\boxed{\text{pour tout ordinal } \gamma\text{, si } \beta \in \gamma \text{ alors } \alpha \cdot \beta \in \alpha \cdot \gamma.}$

2. Fixons trois ordinaux α, β et γ.

Plaçons-nous dans un premier temps dans le cas où $\alpha = 0$.

On a alors $\alpha \cdot \beta = 0 = \alpha \cdot \gamma$ car 0 est absorbant pour la multiplication.

On a donc $\alpha \cdot \beta \subseteq \alpha \cdot \gamma$.

On a donc l'implication $\boxed{\beta \subseteq \gamma \Rightarrow \alpha \cdot \beta \subseteq \alpha \cdot \gamma}$.

Plaçons-nous à présent dans le cas où α est non nul.

Supposons que $\beta \subseteq \gamma$.

On a donc $\beta \in \gamma$ ou $\beta = \gamma$ d'après la proposition 8 page 20.

- Plaçons-nous dans le cas où $\beta \in \gamma$.
  Comme $\alpha \neq 0$, on a $\alpha \cdot \beta \in \alpha \cdot \gamma$ d'après 1.
  En particulier on a $\alpha \cdot \beta \subseteq \alpha \cdot \gamma$ d'après la proposition 8 page 20.
- Plaçons-nous dans le cas où $\beta = \gamma$.
  On a donc $\alpha \cdot \beta = \alpha \cdot \gamma$.
  En particulier on a $\alpha \cdot \beta \subseteq \alpha \cdot \gamma$.

Dans les deux cas on a $\alpha \cdot \beta \subseteq \alpha \cdot \gamma$.

Donc $\boxed{\text{si } \beta \subseteq \gamma \text{ alors } \alpha \cdot \beta \subseteq \alpha \cdot \gamma}$.

3. Fixons deux ordinaux β et γ.

Supposons que $\beta \subseteq \gamma$.

Posons $Q_{\beta,\gamma}$ l'assertion à paramètre définie pour tout ordinal par

$$Q_{\beta,\gamma}(\alpha) \iff \beta \cdot \alpha \subseteq \gamma \cdot \alpha$$

Montrons le résultat par le principe faible d'induction.

► *Initialisation*

Par définition de la multiplication on a $\beta \cdot 0 = 0 = \gamma \cdot 0$.

En particulier on a $\beta \cdot 0 \subseteq \gamma \cdot 0$.

Autrement dit on a $Q_{\beta,\gamma}(0)$.

► *Hérédité*

Soit α un ordinal tel que $Q_{\beta,\gamma}(\alpha)$.

Autrement dit on a $\beta \cdot \alpha \subseteq \gamma \cdot \alpha$.

On a donc $\beta \cdot \alpha + \beta \subseteq \gamma \cdot \alpha + \beta$ par croissance de l'addition à gauche.

Or on a fait l'hypothèse que $\beta \subseteq \gamma$.

Donc $\gamma \cdot \alpha + \beta \subseteq \gamma \cdot \alpha + \gamma$ par croissance de l'addition à droite.

Ainsi on a

$$\begin{aligned}
\beta \cdot S(\alpha) &= \beta \cdot \alpha + \beta \text{ par définition de la multiplication} \\
&\subseteq \gamma \cdot \alpha + \beta \text{ par ce qui précède} \\
&\subseteq \gamma \cdot \alpha + \gamma \text{ par ce qui précède} \\
&= \gamma \cdot S(\alpha) \text{ par définition de la multiplication}
\end{aligned}$$

On a donc $\beta \cdot S(\alpha) \subseteq \gamma \cdot S(\alpha)$.

Autrement dit on a $Q_{\beta,\gamma}\big(S(\alpha)\big)$.

Donc pour tout ordinal α, si $Q_{\beta,\gamma}(\alpha)$ alors $Q_{\beta,\gamma}\big(S(\alpha)\big)$.

► *Hérédité limite*

Soit α un ordinal limite non nul tel que $\forall \delta \in \alpha, Q_{\beta,\gamma}(\delta)$.

Soit $\delta \in \alpha$. On a alors

$$\begin{aligned}
\beta \cdot \delta &\subseteq \gamma \cdot \delta \text{ d'après } Q_{\beta,\gamma}(\delta) \\
&\subseteq \sup_{\varepsilon \in \alpha}(\gamma \cdot \varepsilon) \text{ car la borne supérieure est un majorant} \\
&= \gamma \cdot \alpha \text{ par définition de la multiplication}
\end{aligned}$$

On a donc $\beta \cdot \delta \subseteq \gamma \cdot \alpha$.

Donc pour tout $\delta \in \alpha$ on a $\beta \cdot \delta \subseteq \gamma \cdot \alpha$.

Donc $\sup\limits_{\delta \in \alpha}(\beta \cdot \delta) \subseteq \gamma \cdot \alpha$ par minimalité de la borne supérieure.

Donc $\beta \cdot \alpha \subseteq \gamma \cdot \alpha$ par définition de la multiplication.

Autrement dit on a $Q_{\beta,\gamma}(\alpha)$.

Donc pour tout ordinal limite non nul γ, si $\forall \delta \in \alpha, Q_{\beta,\gamma}(\delta)$ alors $Q_{\beta,\gamma}(\alpha)$.

