Introduction à la théorie des ensembles*

Paris, 2002

1 Ordinaux et cardinaux

1.1 Introduction et présentation informelle

Comme il l'a été dit en introduction, Cantor s'est d'abord intéressé au problème de la formalisation de l'infini. Il s'agissait de définir ce qu'est un ensemble infini, et de pouvoir comparer différents infinis. Certains sont plus gros que d'autres. Ainsi, $\mathbb{N}$ et $\mathbb{R}$ sont tous les deux infinis, mais intuitivement, $\mathbb{R}$ est plus gros que $\mathbb{N}$.
Pour avoir une bonne intuition des ordinaux et des cardinaux, on va définir une *relation d'ordre* sur la catégorie des ensembles ($\mathcal{S}et$).

Définition 1 . *Pour tous ensembles A et B, on note $A \sim B$ lorsqu'il existe une bijection de A sur B. On dit alors que A et B sont* **équipotents** *ou ont même* **puissance**.

Définition 2 . *Pour tous ensembles A et B, on note $A \preceq B$ s'il existe une injection de A dans B.*

Proposition 3 . *$\sim$ définit une relation d'équivalence sur ($\mathcal{S}et$).*

Proposition 4 . *Sur le quotient $(\mathcal{S}et)/\sim$, $\preceq$ définit alors une relation d'ordre.*

⋄ **Réflexivité** : $A \preceq A$
⋄ **Antisymétrie** : $(A \preceq B \wedge B \preceq A) \rightarrow A \sim B$ (**Théorème de Cantor-Bernstein**)
⋄ **Transitivité** : $(A \preceq B \wedge B \preceq C) \rightarrow A \preceq C$
De plus, si on suppose l'axiome du choix, alors cet ordre est total:
⋄ $(A \preceq B \vee B \preceq A)$ (**Théorème de trisection de Zermelo**).

On peut ainsi classer les ensembles par leur taille et dire que la classe d'un ensemble modulo $\sim$ est le **cardinal** de cet ensemble. Mais cette classe n'est pas un ensemble. On voudrait bien que le cardinal d'un ensemble soit un ensemble. Il faudrait donc un représentant canonique de chacune de ces classes. La théorie des cardinaux va permettre un tel choix, à condition de supposer l'axiome du choix.
En fait, pour définir la notion de cardinal, on utilise la notion d'ordinal, puisqu'un cardinal sera un ordinal particulier. Plusieurs ordinaux pourront avoir le même cardinal. La notion d'ordinal est donc plus fine. En outre, on peut la poser sans recourir à l'axiome du choix.

*Julien Page, Équipe de logique mathématique, Université Paris 7 - C.N.R.S.

Définition 5 . *On dit qu'un ensemble est bien ordonné, s'il est totalement ordonné et si toute partie non vide admet un élément minimum.*

On va voir, chose qui sera démontrée par la suite, que comme sur la catégorie $\mathcal{S}et$, on peut poser sur la catégorie des ensembles bien ordonnés ($\mathcal{W}ell\ \mathcal{O}rd$) (les morphismes sont les applications croissantes) une *relation d'ordre totale.*

Définition 6 . *Pour tout ensemble A et B, on note $A \sim_{WO} B$ lorsque A et B sont isomorphes pour la catégorie ($\mathcal{W}ell\ \mathcal{O}rd$).*

Définition 7 . *Pour tout A et B, on note $A \preceq_{WO} B$ s'il existe un plongement (un monomorphisme) de A dans B.*

Proposition 8 . *$\sim_{WO}$ définit une relation d'équivalence sur ($\mathcal{W}ell\ \mathcal{O}rd$).*

Proposition 9 . *Sur le quotient $(\mathcal{W}ell\ \mathcal{O}rd)/\sim_{WO}$, $\preceq_{WO}$ définit une relation d'ordre totale.*

La démonstration de *l'antisymétrie* et de la *totalité de l'ordre* sera donnée plus tard mais, contrairement au cas précédent, la preuve que l'*ordre* est *total* ne nécessite pas l'axiome du choix. Intuitivement, un **ordinal** correspond à une classe pour $\sim_{WO}$. Là encore, on voudrait avoir un **ensemble** qui représenterait chaque classe *ordinale.* Ceci va être construit dans le chapitre suivant.

1.2 Les ordinaux

Définition 10 *(transitivité). On dit qu'un ensemble X est* **transitif** *si*
$\forall t \ \ \forall s \ \ ((t \in s \in X) \to t \in X)$.

Exemple. L'ensemble $E = \{\emptyset, \{\emptyset\}\}$ est transitif.

