PIERRE SAMUEL

**Modèles booléiens et hypothèse du continu (résultats de Paul Cohen par la méthode de D. Scott et R. Solovay)**

*Séminaire N. Bourbaki*, 1968, exp. nº 317, p. 61-72

<http://www.numdam.org/item?id=SB_1966-1968__10__61_0>

Séminaire BOURBAKI
19e année, 1966/67, n° 317

Novembre 1966

# MODÈLES BOOLÉIENS ET HYPOTHÈSE DU CONTINU

(Résultats de Paul COHEN [1] par la méthode de D. SCOTT [3] et R. SOLOVAY [4] )

par Pierre SAMUEL

NB - Les symboles mathématiques usuels ($=$, $\Longrightarrow$, etc) seront utilisés dans la métathéorie ; celle-ci utilisera librement toutes les ressources de la mathématique ordinaire. (Ce n'est donc pas une démonstration finitiste comme celle de P. COHEN ; mais les logiciens ont un procédé canonique pour rendre finitiste de telles démonstrations). Les systèmes formalisés étudiés par cette métathéorie utilisent d'autres symboles, voisins mais typographiquement distincts.

## I - Rappel sur les systèmes formels.

Nous considérerons des systèmes formels égalitaires avec :

- les signes logiques ( , $\vee$, $\to$ , $\leftrightarrow$ , $\forall$ , $\exists$,...)
- des symboles $R_0$, $R_1$,... formateurs de relations ou "formules")
  $R_i(x_1,\ldots,x_{n(i)})$ (1)
- parmi eux un symbole d'égalité, noté $\equiv$ ;
- un ensemble $A$ de lettres (appelées les individus), qu'on met dans les relations: on écrit $R_i(x_1,\ldots,x_{n(i)})$ avec $x_j \in A$ pour $j = 1,\ldots,n(i)$.

parmi les axiomes et schémas d'un tel système $\underline{S}$ figurent les axiomes et schémas de la logique classique avec égalité (en gros, Bourbaki, Ens. I). Par exemple :

- $(\forall x)(x \equiv x)$ ,
- $(\forall x,y)(x \equiv y \to (\Phi(x) \leftrightarrow \Phi(y)))$, où $\Phi$ est une relation, et où l'on fixe son attention sur une des occurences des lettres figurant dans $\Phi$.

Un système du type précédemment décrit est dit du premier ordre.

Dans les systèmes dits du second ordre, on se donne de plus une partition de $A$ en 2 parties (les "individus" notés $x,y,z,\ldots$, et les "prédicats" notés $p,q,r\ldots$) ; à tout prédicat est associé un entier $n \geq 1$, son ordre ; si $p$ est

(1) Le mot "relation" est celui de Bourbaki ; les logiciens disent plutôt "formules".

un prédicat d'ordre n, on a le droit d'écrire $p(x_1,\ldots,x_n)$, et c'est une relation. On quantifie sur les prédicats. On suppose les axiomes de l'égalité valables tant pour les individus que pour les prédicats. De plus on pose les axiomes suivants :

- ("Extensionnalité") $((\forall x_1,\ldots,x_n)(p(x_1,\ldots,x_n) \leftrightarrow q(x_1,\ldots,x_n)) \leftrightarrow (p \equiv q)$
- ("Compréhension") - Soit $\Phi(x_1,\ldots,x_n)$ une relation ; alors

$$(\exists\, p)(p(x_1,\ldots,x_n) \leftrightarrow \Phi(x_1,\ldots,x_n)).$$

On définit de même les systèmes du troisième ordre, etc.., avec des prédicats portant sur des prédicats, etc.

Exemple.- Considérons l'arithmétique de Peano. C'est un système du 1er ordre $\underline{S}$, avec $A = \mathbb{N}$, et les symboles $\equiv$, + et . (d'égalité, somme et produit). Le théorème du bon ordre (disant que $\underline{P}(\mathbb{N})$ peut être bien ordonné) et l'hypothèse du continu peuvent s'exprimer dans le système du troisième ordre construit sur $\underline{S}$. En effet les parties de $\mathbb{N}$ correspondent aux prédicats unaires $p(x)$ $(x \in \mathbb{N})$, et l'hypothèse du continu (par exemple) se traduit par l'existence d'un prédicat binaire de prédicats $R(p,q)$ ayant certaines propriétés (qui traduisent le fait que (2) $R(p,q)$ est une relation de bon ordre pour laquelle tout segment initial est dénombrable).

