Sylvain Poirier
http://spoirier.lautre.net/

Fondements des mathématiques

5. Brouillon de la suite

Autres propriétés des ensembles finis

Proposition. *Soient un ensemble fini X et un ensemble Y. Alors il existe une injection de X dans Y ou il existe une injection de Y dans X.*

Preuve: supposons qu'il n'existe pas d'injection de Y dans X. Il existe une injection de $\emptyset$ dans Y. Puis, pour tous $A \subset X$ et $x \in X - A$, s'il existe une injection j de A dans Y, elle ne peut pas être surjective (sinon son inverse serait une injection de Y dans X), donc $\exists y \in Y, y \notin \mathrm{Im}\, j$. Donc il existe une injection j' de $A \cup \{x\}$ dans Y qui prolonge j par $j'(x) = y$. Ceci étant pour tous A et $x \in X - A$, il en résulte l'existnce d'une injection de X dans Y. CQFD

Proposition. *Si X est fini et Y est infini alors il existe une injection de X dans Y.*

En effet, si X est fini et Y est infini, alors il n'existe pas d'injection de Y dans X, donc il existe une injection de X dans Y.

Proposition. *Pour tout ensemble X on a (X est fini) $\Leftrightarrow$ ($\mathcal{P}(X)$ est fini).*

Preuve: Si X est fini alors $\mathcal{P}(X) \simeq \prod_{x \in X} \{\emptyset, \{x\}\}$ aussi. Réciproquement, l'injection $x \mapsto \{x\}$ de X dans $\mathcal{P}(X)$ montre que si $\mathcal{P}(X)$ est fini alors X aussi.

Théorème. *Pour tout ensemble X, les énoncés suivants sont équivalents:*
1) X est fini
2) la relation $\mathcal{S}$ dans $\mathcal{P}(X)$ est bien-fondée
3) la stricte inclusion dans $\mathcal{P}(X)$ est bien-fondée.
4) Tout $K \subset \mathcal{P}(X)$ non vide a un élément maximal (i.e. qui n'est inclus dans aucun autre).

Commençons par les preuves faciles:
3) $\Rightarrow$ 2) car $\mathcal{S}$ est inférieure à la stricte inclusion.
2) $\Rightarrow$ 1) : soit K l'ensemble des parties finies de X. On a

$$\begin{aligned} &\emptyset \in K \text{ et } \forall A, B \subset X, ((A \mathcal{S} B \text{ et } A \in K) \Rightarrow B \in K) \\ \Leftrightarrow\ &\forall B \subset X, (B = \emptyset \text{ ou } \exists A \subset X, A \mathcal{S} B \text{ et } A \in K) \Rightarrow B \in K \\ \Rightarrow\ &\forall B \subset X, (\forall A \subset X, A \mathcal{S} B \Rightarrow A \in K) \Rightarrow B \in K \end{aligned}$$

qui implique $K = \mathcal{P}(X)$ si $\mathcal{S}$ est bien-fondée.

2) $\Rightarrow$ 3) : utilise 2) $\Rightarrow$ 1), le corollaire 3 et un théorème vu sur les relations bien-fondées.

3) $\Leftrightarrow$ 4) à travers le remplacement de chaque partie par son complémentaire.

Il reste à faire l'étape la plus subtile: 1) $\Rightarrow$ 2). Pour cela, je propose trois preuves.

Première preuve : comme évidemment $\emptyset \in \mathcal{F}_{\mathcal{S}}$, la question est de montrer que $\mathcal{F}_{\mathcal{S}} \in \mathrm{Cut}(\mathcal{S})$. Soit donc $A \in \mathcal{F}_{\mathcal{S}}$, et $B \in X$ tel que $A \mathcal{S} B$. Soit $A' \subset X$ tel que $A' \mathcal{S} B$. Notons $x \in B - A$ et $x' \in B - A'$. Soit σ la permutation de X qui échange x et x' et laisse fixes les autres éléments. Elle induit l'échange de A et A'. La définition de $\mathcal{F}_{\mathcal{S}}$ n'étant pas affectée par σ, de $A \in \mathcal{F}_{\mathcal{S}}$ il résulte $A' \in \mathcal{F}_{\mathcal{S}}$. Ceci étant vrai pour tout A' tel que $A' \mathcal{S} B$, il en résulte $B \in \mathcal{F}_{\mathcal{S}}$. CQFD

Deuxième preuve: soit $K \subset \mathcal{P}(X)$ tel que $\forall B \in K, \exists A \in K, A \mathcal{S} B$. Il s'agit de montrer que $K = \emptyset$. Soit alors

$$L = \{C \subset X | \exists A \in K, \exists \phi \text{ permutation de } X, \phi[C] = A\}.$$

Comme $0 \notin K$ on a $\emptyset \notin L$. Puis, si $C \mathcal{S} D$, montrons que $C \notin L \Rightarrow D \notin L$, autrement dit $D \in L \Rightarrow C \in L$. On peut y arriver en manipulant bien les permutations...

Troisième preuve: soient A, B tels que $A \mathcal{S} B$ et $P(A)$ est bien-fondée. Notons $x \in B - A$, et montrons que $\mathcal{P}(B)$ est bien-fondée. Soit donc une partie non vide K de $\mathcal{P}(B)$. De deux choses l'une:

- Ou bien $K \cap \mathcal{P}(A) = K' \neq \emptyset$, auquel cas il existe $C \in K'$ tel que $\overleftarrow{\mathcal{S}}(C) \cap K' = \emptyset$. Alors $C \subset A$ donc $\overleftarrow{\mathcal{S}}(C) \subset \mathcal{P}(A)$ et donc $\overleftarrow{\mathcal{S}}(C) \cap K = \emptyset$.

- Ou bien $K \cap \mathcal{P}(A) = \emptyset$, auquel cas K est l'image fidèle d'une partie de $\mathcal{P}(A)$ (obtenue en ôtant de tout $C \in K$ son élément x), ce qui permet de conclure en utilisant encore que $P(A)$ est bien-fondée.

Proposition. *L'union de toute famille finie d'ensembles finis est finie.*

Preuve 1: si deux ensembles C et D sont finis alors $C \cup D$ est l'union des ensembles finis disjoints C et $D - C$ donc est finie; puis, si X est fini et $\forall x \in X, E_x$ est fini, alors si $B = A \cup \{x\} \subset X$ et $\bigcup_{y \in A} E_y$ est fini alors $\bigcup_{y \in B} E_y = E_x \cup \bigcup_{y \in A} E_y$ est fini.

Preuve 2: on utilise le résultat sur les ensembles disjoints et la surjection de $\coprod_{x \in X} E_x$ dans $\bigcup_{x \in X} E_x$.

Proposition. *Toute injection d'un ensemble fini dans lui-même est bijective.*

Preuve: soit f injection de X dans lui-même. Alors $A \mapsto f[A]$ est strictement croissante. Soit K l'ensemble des $A \subset X$ tels que $f[A] \underset{\neq}{\subset} A$. Alors $\forall A \in K, f[f[A]] \underset{\neq}{\subset} f[A]$, donc $f[A] \in K$. Ainsi K n'a pas d'élément minimal. Donc si X est fini alors $K = \emptyset$. CQFD

Proposition. *Toute surjection d'un ensemble fini dans lui-même est bijective.*

Preuve: par le théorème du choix fini, si f est surjective de X dans X alors il existe g injective de X dans X telle que $f \circ g = \mathrm{Id}_X$. D'après la proposition précédente, g est bijective. Donc f est bijective.

Proposition. *Dans un ensemble fini, toute relation antiréflexive dont le préordre engendré est un ordre, est bien-fondée.*

Preuve: soit R une telle relation sur X fini, et $\pi = \overleftarrow{\langle R \rangle}$ application de X dans $\mathcal{P}(X)$. Pour tous $x, y \in X$ tels que xRy on a d'une part $x \neq y$ car R est antiréflexive, d'autre part $x \langle R \rangle y$. Puis, π étant strictement croissante de l'ordre $\langle R \rangle$ vers l'ordre d'inclusion, il en résulte $\pi(x) \underset{\neq}{\subset} \pi(y)$. Alors la conclusion vient du fait que $\underset{\neq}{\subset}$ est bien-fondée.

Axiomes supplémentaires

Définition. *Soit une relation R sur un ensemble E. On dit que R est un ordre total, ou que E est totalement ordonné par R, si R est une relation d'ordre telle que $\forall x, y \in E, xRy$ ou yRx.*

Deux ensembles E et F seront dits *équipotents* s'il existe une bijection entre E et F. Cette relation est réflexive (Id_E bijection de E sur E), symétrique (par inversion) et transitive (par composition). C'est donc une relation d'équivalence sur l'univers.

On appelle *cardinal* d'un ensemble E et on note $\#E$ sa classe d'équivalence pour cette relation. Ainsi définis, les cardinaux ne sont pas en toute rigueur des objets de l'univers, mais des classes. Cependant, mieux que d'autres classes ils se manipulent comme des objets, parce que ce qu'on en dira peut formellement se traduire en remplaçant chaque cardinal $\#E$ par la donnée de E, et chaque énoncé sur $\#E$ par un énoncé sur E dont la valeur reste inchangée si on remplace E par tout autre ensemble en bijection avec E. Ce sont ainsi les énoncés sur les ensembles qui ont cette propriété d'invariance, qui serviront à définir des notions sur les cardinaux. En particulier, l'énoncé $\#E = \#F$ s'interprète comme abbréviation de l'existence d'une bijection entre E et F.

Entre les cardinaux on définit la relation d'ordre: $\#E \leq \#F$ ssi il existe une injection de E dans F. En effet, par composition il apparaît que cette relation ne dépend que des cardinaux de E et de F. C'est un préordre pour les mêmes raisons que la relation d'équipotence, et sur les cardinaux il est antisymétrique d'après le théorème suivant:

Théorème de Cantor-Bernstein. *Soient deux ensembles E et F, et soient $f : E \to F$ et $g : F \to E$ deux applications injectives. Alors il existe une bijection entre E et F.*

Preuve: l'application de l'ensemble des parties de E dans lui-même définie par

$$P \mapsto E\backslash g[F\backslash f[P]]$$

étant croissante (comme composée de 4 applications dont deux croissantes et deux décroissantes), a un point fixe A. Notant $B = F\backslash f[A]$, on a $g[B] = E\backslash A$.

D'autre part, toute restriction d'une injection étant une injection, les applications $f_{|A}$ et $g_{|B}$ sont des bijections respectivement de A sur $F\backslash B$ et de B sur $E\backslash A$. On en conclut que

$$E \ni x \mapsto (f(x), (g_{|B})^{-1}(x))(x \in A)$$

est une bijection de E sur F.

CQFD

On peut définir un autre préordre entre cardinaux, par l'existence d'une surjection de F dans E: notons-le $\preceq$. Sauf pour $\#\emptyset$ qui n'est alors comparable à aucun autre cardinal, ce préordre est plus large que l'ordre ci-dessus.

Dans le cadre de la théorie des ensembles avec axiome du choix, $\preceq$ et $\leq$ coïncident (sauf pour $\#\emptyset$). En fait, l'axiome du choix entraîne aussi un résultat plus fort (mais nettement plus difficile à démontrer) : $\leq$ devient un ordre total. Mais laissons cela de côté.

Pour tout ensemble E, tout cardinal inférieur à $\#E$ est celui d'une partie de E. Ainsi, on peut employer au titre d'ensemble des cardinaux inférieurs à $\#E$, l'ensemble quotient de $\mathcal{P}(E)$ par la relation d'équipotence.