Définition 11 *(ordinal). Un ensemble α est appelé un ordinal si*
$\diamond$ *α est transitif*
$\diamond$ *$(\alpha, \in)$ est bien ordonné (i.e la relation d'appartenance sur α est un bon ordre strict)*

Exemples.
$\star$ L'ensemble E ci-dessus est un ordinal.
$\star$ L'ensemble $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ est un ordinal.
$\star$ Si α est un ordinal, $\alpha \cup \{\alpha\}$ est aussi un ordinal.

1.2.1 La classe des ordinaux

Proposition 12 . *Les ordinaux forment une classe, notée Ord.*

Démonstration: il faut trouver un formule qui permette de définir les ordinaux; or le fait d'être transitif est représentable par une formule (celle donnée dans la définition ?) et le fait d'être bien ordonné pour la relation d'appartenance est aussi énonçable grâce à une formule. Il suffit donc de prendre la conjonction des deux pour obtenir une des formules possibles représentant les ordinaux.$\square$

Par la suite, si α et β sont deux ordinaux, on notera indifféremment $\alpha \in \beta$ et $\alpha < \beta$.

Définition 13 . *Si α est un ordinal, on note α^+ ou $\alpha+1$, l'ordinal $\alpha \cup \{\alpha\}$; on appelle cet ordinal, l'ordinal successeur de α.*

Définition 14 . *Soit α, un ordinal. S'il existe un ordinal β tel que $\alpha = \beta^+$, on dit que α est un* **ordinal successeur**. *Sinon, c'est un* **ordinal limite**.

On va montrer que la méta-relation $<$ $(=\in)$, sur la classe des ordinaux (d'un univers $\mathcal{U}$), est un bon ordre. Pour cela, il nous suffit de prouver le théorème:

Théorème 15 . *Soient α et β des ordinaux, alors, une et une seule des 3 éventualités suivantes se produit:*
1) $\alpha \in \beta$
2) $\beta \in \alpha$
3) $\alpha = \beta$

Corollaire 16 . *$(Ord, \in) = (Ord, <)$ est bien ordonnée, i.e. pour toute sous-classe $\mathcal{C}$ non vide de Ord définie par une formule ϕ, $\mathcal{C}$ admet un élément minimum pour $<$.*

Démonstration: on vérifie facilement que $<$ est transitive (un ordinal est transitif par définition), antiréflexive et totale. C'est un bon ordre car, si $\alpha \in \mathcal{C}$, alors l'élément minimum de l'ensemble $X = \{\beta \in \alpha : \phi(\beta)\}$ est minimum pour $\mathcal{C}$.$\Box$

Pour prouver le théorème 1, on va d'abord prouver le théorème fondamental suivant que l'on a implicitement évoqué dans l'introduction aux ordinaux.

Définition 17 . *Soit $(X, <)$, ensemble totalement ordonné. On dit que $Y \subset X$ est un segment initial de X si pour tout $y \in Y$, et pour tout $x \in X$, $x < y \rightarrow x \in Y$.*

Théorème 18 . *Soient (X, R) et (Y, S) deux ensembles bien ordonnés strictement. Alors un des deux cas suivants se produit:*
1) Il existe un unique segment initial Y_1 de Y et un unique isomorphisme d'ensembles ordonnés f de (X, R) sur $(Y, S|_{Y_1})$
2) Il existe un unique segment initial X_1 de X et un unique isomorphisme d'ensembles ordonnés g de (Y, S) sur $(X, R|_{X_1})$
3) Si de plus, a), et b) ont lieu simultanément, alors,$X = X_1$, $Y = Y_1$ et f et g sont inverses l'une de l'autre.

Démonstration:
Unicité : supposons qu'il existe deux segments initiaux Y_1 et $_2$ de Y et deux isomorphismes f_1 et f_2 de (X, R) sur $(Y, S|_{Y_1})$ et $(Y, S|_{Y_2})$ respectivement. Soit $Z = \{x \in X : f_1(x) \neq f_2(x)\}$. On va montrer que Z est vide. Sinon, soit x_0 son élément R-minimum. Supposons par exemple que $f_1(x_0) S f_2(x_0)$. Comme Y_2 est un segment initial de Y, $f_1(x_0) \in Y_2$ et donc, il existe $x_1 \in X$ tel que $f_2(x_1) = f_1(x_0) S f_2(x_0)$. Par isomorphisme, on a donc: $x_1 R x_0$ et $x_1 \in Z$ ce qui contredit la minimalité de x_0. L'unicité pour b) se prouve pareillement.
Preuve du c) : pour prouver par exemple que $g \circ f = Id_X$, il suffit de voir que $g(Y_1)$ est un segment initial de X et d'appliquer l'unicité du a).
Existence : on note, pour tous les $x \in X$ et $y \in Y$, $R_x = \{t \in X : tRx\}$ et $S_y = \{t \in Y : tSy\}$. Soient $f = \{(x, y) \in X \times Y$;il existe un isomorphisme entre R_x et $S_y\}$ et $g = \{(y, x) \in Y \times X$:il