Ainsi $Q_{\beta,\gamma}$ vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal α on a $Q_{\beta,\gamma}(\alpha)$.

Autrement dit pour tout ordinal α, on a $\beta \cdot \alpha \subseteq \gamma \cdot \alpha$.

Donc pour tout ordinal α, $\boxed{\text{si } \beta \subseteq \gamma \text{ alors } \beta \cdot \alpha \subseteq \gamma \cdot \alpha}$.

CQFD.

Remarque :
Pour tout $n \in \omega$ on a $2 \cdot n \in \omega$ d'après la proposition 47 page 128.
On a donc $2 \cdot \omega = \sup_{n \in \omega}(2 \cdot n) \subseteq \omega$ par minimalité de la borne supérieure.

Par définition de 2 on a $2 = S(1)$.
On a donc $1 \in 2$ d'après la proposition 12 page 33.
En particulier on a $1 \subseteq 2$ d'après la proposition 8 page 20.
On a donc $1 \cdot \omega \subseteq 2 \cdot \omega$ par croissance de la multiplication à gauche.
Or on a $1 \cdot \omega = \omega$ car 1 est neutre pour la multiplication.
On a donc $\omega \subseteq 2 \cdot \omega$ et donc finalement $\boxed{\omega = 2 \cdot \omega}$.

Mais on a dit que $1 \in 2$ donc $\omega \cdot 1 \in \omega \cdot 2$ par stricte croissance de la multiplication à droite.
Or on a $\omega \cdot 1 = \omega$ car 1 est neutre pour la multiplication.
On a donc $\omega \in \omega \cdot 2$, donc en particulier $\omega \neq \omega \cdot 2$.
On en déduit que $2 \cdot \omega \neq \omega \cdot 2$ par ce qui précède.
Et oui, la multiplication des ordinaux n'est elle non plus pas commutative.
Nous verrons cependant qu'elle l'est dans le cas particulier des entiers naturels.

Le fait que $2 \cdot \omega = \omega$ ne soit là aussi pas nous surprendre. En effet par définition $2 \cdot \omega$ est la borne supérieure de l'ensemble $\{2 \cdot 0, 2 \cdot 1, 2 \cdot 2, \dots\}$, c'est-à-dire de l'ensemble des entiers pairs $\{0, 2, 4, \dots\}$, et là aussi on se doute qu'il s'agit de ω.

Proposition 49 (Régularité à gauche de la multiplication)

Soient α, β et γ trois ordinaux, avec α **non nul**.
Si $\alpha \cdot \beta = \alpha \cdot \gamma$ alors $\beta = \gamma$.
On dit que la multiplication des ordinaux est **régulière à gauche**.

Démonstration

Montrons-le par contraposition.

Supposons que $\beta \neq \gamma$.

On a donc $\beta \in \gamma$ ou $\gamma \in \beta$ d'après le théorème 1 page 21.

Si $\beta \in \gamma$ alors $\alpha \cdot \beta \in \alpha \cdot \gamma$ par stricte croissance de la multiplication à gauche.

Si $\gamma \in \beta$ alors $\alpha \cdot \gamma \in \alpha \cdot \beta$ par stricte croissance de la multiplication à gauche.

Dans les deux cas on a $\alpha \cdot \beta \neq \alpha \cdot \gamma$ par antiréflexivité de $\in$ chez ON.

Donc si $\beta \neq \gamma$ alors $\alpha \cdot \beta \neq \alpha \cdot \gamma$.

Donc par contraposition, $\boxed{\text{si } \alpha \cdot \beta = \alpha \cdot \gamma \text{ alors } \beta = \gamma}$.

CQFD.

Remarque :
Malheureusement la multiplication n'est pas régulière à droite.
En effet, on a vu que $1 \cdot \omega = \omega = 2 \cdot \omega$ alors que $1 \neq 2$.

Proposition 50 (Continuité à droite de la multiplication)

Soient α un ordinal et X un ensemble non vide d'ordinaux.
On a $\sup\limits_{\xi \in X}(\alpha \cdot \xi) = \alpha \cdot \sup\limits_{\xi \in X} \xi$.
Autrement dit la multiplication à droite est continue.

Démonstration

Par définition de la multiplication des ordinaux, pour tout ordinal limite non nul γ, on a

$$\alpha \cdot \gamma = \sup_{\delta \in \gamma}(\alpha \cdot \delta)$$

On peut alors appliquer la proposition 38 page 102 pour conclure.

CQFD.

Remarque :
Malheureusement, la multiplication des ordinaux n'est pas continue à gauche.
En effet, prenons $X = \omega = \alpha$. À la manière de la remarque où l'on a montré que $2 \cdot \omega = \omega$, on peut montrer que pour tout entier naturel non nul n, on a $n \cdot \omega = \omega$.
On a donc $\sup\limits_{n \in \omega}(n \cdot \omega) = \sup\limits_{n \in \omega} \omega = \omega$.

Mais comme ω est un ordinal limite, on a $\sup\limits_{n \in \omega} n = \omega$ donc $\left(\sup\limits_{n \in \omega} n\right) \cdot \omega = \omega \cdot \omega$.

Or par définition de la multiplication on a $\omega \cdot \omega = \sup\limits_{n \in \omega}(\omega \cdot n)$.

