I Introduction

Le forcing est une méthode mise au point par Paul Cohen (1934 - 2007), un mathématicien américain (médaille Fields 1966), afin de démontrer des théorèmes d'indépendance pour la théorie des ensembles ZF (Zermelo-Fraenkel).

Un théorème d'indépendance consiste à démontrer qu'une formule donnée ne peut être démontrée dans une théorie donnée, mais que son contraire ne peut pas être démontré non plus (ces formules sont dites ≪ indécidables ≫ dans cette théorie)

Les deux premières formules auxquelles Paul Cohen a appliqué la méthode du forcing sont :

1. L'axiome du choix, en 1938 Kurt Gödel démontre que ZF + AC est iso-consistante avec ZF et en 1963 Paul Cohen démontre que ZF + ¬ AC est iso-consistante avec ZF.
2. L'hypothèse du continu, en 1938 Kurt Gödel démontre que ZFC + HC est iso-consistante avec ZFC et en 1963 Paul Cohen démontre que ZFC + ¬ HC est iso-consistante avec ZFC.

Ce sont donc les résultats de P. Cohen qui ont permis de finaliser la démontration des deux résulats d'indépendance les plus connus.

II Rappel de quelques notions et notations

Un langage est la données d'un certain nombre de symboles :

- Symboles de variables $(x, y, x_0, x_1, \cdots)$
- Symboles de constantes $(\pi, 0, C_i \cdots)$
- Symboles de fonctions $(+, s, \mathcal{F}_i^{n_i} \cdots)$
- Symboles de relations $(\leq, \sim, \mathcal{R}_i^{n_i}, \cdots)$

L'exposant n_i ci-dessus est l'arité de la fonction ou de la relation.

La logique du premier ordre est une logique dont les langages sont de type $\mathcal{L}_{\omega,\omega}$; cette notation signifie que l'on peut utiliser au plus ω symboles de constantes (donc un nombre au plus dénombrable), que l'on s'autorise les conjonctions (et donc les disjonctions) de longueur strictement inférieure à ω (donc finie), et les quantifications de longueur strictement inférieure à ω (donc finie).

Par exemple $\mathcal{L}(0, 1, +, \times, <)$ est un langage avec

- 2 symboles de constantes (0 et 1)
- 2 symboles de fonctions binaires (+ et $\times$)
- 1 symbole de relation binaire (<)

C'est, par exemple le langage qui va permettre de définir les corps ordonnés.

Remarque 1 : Le symbole de l'égalité (=) est absent, celui-ci étant souvent sous-entendu et encore plus souvent seulement évoqué en parlant de langage égalitaire (ce qui sera exclusivement le cas ci-dessous).

Remarque 2 : Les symboles de variables sont absents ; en général on ne précise rien, ou alors une précaution liminaire du genre ≪ plus les symboles de variables dont nous aurons besoin par la suite ≫. Les symboles de variables apparaissent quand leur utilité se fait jour, et leur statut est très généralement, évident.

La collection des termes d'un langage $\mathcal{L}$ est définie de la façon suivante :

- Les variables de $\mathcal{L}$ sont des termes.
- Les constantes de $\mathcal{L}$ sont des termes.
- Si $t_1, t_2, ...t_n$ sont des termes, et, si $\mathcal{F}$ est une fonction n-aire (d'arité n, c'est à dire avec n variables), alors $\mathcal{F}(t_1, t_2, ...t_n)$ est un terme.

La collection des formules atomiques d'un langage $\mathcal{L}$ est définie de la façon suivante :

- Si t_1 et t_2 sont des termes, alors $t_1 = t_2$ est une formule atomique (puisque que nous ne considérons que des langages égalitaires).
- Si $t_1, t_2, ...t_n$ sont des termes, et, si $\mathcal{R}$ est une relation n-aire (d'arité n), alors $\mathcal{R}(t_1, t_2, ...t_n)$ est une formule atomique.

La collection des formules [1] d'un langage $\mathcal{L}$ est définie de la façon suivante :

- Les formules atomiques sont des formules
- Si φ est une formule, $\neg\varphi$ est une formule
- Si φ et ψ sont des formules, $\varphi \wedge \psi$ est une formule
- Si φ est une formule et x une variable, $\forall x\varphi$ est une formule

Soit $\mathcal{L}$ un langage, $\mathcal{T}$ une théorie du langage $\mathcal{L}$ et φ une formule du langage $\mathcal{L}$.

La notation $\mathcal{T} \vdash \varphi$ indique que φ est une conséquence syntaxique (ou formelle) de $\mathcal{T}$ (φ est démontrable dans la théorie $\mathcal{T}$).

La notation $\mathcal{T} \models \varphi$ indique que φ est une conséquence sémantique de $\mathcal{T}$ (toutes les structures vérifiant les formules de $\mathcal{T}$, vérifient aussi φ).

