Kenneth Mc Aloon

Formes combinatoires du théorème d'incomplétude

Séminaire N. Bourbaki, 1979, exp. n° 521, p. 263-276
<http://www.numdam.org/item?id=SB_1977-1978__20__263_0>

Séminaire BOURBAKI
30e année, 1977/78, n° 521

FORMES COMBINATOIRES DU THÉORÈME D'INCOMPLÉTUDE

[d'après J. PARIS et d'autres]

par Kenneth MC ALOON

§ 1. Introduction

Le célèbre Théorème d'Incomplétude de Gödel de 1931 démontre qu'à tout système mathématique suffisamment puissant et récursivement axiomatisable est associée une formule close qui est vraie mais qui n'est pas prouvable dans le système donné, pourvu, bien sûr, que ce système soit lui-même non-contradictoire. Or, pour cette démonstration, Gödel a ramené par un système de codages des énoncés de type combinatoire à des énoncés sur les entiers naturels ; et la formule de Gödel pour les systèmes usuels est celle qui exprime la non-contradiction même du système en question. D'après les travaux de J. Robinson - Y. Matijasevich et al., toute formule de Gödel est équivalente à l'insolubilité dans les entiers naturels $\mathbb{N}$ d'une certaine équation diophantienne. Le Théorème d'Incomplétude de Gödel est donc extrêmement puissant dans la mesure où il situe le phénomène d'incomplétude au niveau de l'arithmétique même. Cependant les formules de Gödel ne correspondent pas à des problèmes et des questions traités préalablement par des mathématiciens et l'élaboration même de ces énoncés établit leur vérité au sens intuitif. Donc ce sont des propositions formellement indécidables mais mathématiquement établies ; ceci laisse ouverte la question de savoir si tout problème mathématiquement élaboré est mathématiquement décidable, voir [G]. Le fait que, d'après les travaux de Gödel et de Cohen, l'Hypothèse du Continu n'est ni prouvable ni réfutable dans la Théorie des Ensembles de Zermelo-Fraenkel avec l'Axiome du Choix, notée ZFC, illustre bien le phénomène d'incomplétude au niveau d'un problème mathématiquement élaboré préalablement. Or, depuis, on a vu une longue suite de problèmes classiques établis comme non-décidables dans ZFC - Problème de Souslin, Problème de Whitehead,... . Il est actuellement débattu si, indépendamment de ces résultats, le Problème du Continu, par exemple, reste ouvert et susceptible de solution ou si un certain pluralisme s'installe de force dans la Théorie des ensembles. Toujours est-il que les problèmes que nous avons cités se situent à un niveau supérieur de la hiérarchie des types, typiquement au niveau des parties des nombres réels $\mathbb{R}$, autrement dit, au niveau des parties des parties de $\mathbb{N}$. D'autre part, d'après de récents travaux de Friedman et de Martin, il s'avère que la détermination des jeux Boréliens revête aussi un phénomène d'incomplétude ; leur analyse établit que pour avoir la détermination des jeux de rang de Borel α , il faut avoir une hiérarchie de types de hauteur (à peu près) α ; il en suit que la détermination des jeux Boréliens, qui est prouvable dans ZFC, voir [M], ne l'est pas dans la Théorie des Types ni dans la Théorie des Ensembles de Zermelo, [F]. De nouveau, il s'agit de résultats qui ne portent pas sur l'arithmétique mais cette fois sur $\mathbb{R}$, autrement dit, sur les parties de $\mathbb{N}$. Il est à signaler aussi que les travaux de Friedman et de Martin établissent un interclassement entre des énoncés mathématiquement élaborés et des énoncés d'inspiration métamathématique tout à fait analogues à ceux de Gödel.