En particulier on a $\omega \cdot 2 \subseteq \sup\limits_{n \in \omega}(\omega \cdot n)$ donc $\omega \cdot 2 \subseteq \omega \cdot \omega$.

Or on a montré plus tôt que $\omega \in \omega \cdot 2$, donc $\omega \in \omega \cdot \omega$ par transitivité de $\in$ chez ON.

En particulier $\omega \neq \omega \cdot \omega$ et donc $\sup\limits_{n \in \omega}(n \cdot \omega) \neq \left(\sup\limits_{n \in \omega} n\right) \cdot \omega$.

Proposition 51 (Distributivité de la multiplication sur l'addition)

Pour tout ordinaux α, β et γ, on a l'égalité

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

On dit que la multiplication à gauche est **distributive** sur l'addition.

Démonstration

Fixons deux ordinaux α et β.

Posons $P_{\alpha,\beta}$ l'assertion à paramètre définie pour tout γ par

$$P_{\alpha,\beta}(\gamma) \iff \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

Montrons le résultat par le principe faible d'induction.

► *Initialisation*
On a

$$\begin{aligned}\alpha \cdot (\beta + 0) &= \alpha \cdot \beta \text{ car } 0 \text{ est neutre pour l'addition} \\ &= \alpha \cdot \beta + 0 \text{ car } 0 \text{ est neutre pour l'addition} \\ &= \alpha \cdot \beta + \alpha \cdot 0 \text{ car } 0 \text{ est absorbant pour la multiplication}\end{aligned}$$

On a donc $\alpha \cdot (\beta + 0) = \alpha \cdot \beta + \alpha \cdot 0$.
Autrement dit on a $P_{\alpha,\beta}(0)$.

► *Hérédité*
Soit γ un ordinal tel que $P_{\alpha,\beta}(\gamma)$.
Autrement dit on a $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.
On a alors

$$\begin{aligned}\alpha \cdot \big(\beta + S(\gamma)\big) &= \alpha \cdot S(\beta + \gamma) \text{ par définition de l'addition} \\ &= \alpha \cdot (\beta + \gamma) + \alpha \text{ par définition de la multiplication} \\ &= \alpha \cdot \beta + \alpha \cdot \gamma + \alpha \text{ par } P_{\alpha,\beta}(\gamma) \\ &= \alpha \cdot \beta + \alpha \cdot S(\gamma) \text{ par définition de la multiplication}\end{aligned}$$

Ainsi on a $\alpha \cdot \big(\beta + S(\gamma)\big) = \alpha \cdot \beta + \alpha \cdot S(\gamma)$.
Autrement dit on a $P_{\alpha,\beta}\big(S(\gamma)\big)$.
Donc pour tout ordinal γ, si $P_{\alpha,\beta}(\gamma)$ alors $P_{\alpha,\beta}\big(S(\gamma)\big)$.

► *Hérédité limite*
Soit γ un ordinal limite non nul tel que $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$.
On a alors

$$\begin{aligned}\alpha \cdot (\beta + \gamma) &= \alpha \cdot \sup_{\delta \in \gamma}(\beta + \delta) \text{ par définition de l'addition} \\ &= \sup_{\delta \in \gamma} \big(\alpha \cdot (\beta + \delta)\big) \text{ par continuité de la multiplication à gauche} \\ &= \sup_{\delta \in \gamma}(\alpha \cdot \beta + \alpha \cdot \delta) \text{ puisque } \forall \delta \in \gamma, P_{\alpha,\beta}(\delta) \\ &= \alpha \cdot \beta + \sup_{\delta \in \gamma}(\alpha \cdot \delta) \text{ par continuité de l'addition à gauche} \\ &= \alpha \cdot \beta + \alpha \cdot \gamma \text{ par définition de la multiplication}\end{aligned}$$

Ainsi on a $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Autrement dit on a $P_{\alpha,\beta}(\gamma)$.

Ainsi pour tout ordinal limite non nul γ, si $\forall \delta \in \gamma, P_{\alpha,\beta}(\delta)$ alors $P_{\alpha,\beta}(\gamma)$.

Ainsi $P_{\alpha,\beta}$ vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal γ on a $P_{\alpha,\beta}(\gamma)$.

Autrement dit pour tout ordinal γ, on a $\boxed{\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma}$.

CQFD.

Remarque :
Malheureusement la multiplication à droite n'est pas distributive.
En effet, on a déjà vu que $(1 + 1) \cdot \omega = 2 \cdot \omega = \omega$.
On a aussi vu que $1 \cdot \omega + 1 \cdot \omega = \omega + \omega$.
Comme $\omega \neq \omega + \omega$, on a $(1 + 1) \cdot \omega \neq 1 \cdot \omega + 1 \cdot \omega$.

Proposition 52 (Associativité de la multiplication)

Pour tout ordinaux α, β et γ, on a l'égalité

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

On dit que la multiplication des ordinaux est **associative**.

Démonstration

Fixons deux ordinaux α et β.

Posons $P_{\alpha,\beta}$ l'assertion à paramètre définie pour tout ordinal γ par

$$P_{\alpha,\beta}(\gamma) \iff (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

Montrons le résultat par le principe faible d'induction.

► *Initialisation*

On a $(\alpha \cdot \beta) \cdot 0 = 0 = \alpha \cdot 0 = \alpha \cdot (\beta \cdot 0)$.