On notera qu'un tel système du troisième ordre sur l'arithmétique péanienne est moins fort que la théorie des ensembles ; les démonstrations d'indépendance esquissées ci-dessous vont donc moins loin que celles de P. COHEN [1] . Une nouvelle version de ce qui est esquissé ici (Scott [5] ) renforce ces démonstrations par utilisation d'une théorie des "types transfinis" (équivalente à la théorie des ensembles) ; l'exposé étant fait par un non-logicien à l'intention de non-logiciens, nous ne développerons pas ce point.

---

(2) Dans ce système du troisième ordre où l'ensemble des individus est $\mathbb{N}$, on devrait normalement prendre un ensemble de prédicats de cardinal $2^{\mathbb{N}}$ , un ensemble de prédicats de prédicats de cardinal $2^{2^{\mathbb{N}}}$ , etc, donc l'ensemble A relatif à ce système aurait un très gros cardinal. En fait il est plus commode de prendre ici pour A un ensemble contenant $\mathbb{N}$ comme "partie du 1er ordre", et par ailleurs arbitraire.

## II - Rappel sur les anneaux booleiens.

Un anneau booleien $\underline{B}$ est un anneau tel que $x^2 = x$ pour tout $x \in \underline{B}$. Alors $\underline{B}$ est commutatif et de caractéristique 2. La relation $xy = x$ est une relation d'ordre sur $\underline{B}$, qu'on note $x \leq y$ ; le plus grand élément est 1, et le plus petit est 0. L'anneau $\underline{B}$ est réticulé, et on a :

$$\inf(x,y) = xy \quad , \quad \sup(x,y) = x+y+xy \quad (\text{noté } x \cup y) ;$$

les sup et inf (finis) sont distributifs l'un par rapport à l'autre. Tout élément $x$ admet un "complémentaire" $y$ caractérisé par

$$\sup(x,y) = 1 \quad , \quad \inf(x,y) = 0,$$

et ce complémentaire est $1+x$. Par analogie avec le calcul logique on définit :

$$x \text{ impl } y = y \cup (1+x) = 1+x+y+y(1+x) = 1+x+xy$$

$$x \text{ eq } y = (x \text{ impl } y)(y \text{ impl } x) = (1+x+xy)(1+y+xy) = 1+x+y.$$

Un anneau booleien $\underline{B}$ est dit <u>complet</u> si <u>toute</u> famille d'éléments de $\underline{B}$ admet un sup ; toute famille d'éléments de $\underline{B}$ admet alors un inf par complémentation. Par définition un <u>morphisme</u> d'anneaux booleiens complets sera supposé conserver les sup (et donc les inf). D'où une catégorie qu'on pourrait étudier en tant que telle.

<u>Exemples d'anneaux booleiens complets.</u>

1) L'ensemble $\underline{P}(X)$ des <u>parties</u> d'un ensemble $X$, mieux décrit comme l'anneau produit $(\underline{F}_2)^X$ des fonctions caractéristiques à valeurs dans le corps à deux éléments.

2) Soit $X$ un espace topologique. Pour $Y \subset X$, nous noterons $\mathrm{adh}(Y)$ et $\mathrm{int}(Y)$ l'adhérence et l'intérieur de $Y$. Un ouvert $U$ de $X$ est appelé un "<u>bon</u>" ouvert ("regular open set" de la terminologie américaine) si $U = \mathrm{int}(\mathrm{adh}(U))$. L'ensemble $\underline{B}$ des <u>bons ouverts</u> de $X$ est un anneau booleien complet pour les opérations suivantes (où $\underline{U}$ désigne une partie de $\underline{B}$)

- $\sup(\underline{U}) = \mathrm{int}(\mathrm{adh}(\bigcup_{Y \in \underline{U}} Y))$ , ainsi $\sup(Y,Y') \supset Y \cup Y'$ (l'égalité n'a pas toujours lieu, comme le montre l'exemple de deux intervaux ouverts contigus de $\underline{R}$) ;
- $\inf(\underline{U}) = \mathrm{int}(\bigcap_{Y \in \underline{U}} Y)$ , ainsi $\inf(Y,Y') = Y \cap Y'$ ;
- le "complémentaire" de $Y \in \underline{B}$ est $\mathrm{int}(X - Y)$ ;
- l'addition qui se déduit formellement de ce qui précède.