Complétude	**:**	$(\mathcal{T} \models \varphi)$	$\Rightarrow$	$(\mathcal{T} \vdash \varphi)$
Correction	**:**	$(\mathcal{T} \vdash \varphi)$	$\Rightarrow$	$(\mathcal{T} \models \varphi)$

Une structure interprétant un langage $\mathcal{L}$ est un couple $\mathfrak{A} =< A, \mathcal{I} >$, où A est un ensemble, et $\mathcal{I}$ une fonction d'interprétation qui :

- A chaque constante de $\mathcal{L}$ fait correspondre un élément de A,
- A chaque relation n-aire de $\mathcal{L}$ fait correspondre une relation $\mathcal{R} \subset A^n$,
- A chaque fonction m-aire de $\mathcal{L}$ fait correspondre une fonction : $A^m \to A$.

Un modèle d'une théorie $\mathcal{T}$ (intuitivement : un « Monde possible ») est une structure interprétant le langage de $\mathcal{T}$, et vérifiant les axiomes de $\mathcal{T}$, ce que l'on note $\mathfrak{A} \models \mathcal{T}$.

Pour les définitions des notions d'ordinal ou de cardinal, nous renvoyons à : Chapitres VI.1 et VI.2.

Nous utilisons la notation $|X|$ pour désigner le cardinal de l'ensemble X.
Rappelons, néanmoins, une définition importante, celle de la suite $\aleph$ d'ensembles indexée par les ordinaux :

$$\begin{aligned} \aleph_0 &= |\omega| \\ \aleph_{\alpha+1} &= \aleph_\alpha^+ \ \text{(c'est à dire le cardinal successeur)} \\ \aleph_\lambda &= \bigcup_{\alpha<\lambda} \aleph_\alpha \ \text{(où } \lambda \text{ est un ordinal limite)} \end{aligned}$$

1. En anglais on parle de « formules bien formées », ou *wff*.

III Le principe fondateur

Si on est capable de construire **un** modèle d'une théorie, vérifiant une formule, on peut en déduire que le contraire de cette formule n'est pas démontrable dans cette théorie (puisqu'une formule démontrable dans une théorie est vérifiée dans tous les modèles de cette théorie). Autrement dit, pour démontrer qu'une formule est indécidable dans une théorie, « il suffit » d'exhiber un modèle la vérifiant et un modèle vérifiant son contraire.

Par exemple si on pose $\mathcal{L} = \{\star, 1\}$ le langage constitué d'un symbole d'opération binaire et d'un symbole de constante, la théorie des groupes peut s'axiomatiser dans ce langage :

1. $\forall x \, \forall y \, \forall z \, ((x \star y) \star z = x \star (y \star z))$
2. $\forall x \, (1 \star x = x \star 1 = x)$
3. $\forall x \, \exists y \, (x \star y = y \star x = 1)$

Pour montrer que la commutativité est indécidable dans la théorie des groupes, il suffit d'exhiber un groupe commutatif et un groupe non commutatif, ce qui, dans ce cas est très facile :

$(\{1\}, \star)$ est clairement un groupe commutatif, et il est bien connu que $\mathcal{S}_3$, le groupe des symétries d'un triangle équilatéral, n'est pas commutatif.

Malheureusement, dans le cas de la théorie des ensembles ZF, on ne sait pas construire de modèles, on va donc utiliser une astuce, consistant à fabriquer une modèle vérifiant une formule donnée **à partir d'un modèle supposé exister**.

Avec la théorie des groupes on peut compliquer[2] un peu les choses : montrer que la commutativité est indécidable dans la théorie des groupes infinis avec au moins un élément d'ordre infini, c'est à dire vérifiant l'ensemble des formules (indexées par n) définies par :

$$\exists x \left(\bigwedge_{i=2}^{n} (x^i \neq 1) \right)$$

Sans chercher un modèle de cette théorie (il n'est même pas nécessaire de savoir si elle est consistante ou non), on peut faire les raisonnements suivants :

1) Si $(G, \star)$ est un modèle, et α est un élément d'ordre infini, alors $(\{\alpha^n\}_{n \in \mathbb{N}}, \star)$ est bien un groupe vérifiant les conditions supplémentaires, de plus il est abélien. C'est à dire qu'à partir d'un modèle[3] quelconque de la théorie, on fabrique un **sous-groupe** vérifiant la condition supplémentaire (c'est le principe des démonstrations de Gödel).

Dans l'autre sens le problème est plus compliqué, car, si à partir d'un groupe non commutatif on peut espérer extraire un sous-groupe commutatif, au contraire à partir d'un groupe commutatif, il n'est pas possible d'extraire un sous-groupe non commutatif. Donc, pour contruire un modèle il va falloir ajouter des éléments possédant des propriétés particulières, tout en conservant les propriétés de la théorie de départ, donc de groupe en particulier (c'est le principe des démonstrations de Cohen).

Par exemple si on part du groupe $(\mathbb{Z}, +)$, il ne suffit pas d'ajouter un élément ω et de poser $1+\omega \neq \omega+1$ pour obtenir un groupe non commutatif (puisqu'il faut définir $n+\omega, \omega+n, \omega+\omega, \cdots$, tout en continuant de respecter tous les axiomes de groupe).