On a donc $P_{\alpha,\beta}(0)$.

► *Hérédité*

Soit γ un ordinal tel que $P_{\alpha,\beta}(\gamma)$.

Autrement dit on a $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

On a alors

$$\begin{aligned}(\alpha\cdot\beta)\cdot S(\gamma) &= (\alpha\cdot\beta)\cdot\gamma+\alpha\cdot\beta \text{ par définition de la multiplication}\\ &= \alpha\cdot(\beta\cdot\gamma)+\alpha\cdot\beta \text{ par hypothèse}\\ &= \alpha\cdot(\beta\cdot\gamma+\beta) \text{ par distributivité}\\ &= \alpha\cdot\big(\beta\cdot S(\gamma)\big) \text{ par définition de la multiplication}\end{aligned}$$

Ainsi on a $(\alpha\cdot\beta)\cdot S(\gamma)=\alpha\cdot\big(\beta\cdot S(\gamma)\big)$.

Autrement dit on a $P_{\alpha,\beta}\big(S(\gamma)\big)$.

Donc pour tout ordinal γ, si $P_{\alpha,\beta}(\gamma)$ alors $P_{\alpha,\beta}\big(S(\gamma)\big)$.

► *Hérédité limite*

Soit γ un ordinal limite tel que $\forall\delta\in\gamma, P_{\alpha,\beta}(\delta)$.

On a alors

$$\begin{aligned}(\alpha\cdot\beta)\cdot\gamma &= \sup_{\delta\in\gamma}\big((\alpha\cdot\beta)\cdot\delta\big) \text{ par définition de la multiplication}\\ &= \sup_{\delta\in\gamma}\big(\alpha\cdot(\beta\cdot\delta)\big) \text{ car } \forall\delta\in\gamma, P_{\alpha,\beta}(\delta)\\ &= \alpha\cdot\sup_{\delta\in\gamma}(\beta\cdot\delta) \text{ par continuité de la multiplication à gauche}\\ &= \alpha\cdot(\beta\cdot\gamma) \text{ par définition de la multiplication}\end{aligned}$$

Ainsi on a $(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$.

Autrement dit on a $P_{\alpha,\beta}(\gamma)$.

Ainsi pour tout ordinal limite non nul γ, si $\forall\delta\in\gamma, P_{\alpha,\beta}(\delta)$ alors $P_{\alpha,\beta}(\gamma)$.

Ainsi $P_{\alpha,\beta}$ vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal γ on a $P_{\alpha,\beta}(\gamma)$.

Autrement dit pour tout ordinal γ, on a $\boxed{(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)}$.

CQFD.

Remarque :
Désormais pour trois ordinaux α, β et γ trois ordinaux on notera $\alpha\cdot\beta\cdot\gamma$ pour désigner indifféremment $(\alpha\cdot\beta)\cdot\gamma$ et $\alpha\cdot(\beta\cdot\gamma)$, puisque l'on vient de voir qu'il s'agit du même ordinal.

On a vu lors de la proposition 45 page 126 que 0 est absorbant pour la multiplication. Autrement dit pour deux ordinaux, si au moins l'un des deux est nul alors leur produit sera nul. Mais la réciproque est-elle vraie ? Autrement dit, si le produit de deux ordinaux est nul, cela veut-il dire qu'au moins un des deux est nul ? La réponse est oui : on parle cette fois d'intégrité.

Proposition 53 (Intégrité de la multiplication des ordinaux)

Soient α et β deux ordinaux.
Si $\alpha \cdot \beta = 0$ alors $(\alpha = 0$ ou $\beta = 0)$.
On dit que la multiplication des ordinaux est **intègre**.

Démonstration

Supposons que $\alpha \cdot \beta = 0$ et que $\alpha \neq 0$.

On sait que $\alpha \cdot 0 = 0$ car 0 est absorbant pour la multiplication.

Ainsi on a $\alpha \cdot \beta = \alpha \cdot 0$.

Or α est non nul par hypothèse.

On a donc $\beta = 0$ par régularité de la multiplication à gauche.

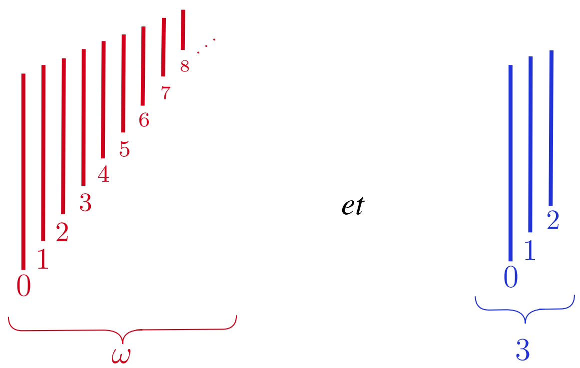
Donc si $(\alpha \cdot \beta = 0$ et $\alpha \neq 0)$ alors $\beta = 0$.

Donc $\boxed{\text{si } \alpha \cdot \beta = 0 \text{ alors } (\alpha = 0 \text{ ou } \beta = 0)}$.

CQFD.