On notera que les ouverts-fermés de $X$ sont de bons ouverts.

La condition des chaines dénombrables.

Dans un anneau booleien $\underline{B}$ la "condition des chaines dénombrables" est la relation :
"Toute partie de $\underline{B}$ formée d'éléments deux à deux disjoints (i.e. tels que $x.y = 0$ pour $x \neq y$) est dénombrable". Il revient au même de dire que toute partie bien ordonnée de $\underline{B}$ est dénombrable.

Lemme. Soient $I$ un ensemble, $X$ l'ensemble $2^I$ muni de la topologie produit des topologies discrètes, et $\underline{B}$ l'anneau booleien complet des bons ouverts de $X$. Alors $B$ satisfait à la condition des chaines dénombrables.

En effet, si on munit chacun des deux parties de $2$ de la masse $1/2$ et $2^I$ de la mesure produit, tout ouvert élémentaire non vide de $2^I$ a une mesure de la forme $(1/2)^n$. Ainsi tout ouvert non vide de $2^I$ a une mesure $> 0$.

III - Modèles booleiens d'un système formel.

Soit $\underline{S}$ un système formel au sens du § I (avec un ensemble $A$ de lettres, des symboles $R_i$ à $n(i)$ arguments formateurs de relations ; parmi eux le symbole d'égalité $\equiv$ ; les relations de $\underline{S}$ sont notées par des majuscules helléniques $\Phi, \Psi, \ldots$).

Soit $\underline{B}$ un anneau booleien complet. Un prémodèle de $\underline{S}$ dans $\underline{B}$ est la donnée, pour toute relation $\Phi$ de $\underline{S}$, d'une valeur $|\Phi| \in \underline{B}$ de sorte que :

$$|\neg \Phi| = 1 + |\Phi|$$

$$|\Phi \vee \Psi| = |\Phi| \cup |\Psi|$$

$$|\exists\, x\ \Phi(x)| = \sup_{a\in A} |\Phi(a)|$$

$$|\forall x\ \Phi(x)| = \inf_{a\in A} |\Phi(a)|\,.$$

On suppose ici tous les symboles logiques définis à partir de la négation $\neg$ et de la disjonction $\vee$. Naturellement les $|\Phi|$ sont déterminés dès qu'on connait les $R_i(x_1,\ldots,x_{n(i)}) \in \underline{B}$ pour toutes les valeurs des $x_j \in A$.

Une relation $\Phi$ est dite valide dans le prémodèle $(\underline{B}, |\ |)$ si $|\Phi| = 1$. Un prémodèle $(\underline{B}, |\ |)$ de $\underline{S}$ est appelé un modèle booleien (ou modèle) de $\underline{S}$ si les théorèmes de $\underline{S}$ y sont valides. Il résulte des formules ci-dessus et des règles du raisonnement qu'il suffit pour cela que les axiomes et schémas de $\underline{S}$ soient valides. Le composé d'un modèle et d'un morphisme d'anneaux booleiens complets est encore un modèle de $\underline{S}$ (situation éminemment propice à la recherche d'un modèle "universel" de $\underline{S}$ ; il existe, par le procédé breveté de Bourbaki, Ens. IV).

On démontre :

a) Si $\underline{S}$ est un système du premier ordre, une relation $\Phi$ de $\underline{S}$ est démontrable si elle est valide dans tout modèle booleien de $\underline{S}$ (c'est-à-dire dans le modèle universel de $\underline{S}$ ).

b) Si $\underline{S}$ est un système formel d'ordre quelconque, les assertions suivantes sont équivalentes :

1) $\underline{S}$ est non-contradictoire ;

2) $\underline{S}$ admet un modèle booleien $(\underline{B}, |\ |)$ avec $\underline{B} \neq 0$ ;

3) $\underline{S}$ admet un modèle booleien à valeurs dans $\mathbb{F}_2$ .