2) Si $(G, \star)$ est un modèle commutatif[4], alors $((G \times \{0, 1\}), \circ)$ ou $\circ$ est définie par :

2. Néanmoins, on pourrait facilement trouver des exemples.
3. Supposé exister.
4. Si $(G, \star)$ est un modèle non commutatif, le problème est résolu

$\circ$	$(y,0)$	$(y,1)$
$(x,0)$	$(x\star y,0)$	$(x\star y,1)$
$(x,1)$	$(x\star y^{-1},1)$	$(y^{-1}\star x,0)$

C'est bien un modèle de notre théorie, c'est un groupe, infini, $(\alpha,0)$ est d'ordre infini de plus $(1,1)\circ(\alpha,0)=(\alpha^{-1},1)$ et $(\alpha,0)\star(1,1)=(\alpha,1)$, or $\alpha^{-1}\neq\alpha$, puisque α est d'ordre infini, et donc $((G\times\{0,1\}),\circ)$ n'est pas commutatif.

IV Le forcing

To be continued ...

V Axiome du choix

Pour toute famille non vide d'ensembles non vides, il existe une « **Fonction de Choix** », c'est à dire une fonction qui à chaque ensemble de la famille fait correspondre un élément de cet ensemble. Plus formellement :

$$(\forall X)\ \ (X\neq\emptyset\wedge(\emptyset\notin X))\Rightarrow\left(\exists f:X\to\bigcup_{Y\in X}Y,\ \forall x\in X,\ \ f(x)\in x\right)$$

Attention

1. L'axiome du choix n'est pas constructif, il ne permet pas d'expliciter cette fonction de choix, il dit juste qu'elle existe.
2. Dans certains cas l'axiome du choix n'est pas nécessaire pour qu'une fonction de choix existe (on peut même parfois l'expliciter).

Soit $\underset{\mathbb{Z}}{\sim}$, la relation sur $\mathbb{R}$ définie par

$$\forall x\in\mathbb{R}\,\forall y\in\mathbb{R}\,((x\underset{\mathbb{Z}}{\sim}y)\Leftrightarrow((x-y)\in\mathbb{Z}))$$

Ainsi que $\underset{\mathbb{Q}}{\sim}$, la relation sur $\mathbb{R}$ définie par

$$\forall x\in\mathbb{R}\,\forall y\in\mathbb{R}\,((x\underset{\mathbb{Q}}{\sim}y)\Leftrightarrow((x-y)\in\mathbb{Q}))$$

Ces deux relations définissent, chacune, une famille d'ensembles, les classes d'équivalence, une fonction de choix sur ces familles consiste à choisir un représentant dans chaque classe ; dans le cas de $\underset{\mathbb{Z}}{\sim}$, c'est facile, il suffit de prendre le seul élément de chaque classe appartenant à $[0,1[$ (qui est égal à $x-\lfloor x\rfloor$), par contre pour $\underset{\mathbb{Q}}{\sim}$ il n'y a pas de moyen simple (et aucun, même compliqué, qui soit connu) pour choisir un représentant dans chaque classe, néanmoins, l'axiome du choix, garantit l'existence d'une telle fonction de choix.

VI Hypothèse du continu

$$\forall X((|X| > \aleph_0) \Rightarrow (|X| \geq 2^{\aleph_0})$$

Une autre façon d'exprimer cette formule : $\aleph_1 = 2^{\aleph_0}$

Une conséquence immédiate de l'hypothèse du continu est que tous les sous-ensembles de $\mathbb{R}$ sont, soit :

1. Fini.
2. De même cardinal que $\mathbb{N}$, c'est à dire $\aleph_0$.
3. De même cardinal que $\mathbb{R}$, c'est à dire $2^{\aleph_0}$.

Un point très important à comprendre est la signification profonde de l'axiome des parties :

Axiome des Parties : Pour chaque ensemble x, il existe un ensemble $\mathfrak{P}(x)$ dont les éléments sont exactement tous les sous-ensembles de x.

La définition ci-dessus semble donner une signification sans ambiguïté à $\mathfrak{P}(x)$, mais ce n'est pas le cas, en effet, le mot « tous » ne renvoit à rien de précis dans le langage naturel, contrairement au langage formel, aussi nous allons reformuler cet axiome :

Axiome des Parties : $\forall x \, \exists y \, \forall z \, [z \in y \Leftrightarrow \forall w \, (w \in z \Rightarrow w \in x)]$, ce qui pourrait s'exprimer en langage naturel : pour chaque ensemble x, il existe un ensemble $\mathfrak{P}(x)$ dont les éléments sont exactement tous les **ensembles qui sont des** sous-ensembles de x.

Dans le cas d'un ensemble x fini, il n'y a aucune différence entre ces deux définitions car tous [5] les sous-ensembles de x sont définissables, donc existent, donc appartiennent bien à $\mathfrak{P}(x)$, mais dans le cas d'un ensemble infini, ce n'est pas le cas (ce qui a donné naissance au paradoxe de Skolem).

VII Références

1. K. Kunen, *Set Theory - An Introduction to Independence Proofs*, North Holland, 1980.

5. au sens du langage naturel.