existe un isomorphisme entre S_y et $R_x\}$. Montrons que f et g sont des solutions du problème:
$\diamond$ si on a $f(x) = y$ et $f(x) = z$, alors on aurait deux isomorphismes de R_x sur S_y et S_z respectivement. Ainsi, d'après c), $S_y = S_z$, et donc $y = z$. f est donc une application de domaine A_1 et d'image A_2. On montre de même que g est une application. Et il est facile de voir que f et g sont en fait réciproques l'une de l'autre. f et g sont donc deux bijections réciproques.
$\diamond$ A_1 est un segment initial de X: en effet, si $x \in A_1$ et zRx alors il exite un isomorphisme i de R_x sur $S_{f(x)}$. Mais alors, $i|_{R_z}$ est un isomorphisme de R_z sur $S_{i(z)}$ et donc, $z \in A_1$. De même, A_2 est un segment initial de Y.
$\diamond$ f est croissante: en effet, si x et z sont dans A_1 et que zRx, alors, il existe un isomorphisme i de R_x sur $S_{f(x)}$ et $i|_{R_z}$ est un isomorphisme de R_z sur $S_{i(z)} = S_{f(z)}$ par l'unicité de a). Ainsi, $S_{f(z)} \subset S_{f(x)}$ et donc, $f(z)Rf(x)$. f et g sont donc des isomorphismes.
$\diamond$ Finalement, si $A_1 = X$ alors, a) est vrai; et si $A_2 = Y$ alors, b) est vrai. Montrons qu'on ne peut pas avoir $A_1 \neq X$ et $A_2 \neq Y$. Sinon, soit $x = Min_R(X - A_1)$. Alors, $A_1 = R_x$ car pour tout $t \in A_1$, $t \in R_x$ sinon $x \leq t$ et donc x serait dans A_1. De plus, pour tout $t \in R_x$, $t \in A_1$ par minimalité de x. De même, on montre qu'il existe y tel que $A_2 = S_y$. Mais alors, f fournit un isomorphisme entre R_x et S_y. On aurait donc: $x \in A_1 = R_x$, ce qui est impossible, car la relation R est stricte.$\square$

On est maintenant en mesure de prouver le théorème 1, en utilisant:

Lemme 19 . *Si α et β sont des ordinaux, f un isomorphisme de α sur β. Alors, $\alpha = \beta$ et $f = Id_\alpha$.*

Démonstration: soit $X = \{x \in \alpha : f(x) \neq x\}$. Si X n'était pas vide, soit x_0 son plus petit élément. Pour tout $t \in x_0, t \in \alpha$ (par transitivité), et donc, $f(t) \in f(x_0)$. Or par minimalité de x_0, on a $t = f(t)$, et donc, $x_0 \subseteq f(x_0)$. De plus, pour tout $t \in f(x_0), t \in \beta$ et il existe $z \in \alpha / f(z) = t$. Ainsi, $z \in x_0$ et par minimalité de x_0, $z = f(z) = t \in x_0$. Ainsi, $f(x_0) \subseteq x_0$. Finalement, $x_0 = f(x_0)$, ce qui est une contradiction.$\square$

Démonstration du théorème 1.
Comme $\alpha \notin \alpha$, il est déjà facile de voir que l'on ne peut pas avoir 2 des trois alternatives simultanément. On conclut en utilisant le Lemme 3 et le fait qu'un segment initial d'un ordinal est encore un ordinal.$\square$

Proposition 20 . *La classe des ordinaux n'est pas un ensemble.*

Démonstration: sinon, $(Ord, \in)$ serait un ensemble transitif bien ordonné. Donc, Ord serait un ordinal, par définition et on aurait $Ord \in Ord$, ce qui est impossible.$\square$

Corollaire 21 *Soit (X, R) un ensemble bien ordonné. Alors il existe un unique ordinal α et un unique isomorphisme entre (X, R) et α.*