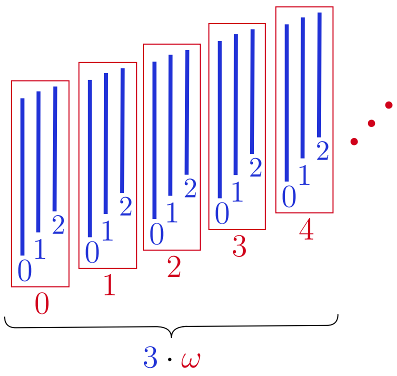
3.2 Interprétation graphique : le produit cartésien

La multiplication des ordinaux a aussi une interprétation graphique : visualisons par exemple l'addition des ordinaux ω et 3. Comme précédemment, commençons par les représenter tous les deux avec des bâtons indépendemment l'un de l'autre, ω et ses éléments étant en **rouge** et 3 est ses éléments étant en **bleu**.

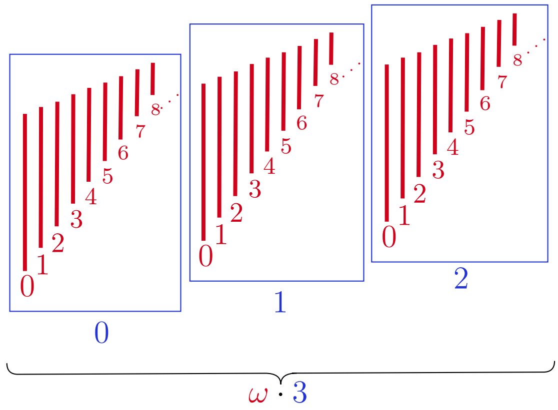


Rappelons à nouveau qu'ici seul l'ordre d'arrivée de la gauche vers la droite importe (pour traduire l'ordre sur les ordinaux), la taille verticale des bâtons n'est qu'une astuce pour visualiser une infinité de bâtons.

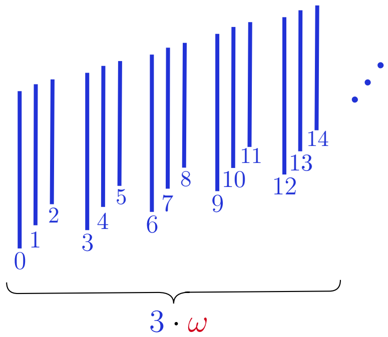
Pour représenter visuellement $\alpha \cdot \beta$, on vient remplacer chaque bâton de β par une copie de l'ensemble des bâtons constitutifs de α, ce qui dans notre cas donne



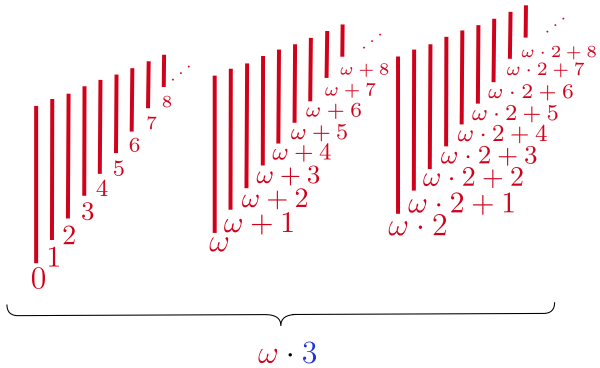
ou bien



Enfin, comme pour l'addition on renumérote les bâtons en fonction de leur ordre d'arrivée de la gauche vers la droite, ce qui nous donne

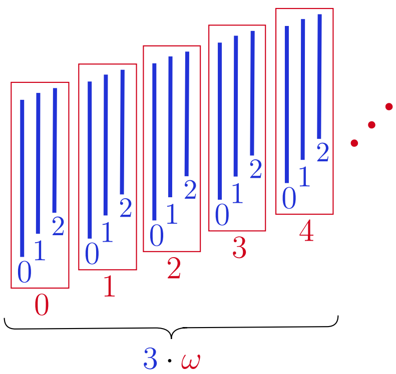


ou bien



On constate bien par exemple que $3 \cdot \omega = \{0, 1, 2, 3, 4, 5, \ldots, \} = \omega$, comme nous l'avons explicité plus tôt.

Quand il a fallu formaliser l'interprétation graphique de l'addition, nous avons dû introduire une nouvelle notion : celle de l'union disjointe ainsi que de l'ordre de concaténation. En ce qui concerne la multiplication, nous avons déjà tous les outils pour cela, puisqu'il s'agit du **produit cartésien**. En effet, si l'on reprend ce dessin d'interprétation de $3 \cdot \omega$



Le premier rectangle rouge tout à gauche peut être vu comme l'ensemble $\big\{(0, 0), (0, 1), (0, 2)\big\}$, le deuxième comme l'ensemble $\big\{(1, 0), (1, 1), (1, 2)\big\}$, le troisième comme l'ensemble $\big\{(2, 0), (2, 1), (2, 2)\big\}$, le quatrième comme l'ensemble $\big\{(3, 0), (3, 1), (3, 2)\big\}$, et ainsi de suite, avec un rectangle pour chaque $n \in \omega$ de la forme $\big\{(n, 0), (n, 1), (n, 2)\big\}$. En réunissant tous ces rectangles, on reconnaît précisément le produit cartésien $\omega \times \{0, 1, 2\} = \omega \times 3$. Oui, il faudra prendre garde au fait que la multiplication $3 \cdot \omega$ est associée au produit cartésien $\omega \times 3$, il y a une inversion du sens.