En effet, il est clair que 2) (ou 3)) implique 1) car la négation d'un théorème a alors la valeur $0 \neq 1$ et ne peut être un théorème. Il est clair que 3) implique 2) ; et 1) $\Rightarrow$ 3) constitue le théorème de complétude d'Herbrand-Gödel.

Exemple. Soit $\underline{S}$ l'arithmétique péanienne. Une formule élémentaire de $\underline{S}$ (c'est-à-dire de la forme $\equiv (x,y)$ , $+ (x,y,z)$ , $.(x,y,z)$ avec $x$ , $y$ , $z \in \underline{N}$ explicités) est pratiquement décidable par un simple calcul ; on lui assigne la valeur 1 (resp. 0 ) si elle est vraie (resp. fausse). Les règles données au début du § permettent alors (en théorie, pas en pratique) d'assigner une valeur 0 ou 1 à toute formule construite à partir des formules élémentaires au moyen des symboles logiques et des quantificateurs. On obtient ainsi un modèle de $\underline{S}$ à valeurs dans $\underline{F}_2$ (et donc dans n'importe quel anneau booleien complet $\underline{B}$ ) ; on l'appelle le modèle standard de $\underline{S}$ . Les démonstrations de non-contradiction relative qui nous intéressent concernent, comme on l'a vu au § 1, des extensions $\underline{S}'$ du troisième ordre de $\underline{S}$ ; il va s'agir de fabriquer des anneaux booleiens $\underline{B}$ et des modèles $\underline{S}' \to \underline{B}$ qui étendent le modèle standard $\underline{S} \to \underline{B}$ .

IV - Adjonction de prédicats. Description de la méthode suivie.

Etant donnés un système formel $\underline{S}$, une relation (ou un prédicat) R à n variables, et un modèle booleien $(\underline{B}, |\ |)$ de $\underline{S}$, l'application

$$(x_1,\dots,x_n) \mapsto |R(x_1,\dots,x_n)| \quad (x_i \in A)$$

satisfait à la condition :

$$(x_1 \equiv y_1, \dots, x_n \equiv y_n) \Longrightarrow |R(x_1,\dots,x_n)| \text{ eq } |R(y_1,\dots,y_n)| = 1.$$

De plus, pour deux relations (ou prédicats) équivalent(e)s, R et R', on a

$$|R(x_1,\dots,x_n)| \text{ eq } |R'(x_1,\dots,x_n)| = 1.$$

Par définition un B-prédicat de $\underline{S}$ est une application $P : A^n \to \underline{B}$ telle que :

$$(IV.1) \qquad (x_1 \equiv y_1, \dots, x_n \equiv y_n) \Longrightarrow P(x_1,\dots,x_n) \text{ eq } P(y_1,\dots,y_n) = 1.$$

Ce n'est pas là une notion relative au système formel $\underline{S}$, mais au modèle $\underline{B}$ considéré. Un $\underline{B}$-prédicat se comporte comme la valeur dans $\underline{B}$ d'un prédicat (ou d'une relation) ordinaire.

Le but de l'exposé est de montrer que certaines relations (hypothèse du continu, son contraire, axiome de choix, son contraire) sont compatibles avec un certain système formel $\underline{S}$ supposé non contradictoire (p.ex. l'arithmétique péanienne, ou la théorie des ensembles de Zermelo-Fraenkel). Or une telle relation s'exprime par l'existence d'un prédicat ayant certaines propriétés.

Par exemple l'assertion qu'un ensemble peut être totalement ordonné s'exprime par l'existence d'un prédicat binaire $r(x,y)$ tel que

$$(IV.2) \qquad (\forall x)r(x,x),\ (\forall x,y,z)(r(x,y) \text{ et } r(y,z) \to r(x,z)), \text{ etc}$$

La méthode suivie par Dana Scott consiste à construire un modèle booleien convenable $\underline{B}$ de $\underline{S}$, et un $\underline{B}$-prédicat P ayant les propriétés correspondant à celles du prédicat r cherché.