Nous adopterons dorénavant l'axiome suivant:

Axiome de l'infini. *Il existe un ensemble infini.*

C'est le seul axiome qui sera nécessaire pour nos besoins, au-delà de ce que nous avions déjà admis. Les autres axiomes qui seront évoqués (dont l'axiome du choix) le seront à titre de curiosité.

D'après les résultats précédents, tout ensemble fini est de cardinal inférieur à tout ensemble infini. Par conséquent, étant donné un ensemble infini E, le quotient de l'ensemble des parties finies de E par la relation d'équipotence, figure l'ensemble de tous les cardinaux finis (i.e. cardinaux des ensembles finis). Ainsi peut-on définir l'ensemble $\mathbb{N}$ des nombres entiers, et pour tout ensemble fini F définir $\#F \in \mathbb{N}$, comme étant l'ensemble de toutes les images d'injections de F dans E.

Les bijections canoniques remarquables que nous avions exposées, se traduisent par le cardinal en les identités remarquables plus familières dans $\mathbb{N}$.

S'il existe une injection de X vers un ensemble Y alors $\mathrm{Choix}(Y) \Rightarrow \mathrm{Choix}(X)$. En particulier s'il existe une bijection entre X et Y alors $\mathrm{Choix}(Y) \Leftrightarrow \mathrm{Choix}(X)$, et si $X \subset Y$ alors $\mathrm{Choix}(Y) \Rightarrow \mathrm{Choix}(X)$. De plus on peut voir que $(\mathrm{Choix}(X)$ et $\mathrm{Choix}(Y)) \Rightarrow \mathrm{Choix}(X \cup Y)$ et plus généralement pour toute famille d'ensembles $(X_i)_{i\in I}$ on a $(\mathrm{Choix}(I)$ et $\forall i \in I, \mathrm{Choix}(X_i)) \Rightarrow \mathrm{Choix}(\coprod_{i\in I} X_i)$, et si I est fini et $\forall i \in I, \mathrm{Choix}(X_i)$ alors $\mathrm{Choix}(\bigcup_{i\in I} X_i)$.

(D'autres choses seront insérées ici; la numérotation de la section suivante sera déterminée ultérieurement)

Ce que le schéma de remplacement signifie vraiment

Le schéma de remplacement est la liste infinie des énoncés construits chacun à partir d'un énoncé F quelconque à au moins deux variables libres x, y, et pouvant admettre des quantificateurs ouverts (sans domaine), comme suit:

$$\forall(\text{autres paramètres de } F), \forall A \text{ ensemble}, (\forall x \in A, \exists y, F(x, y)) \Rightarrow (\exists B, \forall x \in A, \exists y \in B, F(x, y)).$$

Expliquons d'abord pourquoi son interprétation naïve telle qu'elle est traditionnellement insinuée dans tous les cours introductifs à la théorie des ensembles est fausse.

Le problème est qu'il s'applique à toute formule avec des quantificateurs non limités par des ensembles, mais portant sur l'univers. Par conséquent, à la base, l'interprétation de ces formules n'est pas absolue, mais fonction de l'univers dans lequel elles sont interprétées. Alors, allons-y: prenons un univers U, et interprétons dedans une formule à utiliser dans un axiome de remplacement. Dedans on prend un ensemble A, on définit une application f de domaine A à partir de la formule où tous les quantificateurs écrits sans domaine sont interprétés comme étant de domaine U. Cette application étant bien définie dans U de domaine l'ensemble A, son ensemble image peut à juste titre être considéré comme un ensemble, à savoir défini par compréhension dans U: il n'est pas potentiellement capable de contenir d'éléments hors de U à l'avenir. Bien. Seulement, en ce sens, ce n'est un ensemble que du point de vue où U est un ensemble, autrement dit, du point de vue d'un univers U' ultérieur à U.

Question: dans quel univers cet axiome de remplacement doit-il être interprété ?

En effet, la formule qu'il utilise était à interpréter dans l'univers U, mais l'ensemble image dont il nous apprend l'existence n'existe que dans U'. On pourrait dire: allons-y, interprétons le tout dans U'. Oui mais cela fait interpréter différemment la formule de définition de f de sorte qu'on n'a plus affaire à un énoncé sur f et son image, mais un énoncé sur une application f" définie par la même formule que f mais dans U' au lieu de U: ces deux application n'ont a priori aucune raison d'être égales. Ainsi, U' a beau contenir l'ensemble image de f, cela ne rend pas l'axiome vrai dedans pour autant, puisque cet axiome y parle de f' et de son image, a priori différente de celle de f que contenait U'.

Ainsi, l'interprétation naïve des axiomes de remplacement viole les règles de correction qui doivent normalement être respectées pour s'assurer contre les contradictions du type paradoxe de Russel lorsqu'on oublie la distinction entre ensembles et classes.

Certains seraient peut-être tentés d'objecter à la critique plus haut: l'image de f n'est pas à interpréter comme définie par compréhension dans U, mais comme un simple ensemble pour la seule raison qu'il est en bijection avec A. Réponse: cette remarque est hors sujet, du fait que ce qui distingue un ensemble d'une classe dans un univers n'est pas une question de cardinalité, mais une question d'époque d'apparition de ses éléments. L'univers U apparaît comme ensemble immédiatement après que tous ses éléments soient arrivés à l'existence. On ne peut intepréter la formule dans U que lorsque tous ses éléments sont bien apparus, et alors U est essentiellement un ensemble. Avant cela, il manquait encore des éléments à l'univers U, de sorte que l'image de f en tant que partie de U, pouvait dans certains cas rester capable de contenir certains éléments de U qui n'existaient pas encore. Ce n'était donc pas un ensemble, quand bien même on définirait exactement combien d'éléments manquaient à l'appel. Il n'y a même pas besoin qu'il en manque beaucoup, un seul suffit. Par exemple U est lui-même un seul objet, mais il n'est pas objet de lui-même parce qu'il apparaît plus tard.

Alors, le schéma de remplacement est-il idiot et faux, et les logiciens ont-ils fait fausse route de baser dessus tous leurs travaux ? Non, au contraire, il est génial, encore faut-il expliquer pourquoi. Les professionnels le savent, mais l'explication reste méconnue. Enfin, on pourrait dire que deux explications philosophiques sont possibles.

L'une (axiome de l'inaccessible) serait relativement simple à présenter à partir de la connaissance des ordinaux, mais exprime un postulat arbitraire philosophiquement injustifiable, et donc hasardeux: ce n'est pas vraiment une justification.

Nous allons maintenant présenter la bonne justification. La "construction philosophique" qui suit s'inspire de l'exposé du *schéma de réflexion* et des preuves de l'équivalence entre schéma de remplacement et schéma de réflexion, qui se trouve dans le livre de théorie des ensembles de J-L Krivine, et dont la lecture peut utilement compléter la compréhension du sujet. (Quelques trucs se trouvent aussi par google: "reflection principle" ZF, mais à son survol je n'y ai rien vu de clair).

Il s'agit d'interpréter les formules d'une manière "absolue" et par induction sur les symboles de variables liées sans domaine, suivant l'ordre dans lequel ils sont disposés dans la forumule. Pour simplifier l'explication, réécrivons les formules en traduisant tous les quantificateurs par $\exists$, éventuellement encadré par autant de négations que nécessaire.

D'abord pour les formules dépourvues de variable liée sans domaine, leur interprétation n'a pas d'ambiguïté. Qu'en est-il ensuite des formules ayant une seule telle variable ? Interprétons l'énoncé d'existence d'une valeur de la variable ayant la propriété, sous la forme de la question absolue de l'existence d'une telle valeur quelque part parmi tous les univers qui pourront jamais arriver à exister. Comme ils n'existent pas encore, on ne peut pas le savoir, mais si on croit en Dieu, alors on peut admettre que Celui-ci le sait. Alors on adresse à Dieu cette prière: O mon Dieu, si un élément ayant cette propriété arrivera finalement à exister quelque part dans un univers parmi toutes les éternités à venir que Tu connais, montre-le moi ! Et alors Dieu, qui est gentil (du moins dans le monde abstrait hypothétique des maths), nous le révèle, nous projetant pour cela tout de suite à travers toutes les éternités (tous les univers) nécessaires pour y parvenir. Et voilà, cet élément existe désormais dans notre univers, qui, bien que n'achevant pas l'inachevable éternité de tous les univers que Dieu connaît, commence déjà à ressembler un peu à celle-ci, puisque la question de l'existence d'un élément ayant cette propriété est de même réponse. (Non hélas, ça ne marche pas avec les filles, du moins pas de manière injective).

Et s'il y a plusieurs variables liées sans domaine, on répète le même principe d'interprétation absolue en le réimbriquant dans lui-même par récurrence: toute formule de la forme $(\exists x, F(x))$ s'interprète absolument après avoir interprété absolument $F(x)$, comme signifiant l'existence d'un objet x quelque part dans tous les univers à venir, qui arrivera à satisfaire F suivant son sens absolu.

Remarque, par ce jeu d'imbrications, la signification en vient à s'effilocher: dans une formule $\exists x, \forall y, F(x, y)$ où F n'a pas de quantificateur sans domaine, on pourrait presque considérer sa signification absolue comme éventuellement indécidable: au cours de quelques éternités, on peut ne pas trouver de x, mais si on en trouve un, cela risque d'en être un faux, pour lequel on n'est pas encore assez monté dans les univers pour découvrir un contre-exemple de valeur de y. Mais si on en trouve, cela ne réfute pas la formule pour autant, mais signifie seulement qu'on n'a peut-être pas encore trouvé la bonne valeur de x. Peut-être ainsi la valeur apparente de la formule alternera-t-elle indéfiniment d'un univers à l'autre. Si elle alterne indéfiniment, alors en définitive elle est fausse, tous les x ayant été trouvés étant finalement des faux. Oui mais ça peut aussi n'être là encore qu'une apparence, du fait qu'il faudrait attendre encore plus pour trouver l'éventuel bon x. Et ainsi de suite. Dieu est libre de nous révéler arbitrairement ce qu'il veut. Il n'y a aucun moyen de le vérifier, sauf bien sûr dans des cas particuliers de formule F.

Mais revenons-en aux axiomes de remplacement.

Cette fois-ci, écrivons les quantificateurs dans une formule F sous leurs deux formes sans utiliser de négations, autrement dit, écrivons $F(x, y)$ comme une pure succession de quantificateurs suivie d'une formule sans quantificateur (c'est possible, petit exercice de manipulation de formules).

Demandons à Dieu de nous révéler pour tout x au moins un exemple d'élément y s'il en existe un tel que $F(x, y)$ interprété au sens absolu. Demandons-lui même un tout petit peu plus (enfin c'est un peu la même chose), à savoir que pour tout ensemble A on dispose d'un ensemble B contenant pour tout $x \in A$ au moins un y tel que $F(x, y)$ s'il en existe. Et aussi, de nous révéler au moins un exemple de valeur pour tout quantificateur d'existence dans l'écriture de F qui se trouverait absolument vrai, pour chaque valeur possible des paramètres liés par des $\forall$ respectivement extérieurs à ces $\exists$.

Demandons-le lui encore de même avec (non F), réécrit normalement en remplaçant tout symbole $\exists$ dans F par un $\forall$ et inversement. Et aussi avec d'autres énoncés.

Tous ces nouveaux éléments révélés pouvant eux-mêmes à nouveau servir de nouvelles valeurs à ces paramètres ainsi qu'à x, il faut donc recommencer cette procédure à l'infini. Par chance, la simple récurrence sur $\mathbb{N}$ suffit à cela. Profitons-en pour enrichir à chaque étape la liste des énoncés à demander ainsi: à la n-ième étape, demandons ainsi pour tous les énoncés syntaxiquement corrects de longueur au plus n.