De quel ordre munir alors $\omega \times 3$? En fait, nous l'avons évoqué dans le premier livre et le premier chapitre : il s'agit de l'ordre lexicographique (en référence à l'ordre avec lequel fonctionne un dictionnaire). En effet, toujours avec le même dessin, on peut voir que tous les éléments du rectangle 1 sont situés avant tous les éléments du rectangle 2 : pour comparer les éléments du produit cartésien, il faut d'abord comparer les premières composantes de chaque couple et éventuellement si elles sont égales comparer les deuxièmes composantes. Nous avons déjà vu lors de la proposition 4 page 13 que si A et B sont munis de deux bons ordres, alors l'ordre lexicographique sur $A \times B$ est aussi un bon ordre. En particulier, si α et β sont deux ordinaux, alors $\alpha \times \beta$ est bien ordonné donc est associé à un unique ordinal (qu'on appelé son **type**). On retombe sur nos pieds : cet unique ordinal est précisément $\beta \cdot \alpha$.

Quel isomorphisme allons-nous construire ? Il s'agit sur l'illustration de trouver, étant donné un rectangle et la position du bâton au sein de ce rectangle, quel sera le numéro du bâton après renumérotation. Pour un couple (γ, δ) de $\alpha \times \beta$, on trouve le bon rectangle en prenant la $\gamma^{\text{ème}}$ copie de β, puis on se déplace de δ bâtons vers la droite, c'est-à-dire $\beta \cdot \gamma + \delta$. Par exemple le bâton 1 au sein du rectangle 2 a bien été renuméroté en $3 \cdot 2 + 1 = 7$ à la fin.

Théorème 8 (Multiplication d'ordinaux et produit cartésien)

Soient α et β deux ordinaux.
On munit $\alpha \times \beta$ de l'ordre lexicographique.
On a alors $\beta \cdot \alpha = \mathrm{type}(\alpha \times \beta)$.

Démonstration

• **Construction de l'isomorphisme**

Soit $(\gamma, \delta) \in \alpha \times \beta$.

On a alors $\gamma \in \alpha$ et $\delta \in \beta$.

Comme $\gamma \in \alpha$ on a $S(\gamma) \subseteq \alpha$ d'après la proposition 12 page 33.

On a donc

$$\begin{aligned}
\beta \cdot \gamma + \delta &\in \beta \cdot \gamma + \beta \text{ par stricte croissance de l'addition à gauche} \\
&= \beta \cdot \gamma + \beta \cdot 1 \text{ car 1 est neutre pour la multiplication} \\
&= \beta \cdot (\gamma + 1) \text{ par distributivité} \\
&= \beta \cdot S(\gamma) \text{ d'après la prop. 33 p. 94} \\
&\subseteq \beta \cdot \alpha \text{ par croissance de la multiplication à gauche}
\end{aligned}$$

On a donc $\beta \cdot \gamma + \delta \in \beta \cdot \alpha$.

Ainsi pour tout $(\gamma, \delta) \in \alpha \times \beta$, on a $\beta \cdot \gamma + \delta \in \beta \cdot \alpha$.

On peut donc considérer l'application $\varphi_\alpha := \left(\begin{array}{ccc} \alpha \times \beta & \longrightarrow & \beta \cdot \alpha \\ (\gamma, \delta) & \longmapsto & \beta \cdot \gamma + \delta \end{array} \right)$.

Le fait d'avoir mis α en indice nous servira pour une preuve par induction sur α.
Montrons que φ_α est un isomorphisme d'ordres.

• Surjectivité
Pour cette partie fixons β.
Montrons que pour tout ordinal α, l'application φ_α est surjective sur $\beta \cdot \alpha$.
Posons P l'assertion à paramètre définie pour tout ordinal α par

$$P(\alpha) \iff \operatorname{im}(\varphi_\alpha) = \beta \cdot \alpha$$

Remarquons que pour α et α' deux ordinaux, si $\alpha \subseteq \alpha'$ alors $\alpha \times \beta \subseteq \alpha' \times \beta$ et pour tout $(\gamma, \delta) \in \alpha \times \beta$ on a $\varphi_\alpha(\gamma, \delta) = \beta \cdot \gamma + \delta = \varphi_{\alpha'}(\gamma, \delta)$, si bien que $\varphi_\alpha = (\varphi_{\alpha'})_{|\alpha \times \beta}$.
En particulier dans ce cas-là on a $\operatorname{im}(\varphi_\alpha) \subseteq \operatorname{im}(\varphi_{\alpha'})$.
Remarquons aussi que pour tout ordinal α on a $\operatorname{im}(\varphi_\alpha) \subseteq \beta \cdot \alpha$ donc on doit seulement montrer l'inclusion réciproque.

► *Initialisation*
Par définition de la multiplication on a $\beta \cdot 0 = 0$.
On a donc $\operatorname{im}(\varphi_0) \subseteq 0$ et comme $0 = \varnothing$ on a donc $\operatorname{im}(\varphi_0) = 0$.
Autrement dit on a $P(0)$.