Dans l'exemple ci-dessus, on doit donc construire $P : A^2 \to \underline{B}$ tel que

$$(IV.2') \qquad \inf_{x\in A} P(x,x) = 1, \quad \inf_{x,y,z\in A} (P(x,y)P(y,z) \text{ impl } P(x,z)) = 1 \text{ etc.}$$

Alors le système formel $\underline{S'}$ obtenu en adjoignant à $\underline{S}$ un prédicat $r(x,y)$ soumis aux axiomes tels que (IV.2) est non-contradictoire : il admet en effet un modèle dans $\underline{B}$ où $|r(x,y)| = P(x,y)$.

Un tel $\underline{B}$-prédicat P s'appellera, suivant les cas, un "$\underline{B}$-ordre total", un "$\underline{B}$-bon ordre", etc. Comme il est souvent plus suggestif d'énoncer des assertions telles que (IV.2) plutôt que (IV.2'), nous décrirons (IV.2') comme étant la <u>traduction booleienne de</u> (IV.2).

V - <u>Préliminaires sur les $\underline{B}$-prédicats de bon ordre</u>.

Comme toujours, $\underline{S}$ désigne un système formel, et $(\underline{B}, |\ |)$ un modèle booleien de $\underline{S}$.

<u>Théorème V.1. Il existe un $\underline{B}$-prédicat de bon ordre sur l'ensemble</u> A <u>des individus de</u> S.

Démonstration facile, du fait qu'on se donne le droit d'utiliser toute la mathématique usuelle dans la métathéorie, en particulier l'existence d'un bon ordre (ordinaire) sur A.

Soit maintenant P un $\underline{B}$-prédicat de bon ordre sur A. Pour tout ordinal $\alpha$ on définit un B-prédicat unaire $T_\alpha : A \to \underline{B}$ par induction transfinie au moyen de :

$$T_\alpha(a) = (\inf_{\beta<\alpha} \sup_x P(x,a)(x \neq a)T_\beta(x)).(\inf_x(P(x,a)(x \neq a) \text{ impl } \sup_{\beta<\alpha}T_\beta(x)) ;$$

plus clairement, $T_\alpha(a)$ est la traduction booleienne de "le segment initial déterminé par a est isomorphe à l'ensemble bien ordonné $\alpha$".

Par traduction booleienne de démonstrations classiques relatives aux ensembles bien ordonnés, on démontre les formules équivalentes :

(V.2) $\quad |x \equiv y| \text{ eq } \sup_\alpha(T_\alpha(x)T_\alpha(y)) = 1 \quad , \quad |x \equiv y| = \sup_\alpha(T_\alpha(x)T_\alpha(y))$.

Par la même méthode on prouve le

<u>Théorème</u> V.3. <u>Si</u> $\underline{B}$ <u>satisfait à la condition des chaines dénombrables, et si</u> P <u>est un $\underline{B}$-prédicat de bon ordre sur</u> A <u>qui satisfait à la traduction booleienne de "tout segment initial de</u> A <u>est dénombrable", alors on a</u>

$$\inf_x \sup_{\beta<\omega_1} T_\beta(x) = 1$$

(où $\omega_1$ désigne le premier ordinal non dénombrable).

VI - <u>L'hypothèse du continu</u>.

Soit $\underline{B}_0$ l'anneau des bons ouverts de $2^{\mathbb{N}}$. Il fournit un modèle de l'arithmétique péanienne (cf. § III). Par adjonction de $\underline{B}_0$-prédicats, et utilisation du fait que les seuls invariants du groupe des automorphismes de $\underline{B}_0$ sont 0 et 1 (noter que les permutations de N fournissent des automorphismes de $B_0$), on démontre la compatibilité de :

(VI.1) l'axiome du choix ;

(VI.2) la négation de l'axiome de constructibilité de Gödel.