Le point est que chaque étape de cette construction par récurrence étant supposément effectuée d'après une lecture absolue de F, les éléments révélés à une étape demeureront valables lors de l'interprétation absolue de F qui sera effectuée à toute étape ultérieure de la récurrence. On a alors une suite croissante d'univers, et il suffit d'en prendre l'union.

On arrive ainsi à un gros univers $\mathcal{U}$ contenant au moins un exemplaire de "vraie" image y par

F de tout élément x qui a au moins une image par F au sens absolu. De plus, ces images seront effectivement toutes reconnues comme telles dans $\mathcal{U}$, puisque pour tout quantificateur existentiel de F muni de valeurs données de ses variables libres qui soit vrai, un exemple de valeur en est donné dès l'univers qui suit celui contenant toutes les valeurs des variables libres (ce dernier existe puisqu'il n'y a qu'un nombre fini de symboles de variables dans la formule). Et tout quantificateur universel absolument vrai est évidemment vrai en particulier dans $\mathcal{U}$.

Et inversement, s'il semble que $F(x, y)$ dans $\mathcal{U}$ alors cela est également vrai absolument à cause de tous les éléments créés pour la négation de F (les quantificateurs universels de F). En effet, si tel n'était pas le cas, (non $F(x, y)$) serait absolument vrai, de sorte que la révélation qui a été effectuée des éléments qui témoignent de la véracité de chacun de ses constituants, l'auraient déjà rendue vraie dans $\mathcal{U}$.

Concluons : si dans $\mathcal{U}$ on a un ensemble A, forcément apparu à une des étapes de la récurrence, la formule $\forall x \in A, \exists y, F(x, y)$ est vraie, alors elle est aussi vraie absolument. Alors, les constructions précédentes nous ont d'abord donné, à l'étape suivante, un ensemble E' de valeurs de y telles que $\forall x \in A, \exists y \in B, F(x, y)$ en un sens absolu. Puis ont fait construire finalement notre univers $\mathcal{U}$ de sorte que pour chaque valeur donnée de x et de y, on ait $F(x, y)$ vraie dans $\mathcal{U}$ dès qu'elle est vraie absolument. Voilà pourquoi la conclusion $\forall x \in A, \exists y \in B, F(x, y)$ est vraie dans $\mathcal{U}$.

CQFD

Ainsi nous avons "trouvé" un univers dans lequel le schéma de remplacement est vrai, mais où son interprétation naïve est fausse, puisqu'il a été construit explicitement comme union d'une suite d'ensembles indexée par $\mathbb{N}$. Cela n'entraîne pas la contradiction qui semblerait pointer son nez ici, du fait qu'il est impossible d'écrire, même à l'aide de quantificateurs ouverts, un énoncé $V(F, x)$ qui pour toute formule F à quantificateurs ouverts sans limite de nombre de variables liées, formalisable comme objet mathématique, soit toujours équivalent à $F(x)$. (La multiplicité des paramètres pouvant facilement se traduire en prenant pour x un n-uplet). Eh oui, ce n'est pas pour rien que le schéma de remplacement reste intraduisible en une liste finie d'axiomes sauf à introduire les classes comme une autre espèce d'objets !

(Et à qui après avoir assimilé tout cela douterait encore de la pertinence de cette analyse, j'ajouterai que, d'après ce que j'ai vu passer dans mes lectures, les énoncés suivants seraient consistants dans ZF sans axiome du choix : "$\mathcal{P}(\mathbb{N})$ est une union dénombrable d'ensembles dénombrables" et même "tout ordinal est de cofinalité dénombrable" !)

Bien sûr, sans s'aventurer jusque-là, on peut vouloir dire malgré tout quelque chose en première année pour signaler qu'il existe quelque chose nommé schéma de remplacement, mais quoi ? Que c'est quelque chose d'exrêmement puissant généralisant le schéma de compréhension, et dont la conséquence la plus élémentaire qui ne peut pas s'obtenir par la seule axiomatique de Zermelo, est l'existence, comme objet de l'univers mathématique dans lequel on travaille, d'une suite d'ensembles $(E_n)_{n\in\mathbb{N}}$ telle que $E_0 = \mathbb{N}$ (ensemble des entiers naturels), et pour tout $n \in \mathbb{N}$, E_{n+1} est l'ensemble de toutes les parties de E_n; résultat qui est déjà largement inutile aux mathématiques de base.

Algèbres universelles

Remarque. *La condition pour qu'une τ-application d'une écriture $(E\lambda)$ vers une écriture (F, λ') soit un L-morphisme, s'écrit $f_L \circ \lambda = \lambda' \circ f$. Tout morphisme bijectif entre deux écritures est un isomorphisme.*

Preuve. La traduction de la condition de L-morphisme en la formule est immédiate. Si g est l'inverse de f, on a

$$g_L \circ \lambda' = g_L \circ \lambda' \circ f \circ g = g_L \circ f_L \circ \lambda \circ g = \lambda \circ g.$$

CQFD

Une L-algèbre (E, ϕ) sera qualifiée d'*injective*, *surjective*, *bijective*, suivant la propriété correspondante de ϕ comme application de $O_L(E)$ dans E.

Théorème. *Il existe une L-algèbre injective.*

Preuve non-rigoureuse: l'univers mathématique a une structure de L-algèbre injective Id_{O_L}.

Preuve rigoureuse:

Grâce à l'axiome de l'infini, prenons I un ensemble infini fixé, et m un élément pur indépendant. Soit $\mathcal{T}$ le τ-ensemble des termes (T, λ) où $\mathcal{T} \subset X \times I$, classifié suivant le plus grand élément du terme.

Soit E l'ensemble quotient de $\mathcal{T}$ par la relation d'isomorphisme, et π la surjection canonique de $\mathcal{T}$ dans E. Comme π est surjective et $\forall x, x' \in E, \pi(x) = \pi(x') \Rightarrow \tau(x) = \tau(x')$ (deux termes isomorphes ont la même espèce), il existe donc un unique $\tau' \in X^E$ tel que $\tau = \tau' \circ \pi$. Ceci définit donc une classification de E.

Soit $(s, u) \in O_L(\mathcal{T})$. Notons $\forall a \in [s], u(a) = (T(a), \lambda_a)$. Soit $K(s, u)$ le terme constitué de l'ensemble

$$\{m_s\} \cup \coprod_{a \in [s]} T(a)$$

où $m_s = (\tau(s), m)$, muni des structures suivantes. Notant $\forall a \in [s], j_a = (x \mapsto (a, x))$ la famille des injections canonique des $T(a)$ dans $K(s, u)$, on le classifie par $\coprod_{a\in[s]} \tau_{|T(a)}$ de sorte que les j_a soient des τ-applications. Sa structure λ sera ainsi définie de la manière suivante:

- $\lambda(m_s) = (s, (a \mapsto m_{u(a)}))$, où $m_{u(a)}$ est le plus grand élément du terme $u(a)$ comme expliqué plus haut. - Sur le coproduit elle se définit par transport des structures λ_a, à savoir $\coprod_{a\in[s]} \hat{\supset}_a \circ \lambda_a$.

On vérifie que c'est bien un terme, de la manière suivante:

L'élément m_s est le plus grand élément de $K(s, u)$ car, par transport de structure, chaque élément de $\{a\} \times T(a)$ est inférieur à $m_{u(a)}$ et $m_{u(a)} R m_s$.

Par transport de structure encore, chaque $m_{u(a)}$ est fondé pour R; ce sont les éléments de $\overleftarrow{R}(m_s)$, donc aussi m_s est fondé pour R. Comme c'est le plus grand élément pour l'ordre engendré, il en résulte que $K(s, u)$ est bien-fondé.

Ayant donc bien défini le terme $K(s, u)$ pour tout $(s, u) \in O_L(\mathcal{T})$, vérifions qu'il existe dans $\mathcal{T}$ un terme isomorphe à $K(s, u)$. Comme c'est un terme, il est fini, donc il a une injection dans I. On en tire une τ-applicationinjective à valeurs dans $X \times I$. Ceci permet de construire, par transport de structure, un élément de $\mathcal{T}$ isomorphe à $K(s, u)$.

Par conséquent, l'ensemble des éléments de $\mathcal{T}$ isomorphes à $K(s, u)$ est non vide; c'est une classe d'équivalence de $\mathcal{T}$ pour la relation d'isomorphisme, donc cela définit un élément de E noté $\lambda'(s, u)$.

Par ailleurs, on peut facilement vérifier que pour tous (s, u) et (s', u') dans $O_L(\mathcal{T})$ tels que $\hat{\pi}(s, u) = \hat{\pi}(s', u')$ (autrement dit $s = s'$ et $\pi \circ u = \pi \circ u'$), les termes $K(s, u)$ et $K(s', u')$ sont isomorphes, grâce au théorème du choix fini appliqué à $[s]$. Il en résulte que $\lambda'(s, u) = \lambda'(s', u')$.

Nous avons donc trois ensembles $O_L(\mathcal{T})$, $O_L(E)$ et E, avec:

- Une τ-application surjective $\hat{\pi}$ de $O_L(\mathcal{T})$ dans $O_L(E)$.

- Une τ-application λ' de $O_L(\mathcal{T})$ dans E.

tels que $\forall x, x' \in O_L(\mathcal{T}), \hat{\pi}(x) = \hat{\pi}(x') \Rightarrow \lambda'(x) = \lambda'(x')$.

Il existe donc un unique $\lambda \in E^{O_L(E)}$ tel que $\lambda' = \lambda \circ \hat{\pi}$, et même plus précisément $\lambda \in E_\tau^{O_L(E)}$.

Il ne reste plus qu'à vérifier que λ est injective. Exprimons cet énoncé comme représenté à travers la surjection $\hat{\pi}$:

Soient donc (s, u) et (s', u') dans $O_L(\mathcal{T})$ tels que $\lambda'(s, u) = \lambda'(s', u')$, autrement dit que $K(s, u)$ et $K(s', u')$ sont isomorphes. On cherche à montrer que $\hat{\pi}(s, u) = \hat{\pi}(s', u')$, autrement dit que $s = s'$ et $\pi \circ u = \pi \circ u'$.

Notant λ_1 et λ_2 les structures respectives de $K(s, u)$ et $K(s', u')$, et f un isomorphisme entre eux. On a $f_L \circ \lambda_1 = \lambda_2 \circ f$.

f transporte le plus grand élément m_s de $K(s, u)$ en le plus grand élément $m_{s'}$ de $K(s', u')$. Donc $f_L(\lambda_1(m_s)) = \lambda_2(m_{s'})$. Donc $s = s'$ et $\forall a \in [s], f(m_{u(a)}) = m_{u'(a)}$.

On a $\forall a \in [s], \operatorname{Im} j_a = \overleftarrow{\langle R \rangle}(m_{u(a)})$ (où R est définie au moyen de λ_1 sur $K(s, u)$). Par conséquent, comme f est un isomorphisme, $\forall a \in [s], f[\operatorname{Im} j_a] = \operatorname{Im} j'_a$. Donc $u(a)$ et $u'(a)$ sont isomorphes, soit $\pi(u(a)) = \pi(u'(a))$. Ainsi $\pi \circ u = \pi \circ u'$. CQFD.

Proposition et définition. *Les conditions suivantes sur un L-magma sont équivalentes*
1) C'est une L-écriture dont la structure λ est bijective

2) C'est à la fois une L-écriture et une L-algèbre
3) C'est une L-algèbre injective et minimale
4) C'est une L-algèbre bijective et minimale
Un tel magma est appelé une L-algèbre universelle.