Le système formel du premier ordre qui correspond à la structure des entiers naturels $\mathbb{N}$ munis des opérations de l'arithmétique s'appelle l'Arithmétique de Peano et se note $\mathcal{P}$. Cette théorie est formulée dans le calcul des prédicats et ses axiomes sont les équations pour l'addition et la multiplication et le schéma d'induction, voir § 2. Le système $\mathcal{P}$ est très puissant et le Théorème de Gödel s'applique à lui. Au moyen des codages, on peut aussi y formuler l'étude des ensembles héréditairement finis - ensembles finis d'entiers, ensembles finis dont les éléments sont des entiers ou des ensembles finis d'entiers, etc. On peut alors y formuler les notions suivantes de combinatoire finie : Soient X un ensemble fini et r un entier ; l'ensemble des parties de X à r-éléments se note $[X]^r$; la cardinalité de X se note $|X|$; son élément minimum se note $\min X$. Si P est une partition de $[X]^r$ en k classes et si $H \subseteq X$ est tel que P soit constante sur $[H]^r$, on dit que H est homogène pour P . La notation $X \longrightarrow (m)^r_k$ signifie que pour toute partition P de $[X]^r$ en k classes, il y a une partie homogène H telle que $|H| \geq m$; la notation $\ell \longrightarrow (m)^r_k$ abrège $[1,\ell] \longrightarrow (m)^r_k$ où en général, $[n,\ell] = \{n , n+1 ,\ldots, \ell\}$. On écrit $[m,n]^k$ pour abréger $[[m,n]]^k$.

Dans $\mathcal{P}$, on peut démontrer le

Théorème de Ramsey.- Pour tous entiers m , r , k , il existe ℓ tel que $\ell \longrightarrow (m)^r_k$.

Le but de cet exposé est de présenter quelques résultats nouveaux, dus principalement à J. Paris, qui établissent l'existence de phénomènes d'incomplétude pour $\mathcal{P}$ de nature combinatoire. Appelons un ensemble fini non-vide d'entiers X un ensemble dense, [P] , ou relativement grand [H,P] , si $|X| \geq \min X$. Nous allons démontrer que certaines variantes du Théorème de Ramsey où l'on demande que la partie homogène soit dense sont vraies (autrement dit, satisfaites) dans $\mathbb{N}$ mais ne sont pas prouvables pour autant dans $\mathcal{P}$; les démonstrations "naturelles" de ces théorèmes utilisent la forme infinie du Théorème de Ramsey et des arguments par compacité qui ne sont pas formalisables dans $\mathcal{P}$. Ces travaux sont développés en trois articles : celui de Kirby-Paris [K,P], celui de Paris [P] et celui de Harrington-

Paris [H,P].

Pour ℓ , m , n , k $\in \mathbb{N}$, écrivons $\ell \underset{*}{\to} (m)_k^r$ si, pour toute partition P de $[1,\ell]^r$ en k-classes, il existe une partie homogène dense H pour P satisfaisant $|H| \geq m$. Nous verrons que, d'une part,

(*) Pour r , k $\in \mathbb{N}$, quel que soit m , il existe ℓ tel que

$$\ell \underset{*}{\to} (m)_k^r$$

mais, d'autre part, (*) n'est pas prouvable dans $\mathcal{P}$. La relation $\underset{*}{\to}$ donne lieu aussi à une fonction $f(r,m,k) = \ell$ qui est récursive mais qui n'admet pas de "majoration explicite" et qui n'est calculable que dans le sens le plus théorique du terme.

De même, étant donnés des entiers r , k , disons qu'un ensemble fini non-vide d'entiers X est O-<u>dense</u> (r,k) si X est dense ; disons que X est (n+1)-<u>dense</u> (r,k) si pour toute partition de $[X]^r$ en k classes il existe une partie homogène n-dense (r,k) . Nous avons d'une part,

(**) Pour r , k $\in \mathbb{N}$: quels que soient m , n , il existe ℓ tel que
$[m,\ell]$ est n-dense (r,k) ,

mais, d'autre part, (**) avec $r \geq 3$, $k \geq 2$, n'est pas prouvable dans $\mathcal{P}$.

Les propositions (*) et (**) sont les conséquences immédiates de la

PROPOSITION.- Tout ensemble infini d'entiers a une sous-partie finie qui est n-dense (r,k) quels que soient n , r , k $\in$ N .

<u>Démonstration</u>. Par induction sur n . Pour le passage de n à n+1 , on raisonne par l'absurde ; soit alors X un ensemble infini d'entiers tel que, en posant $X_s = X \cap [0,s]$, pour tout s , il existe des partitions P_s de $[X_s]^r$ en k-classes sans partie homogène n-dense (r,k) . Notons que si $s' > s$, alors la restriction d'une telle partition $P_{s'}$ à $[X_s]^k$ est une partition P_s sans partie homogène n-dense (r,k) . On définit une suite Q_s , $s \in \mathbb{N}$, de ces partitions, telle que :

(1) $s' > s \Longrightarrow Q_s$ est la restriction de $Q_{s'}$ à $[X_s]^r$;

(2) Q_s a une extension à une partition $P_{s'}$ sans partie homogène n-dense (r,k) pour tout $s' \geq s$.