On considère alors un ensemble $I$ de cardinal $> \aleph_1$ (aleph un), l'espace produit $(2^{\mathbb{N}})^I$, l'anneau booleien $\underline{B}$ de ses bons ouverts, et le groupe $G$ des automorphismes de $\underline{B}$. Les seuls invariants de $G$ sont encore 0 et 1. On a vu (fin du § 3) que $\underline{B}$ fournit un modèle de l'arithmétique péanienne $\underline{S}$. Or l'hypothèse du continu (HC) s'exprime (dans une extension du troisième ordre de $\underline{S}$) par l'existence d'un prédicat de bon ordre sur $2^{\mathbb{N}}$ pour lequel tout segment initial est dénombrable.

Théorème VI.3. La négation de l'hypothèse du continu, ($\neg$HC), est compatible.

Il suffit de montrer que, dans le modèle $\underline{B}$, on a $|\neg \text{HC}| = 1$. Raisonnons par l'absurde ; comme $|\neg \text{HC}|$ est invariant par $G$, on a $|\neg \text{HC}| = 0$, d'où $|\text{HC}| = 1$. Soit $\underline{P}$ l'ensemble des $\underline{B}$-prédicats unaires de $\underline{S}$ (traduction booleienne de l'ensemble des parties de $\mathbb{N}$). Par hypothèse, il existe $R : \underline{P} \times \underline{P} \to \underline{B}$ qui est un $\underline{B}$-prédicat de bon ordre sur $\underline{P}$ et qui satisfait la traduction booleienne de "tout segment initial est dénombrable". (On doit ici se servir du fait que le modèle est "plein" au sens de Scott [3]).

Pour tout $i \in I$, définissons $P_i \in \underline{P}$ par l'équation

$P_i(n) = \{s \in (2^{\mathbb{N}})^I \mid s(i)(n) = 1\}$ (où $n \in \mathbb{N}$ ; noter que $\underline{P}_i$ applique $\mathbb{N}$ dans $\underline{B}$.

Pour $i \neq j$, l'ensemble $\{s \in (2^{\mathbb{N}})^I \mid (s(i)(n) = s(j)(n)$ pour tout $n \in \mathbb{N}\}$ n'a pas de point intérieur. D'après la traduction booleienne de l'axiome d'extensionnalité, ceci signifie que

(a) $$|P_i \equiv P_j| = 0.$$

Pour chaque ordinal $\alpha$ considérons alors le $\underline{B}$-prédicat unaire $T_\alpha : \underline{P} \to \underline{B}$ relatif à $R$, défini au § V. Par le th. V.3 on a :

(b) $$\sup_{\alpha<\omega_1} T_\alpha(P_i) = 1 \quad \text{pour tout} \quad i \in I.$$

Pour tout $i \in I$, on peut donc choisir un $\alpha_i < \omega_1$ tel que $T_{\alpha_i}(P_i) \neq 0$. Comme, par hypothèse sur $I$, on a $\text{card}(I) > \text{card}(\omega_1)$, il existe un $\beta < \omega_1$ tel que

$$J = \{i \in I \mid \alpha_i = \beta\} \text{ soit non dénombrable.}$$

Or on a vu en (a) que $|P_i \equiv P_j| = 0$ pour $i \neq j$. Il résulte alors de (V.2) qu'on a $T_\beta(P_i)T_\beta(P_j) = 0$ pour $i,j \in J$, $i \neq j$. Ceci contredit le fait que $\underline{B}$ satisfait à la condition des chaines dénombrables (lemme du § II). CQFD.

La clef de la démonstration est qu'on a traduit "partie de $\mathbb{N}$" par "$\underline{B}$-prédicat unaire de $\underline{S}$", et qu'on a construit une foultitude de tels B-prédicats $P_i$.

Théorème VI.4. L'assertion suivante est compatible avec les axiomes de la théorie des ensembles et la négation de l'hypothèse du continu :
(H) il existe un ensemble $F$ d'applications $\mathbb{N} \to \mathbb{N}$, de cardinal $\aleph_1$, tels que toute application $\mathbb{N} \to \mathbb{N}$ soit majorée par un élément de $F$.

On remplace ici l'anneau booleien $\underline{B}$ des bons ouverts de $(2^{\mathbb{N}})^I$ par le quotient $\underline{B}'$ de l'anneau des ensembles boréliens de $(2^{\mathbb{N}})^I$ modulo l'idéal des ensembles négligeables (pour la mesure produit). On note que, comme $\emptyset$ est le seul ouvert négligeable de $(2^{\mathbb{N}})^I$, on a un monomorphisme $\underline{B} \to \underline{B}'$. Nous sautons le reste de la démonstration.