On a évidemment 1) $\Leftrightarrow$ 2) et 4) $\Rightarrow$ 3). Pour une L-algèbre, sa bijectivité équivaut au fait que sa structure puisse s'exprimer sous forme d'un $\lambda \in O_L(E)^E_\tau$; sa minimalité traduit le fait que la relation R que nous avons définie pour λ, est bien-fondée. Ainsi 2) $\Leftrightarrow$ 4). Enfin, 3) $\Rightarrow$ 4) parce que toute L-algèbre minimale est surjective. CQFD.

Lemme. *Toute sous-L-algèbre d'une L-algèbre injective est injective.*

En effet, si (E, ϕ) est une L-algèbre injective et F est une sous-L-algèbre de E, alors la structure de F est la restriction de ϕ à $O_L(F)$. Comme toute restriction d'une application injective, elle est également injective.

Proposition. *Il existe une L-algèbre universelle.*

On a vu en effet qu'il existe une L-algèbre injective. Sa sous-L-algèbre minimale est à la fois minimale et injective donc c'est une L-algèbre universelle.

Théorème. *Pour tout L-morphisme f d'une L-algèbre surjective (E, ϕ) dans une L-algèbre injective (F, ϕ'), l'ensemble $M = \{y \in F | \exists! x \in E, f(x) = y\}$ est une sous-L-algèbre de F.*

Preuve:
Soit $(s, v) \in O_L(M)$. On veut montrer que $\phi'(s, v) \in M$, autrement dit que

$$\exists! x \in E, f(x) = \phi'(s, v)$$

Comme $\operatorname{Im} v \subset M$, on a $\forall a \in [s], \exists! y \in E|_{\tau(a)},\ f(y) = v(a)$. Donc

$$\exists! u \in E^{[s]}_\tau, v = f \circ u.$$

On en tire l'existence de x par $\phi'(s, v) = \phi'(s, f \circ u) = f(\phi(s, u))$.

Pour l'unicité, soit maintenant $x \in E$ tel que $f(x) = \phi'(s, v)$. Comme ϕ est surjective, il existe $(s', u') \in O_L(E)$ tel que $\phi(s', u') = x$. On peut alors écrire

$$\phi'(s, v) = f(x) = f(\phi(s', u')) = \phi'(s', f \circ u').$$

Mais ϕ' est injective donc $s = s'$ et $v = f \circ u'$, donc aussi $u = u'$ par unicité de u.

Donc $x = \phi(s', u') = \phi(s, u)$, CQFD.

Corollaire 1. *Tout L-morphisme d'une L-algèbre surjective dans une L-algèbre universelle est un isomorphisme.*

En effet, dans le théorème, M est une sous-L-algèbre de F, de sorte que si F est minimale on a $M = F$ donc f est bijective, donc c'est un isomorphisme.

Corollaire 2. *Si on a un L-morphisme f d'une L-algèbre minimale E dans une L-algèbre injective F alors f est injectif et E est universelle.*

En effet, dans le théorème, comme M est une sous-L-algèbre, $f^*(M)$ l'est également. Si E est minimale on a alors $f^*(M) = E$. On en déduit facilement l'injectivité de f. Alors E est isomorphe à une sous-L-algèbre de F injective donc E est aussi injective. (Autre façon de le voir: l'injectivité de f implique celle de f_L, puis $\phi' \circ f_L = f \circ \phi$ qui est injective puisque ϕ' et f_L le sont, donc ϕ est injective).

Propriété universelle. *Pour toute L-algèbre universelle E et toute L-algèbre F il existe un unique L-morphisme de E dans F.*

Nous l'avons déjà montré pour les écritures, dont les algèbres universelles sont des cas particuliers. Ceci reposait sur le principe de définition par induction, dont la démonstration était un peu longue. Or, en substance, une grande part de cette démonstration vient d'être refaite sous forme d'autres résultats. Il peut donc être intéressant de remarquer comment ces derniers résultats permettent de redémontrer celui-ci:

Soit M la sous-L-algèbre minimale de $E \times_\tau F$. Sa projection sur E est un L-morphisme d'une L-algèbre surjective dans une L-algèbre universelle, donc c'est un isomorphisme. Ainsi M est un graphe d'une τ-application de E dans F, qui est un L-morphisme parce que M est une sous-L-algèbre de $E \times_e F$.

Tout autre L-morphisme de E dans F aurait pour graphe une autre sous-L-algèbre A de $E \times_e F$. Mais alors $A \subset M$ puisque M est minimale. Mais A et M étant des graphes, $A = M$, ce qui donne l'unicité du L-morphisme de E dans F.

CQFD.

Aussi, d'après les résultats précédents, ce L-morphisme de E dans F est injectif si F est injectif, et c'est un isomorphisme si F est universel.

Ainsi, entre deux L-algèbres universelles il existe un unique isomorphisme. A travers ces isomorphismes, ces L-algèbres se comportent comme de simples copies les unes des autres, qui ne peuvent servir à rien de plus qu'une seule d'entre elles. Par exemple on peut choisir celle qui vient des constructions précédentes, à savoir la sous-L-algèbre minimale de la L-algèbre injective que nous avions construite.

Notation. *On désignera par U_L une L-algèbre universelle fixée arbitrairement, et pour toute L-algèbre E on notera Ψ_E l'unique L-morphisme de U_L dans E.*

Proposition. $U_L = \emptyset \Leftrightarrow \forall s \in L, [s] \neq \emptyset$.

En effet, s'il existe un symbole de constante alors $O_L(U)$ est non vide donc U aussi; s'il n'en existe pas, la seule L-algèbre minimale est l'ensemble vide.

Proposition. *Pour toute L-algèbre E,* $\min E = \operatorname{Im} \Psi_E$.

Cela résulte du fait que U_L est minimale.

Définition et remarque. *Le produit de la famille vide de L-algèbre sera appelé la L-algèbre nulle et notée 0_L. Comme ensemble, c'est la copie de X; elle a une propriété universelle analogue à celle de U_L mais avec le sens des morphismes renversés: pour toute L-algèbre F il existe un unique L-morphisme de F dans 0_L.*

Conséquence: décomposition canonique des interprétations:

Soient M une L-écriture, et (E, ϕ) une L-algèbre. Alors l'interprétation de M dans E s'écrit $\Psi_E \circ \pi_M$ où π_M est l'interprétation de M dans U_L.

D'où l'importance de l'interprétation π d'une écriture dans l'algèbre universelle, par lequel l'algèbre universelle contient à elle seule tout symbole de constante qui peut s'obtenir par n'importe quel écriture: pour tout élément d'un écriture (jouant le rôle d'un symbole de constante), son image dans U par interprétation jouera le rôle du même symbole de constante. Les constantes de L elles-mêmes peuvent etre assimilées à leurs valeurs dans U.

On vérifie facilement (par induction) que: si M est injectif alors π est injective; si M est surjectif alors π est surjective.

L'image M' de π est un sous-écriture de U (muni de la structure de écriture inverse de sa structure d'algèbre), ce qui signifie: pour tout $x \in M'$, l'image de f_x est dans M'.

Vérification immédiate: $x = \pi(y) = \phi(s_y, \pi \circ f_y)$, d'où par bijectivité de ϕ avec $x = \phi(s_x, f_x)$, découle $f_x = \pi \circ f_y$.

Ainsi, toute écriture se comporte comme un ensemble de constantes qui s'ajoutent d'elles-mêmes au langage, en laissant intacts les ensembles de morphismes:

Soit M une L-écriture, et L' le langage $L \cup M$ où M est vu comme ensemble de symboles de constantes. Toute L-algèbre (E, ϕ) est naturellement muni d'une structure de L'-algèbre définie par ϕ sur L et l'interprétation de M dans E sur M. Le théorème ci-dessus nous assure que si E et F sont deux L-algèbres et f un L-morphisme de E dans F alors f est également un L'-morphisme de E dans F pour les structures de L'-algèbres sur E et F que nous venons de définir.

Au-delà de la logique du premier ordre

Construction de la puissance et son incomplétude en logique du premier ordre

Le problème de la construction de la puissance.

Cette construction dépend du choix d'un type (de relation ou d'opération).

On introduit une nouvelle espèce sensée représenter l'ensemble des relations ou opérations de ce type. Ce rôle lui est donné par l'ajout au langage d'un symbole de ce type augmenté d'une variable de la nouvelle espèce.

Dans ce qui suit, nous ne parlerons pour simplifier que de la question de construire un ensemble puissance de la forme F^E (ensemble des applications de E dans F) où E et F sont deux espèces. En effet, on peut se ramener au cas d'une seule variable au moyen d'une construction de produit; et le cas d'un type de relation s'y ramène en utilisant une espèce de constantes à deux éléments désignant les valeurs de vérité.

Déjà, où en sommes-nous ? Nous savons que dans tous les cas, une telle opération définit une application de la nouvelle espèce dans l'ensemble des applications voulues. Le problème qui reste est d'axiomatiser l'idée que cette application doit être bijective.

Posons déjà l'axiome exprimant l'injectivité, qui n'est autre que l'énoncé définissant l'égalité entre applications, que nous avons déjà vu:

$$(*). \qquad \forall f, f',\ (\forall x,\ f(x) = f'(x)) \Rightarrow f = f'$$

Mais il n'est généralement pas possible d'exprimer la surjectivité par un axiome, car où peut-on trouver les applications qui doivent être représentées dans notre ensemble puissance ? Faute de l'exprimer, cette construction reste incomplète. Sa simlulation dans le cas général est également impossible.

Constructions incomplètes

Nous avons vu à la section précédente les constructions (combinaisons particulières d'une extension, de structurations et de particularisations) qui sont complètes, c'est-à-dire ayant complètement la qualité de dynamique interne.

Dedans, les axiomes ont deux objectifs. Le premier est d'assurer que l'effet d'extension est anéanti par les nouvelles structures, qui détruisent toute indépendance de la nouvelle espèce par rapport aux précédentes, en sorte qu'on se trouve à une dynamique interne près à une situation où il n'y a que d'éventuelles structurations et particularisations. Le deuxième est d'assurer que cette construction est parfaitement déterministe, c'est-à-dire sans aucun effet de structuration (qui permettrait notamment de définir sur les anciennes espèces une structure qui n'existait pas ni n'était définissable auparavant). Nous ne considérerons que les situations où il n'y a pas d'effet de particularisation, car nous ne décrivons que les situations où la construction est possible (dans les lois décrites précédemment, la question n'intervenait que deux fois, sous forme d'un axiome dont on avait besoin pour permettre à la dynamique de s'appliquer: dans la définition d'une opération et dans la construction du quotient).

Nous appellerons *construction incomplète* une combinaison de dynamiques externes où les axiomes remplissent le premier objectif et non le deuxième. Cela revient à faire une structuration accompagnée d'une construction complète. On obtient naturellement un construction incomplète en ôtant d'une loi de construction l'axiome consacré au deuxième objectif.

Les deux exemples fondamentaux de construction incomplète sont le *quotient indéfini* et la *partie indéfinie*, dans lesquels la structure (la relation d'équivalence, respectivement la relation unaire) qui était utilisée dans la construction complète n'existe pas au préalable. On peut interpréter cette

structure comme ajoutée (structuration) avant de faire une construction complète avec, ou comme définie après la construction incomplète effectuée, ce qui revient au même.