Démonstration: Les unicités ont déjà été vues. On raisonne par l'absurde. Ainsi, chaque ordinal α serait isomorphe à un segment initial de (X, R) d'après le théorème 2. Soit $Y = \{x \in X : x$ est un segment initial de X et x est isomorphe à un ordinal$\}$; soit alors $\phi(x,t)$ la formule: $\phi(x,t) = x \in Y \wedge t$ est un ordinal $\wedge$ il existe un isomorphisme entre x et $t\}$. D'après le Lemme 3, $\phi(x,t)$ est fonctionnelle. Par le schéma de remplacement, son *image* $\phi(Y)$ est un ensemble Y'. Or on a vu que $Y' = Ord$. La classe Ord serait donc un ensemble, ce qui est contradictoire.$\square$

1.2.2 Les ordinaux finis

Définition 22 . *Un ordinal est fini, s'il n'est équipotent à aucune de ses parties propres. Sinon, on dit qu'il est infini. Les ordinaux finis sont encore appelés* **entiers naturels**.

Ainsi par exemple, si on pose $\emptyset = 0, \{0\} = 1, \{0,1\} = 2, \ldots$, on obtient des ordinaux qui sont finis. Mais rien ne prouve qu'il y ait des ordinaux infinis. C'est pourquoi on le pose comme axiome:

Axiome de l'infini. Il existe un ordinal infini.

Le plus petit d'entre eux pour $\in$, qui est un bon ordre, sera appelé **oméga** et sera noté ω. On vérifie que c'est l'ensemble des ordinaux finis.

1.2.3 Opération sur les ordinaux

Addition.
A partir de deux ordinaux α et β, on va définir un unique ordinal $\alpha + \beta$. Pour ce faire, sur l'union disjointe $\alpha \sqcup \beta = \alpha \times \{0\} \cup \beta \times \{1\}$, on définit la relation R par:
$(x,t)R(x',t') \leftrightarrow (t = t' \wedge x \in x')$ ou $(t = 0 \wedge t' = 1)$.

On vérifie alors que R est une relation de bon ordre sur $\alpha \sqcup \beta$. Donc, il existe un unique ordinal γ isomorphe à $(\alpha \sqcup \beta, R)$ d'après le Corollaire 5. On pose par définition $\alpha + \beta = \gamma$.

Multiplication.
A partir de deux ordinaux α et β, on va définir un unique ordinal $\alpha \times \beta$. Pour ce faire, sur $\alpha \times \beta$, on définit la relation S par:
$(x,t)S(x',t') \leftrightarrow (x \in x')$ ou $(x = x' \wedge t \in t')$. C'est l'ordre lexicographique.

On vérifie alors que S est une relation de bon ordre sur $\alpha \times \beta$. Donc, il existe un unique ordinal γ' isomorphe à $(\alpha \times \beta, S)$ d'après le Corollaire 5. On pose par définition $\alpha \times \beta = \gamma'$.

1.3 Les cardinaux

1.3.1 Définition

Définition 23 . *On appelle cardinal un ordinal qui n'est en bijection avec aucun ordinal strictement plus petit.*

On vérifie alors facilement la proposition suivante.

Proposition 24 . *Tous les entiers naturels, i.e. tous les ordinaux finis, sont des cardinaux (finis) et ω est le premier cardinal infini.*

Lorsque ω est vu comme un cardinal, on note $\omega = \aleph_0$ (aleph zéro).

Proposition 25 . *Pour tout ensemble X, il existe un unique cardinal qui lui est équipotent. On le note $Card(X)$.*

Démonstration: d'après le théorème de Zermelo - formulation équivalente de (AC) -, on peut munir X d'un bon ordre. Il existe donc un ordinal qui lui est isomorphe. Soit $F(\alpha)$ la formule exprimant que α est équipotent à X. La classe des ordinaux qui satisfont F est non vide comme on vient de le voir. Elle admet donc un plus petit élément, qui est nécessairement un cardinal unique.$\square$

On a ainsi un représentant canonique de la classe d'équipotence de chaque X.

Remarque. Cette proposition est **équivalente** à l'Axiome du Choix. De plus, la notion de **cardinal d'un ensemble** n'a à priori pas de sens sans l'Axiome du Choix. Sans lui, on ne peut parler que de classe d'équipotence, comme on l'a fait en introduction. On avait alors évoqué le théorème de Cantor-Bernstein, que l'on va prouver maintenant.

1.3.2 Théorème de Cantor-Bernstein

Comme on l'a dit en introduction, sans utiliser l'axiome du choix, on va montrer le théorème de Cantor-Bernstein.