## VII - L'axiome de choix.

Théorème VII.1. La négation du théorème du bon ordre est compatible.

Par "théorème du bon ordre" on entend l'assertion que le continu $2^{\mathbb{N}}$ peut être bien ordonné. On désigne par $I$ un ensemble infini, et par $\underline{B}$ l'anneau des bons ouverts de $(2^{\mathbb{N}})^I$. Rappelons (cf. § VI) que $\underline{B}$ fournit un modèle de l'arithmétique péanienne $\underline{S}$. Soit $G$ le groupe de tous les automorphisme de $\underline{B}$ ; le groupe $G'$ des permutations de $I$ s'identifie à un sous groupe de $G$. Pour $i \in I$, on note $G_i \subset G'$ le stabilisateur de $i$ dans $G'$ ; soit $\Gamma$ le filtre sur $G$ engendré par les $G_i$.

On considère alors l'ensemble $\underline{P}(n, \Gamma)$ des $\underline{B}$-prédicats n-aires $P(x_1,\dots,x_n)$ de $S$ tels que le stabilisateur de $P$ dans $G$ soit élément du filtre $\Gamma$ (ici $g \in G$ opère sur $P$ "par les valeurs" : $(gP)(x_1,\dots,x_n) = g(P(x_1,\dots,x_n))$. On se borne à l'adjonction de ces prédicats (appelés les $(\underline{B}, \Gamma)$-prédicats") pour construire un modèle du système du second ordre sur $\underline{S}$.

Pour alléger, posons $\underline{P} = \underline{P}(1, \Gamma)$. Soit $R : \underline{P} \times \underline{P} \to \underline{B}$ un $(\underline{B}, \Gamma)$-prédicat binaire, et soit $WO(R)$ la formule booleienne qui exprime que $R$ est un $\underline{B}$-prédicat de bon ordre. Par hypothèse le stabilisateur $G_R$ de $R$ est élément de $\Gamma$.

Soit $S : \underline{P} \to \underline{B}$ défini par

(a) $S(X) = \sup_{Z \varepsilon P,\ G_R \subset G_Z} (|X \equiv Z|) \qquad (X \varepsilon \underline{P})$ ;

on a $G_R \subset G_S$, de sorte que $S$ est un $(\underline{B}, \Gamma)$-prédicat unaire. D'autre part le prédicat $P_i : \underline{N} \to \underline{B}$ $(i \varepsilon I)$ défini par

(b) $P_i(n) = \{s \varepsilon (2^{\mathbb{N}})^I \mid s(i)(n) = 1\} \quad (i \varepsilon I,\ n \varepsilon \underline{\mathbb{N}})$

a un stabilisateur qui contient $G_i$ ; c'est donc un $(\underline{B}, \Gamma)$-prédicat. Comme $I$ est infini, l'intersection des $G_i$ n'est pas élément de $\Gamma$; fixons donc un indice $i$ tel que $G_R \not\subset G_i$. Nous allons montrer que, pour cet indice $i$, on a

(c) $S(P_i) = 0$.

Sinon, en effet, il existerait $Z \varepsilon \underline{P}$ tel que $G_R \subset G_Z$ et que $b = |P_i \equiv Z|$ soit $\neq 0$ (par (a)). Comme $b$ est un ouvert non vide d'un produit infini, on peut trouver $g \varepsilon G' \cap G_Z$ tel que $g(i) \neq i$ et que $b.g(b) \neq 0$. Mais alors on a

$$0 < |P_i \equiv Z| \ .\ g(|P_i \equiv Z|) = |(P_i \equiv Z) \text{ et } (P_{g(i)} \equiv Z| \leqq |P_i \equiv P_{g(i)}| = 0$$

(cf. § VI, (a)). Cette contradiction démontre (c).