Les autres cas de construction incomplète se réinterprètent comme construction incomplète de partie ou de quotient à partir de l'espèce obtenue par la construction complète correspondante. Notamment, on peut reformuler et tronquer la loi de produit en sorte d'obtenir une partie indéfinie ou un quotient indéfini du produit, et on peut tronquer la loi de somme en sorte d'obtenir un quotient indéfini de la somme. Ces trois sortes de constructions incomplètes peuvent se reformuler comme étant des structurations suivies de dynamiques internes (les structures ajoutées simulant celles qui définissent ensuite la partie ou le quotient).

La loi de puissance telle que présentée plus haut est une construction incomplète, car elle représente une partie indéfinie de la vraie puissance. Mais contrairement aux cas ci-dessus, on ne peut pas toujours introduire de structure préalable permettant de définir cette partie (mais seulement dans le cas de puissance paramétrée ci-dessous), ni effectuer de construction complète de la puissance avant d'en prendre ainsi une partie.

Complétude dans le cas fini

Considérons la construction incomplète de F^E à laquelle on ajoute les deux axiomes suivants:

$$(A1) \qquad \forall y \exists f \, \forall x \;\; f(x) = y$$

$$(A2) \qquad \forall f \forall x' \forall y \exists f' \forall x \;\; f'(x) = (y, f(x))(x = x').$$

On remarque que cette axiomatisation définit complètement la puissance dans le cas où l'ensemble E est un ensemble fini. D'ailleurs, il est également possible de simuler cette construction lorsque E est une espèce de constantes, car elle s'identifie alors à la construction du produit avec $C = E$. Plus généralement, si E est un ensemble fini dont on connaît le nombre d'éléments, on peut appliquer la même méthode de simulation en considérant E comme étant "virtuellement" une espèce de constantes (voir la section suivante), employant des symboles de variables à la place des symboles de constantes. Cette simulation fait appel à des énoncés qui dépendent du nombre n d'éléments de E: plus ce nombre est grand, plus les énoncés sont longs. Elle peut aussi s'interpréter comme une puissance paramétrée par une partie d'un produit, expression (à traduire en langage mathématique) de l'ensemble des applications définies par des énoncés de la forme

$$f(x_1) = y_1 \text{ et } \cdots \text{ et } f(x_n) = y_n \quad \text{où les } x_i \text{ sont tous distincts.}$$

Nous verrons plus loin que si E est infini et F a plus d'un élément, il est impossible d'axiomatiser complètement cette construction ou de la simuler, pour la logique du premier ordre dans laquelle nous étions. Une telle construction de puissance est alors considérée comme incomplète.

Mais nous allons aborder maintenant une autre logique, une autre philosophie ou interprétation des choses, suivant laquelle on considèrera l'opération de puissance d'un ensemble par un autre comme une construction complète.

Puissance et logique d'ordre supérieur

Ainsi s'exprime l'écart des points de vue entre la logique du premier ordre et la logique d'ordre supérieur: *La logique d'ordre supérieur admet dans son langage de départ la notion de puissance d'ensembles comme ayant une signification absolue "tombée du ciel", tandis que la logique du premier ordre ne la reconnaît que dans la mesure où elle peut la définir complètement (formellement) par des axiomes, en l'occurence précisément lorsque l'exposant E est fini; sans quoi elle la considère comme une construction incomplète.*

Plus précisément, on parle de *logique du second ordre* dans le cas particulier où on n'applique ce principe qu'à une seule construction de puissance, et de logique d'ordre supérieur dans le cas général où on l'applique à un nombre quelconque de telles constructions.

En conclusion, parler de l'ensemble puissance F^E alors que E est infini, c'est quitter la logique du premier ordre et se placer dans une logique du second ordre ou plus. Un résultat de logique est

que, contrairement à la logique du premier ordre, la logique d'ordre supérieur est incomplète, c'est-à-dire qu'on peut l'approcher par certains moyens formels visant à faire ressembler le plus possible l'ensemble puissance à ce qu'on voudrait qu'il soit, mais cette approche ne peut pas être terminée: il est impossible de la réduire à un fondement formel définitif à partir duquel se démontreraient tous les énoncés vrais, on pourra toujours y ajouter des compléments. Les moyens formels peuvent être des axiomes mais aussi des schémas d'axiomes. Un schéma d'axiomes est une liste infinie d'axiomes qui sont les énoncés produits par l'application d'une règle formelle décrite de manière finie.

Propriété universelle de la puissance

Quittant maintenant la logique du premier ordre, formalisons "telle quelle" l'idée que F^E serait l'ensemble de "toutes" les applications de E dans F, par l'axiome de propriété universelle. Puis nous allons illustrer son insuffisance par quelques remarques. (Nous supposerons toujours posé l'axiome $(*)$ pour un ensemble dit de puissance F^E quel qu'il soit).

Nous appellerons *propriété universelle* de l'ensemble puissance* F^E le schéma d'axiomes suivant:

A chaque fois qu'on trouvera dans la théorie (existant initialement ou qui résultera de développements à venir) une espèce A et un symbole d'opération T de type $(F,(A,E))$ (représentant donc une application de $A \times E$ dans F), on ajoutera l'axiome

$$\forall_A x\ \exists_{F^E} f\ \forall_E y\ f(y) = T(x,y),$$

ce qui revient (par une définition et grâce à $(*)$) à ajouter un symbole $\hat{T}$ d'application de A dans F^E et l'axiome

$$\forall x, y,\ \hat{T}(x)(y) = T(x,y).$$

L'utilisation de cette propriété un nombre fini de fois avec des espèces et opérations comme A et T produits par une suite de dynamiques internes *n'utilisant pas l'ensemble puissance* F^E est équivalente à une suite de dynamiques internes, et peut donc être considérée comme faisant partie de la logique du premier ordre. Mais son utilisation avec espèces et opérations qui s'appuient sur F^E lui-même ne fait plus partie de la logique du premier ordre.

Les deux axiomes (A1) et (A2) plus haut, qui suffisent à définir la puissance dans le cas fini, sont deux utilisations de la propriété universelle, qui sont respectivement dans la première et la deuxième situation.

Le "théorème" suivant, avec sa "démonstration", a en fait pour objet de préciser le sens *philosophique* de cet écart entre la logique du premier ordre et la logique d'ordre supérieur :

"Théorème". *La construction de la puissance munie de la propriété universelle est une construction "complète" au sens de la logique d'ordre supérieur.*

En effet, nous avons dit (cf. construction de la copie) que la notion de construction complète se caractérise par le fait que deux espèces construites de la même manière sont la copie l'une de l'autre, la bijection étant définie par la relation de conservation. Ici, si on construit deux versions P et P' d'une même puissance F^E, la propriété universelle de P donne une application de P' dans P, et la propriété universelle de P' donne une application de P dans P', qui sont l'inverse l'une de l'autre et sont définies par la relation de conservation (qui est ici l'égalité en tant qu'applications de E dans F). CQFD.

Bien sûr, en logique du premier ordre cette démonstration n'est pas valable, puisque la propriété universelle de P appliquée à P' suppose que P est construit après P' et à l'aide de lui, tandis que celle de P' appliquée à P suppose l'inverse. De plus, cette construction n'est pas simulable, et les règles que nous avons présentées n'achèvent pas le problème de l'axiomatisation de la puissance : l'axiome du choix, que nous verrons plus tard, est une propriété "intuitive" de la puissance qui n'en résulte pas.

---

* *La notion de propriété universelle est une forme générale de propriété mathématique; des exemples plus nombreux se trouvent dans le domaine de l'algèbre universelle, qui constitue une autre phase des fondements des mathématiques.*

Alors, que dit finalement la propriété universelle ? Précisément, elle signifie que l'ensemble puissance est déterminé de façon unique à une bijection conservative près, non pas d'après les conditions initiales ou dans l'absolu mais seulement *parmi toutes les espèces à disposition de la théorie* après cette "construction de puissance" effectuée !

La plus petite solution

Nous avons écrit des axiomes $(A1)$ et $(A2)$ qui définissent F^E dans le cas de E fini. Ces mêmes axiomes appliqués cette fois dans le cas de E infini admettent pour solution l'ensemble $F^{(E)}$ des applications de E dans F qui sont constantes en dehors d'une partie finie (non fixée) de E.

En particulier, dans le cas où F est une paire pour parler de l'ensemble des parties de E, on aurait l'ensemble $2^{(E)}$ des parties de E finies ou de complémentaire fini, qui jouerait le rôle d'un "ensemble de parties de E" acceptable du point de vue des axiomes ci-dessus.

Il se trouve que ces solutions sont en fait remarquablement résistantes face aux efforts d'axiomatisation de la construction de puissance en logique d'ordre supérieur, en comparaison de ce à quoi leur simplicité et leur "maigreur" manifeste laisseraient supposer.

Vérifions en effet que, en l'absence préalable de structure sur l'ensemble E ou reliant E à autre chose, cette solution passe avec succès l'épreuve de la propriété universelle de F^E.

Il y aurait à cela une démonstration un peu technique valable dans le cas général (avec autant qu'on veut de puissances et leurs propriétés universelles mais sans satisfaire l'axiome du choix). Nous allons donner ici la preuve dans le cas où on n'a rien construit de plus qui s'appuierait sur F^E, mais cela donne en même temps l'idée intuitive de la démonstration générale.

Remarquons d'abord que cet ensemble $F^{(E)}$ préserve la symétrie des rôles de tous les éléments de E, toute permutation de E induisant une permutation de $F^{(E)}$ qui conserve toutes les propriétés. Aucune utilisation d'une variable liée dans un énoncé ne peut rompre cette symétrie, qui ne peut ainsi être rompue que par l'utilisation de variables libres.

Aucune définition ou construction ne peut donc produire une application de E dans F ou une partie de E rompant d'autres symétries que celles rompues par les valeurs de ses variables libres. Chacune de ces variables, soit est dans E et n'en peut distinguer qu'un élément, soit est dans $F^{(E)}$ et n'en peut distinguer qu'un nombre fini, soit est ailleurs et n'en distingue pas du tout. Au total, seuls un nombre fini d'éléments de E peuvent se comporter différemment des autres dans une application ainsi définie. Cette nouvelle application appartient donc elle aussi à $F^{(E)}$, ce qu'il fallait démontrer.

On peut aussi présenter ce phénomène de la manière un peu plus philosophique suivante.

Dans le cas d'un ensemble E qui soit en fait une copie de l'ensemble $\mathbb{N}$ des entiers mais dont la bijection avec $\mathbb{N}$ aurait été oubliée, toutes les parties de E infinies de complémentaire infini (au sens vrai de "toutes", sens extérieur qui échappe à la théorie) se correspondent les unes aux autres par des permutations de E (parmi toutes les vraies permutations, qui échappent à la théorie).

Or, un résultat métamathématique hors de portée du présent chapitre nous enseignent qu'aucune théorie ne peut axiomatiser complètement, pour un ensemble infini E, l'idée que son ensemble de parties 2^E soit le "vrai", contenant toutes les parties.

Mais, comme E n'avait aucune structure au départ, le modèle était symétrique par rapport à toutes ses permutations (au sens vrai, extérieur). Ainsi, tant que cette symétrie est préservée, si on a une partie hors de $2^{(E)}$, on les a toutes, tandis qu'on ne peut exiger de les avoir toutes.

Donc, E étant intialement sans structure, toute axiomatique qui exigera de 2^E qu'il contienne une partie infinie et de complémentaire infini, est une axiomatique qui prend le risque de forcer une brisure de symétrie de la théorie.

Mais la propriété universelle ne brise pas elle-même la symétrie d'une théorie. On ne peut donc s'assurer de sortir de $2^{(E)}$ que par un axiome d'existence plus puissant, qui prend le risque de forcer une brisure de symétrie. Ainsi est l'axiome du choix que nous verrons plus loin.