Soit $Q = \cup Q_s$; alors Q est une partition de $[X]^r$ en k-classes. Par la forme infinie du Théorème de Ramsey, il existe un ensemble infini $Y \subseteq X$ qui est homogène pour Q ; d'après l'hypothèse de récurrence, il existe une partie Y_s finie de Y qui est n-dense (r,k) ce qui contredit le choix de Q_s .

Pour avoir les résultats de non-démontrabilité, nous aurons besoin de développer les méthodes de Kirby et Paris dans le paragraphe suivant. Notons toutefois que la notion d'ensemble dense donne une mesure de la taille d'un ensemble fini d'entiers qui ne dépend pas uniquement de la cardinalité mais aussi de "l'ordinalité" de l'ensemble, c'est-à-dire, sa distribution dans la suite des entiers finis. Du point de vue de la Théorie des ensembles, la distinction entre nombre ordinal et nombre cardinal ne se fait pas au niveau du fini mais elle se discerne seulement au niveau de l'infini. La notion d'ensemble dense de Paris provient finalement, [P], [K,P], d'une intuition "grand cardinal" ; donc il s'agit de la projection sur le fini d'une intuition infinitaire ; cet aspect des choses est rendu encore plus explicite par des travaux récents de Solovay [S] et Ketonen [Ke].

§ 2. La méthode des Indicatrices de Kirby-Paris

Une des retombées des travaux de Kirby et Paris [K,P], est un nouveau type de démonstration de résultats d'incomplétude où l'on construit directement des modèles de $\mathcal{P}$ qui ne satisfont pas les mêmes formules que $\mathbb{N}$ sans passer par la fameuse astuce de Gödel consistant à fabriquer une formule paradoxale qui exprime sa propre non-démontrabilité. Nous allons donc insister ici sur ce nouvel aspect modèle-théorique des choses.

Le langage de $\mathcal{P}$ est le calcul des prédicats du premier ordre avec égalité : on a deux symboles de fonction binaire $+$ (addition) et $\cdot$ (multiplication) et deux constantes individuelles 0 , 1 . L'ensemble des termes de ce langage est défini par induction :

(1) Toute variable et toute constante sont des termes

(2) Si t , s sont des termes, alors $t + s$ et $t \cdot s$ sont des termes.

L'ensemble des formules est défini également par induction :

(1) Si t , s sont des termes, alors $t = s$ est une formule (dite atomique).
(2) Si E et F sont des formules, alors $E \wedge F$, $\neg F$ et $\forall vE$, où v est une variable,

sont des formules.

On écrit $F = F(v_1,\ldots,v_n)$ si F est une formule dont les variables libres sont comprises parmi $v_1,\ldots,v_n$.

Les axiomes de $\mathcal{P}$ sont les équations pour l'addition et la multiplication

$\forall v\ (v + 0 = v)$ $\quad\forall v\ (v \cdot 0 = 0)$ $\quad\forall v\ (v + 1 \neq 0)$ $\quad\forall u\ \forall v\ (u \neq v \longrightarrow u + 1 \neq v + 1)$

$\forall v\ \forall u\ (v + (u + 1) = (v + u) + 1)$ $\qquad\forall v\ \forall u\ (v \cdot (u + 1) = (v \cdot u) + v)$

et le schéma d'induction

$$\forall v_1, \ldots, \forall v_n \quad [(F(O, v_1, \ldots, v_n) \wedge \forall v\ (F(v, v_1, \ldots, v_n) \rightarrow F(v+1, v_1, \ldots, v_n)) \\ \rightarrow \forall v\ \ F(v, v_1, \ldots, v_n)]$$

pour toute formule $F = F(v_1, \ldots, v_n)$.