► *Hérédité*
Soit α un ordinal tel que $P(\alpha)$.
Autrement dit on a $\operatorname{im}(\varphi_\alpha) = \beta \cdot \alpha$.
Soit $\varepsilon \in \beta \cdot S(\alpha)$.
On a alors $\varepsilon \in \beta \cdot \alpha$ ou $\beta \cdot \alpha \subseteq \varepsilon$ d'après le théorème 1 page 21.
Si $\varepsilon \in \beta \cdot \alpha$ alors comme $\beta \cdot \alpha = \operatorname{im}(\varphi_\alpha) \subseteq \operatorname{im}(\varphi_{S(\alpha)})$ on a $\varepsilon \in \operatorname{im}\big(\varphi_{S(\alpha)}\big)$.
Plaçons-nous désormais dans le cas où $\beta \cdot \alpha \subseteq \varepsilon$.
On peut alors définir $\mu := \varepsilon - (\beta \cdot \alpha)$ d'après la proposition 44 page 123.
On a donc $\varepsilon = \beta \cdot \alpha + \mu$.
On a alors $\mu \in \beta$ ou $\beta \subseteq \mu$ d'après le théorème 1 page 21.
Supposons par l'absurde que $\beta \subseteq \mu$.
On a alors

$$\begin{aligned}
\beta \cdot S(\alpha) &= \beta \cdot (\alpha + 1) \text{ d'après la prop. 33 p. 94} \\
&= \beta \cdot \alpha + \beta \cdot 1 \text{ par distributivité} \\
&= \beta \cdot \alpha + \beta \text{ car } 1 \text{ est neutre pour la multiplication}
\end{aligned}$$

$\subseteq \beta \cdot \alpha + \mu$ par croissance de l'addition à gauche

$= \varepsilon$ par définition de μ

On a donc $\beta \cdot S(\alpha) \subseteq \varepsilon$.

C'est absurde puisque par définition de ε on a $\varepsilon \in \beta \cdot S(\alpha)$.

Par l'absurde on vient de montrer que $\mu \in \beta$.

Or on a $\alpha \in S(\alpha)$ d'après la proposition 12 page 33.

On a donc $(\alpha, \mu) \in S(\alpha) \times \beta$.

Donc $\varepsilon = \beta \cdot \alpha + \mu = \varphi_{S(\alpha)}(\alpha, \mu)$ par définition de $\varphi_{S(\alpha)}$.

On a donc $\varepsilon \in \mathrm{im}\big(\varphi_{S(\alpha)}\big)$.

On a donc $\mathrm{im}\big(\varphi_{S(\alpha)}\big) \supseteq \beta \cdot S(\alpha)$ et donc $\mathrm{im}\big(\varphi_{S(\alpha)}\big) = \beta \cdot S(\alpha)$.

Autrement dit on a $P\big(S(\alpha)\big)$.

Donc pour tout ordinal α, si $P(\alpha)$ alors $P\big(S(\alpha)\big)$.

► *Hérédité limite*

Soit α un ordinal limite non nul tel que $\forall \mu \in \alpha, P(\mu)$.

Autrement dit pour tout $\mu \in \alpha$ on a $\mathrm{im}(\varphi_\mu) = \beta \cdot \mu$.

Soit $\varepsilon \in \beta \cdot \alpha$.

Par définition de la multiplication on a $\beta \cdot \alpha = \sup\limits_{\mu \in \alpha}(\beta \cdot \mu) = \bigcup\limits_{\mu \in \alpha}(\beta \cdot \mu)$.

Il existe donc $\mu \in \alpha$ tel que $\varepsilon \in \beta \cdot \mu$.

Or on a $\mathrm{im}(\varphi_\mu) = \beta \cdot \mu$ par hypothèse donc $\varepsilon \in \mathrm{im}(\varphi_\mu)$.

Or on a $\mu \in \alpha$ donc $\mathrm{im}(\varphi_\mu) \subseteq \mathrm{im}(\varphi_\alpha)$ et donc $\varepsilon \in \mathrm{im}(\varphi_\alpha)$.

On a donc $\mathrm{im}(\varphi_\alpha) \supseteq \beta \cdot \alpha$ et donc $\mathrm{im}(\varphi_\alpha) = \beta \cdot \alpha$.

Autrement dit on a $P(\alpha)$.

Donc pour tout ordinal limite non nul α, si $\forall \mu \in \alpha, P(\mu)$ alors $P(\alpha)$.

Ainsi P vérifie les trois conditions du principe faible d'induction.

Donc pour tout ordinal α on a $P(\alpha)$.

Autrement dit pour tout ordinal α, on a $\mathrm{im}(\varphi_\alpha) = \beta \cdot \alpha$.

Autrement dit pour tout ordinal α, $\boxed{\varphi_\alpha \text{ est surjective dans } \beta \cdot \alpha}$.

• **Stricte croissance**

Fixons à nouveau α et β.

Notons $\lhd$ l'ordre lexicographique strict sur $\alpha \times \beta$.

Soient (γ, δ) et (γ', δ') dans $\alpha \times \beta$ tels que $(\gamma, \delta) \lhd (\gamma', \delta')$.

On a donc $\gamma \in \gamma'$ ou $(\gamma = \gamma'$ et $\delta \in \delta')$.

► Plaçons-nous dans le cas où $\gamma \in \gamma'$.