Version faible de la propriété universelle et sa signification

Nous allons faire ici une remarque sur le cas où on restreindrait le schéma de propriété universelle de la puissance à sa version faible ainsi définie: après la construction incomplète de puissance de E par F effectuée, on ne pose ses axiomes d'universalité uniquement que sur les symboles T qu'on

peut obtenir sans nécessiter l'emploi d'une définition dont l'énoncé utilise une variable liée dans F^E ou dans tout autre ensemble construit à partir de lui.

Par exemple, l'axiome (A2) satisfait à cette condition. Bien sûr, le résultat que nous allons voir maintenant n'apporte rien de plus dans le cas précis de ce qui a été dit précédemment, mais son intérêt est que contrairement à l'étude précédente il continue à s'appliquer dans les autres cas, ceux où l'ensemble E avait des structures au départ.

Il suffit alors, pour satisfaire ces axiomes, de prendre en guise d'"ensemble puissance F^E" la réunion de toutes les puissances paramétrées de F par E qu'on peut construire par des successions de dynamiques internes.

En effet, ayant ainsi défini l'ensemble "F^E", vérifions qu'il obéit à toute formule A d'utilisation de la propriété universelle n'utilisant au plus que des paramètres dans F^E et pas de quantificateurs dedans. Chaque valeur de ces paramètres, c'est ainsi une application de E dans F constructible par un moyen fini qui intervient. En assemblant cette construction avec celle donnée par la formule A, on obtient une construction un peu plus complexe de la nouvelle application de E dans F définie par A pour ces valeurs des paramètres. Comme toute construction finie, elle fournit un élément de notre ensemble F^E, ce qu'il fallait démontrer: la formule A est bien toujours vraie dans ce F^E.

Par contre, on ne pourrait rien dire de tel dans le cas d'utilisation d'une formule où interviendrait une variable liée de F^E, ce qui ferait sortir de la logique du premier ordre dans une bien plus large mesure.

Axiome du choix de la logique d'ordre supérieure

Enoncés

L'axiome du choix est un axiome de la théorie des ensembles, que la plupart des mathématiciens décident d'adopter. Cependant, on peut aussi trouver un certain intérêt à le refuser, notamment dans les situations où il est source (permet de démontrer l'existence) de "monstres mathématiques", certains objets aux propriétés dont on préfèrerait dans tel ou tel contexte qu'ils n'existent pas.

Il peut se formuler sous forme de plusieurs énoncés dont l'équivalence est facile à démontrer. Ces énoncés, repris tels quels (sauf le premier) comme énoncés en logique du second ordre (ou d'ordre supérieur) en prenant pour E et F des espèces, et pour opérations des structures de la théorie considérée, apparaissent alors comme étant des schémas d'axiomes servant de complément à la propriété universelle.

(AC1) Tout produit d'ensembles non vides est non vide.

(AC2) Pour tous ensembles E et F et toute relation $R \subset E \times F$,

$$(\forall_E x\ \exists_F y\ xRy) \Rightarrow (\exists f \in F^E\ \forall_E x,\ xRf(x))$$

(AC3) Pour toute surjection s de F sur E,

$$\exists f \in F^E\ \forall_E x\ s(f(x)) = x$$

(AC4) Pour toute relation d'équivalence R sur un ensemble E,

$$\exists A \in 2^E\ \forall x \exists! y\ (y \in A \text{ et } xRy)$$

Un tel ensemble A s'appelle un *système de représentants* de la relation R.

(AC5) Sur tout ensemble E il existe une fonction de choix, application qui à toute partie de E non vide associe un de ses éléments.

L'équivalence de ces énoncés se voit ainsi: on remarque que (AC1) et (AC2) sont synonymes (en prenant pour F la réunion de ces ensembles), que (AC3) est le cas particulier de ($AC2$) où R est définie par l'énoncé $x = s(y)$, que (AC1) (resp. (AC2)) se déduit de (AC3) en prenant pour F de (AC3) la somme de ces ensembles (resp. l'ensemble R), et (AC4) est la traduction de (AC3) où F est le quotient de E par R. Enfin, l'équivalence entre (AC2) et (AC5) se vérifie facilement.

Remarques:

• Dans le cas où E est fini, ces énoncés sont des théorèmes.

• De ces axiomes posés dans les cas où les symboles qui interviennent (s, R) appartiennent au langage de la théorie considérée, on déduit leur validité dans le cas général (où ils sont éléments de puissances paramétrées). Tout cela se démontre facilement.

• Nous avons dit que l'axiome du choix prend le risque de briser la symétrie de la théorie. Alors, au lieu de faire semblant de ne pas le faire en écrivant dans (AC2) ou (AC3) "$\exists f \in F^E$", on peut aussi le faire franchement en introduisant f comme nouveau symbole de la théorie. Ou on peut, plus doucement, se contenter d'introduire en tant qu'ensemble F^E une simple construction incomplète de puissance (sans la propriété universelle), tout en cachant tout aspect visible de cette brisure de symétrie: n'opérant ni définition ni construction dépendant de f ou de F^E et ne retenant de leur existence que les théorèmes qui résultent.

Interventions de l'axiome du choix, contre-exemples

Nous allons voir ici quelques exemples d'utilisation de l'axiome du choix, à titre purement illustratif car leur justification dépasserait le niveau de difficulté du présent chapitre.

Contrairement à ce que la présentation ci-dessus laisse entendre, il arrive souvent d'appliquer l'axiome du choix à une puissance, non pour elle-même mais pour préciser la construction d'une autre puissance précédemment construite.

Ainsi, si E n'a aucune structure préalable, on ne peut pas trouver les conditions d'appliquer l'axiome du choix directement à un ensemble F^E pour rejeter la solution $F^{(E)}$ (ou $2^{(E)}$ si F est une paire) . Mais il est possible de le faire, par exemple au moyen de (AC5) appliqué à E mais cela n'est pas encore suffisant: il faut aussi employer la propriété universelle de $2^{E\times E}$ ou encore de l'ensemble $E^{(\mathbb{N})}$ des applications des parties finies de $\mathbb{N}$ dans E si l'ensemble $\mathbb{N}$ des nombres entiers figure par ailleurs dans la théorie. Signalons qu'on ne peut pas construire l'ensemble $\mathbb{N}$ des nombres entiers dans une théorie en termes de la seule logique du premier ordre (ceci est relié aux théorèmes d'incomplétude).

Mais il y a un autre exemple de puissance minimale en son genre qui contredit directement l'axiome du choix: c'est le cas d'un ensemble E ayant pour seule structure préalable une surjection s de E dans un ensemble infini F, par laquelle tout élément de F a au moins deux antécédents. Alors, pour toute espèce G initialement indépendante de E, on peut prendre en guise de puissance G^E l'ensemble des f tels qu'il existe $g \in G^F$ pour lequel f coïncide avec $g \circ s$ en dehors d'une partie finie de E. On voit alors immédiatement que cette situation contredit l'axiome (AC3) appliqué à ce s.

Donnons maintenant des exemples de "mauvaise" utilisation de l'axiome du choix, démontrant l'existence d'objets mathématiques "monstrueux" dont on se passerait volontiers (nous n'expliquerons pas ici pourquoi). Il y a ainsi plusieurs types d'utilisation gênantes, plus ou moins compliqués. En voici deux exemples simples, qui sont d'ailleurs quasiment du même type: c'est l'existence de systèmes de représentants des relations d'équivalence suivantes:

• La relation entre les nombres réels x et y qui s'énonce par "$x - y$ est un nombre rationnel".

• La relation entre f et g d'un ensemble F^E où E est infini (typiquement $E = \mathbb{N}$; on suppose à présent que cet F^E n'est pas réduit à $F^{(E)}$!), qui s'énonce par "l'ensemble des x tels que $f(x) \neq g(x)$ est fini".

Théorème d'incomplétude

Les idées que nous avons évoquées le long de ce chapitre rappelleront à beaucoup le fameux théorème d'incomplétude de Gödel. Ils souhaiteront alors en voir maintenant sa formulation précise et sa démonstration. En effet, on entend dire facilement de-ci, de-là, des commentaires philosophiques plus ou moins sérieux sur ce théorème, en sorte que cela nous inciterait à mettre les choses au clair sur ce sujet sans trop tarder. Cependant, cela n'est pas forcément la meilleure option, car, s'il est vrai que ce théorème a sa place dans les fondements des mathématiques, nous n'avons pas encore introduit ici toutes les notions sur lesquelles il repose. Mais, ces avertissements étant faits, nous allons malgré tout présenter ici ce théorème, cédant ainsi à la mode de façon quelque peu démagogique (sous réserve de le renvoyer éventuellement à un chapitre ultérieur lorsque la rédaction

de la suite aura avancé). Heureusement que nous avons déjà maintenant introduit assez de choses pour n'être pas complètement perdus.

Précisons encore que cette signification n'est pas en proportion avec les motifs de sa célébrité, car pour introduire les choses dans l'ordre il faudrait commencer par le théorème de complétude (voir paragraphe 4.1.), qui joue un rôle légèrement plus fondamental de par son énoncé plus clair et ses implications plus directes en fondements des mathématiques.

En effet, le théorème de complétude a notamment pour intérêt de parler du sens des théories (le côté face) alors que le théorème d'incomplétude ne s'occupe que de la capacité à démontrer (côté pile) ce qui rend son interprétation moins évidente. En fait, ces deux théorèmes qui sembleraient naïvement s'opposer, s'enrichissent l'un l'autre de leur confrontation en mettant en évidence les contours de chacun: ces objets équivalents du théorème de complétude (indémontrabilité d'un énoncé et existence d'un contre-exemple), ne sont pas décidables de façon générale; il y a des énoncés pour lesquels on ne peut pas savoir s'ils sont indémontrables ou si leur démonstration n'a simplement pas encore été trouvée, car peut-être que leur démonstration n'existe que comme objet d'un faux modèle de la théorie des nombres entiers, démonstration qui n'étant pas de longueur réellement finie permet d'aboutir à une conclusion fausse sans commettre d'erreur à aucun moment particulier.

Mais revenons un peu sur terre.

Nous avons énoncé, sans les moyens de le démontrer, le théorème de complétude: "tout énoncé vrai sur tout modèle d'une théorie en logique du premier ordre est démontrable", suivant des règles de démonstration connues dans le cas général (trop compliquées pour le présent chapitre).

Le théorème d'incomplétude dit notamment qu'il existe des énoncés sur les nombres entiers qu'aucun formalisme ne peut démontrer ni réfuter.

En confrontant ces deux théorèmes, on en déduit qu'il n'existe pas d'axiomatisation complète des nombres entiers en logique du premier ordre. Comment cela se fait-il ? C'est qu'à chaque fois qu'on veut définir l'ensemble $\mathbb{N}$ des nombres entiers en sorte que son unicité en résulte, on est obligé d'invoquer l'ensemble de ses parties: soit dans l'axiome de récurrence, soit dans "toute partie non vide a un plus petit élément", ces deux énoncés étant équivalents.

Or nous avons vu que l'ensemble des parties d'un ensemble infini ne peut pas se définir complètement en logique du premier ordre, et l'ensemble des parties de $\mathbb{N}$ ne fait pas exception à cette règle.

Ne pouvant pas définir $2^{\mathbb{N}}$ par des moyens du premier ordre, nous ne pouvons pas non plus axiomatiser $\mathbb{N}$. Ou plutôt, nous nous trouvons ici démunis dans la tentative naturelle de le faire. Et ce que les théorèmes de complétude et d'incomplétude réunis nous enseignent alors, c'est qu'il est impossible de combler ce vide par un autre moyen.