Soit A un anneau commutatif unitaire ordonné. Soit M les éléments non-négatifs de A ; M est donc une structure pour le langage de $\mathcal{P}$; si $t(v_1, \ldots, v_n)$ est un terme à n-variables libres et si $a_1, \ldots, a_n \in M$, alors la valeur de $t(a_1, \ldots, a_n)$ se calcule à partir des opérations de l'anneau A . La relation de satisfaction entre les formules et les suites finies d'éléments de M se définit alors par récurrence sur les formules, les connecteurs et les quantificateurs ayant leurs sens usuels. Si les axiomes de $\mathcal{P}$ sont toujours satisfaits dans M , nous disons que M est un <u>modèle</u> de $\mathcal{P}$. <u>Dans toute la suite, on ne considèrera que des modèles dénombrables de</u> $\mathcal{P}$. Tout modèle M de $\mathcal{P}$ est un ensemble totalement ordonné et les entiers naturels $\mathbb{N}$ s'identifient avec un segment initial de M . Si $\mathbb{N}$ est un segment initial propre de M , alors M est dit <u>non-standard</u> ; si I est un segment initial propre de M , on écrit $I < M$; pour $\alpha \in M$, on écrit $\alpha < I$ si $\alpha \in I$, $I < \alpha$ si $\alpha \notin I$; si $\mathbb{N} < \alpha$, α est un <u>entier infini</u> de M . Un segment $I < M$ clos pour l'addition et la multiplication de M est aussi une structure pour le langage de $\mathcal{P}$; nous nous intéresserons surtout de trouver $I < M$, $\mathbb{N} < I$ tel que I est un modèle de $\mathcal{P}$.

Si $F = F(v_1, \ldots, v_n)$ est une formule et si $a_1, \ldots, a_n \in M$, on écrit $M \models F(a_1, \ldots, a_n)$ si la suite $a_1, \ldots, a_n$ satisfait F dans M . Une partie X de M est <u>définissable</u> s'il existe $F(v, v_1, \ldots, v_n)$ et $a_1, \ldots, a_n$ tels que $b \in X \iff M \models F(b, a_1, \ldots, a_n)$. Si $M \models \mathcal{P}$, alors toute partie définissable non-vide de M possède un plus petit élément (au sens de l'ordre sur M). Il en suit que, si M est non-standard, le segment initial $\mathbb{N}$ n'est pas définissable dans M ; plus généralement aucun segment initial propre de M clos pour successeur n'est définissable dans M . On remarque également que si X est une partie définissable de M qui est bornée supérieurement dans M , alors X a un plus grand élément ; de plus, un tel ensemble X est codé dans M en tant qu'ensemble fini.

Une <u>fonction définissable</u> de $\mathcal{P}$ est la donnée d'une formule $Y = Y(v_1, \ldots, v_n, v)$ telle que pour tout modèle M de $\mathcal{P}$, $\{\langle a_1, \ldots, a_n, b\rangle : M \models Y(a_1, \ldots, a_n, b)\}$ est une fonction de M^n dans M , notée Y_M . Une fonction Y définissable dans $\mathcal{P}$ est <u>absolue</u> si pour tout modèle M de $\mathcal{P}$, pour tout $I < M$ tel que $I \models \mathcal{P}$, Y_I est la restriction de Y_M à I^n . Une fonction absolue $Y = Y(v_1, v_n)$ est <u>monotone</u> si $Y_M(\alpha', \beta) \leq Y_M(\alpha, \beta')$ quels que soient $\alpha' \leq \alpha \leq \beta \leq \beta' \in M$, quel que soit le modèle M de $\mathcal{P}$.

Soit $\mathcal{J}$ une théorie qui étend $\mathcal{P}$. Une fonction absolue et monotone Y est une <u>indicatrice</u> pour $\mathcal{J}$ si pour tout M , pour tous $\alpha , \beta \in M$,

$$Y_M(\alpha,\beta) > \mathbb{N} \implies \exists\, I \ (\alpha < I < \beta \text{ et } I \models \mathcal{J}) .$$