On a donc $S(\gamma) \subseteq \gamma'$ d'après la proposition 12 page 33.

On a donc

$$\begin{aligned}
\beta \cdot \gamma + \delta &\in \beta \cdot \gamma + \beta \text{ par stricte croissance de l'addition à gauche} \\
&= \beta \cdot \gamma + \beta \cdot 1 \text{ car } 1 \text{ est neutre pour la multiplication} \\
&= \beta \cdot (\gamma + 1) \text{ par distributivité} \\
&= \beta \cdot S(\gamma) \text{ d'après la prop. 33 p. 94} \\
&\subseteq \beta \cdot \gamma' \text{ par croissance de la multiplication à gauche} \\
&= \beta \cdot \gamma' + 0 \text{ car } 0 \text{ est neutre pour l'addition} \\
&\subseteq \beta \cdot \gamma' + \delta' \text{ par croissance de l'addition à gauche}
\end{aligned}$$

On a donc $(\beta \cdot \gamma + \delta) \in (\beta \cdot \gamma' + \delta')$.

Donc $\varphi_\alpha(\gamma, \delta) \in \varphi_\alpha(\gamma', \delta')$.

► Plaçons-nous dans le cas où $\gamma = \gamma'$ et $\delta \in \delta'$.

On a alors $(\beta \cdot \gamma + \delta) \in (\beta \cdot \gamma + \delta')$ par stricte croissance de l'addition à gauche.

Comme $\gamma = \gamma'$, on a donc $(\beta \cdot \gamma + \delta) \in (\beta \cdot \gamma' + \delta')$.

Donc $\varphi_\alpha(\gamma, \delta) \in \varphi_\alpha(\gamma', \delta')$.

Dans les deux cas on a donc $\varphi_\alpha(\gamma, \delta) \in \varphi_\alpha(\gamma', \delta')$.

Donc pour tout (γ, δ) et (γ', δ') dans $\alpha \times \beta$, si $(\gamma, \delta) \lhd (\gamma', \delta')$ alors $\varphi_\alpha(\gamma, \delta) \in \varphi_\alpha(\gamma', \delta')$.

Donc φ_α est strictement croissante.

Or $\mathrm{dom}(\varphi_\alpha) = \alpha \times \beta$ est bien ordonné d'après la proposition 4 page 13.

En particulier $\mathrm{dom}(\varphi_\alpha)$ est totalement ordonné d'après la proposition 2 page 11.

Donc $\boxed{\varphi_\alpha \text{ est injective et croissante}}$.

• **Conclusion**

Ainsi φ_α est croissante, injective et surjective sur $\beta \cdot \alpha$.

Or on vient de dire que $\mathrm{dom}(\varphi_\alpha) = \alpha \times \beta$ est totalement ordonné.

Donc φ_α est un isomorphisme d'ordres de $\alpha \times \beta$ vers $\beta \cdot \alpha$.

Ainsi $\alpha \times \beta$ et $\beta \cdot \alpha$ sont isomorphes, et donc $\boxed{\beta \cdot \alpha = \mathrm{type}(\alpha \times \beta)}$.

CQFD.

Proposition 54 (Division ordinale)

Soient α et β deux ordinaux, avec α **non nul**.

Il existe un unique couple d'ordinaux (ρ, σ) tel que $\beta = \alpha \cdot \sigma + \rho$ avec $\rho \in \alpha$ et $\sigma \subseteq \beta$.

Démonstration

Par définition α est non nul donc $0 \in \alpha$.

On a donc $1 = S(0) \subseteq \alpha$ d'après la proposition 12 page 33.

De même on a $\beta \in S(\beta)$ d'après la proposition 12 page 33.

On a donc

$$\begin{aligned} \beta &= 1 \cdot \beta \text{ car } 1 \text{ est neutre pour la multiplication} \\ &\subseteq \alpha \cdot \beta \text{ par croissance de la multiplication à droite} \\ &\in \alpha \cdot S(\beta) \text{ par stricte croissance de la multiplication à gauche} \end{aligned}$$

Ainsi on a $\beta \in \alpha \cdot S(\beta)$.

Or on a vu dans la preuve du théorème 8 page 140 que l'application

$\varphi := \begin{pmatrix} S(\beta) \times \alpha & \longrightarrow & \alpha \cdot S(\beta) \\ (\sigma, \rho) & \longmapsto & \alpha \cdot \sigma + \rho \end{pmatrix}$ est bijective de $S(\beta) \times \alpha$ dans $\alpha \cdot S(\beta)$.

Il existe donc un unique $(\sigma, \rho) \in S(\beta) \times \alpha$ tel que $\beta = \varphi(\rho, \sigma) = \alpha \cdot \sigma + \rho$.

Comme $\sigma \in S(\beta)$ on a $\sigma \subseteq \beta$ d'après la proposition 12 page 33.

CQFD.

Remarque :
Bien que cette division ressemble à la division euclidienne, il faut prendre garde au fait que le quotient σ peut être égal au dividende β. Par exemple on a $\omega = 2 \cdot \omega + 0$.

Bibliographie

- Wikipédia
- Kenneth Kunen, *The Foundations of Mathematics*, 29 octobre 2007.
- Jean-Louis Krivine, *Théorie des ensembles*, 1998, éditions Cassini.

Mathématiciens