Mais il existe des axiomatisations incomplètes, celle de Péano par exemple, qui se contente de regarder les parties définissables par des énoncés au lieu de les prendre toutes. (Un tel système réduit n'entraîne pas l'unicité de $\mathbb{N}$ mais suffit pour formuler et démontrer le théorème d'incomplétude).

Donnons maintenant une présentation synthétisée des résultats de Gödel.

Théorème 1. *On peut obtenir une théorie des énoncés et des démonstrations par développements à partir d'une théorie des nombres entiers.*

Nous avons défini la notion de développement d'une théorie (lois de la dynamique interne). Nous n'avons pas précisé la constitution d'une théorie des nombres entiers, ni d'une théorie des énoncés et des démonstrations. Nous n'allons pas le faire ici, renvoyant le lecteur curieux à la littérature en attendant de le faire dans un avenir indéterminé. Précisons que ce développement est la partie la plus fastidieuse de la démonstration de Gödel, sans doute plus que nécessaire à cause des choix non optimisés des conventions choisies, ceux formalisant la théorie des énoncés et des démonstrations pesant peut-être le plus lourdement dans la balance. Mais qu'importe, seul compte pour nous le fait de savoir que tout cela existe.

Et l'intérêt de cela, c'est que les résultats d'incomplétude que nous obtiendrons dans la suite sur la théorie des énoncés et des démonstrations, engendrent des résultats d'incomplétude analogues sur la théore des nombres entiers, en revenant en arrière de ces développements par leur simulation.

Avant d'aller plus loin, précisons un tout petit peu ce que peut représenter cette notion de démonstration toujours évoquée.

Le choix le plus naturel est de prendre la notion de démonstration qui intervient dans le théorème de complétude. Mais on peut ne pas s'en satisfaire, voulant aller au-delà de la logique du premier ordre. Ce qu'on voudrait alors y ajouter prend souvent la forme d'un shéma d'axiomes comme nous avons vu. Cette distinction entre axiomes et démonstrations peut être contestée, du point de vue de la logique d'ordre supérieur, en traitant ces axiomes à égalité avec les règles de démonstration propres à la logique du premier ordre. On peut donc décider d'amalgamer le tout en une grande loi de démonstration définissant la liste de tous les "théorèmes" qu'on pourrait tout aussi bien appeler les axiomes.

En résumé, l'énoncé "A est démontrable" où la variable A représente un énoncé, sera considérée comme une boîte noire supposée fixée une fois pour toutes mais dont le contenu n'est pas précisé, si ce n'est que:

1) Il est de la forme "il existe un système fini relié à A tel que (...)", ce système étant nommé *démonstration de* A et la condition (...) désignant des propriétés internes de ce système fini. Ceci permet notamment que la démontrabilité d'un énoncé de la théorie soit un autre énoncé de la même théorie.

2) Il englobe la logique naturelle, en sorte que tout ce qu'on démontrera par des méthodes naïves sera reconnu comme démontrable.

Théorème 2. *Il existe un énoncé G dont on vérifie que :*

$$G \Leftrightarrow (G \text{ n'est pas démontrable})$$

En effet, soit x une variable dont l'espèce est celle des énoncés à une variable libre.

Soit ensuite l'énoncé $F(x)$ de variable libre x qui s'écrit "$x(x)$ n'est pas démontrable". (On remarque bien que x n'ayant qu'une variable libre, $x(x)$ est un énoncé clos, donc sa démontrabilité a un sens).

Enfin, soit G l'énoncé $F(F)$. Il s'énonce donc "$F(F)$ n'est pas démontrable", ce qui est identique à "G n'est pas démontrable".

Théorème 3. *Pour tout énoncé clos A on démontre que*

$$A \text{ est démontrable} \Rightarrow (A \text{ est démontrable}) \text{ est démontrable}$$

Cela se vérifie naturellement (évoquons-en seulement l'idée, faute des outils pour le démontrer réellement): si on a trouvé une démonstration, alors on en déduit qu'une démonstration existe. (Mais la réciproque est fausse.)

On peut remarquer qu'en reversant ces notions en des notions du côté face par le théorème de complétude, cela donne une autre remarque qui se vérifie facilement également: si un univers virtuel considère contenir un système ayant telles propriétés du premier ordre, alors ce système existe également de l'extérieur et ces propriétés y sont toujours vraies.

Théorème 4. *Si on a démontré sur un énoncé G qu'on a $G \Leftrightarrow (G$ n'est pas démontrable$)$, on peut en déduire que $G \Leftrightarrow C$ où C est l'énoncé de consistance de la théorie, "Faux n'est pas démontrable"*

En effet, il s'agit de démontrer : (G est démontrable) $\Leftrightarrow$ (Faux est démontrable). L'implication se vérifie ainsi:

G est démontrable
$\Rightarrow$ (G est démontrable) est démontrable (par le théorème 3).
$\Rightarrow$ (non G) est démontrable
Ainsi G et non G sont tous deux démontrables
$\Rightarrow$ (G et non G) est démontrable
$\Rightarrow$ Faux est démontrable.

La réciproque est immédiate, comme Faux $\Rightarrow G$.

De tout cela on peut conclure que $C \Leftrightarrow (C$ n'est pas démontrable).

Comment le théorème de complétude se concilie-t-il avec le théorème de complétude ?

Précisons d'abord sur quoi porte ce théorème d'incomplétude: sur la théorie des nombres entiers (arithmétique de Peano) ainsi que toute théorie mathématique qui l'englobe (qui contient l'ensemble des entiers dans son langage ou permet d'une quelconque manière de le constuire), comme par exemple la théorie des ensembles.

Chose curieuse, il y a une théorie de la géométrie euclidienne qui est complète, à savoir que tout énoncé y est démontrable ou réfutable. Elle échappe donc au théorème de complétude. Comme nous avons dit que pour tout système infini il existe d'autres systèmes non isomporphes ayant les mêmes vérités, cela est aussi valable pour la géométrie euclidienne. Par exemple l'ensemble des points du plan dont les coordonnées sont des nombres algébriques (solutions d'équations algébriques à coefficients rationnels) est un autre modèle de la géométrie euclidienne.

Cette géométrie euclidienne permet certes de reconstruire une théorie de l'ensemble des nombres réels et même l'ensemble des réels positifs, mais cela ne permet pas pour autant de reconstruire une théorie de l'ensemble des nombres entiers, car il n'existe pas d'énoncé permettant de distinguer si un nombre réel positif est ou non un entier, à moins bien sûr de se limiter à la reconnaissance d'un nombre limité d'entiers. Ainsi la géométrie n'englobant pas la théorie des nombres entiers, peut échapper au théorème d'incomplétude.

Revenons au théorème d'incomplétude: il s'énonce de la manière suivante.

Pour toute théorie axiomatique non contradictoire, englobant celle de l'ensemble des entiers et dont l'ensemble des axiomes est fini ou récursivement énumérable (i.e. il existe un algorithme qui le produit, de même que par exemple d'après le théorème de complétude il existe un algorithme qui produit l'ensemble des théorèmes d'une théorie donnée), il existe des énoncés clos ni démontrables ni réfutables.

Pour le dire autrement, l'arithmétique ne peut pas être complètement axiomatisée.

Pourtant on a tendance à dire qu'un énoncé d'arithmétique est en réalité soit vrai, soit faux. C'est parce qu'on a l'idée d'un modèle unique noté $\mathbb{N}$ de cette théorie, et que tout autre modèle est "un faux". De tels modèles de $\mathbb{N}$ autres que "celui auquel on pense" sont appelés des modèles *non-standard* de l'arithmétique. Ils sont constitués des nombres entiers habituels (de $\mathbb{N}$) dits entiers *standard* mais aussi d'autres éléments, dits entiers *non-standard*, qui sont supérieurs à tout entier standard.

Toute arithmétique admet donc une infinité de modèles non-standard, à la fois des modèles ayant le même ensemble de vérités et aussi des modèles ayant des ensembles de vérités différents.

Si donc on se dit qu'on choisit de parler uniquement de l'ensemble $\mathbb{N}$ des entiers standard (hypothèse mathématiquement inexprimable), alors tout énoncé portant dessus sera soit vrai, soit faux, mais parmi les énoncés ainsi vrais il en est (une infinité) qui sont indémontrables.

Donc, en un certain sens en dehors de la logique du premier ordre, on peut dire qu'il y a des vérités inaccessibles par les démonstrations.

Bilan et perspectives

Nous avons décrit dans ce qui précède le contenu des colonnes "Fondement" et "dynamique" de l'hélice des théories, à l'exception des règles formelles de démonstration (côté pile), et nous allons maintenant effleurer quelques propriétés de la colonne "Réalité" de cette hélice.

Cette description qui précède a pris la forme d'une suite particulière de constructions et de définitions suivant quasiment le sens que nous avons donné à ces mots dans cette description même.

Cependant, une telle formalisation de cette théorie des théories dans son propre cadre (notamment de la notion de passage du temps) n'a pas été précisée; nous n'allons pas chercher maintenant à le faire (elle serait très compliquée). Pour le faire, il faudrait sortir des cadres de la logique du premier ordre et même de celle d'ordre supérieur telle que nous les avons indiquées, introduisant de nouveaux ensembles qui n'existaient pas au départ suivant encore de nouvelles règles, réalisant des jeux de miroirs entre théorie et métathéorie. Si on veut encore formaliser ces nouvelles règles comme extension des métathéories précédentes, le résultat complique encore ces nouvelles règles, et ainsi de suite indéfiniment:

Côté pile, on observe cette impossiblilité radicale d'épuiser les ressources des extensions possibles de théories en métathéories par des règles formelles (impossibilité attestée par la connaissance d'une méthode formelle générale d'extension d'une théorie formelle quelconque à sa métathéorie strictement plus grande); Il s'agit là d'un processus répétable autant de fois qu'on veut indéfiniment, mais qu'il est impossible d'épuiser par des règles, même dans l'infini.

Côté face, cela nous renvoie à l'inépuisabilité de la hiérarchie des ensembles que nous (ou plutôt telle ou telle théorie) n'avons pas encore appréhendés, qui se développe en infinités d'infinités, indéfiniment.

Ce sont là les deux faces d'une même incomplétude (ou inépuisabilité) qui se répercute sur le problème de la réalisation (accessibilité par la dynamique formelle) des trois niveaux de la colonne des "Réalités", même si la distinction intrinsèque de leur nature s'exprime simplement: le sens des "vérités" a été simplement exprimé en termes d'existence de modèles, sans achever pour autant le problème des règles de démonstrations (en fait achevable en logique du premier ordre mais non au-delà); le sens des "invariants" est également simple et sera étudié dans un prochain chapitre, sans qu'on puisse pour autant achever le problème de leur définition; le sens des "objets bien fondés", dont nous n'aurons pas besoin avant longtemps, sera lui aussi simple sans qu'on puisse achever le problème de leur construction.

En effet, une étude poussée amène à constater que même l'avancée dans la définissabilité des éléments d'un ensemble d'invariants construits une fois pour toutes, et l'avancée dans la démontrabilité des vérités parmi un système d'énoncés au sens défini une fois pour toutes, peut le cas échéant être inépuisable et avoir finalement pour seul générateur de nouvelles ressources le fait de s'appuyer sur des axiomes d'existence de la hiérarchie inépuisable des ensembles (objets fondés) qui s'étend bien au-delà.