Théorème 26 *(Cantor-Bernstein).* $(A \preceq B \wedge B \preceq A) \to A \sim B$.

Démonstration: si $f_1 : A \to B$, et $f_2 : B \to A$ sont des injections, alors si on pose $B' = f_2(B)$ et $A_1 = f_2(f_1(A))$, on a $A_1 \subseteq B' \subseteq A$, et $B \sim B'$. Il suffit donc de montrer que $A \sim B'$. Soit $f = f_2 \circ f_1$, qui est une bijection de A sur A_1. On définit alors par récurrence:
$\diamond$ $A_0 = A,\ \ A_{n+1} = f(A_n)$
$\diamond$ $B_0 = B',\ \ B_{n+1} = f(B_n)$
On vérifie que l'on a $A_0 \supseteq B_0 \supseteq A_1 \supseteq B_1 \supseteq A_2 \supseteq \ \ldots \ \supseteq A_n \supseteq B_n \supseteq A_{n+1} \supseteq B_{n+1} \supseteq \ \ldots$. On définit alors sur A la fonction g par:
$g(x) = f(x)$ si $x \in A_n - B_n$ pour un certain n, $g(x) = x$ sinon. On voit dès lors que g est bijective d'image B'.$\square$

1.3.3 Opération sur les cardinaux

Pour tous ordinaux α et β, on définit grâce à (AC):

$\star$ $\alpha + \beta = Card(\alpha \sqcup \beta)$

$\star$ $\alpha \times \beta = Card(\alpha \times \beta)$

$\star$ $\alpha^\beta = Card(\alpha^\beta)$

Par récurrence transfinie, on montre alors la proposition suivante.

Proposition 27 . *Si α et β sont des ordinaux infinis alors, $\alpha + \beta = \alpha \times \beta = max(\alpha, \beta)$.*

Le résultat suivant est dû à Cantor.

Proposition 28 . *Pour tout cardinal $\alpha, \alpha < 2^\alpha$.*

Démonstration: on a une injection i de α dans $\mathcal{P}(\alpha)$ définie par $i(x) = \{x\}$. Donc, $\alpha \leq 2^\alpha$. De plus, l'inégalité est stricte, sinon, il existerait une surjection f de α sur $\mathcal{P}(\alpha)$. Or la partie $X = \{x \in \alpha : x \notin f(x)\}$ n'est pas dans $f(\alpha)$ - ce qui donnera une contradiction. En effet, si on avait un x tel que $f(x) = X$, on aurait $x \in X \leftrightarrow x \notin X$.$\square$

1.4 Le fini, le dénombrable et le non dénombrable

1.4.1 Ordinaux et cardinaux finis

Proposition 29 . *Les ordinaux finis sont exactement les cardinaux finis.*

De plus, on peut vérifier que sur les ordinaux finis, le $+$ ordinal coïncide avec le $+$ cardinal et aussi avec le $+$ usuels sur les entiers naturels. Il en est de même pour $\times$. Muni de ces opérations, ω peut être noté $\mathbb{N}$.
Dans tout univers $\mathcal{V}$ modèle de ZF, on peut donc définir un ω et donc un $\mathbb{N}$.

Définition 30 . *On dit qu'un ensemble est fini s'il est équipotent à un entier naturel.*

1.4.2 L'hypothèse du continu

Définition 31 . *On dit qu'un ensemble est dénombrable s'il est équipotent à ω.*

Se demandant si l'on pouvait dénombrer la droite réelle, appelée le **continu**, Cantor a montré la proposition suivante.

Proposition 32 . $Card(\mathbb{R}) = 2^{\aleph_0}$.

2 Bibliographie

• introduction élémentaire

[B] R.Cori & D.Lascar (Ed.), *Logique mathématique, volume 2*, Masson, Paris 1993

• théorie des ensembles

[K] J-L. Krivine, *Théorie des ensembles*, Cassini, Paris 1998

[J] T. Jech, *Set theory*, Academic Press, 1978

[Ku] K. Kunnen, *Set theory, an introduction to independence*, North Holland, Paris 1980

• théorie descriptive des ensembles

[Ke] A. Kechris, *Classical descriptive set theory*, Springer-Verlag, 1994

• théorie des ensembles plus poussée

[Ka] A. Kanamori, *The higher infinite*, Springer-Verlag, 1991

• fondation catégorique des mathématiques

[G] R. Goldblatt, *Topoï, the categorical analysis of logic*, North Holland, 1975

[MM] S. MacLane & I. Moerdijk, *Sheaves in geometry and logic, a first introduction*, Springer-Verlag, 1992