PROPOSITION.- Soit Y une indicatrice pour $\mathcal{J}$, soit M un modèle non-standard de $\mathcal{P}$ et soient $\alpha , \beta \in M$ tels que $\mathbb{N} < \alpha , \beta$ et $Y_M(\alpha,\beta) > \mathbb{N}$. Alors, il existe I , $\alpha < I < \beta$, $I \models \mathcal{J}$ et

$$I \models \exists x \exists y \forall z \ [Y(x,z) \leq y] .$$

<u>Démonstration</u>. Pour $m \in \mathbb{N}$, on a $Y_M(m,\beta) \geq Y_M(\alpha,\beta) > \mathbb{N}$. Soit donc α' le plus grand élément de M tel que

$$M \models \alpha' < \beta \ \wedge \ Y(\alpha',\beta) > \alpha' .$$

Forcément $\alpha' > \mathbb{N}$ et $Y_M(\alpha',\beta) > \mathbb{N}$. Soit γ le plus grand élément de M tel que $M \models \alpha' \leq \gamma \leq \beta \wedge Y(\alpha', \gamma) \leq \alpha'$. Notons que, de façon générale, $Y_M(\eta,\xi) < \mathbb{N} < \beta \implies Y_M(\eta ; \xi + 1) < \mathbb{N} < \beta$ quels que soient $\eta , \xi \in M$. Nous avons donc $\mathbb{N} < Y(\alpha', \gamma) \leq \alpha'$. Soit I tel que $\alpha' < I < \gamma$, $I \models \mathcal{J}$. Alors $I < M$ et $I \models \forall x \ (Y(\alpha',x) \leq \alpha')$. C.Q.F.D.

Disons qu'une indicatrice Y pour $\mathcal{J}$ est <u>admissible</u> si $\mathbb{N} \models \forall m \forall n \exists \ell \ [Y(m,\ell) \geq n]$. Moyennant l'existence d'indicatrices admissibles, nous avons un théorème d'incomplétude,

THÉORÈME (Kirby-Paris).- Soit Y une indicatrice admissible pour $\mathcal{J}$. Alors l'énoncé $\forall x \forall z \exists y \ [Y(x,y) \geq z]$ n'est pas démontrable dans $\mathcal{J}$ bien que satisfait dans $\mathbb{N}$.

<u>Démonstration</u>. Soit M un modèle non-standard de $\mathcal{J}$ et soit β_o un entier infini de M . Posons $X = \{a \in M : M \models \exists y \ [Y(a,y) > a \wedge a < \beta_o]\}$. Alors $\mathbb{N} \subseteq X$ et X est borné supérieurement par β_o ; soit α le plus grand élément de X . On a $\alpha > \mathbb{N}$ et il existe $\beta \in M$ tel que $M \models Y(\alpha,\beta) > \alpha$. Par la proposition précédente, il existe I tel que $\alpha < I < \beta$, $I \models \mathcal{J}$ et $I \models \exists x \ \exists z \ \forall y \ [Y(x,y) \leq z]$. C.Q.F.D.

<u>Remarque</u>.- Kirby et Paris ont démontré que toute théorie récursivement axiomatisable admet une indicatrice admissible Y satisfaisant même $\mathcal{J} \vdash \forall x \exists y \ [Y(x,y) \geq \overline{n}]$ quel que soit $n \in \mathbb{N}$. Pour éviter un détour trop long, nous nous contenterons ici d'étudier deux exemples d'indicatrices admissibles pour $\mathcal{P}$.

On définit deux fonctions Z et W dans $\mathcal{P}$ au moyen des définitions suivantes :

$Z(x,y) = z \iff z$ est le plus grand entier tel que $[x,y]$ est est z-dense $(3,2)$

$W(x,y) = z \iff z$ est le plus grand entier tel que

$$[x,y] \underset{*}{\to} (2z)^z_z \ .$$

On remarque que Z et W sont des fonctions absolues et monotones.

THÉORÈME (Kirby, Paris, Harrington).- Les fonctions Z et W sont des indicatrices admissibles pour $\mathcal{P}$.

Démonstration (Z). Soit M un modèle de $\mathcal{P}$ et soient $\mathbb{N} < \alpha < \beta \in M$ tels que $M \models Z(\alpha,\beta) = \gamma$, $\gamma > \mathbb{N}$. Soit P_o , P_1 ,... une énumération des partitions définissables de $[M]^3$ dans 2 classes telles que chaque partition définissable apparaisse infiniment souvent. Soit S_o , S_1 ,... une suite de parties de $[\alpha,\beta]$ satisfaisant $S_o = [\alpha,\beta]$ et

(1) chaque S_n est définissable dans M

(2) S_{n+1} est homogène pour P_n et $S_{n+1} \subseteq S_n$

(3) $M \models S_n$ est $\gamma - n$ dense $(3,2)$.