Simulations de dynamiques externes

Nous allons voir maintenant comment certains changements de théories (dyamiques externes modifiant une théorie donnée) peuvent s'effectuer de manière virtuelle, c'est-à-dire en restant formellement à l'intérieur de la théorie de départ, à des dynamiques internes près. Ce qui fait la différence avec les dynamiques internes virtuelles que nous avons décrites précédemment est que la règle de simulation des nouveaux constituants comme construits à partir des anciens était intégrée explicitement dans la nouvelle théorie, permettant à l'intérieur de la nouvelle théorie de tout retraduire en termes des anciens constituants, tandis qu'ici cette règle sera effacée du contenu de la nouvelle théorie, ne laissant généralement pas la possibilité de reconstituer cette correspondance (du côté face en tout cas).

Particularisation virtuelle

L'ajout d'un axiome est la *particularisation* d'une théorie, et la suppression d'un axiome est sa *généralisation*.

Soit un énoncé clos A, qu'on voudrait ajouter comme axiome à une théorie donnée T pour obtenir une théorie T'. Cette particularisation peut se faire de manière virtuelle, en simulant chaque énoncé clos $\mathcal{E}$ (éventuel théorème) de la théorie T' par l'énoncé $(A \Rightarrow \mathcal{E})$ de la théorie T.

(Il apparaît un petit problème du fait que les dynamiques internes de T' ne peuvent toutes être figurées par des dynamiques internes de T; seules leurs simulations peuvent toujours l'être. En particulier, une définition d'opération dans T' ne peut généralement pas être effectuée dans T, si l'énoncé d'existence et d'unicité sur lequel il s'appuie n'est pas valable dans T. C'est donc sa simulation qu'il faut manipuler. Pour le quotient on peut encore faire un arrangement, mais à part cela, de deux choses l'une. Ou bien on admet que des espèces soient peut-être vides, auquel cas la construction de la somme ne peut être généralement simulée (si une des espèces sommées est peut-être vide dans T) qu'en simuant les opérations à valeurs dans la somme par les relations correspondantes. Ou bien on a un problème pour construire une partie qui peut être vide dans T.)

On pourrait dire que la dynamique inverse, celle de la généralisation, se simule par le fait de ne pas utiliser un axiome donné A, lors des démonstrations. Mais une telle approche laisse un gros trou du côté face: si on ne connaissait que les systèmes dans lesquel A est vrai, où peut-on retrouver ceux où il est faux, sans utiliser la construction générale des modèles de théories consistantes ? Il faudrait

connaître aussi les modèles de la théorie obtenue en remplaçant A par non A dans les axiomes, ou de plusieurs théories correspondant à différentes situations possibles où A est faux. Maheureusement, il sera le plus souvent impossible de fournir simplement des modèles de ces contre-théories qui représentent de manière significative les contre-exemples cherchés, à partir seulement des modèles de la théorie de départ. C'est pouquoi nous abandonnerons ici cette idée de généralisation virtuelle.

Dans les simulations suivantes, on s'attachera particulièrement au respect du côté face: les règles de simulation devront faire que chaque modèle de la théorie initiale "simule" (contient ou engendre) un ou un ensemble de modèles de la théorie simulée, de sorte que tout modèle de la théorie simulée peut s'obtenir par une telle simulation.

Structuration virtuelle (brisure spontanée de symétrie)

L'ajout d'un nouveau symbole à une théorie, et donc d'une structure supplémentaire sur ses systèmes, sera appelée la *structuration* ou *brisure de symétrie*. La dynamique inverse, effacement de structures, s'appelle l'*oubli*. Par exemple le passage de la géométrie euclidienne à la géométrie affine est un oubli.

Le moyen fondamental de simuler l'ajout d'une structure à une théorie $\mathcal{T}$ consiste à *fixer une variable*. Autrement dit, il consiste à choisir une espèce non vide I et à prendre un symbole de variable i de cette espèce, pour lui faire jouer un rôle de symbole de constante. Notons $\mathcal{T}(i)$ la théorie simulée, qui interprète i comme étant une constante.

Remarque: lorsqu'on parle de fixer une variable, il n'est pas question de définir sa valeur. En effet, si on pouvait définir sa valeur, ce serait la définition d'une constante, et l'ajout de cette constante à la théorie serait reconnue comme une dynamique interne. Or, notre but ici est justement de quitter la dynamique interne.

Ainsi exprimé, ce moyen de simuler une structuration semble très restrictif, ne concernant que les ajouts de constantes. En fait, il a une portée plus générale, à travers la possibilité d'effectuer des dynamiques internes. En effet, l'ajout d'un symbole d'opération revient à fixer un élément de l'ensemble puissance correspondant au type de cette opération (et de même pour les relations comme cas particuliers d'opérations). Ainsi se trouve immédiatement simulée n'importe quelle structuration en logique d'ordre supérieur, par une construction de puissance suivie d'une fixation de variable.

Par contre, en logique du premier ordre, on se trouve limité par le fait que la puissance n'est pas une construction complète. Mais on peut la remplacer par une construction de puissance paramétrée P (éventuellement précédée par d'autres dynamiques internes). Dans ce cas, il faut prendre acte de ce qui est réellement simulé: c'est l'ajout d'un symbole d'opération T accompagné de l'ajout de l'axiome traduisant (par simulation des dynamiques internes aboutissant à la construction de P) l'existence d'un élément de P qui coïncide avec T.

Du côté pile, le symbole i étant une variable pour $\mathcal{T}$ mais une constante pour $\mathcal{T}(i)$, les variables de $\mathcal{T}(i)$ se représentent par des variables de $\mathcal{T}$ autres que i.

Décrivons maintenant l'effet de cette structuration virtuelle du côté face. A chaque modèle de $\mathcal{T}$ correspond, non un modèle de $\mathcal{T}(i)$, mais une famille de modèles indexée par la variable $i \in I$: tous ces modèles sont identiques à l'exception de la valeur de la constante i, dont chaque élément de I est une valeur possible qui fournit un modèle différent. Après cette structuration effectuée, dans la nouvelle théorie simulée, la correspondance qui identifie ces modèles les uns aux autres à l'exception de i est perdue, car une théorie ne peut appréhender qu'un seul modèle d'elle-même à la fois (la connaissance de l'existence de plusieurs modèles possibles d'une théorie n'étant pas comprise par cette même théorie).

Cette correspondance existe encore dans la théorie simulante, tant qu'on n'effectue pas de construction de partie ou de quotient qui dépendent de i dans la théorie simulée.

Dans ce cas, on peut simuler un symbole T de $\mathcal{T}(i)$ (dont i n'est pas variable) par un symbole T' ayant i comme variable de plus. La nouvelle théorie hérite des symboles T de l'ancienne théorie au moyen de définitions de la forme $\forall x, i,\ T'(i, x) = T(x)$.

Tout énoncé $\mathcal{E}$ de $\mathcal{T}(i)$ se simule en ajoutant le cas échéant i à ses variables libres (i ne peut pas être une variable de $\mathcal{E}$), comme suit : l'usage de i comme constante devient son usage comme variable; tous les symboles $T'(i, x)$ dépendent de cette même variable libre i. Inversement, un

énoncé de T simule un énoncé de $T(i)$ si et seulement si le rôle de i dans tous ses symboles (s'il y en a) est joué par la même variable (i), qui est alors une variable libre, qui n'est pas reconnue comme variable dans $\mathcal{T}(i)$.

Ainsi, i aura forcément toujours la même valeur pour tous les symboles dépendant de lui. Dans les axiomes, définitions et les théorèmes, s'ajoute à cela le quantificateur universel sur i appliqué en dernier (au niveau le plus extérieur); par contre, la particularisation se simule par la construction d'une partie J de I, qui remplacera le rôle de I dans cette structuration virtuelle.

Mais si on veut effectuer une construction de partie ou de quotient, les choses se compliquent. Alors, soit on ne l'effectue que virtuellement (par simulation de cette dynamique interne), soit on réalise effectivement l'indépendance des différents modèles en remplaçant dans la théorie simulante chaque espèce E par le produit $E \times I$ afin d'employer pour l'espèce E de la théorie à simuler, la simulation de la partie $p^*(i)$ où p est la projection de $E \times I$ sur I. (Ici, on ne peut pas construire la partie $p^*(i)$ mais seulement la simuler parce qu'elle dépend de i tandis qu'une vraie construction de doit pas dépendre d'une variable).

Oubli virtuel

C'est l'opération inverse de la précédente: elle consiste à reconnaître une situation comme étant le résultat d'une structuration virtuelle (théorie simulée) et à passer à la théorie simulante correspondante d'après les règles de simulation ci-dessus.

Plus précisément, on se ramène, par une suite de dynamiques internes renversées ou non (une dynamique interne renversée étant la reconnaissance que des constituants sont de la forme du résultat d'une dynamique interne, et le remplacement de tout ce qui dépend de ces constituants par leur simulation), au cas où on a un symbole de constante qui n'intervient dans aucun axiome. On le supprime alors de la liste des constantes.

Cela fait donc deux conditions à remplir: d'abord, que la structure à oublier soit une constante, ensuite qu'elle n'intervienne dans aucun axiome.

Si on est seulement dans le cas d'une constante c d'espèce I qui intervient dans un nombre fini d'axiomes, on en tire le théorème "$\exists i \in I$, (conjonction des axiomes où c est remplacé par i)". En construisant alors la partie J de I définie par cette conjonction, on se ramène au cas d'une constante c' de J qui n'intervient dans aucun axiome. De cette manière on arrive donc à simuler l'oubli d'une constante qui n'intervient que dans un nombre fini d'axiomes : cette liste d'axiome est à remplacer par l'axiome présenté ci-dessus comme théorème.

Si on est au contraire dans le cas d'une opération qui n'intervient dans aucun axiome, on peut se contenter de la supprimer; mais contrairement au cas d'une constante présentée ci-dessus, les axiomes dépendant d'une opération ne peuvent généralement pas se ramener à des axiomes n'en dépendant pas, en logique du premier ordre. Les théories avec une opération sans axiome n'ayant pas d'intérêt pratique par ailleurs, cela oblige en pratique à chercher d'abord à ramener à des constantes les structures qu'on cherche à oublier virtuellement.

Extension virtuelle

L'*extension* d'une théorie consiste à ajouter une nouvelle espèce représentant de nouveaux objets, sans modifier les ensembles d'objets désignés par les espèces existantes. Le nouvel univers est donc l'ancien univers auquel s'ajoutent les objets de la nouvelle espèce.. La dynamique inverse (suppression d'une espèce) s'appelle la *restriction*.

Une extension pure, ajout d'une nouvelle espèce sans aucune structure la concernant, n'est simulable par les moyens dont nous disposons ici (en logique du premier ordre), que si elle est de cardinal fini connu.

Nous avons vu le cas des constructions, règles d'ajout d'une espèce, de structures et d'axiomes, qui sont des dynamiques internes et donc simulables. Nous allons maintenant voir comment simuler certains ajouts d'une ou plusieurs espèces avec des structures et axiomes plus faibles, qui ne sont alors plus des dynamiques internes.

Il suffit pour cela d'appliquer successivement les méthodes déjà présentées: on commence par effectuer une ou plusieurs constructions, puis on oublie des structures apparues dans ces constructions. Les extensions virtuelles se réalisent donc au moyen d'oublis virtuels.

Nous avons défini les oublis virtuels comme étant des oublis de constantes dont ne dépend aucun axiome, afin que ce ne soit pas en même temps une généralisation (les axiomes dépendant de cette constante ne pouvant pas subsister tels quels).

De même, oublier purement la structure obtenue par une construction aurait finalement le défaut d'être une forme de généralisation: cela fournit certains modèles possibles, mais non pas tous en général à partir des modèles de la théorie initiale.