Il en résulte qu'on a $|(\exists X)(\neg S(X))| = 1$. Soit alors $Q : \underline{\mathbb{N}} \to \underline{B}$ défini par

(d) $Q(n) = |(\exists X)[\neg S(X) \wedge X(n) \wedge (\forall Y)(R(Y,X) \to S(Y))]|$

(en termes imagés $Q(n)$ veut dire qu'il y a un prédicat $X$ qui s'applique à $n$, et qui est le plus "petit" à ne pas avoir la propriété $S$). On a $G_R \subset G_S \subset G_Q$, d'où $G_Q \varepsilon \Gamma$ , et $Q$ est un $(\underline{B}, \Gamma)$-prédicat. D'autre part ce qui précède montre qu'on a $S(Q) = 1$, et aussi $WO(R) \leqq 1 + S(Q)$. On a ainsi prouvé que $WO(R) = 0$. CQFD.

<u>Théorème VII.2. L'assertion qu'il n'existe aucun ordre total sur $\underline{P}(\underline{P}(\underline{\mathbb{N}}))$ est compatible.</u>

Démonstration analogue, utilisant un filtre $\Gamma_0$ moins fin que $\Gamma$ .

Dans ce § la restriction aux $(\underline{B}, \Gamma)$-prédicats (resp. $\Gamma_0$) a considérablement restreint le nombre des relations d'ordre "admissibles" sur $\underline{P}(\underline{\mathbb{N}})$ (resp. $\underline{P}(\underline{P}(\underline{\mathbb{N}}))$)..

<u>Complément historique et bibliographique.</u>

On sait que K. Gödel [2] a démontré en 1937 la non-contradiction relative (ou compatibilité) de l'axiome de choix et de l'hypothèse généralisée du continu avec les autres axiomes de la théorie des ensembles. [ On connaissait déjà la compatibilité de formes assez faibles de la négation de l'axiome de choix ("assez faible", en ce sens qu'elle s'appliquait seulement à des théories contenant des objets qui ne sont pas des ensembles, et que les ensembles non-bien ordonnables de cette théorie sont des ensembles "farfelus" ; non pas $\mathbb{R}$ comme au §7). Ceci avait été suggéré par Fraenkel vers 1930, et démontré par Mostowski en 1939.]

En 1963, Paul Cohen a démontré la compatibilité de la négation de l'hypothèse du continu, sous une forme plus forte que celle donnée ici : le cardinal de $\underline{P}(\mathbb{N})$ peut être $\chi_\alpha$, où $\alpha$ est n'importe quel ordinal non limite. Il démontre aussi la compatibilité de la négation de l'axiome de choix (sous sa forme usuelle), et de nombreuses autres compatibilités. La méthode de Paul Cohen est basée sur la délicate notion de "forcing". Elle a inspiré les travaux de nombreux logiciens.

Tout récemment Dana Scott a donné une version de la méthode de Paul Cohen, qui utilise les modèles booleiens, et qui est nettement plus compréhensible pour des mathématiciens peu versés dans la Logique. C'est cette version qui est exposée ici.

## B I B L I O G R A P H I E

[1] P. COHEN - The independence of the continuum hypothesis. Proc. Nat. Acad. Sci. U.S.A., 50 (1963), 1143-1158 et 51 (1964), 105-110.

[2] K. GODEL - The consistency of the axiom of choice and of the generalized continuum hypothesis. Ann. of Math. Studies, n° 3, Princeton, 1940.

[3] D. SCOTT - Boolean-valued models for higher-order logic. (Polycopié, Logic Seminar, Stanford Univ., Jan. 1966).

Des articles imprimés exposant la méthode de Dana Scott sont en préparation, en particulier :

[4] R. SOLOVAY - Boolean algebras and forcing.

Juste avant la polycopie, on a reçu à Paris un "preprint" de

[5] D. SCOTT - A proof of the independence of the continuum hypothesis. Bien plus lisible que D. SCOTT [3] ; Scott utilise ici le langage des variables aléatoires plutôt que le langage topologique, et explicite la connexion entre ses modèles booleiens et le "forcing" de Paul Cohen.

Je tiens finalement à vivement remercier mon ami D. LACOMBE, qui a relu une première version de ce texte, et en a corrigé de nombreuses erreurs et maladresses. S'il en reste dans la version polycopiée, c'est uniquement de ma faute.