Posons $I = \{a \in M : \text{il existe } n ,\ a < \min S_n\}$. Nous disons que I est un modèle de $\mathcal{P}$. Remarquons d'abord que de façon générale (voulant dire démontrable dans $\mathcal{P}$), si $S = \{s_1,\ldots,s_\ell\}$ est un ensemble fini, $k+1$ dense $(3,2)$ et si $\min S > 3$, alors $S - \{s_1,s_2\}$ et $S - \{s_{\ell-1}, s_\ell\}$ sont tous deux k-dense $(3,2)$: on n'a qu'à poser $Q(a,b,c) = *$ si $a , b = s_1 , s_2$, $**$ sinon, etc ; donc en particulier, $|S| \geq s_3$. Remarquons aussi que pour tout $\delta \in M$, il existe n tel que ou bien $\delta < \min S_n$ ou bien $\delta > \max S_n$: en effet, posons $P(a,b,c) = *$ si $a , b , c \leq \delta$, $**$ sinon ; soit n tel que $P = P_n$; alors S_{n+1} est homogène pour P et ou bien $S_{n+1} \subseteq [0,\delta]$ ou bien $|S_{n+1} \cap [0,\delta]| \leq 2$; par la remarque précédente, il existe n_δ tel que pour tout $m \geq n_\delta$, soit $\delta < \min S_m$ soit $\delta > \max S_m$. Vérifions maintenant que I est clos pour l'addition et la multiplication. On considère la partition P de $[M]^3$ en 2 classes définie par

$P(a,b,c) = *$ si $2a < b$, $P(a,b,c) = **$ si $b \leq a+y < c$ pour un $y \leq a$ où $a < b < c$. Parce que P est définissable, $P = P_n$ pour un $n \in \mathbb{N}$, alors S_{n+1} est homogène pour P . Je dis que P est constamment égale à $*$ sur S_{n+1} : en effet, sinon on aurait, en posant $S_{n+1} = \{s_1,\ldots,s_\ell\}$, qu'il existe dans M une suite $0 < y_2 < \ldots < y_{\ell-1} \leq s_1$ tels que $s_i \leq s_1 + y_i < s_{i+1}$, $2 \leq i \leq \ell - 1$, d'où

$\ell - 2 \leq s_1$ et $M \models |S_{n+1}| \leq \min S_{n+1} + 2$, ce qui est impossible à cause de la densité de S_{n+1} . Donc il existe n_1 tel que $a , b \in S_m$, $a < b \Longrightarrow a+a < b$ quel que soit $m \geq n_1$. Quant à la multiplication, soit $Q(a,b,c) = *$ si $a^2 < b$, $Q(a,b,c) = **$ sinon. Pour $m \geq n_1$, on note que pour $a , b , c \in S_m$, $a < b < c$; $** = Q(a,b,c) \Longleftrightarrow$ il existe $y \leq a$, $b \leq a\cdot y < c$, car $a^2 \geq b \Longrightarrow$ il existe $e \leq a$, $a\cdot e \leq b < a(e+1) \leq b + b < c$. Soit $n \geq n_1$ tel que $Q = P_n$. Je dis que Q est constamment égale à $*$ sur $S_{n+1} = \{s_1,\ldots,s_\ell\}$: en effet, sinon on aurait une suite $1 < y_1 <\ldots< y_{\ell-1} \leq s_1$ telle que $s_i \leq a\cdot y_i < a_{i+1}$, $1 \leq i \leq \ell-1$; alors on aurait $M \models |S_{n+1}| < s_1$, ce qui contredit la densité de S_{n+1} . On en conclut qu'il existe n_2 tel que, pour tout $m \geq n_2$, pour tous $a , b \in S_m$, $a < b \Longrightarrow a^2 < b$. Par récurrence sur k , on démontre de façon analogue qu'il existe n_k tel que $a , b \in S_m$, $a < b \Longrightarrow a^k < b$ quel que soit $m \geq n_k$.

Soit $F : M^k \longrightarrow M$ une fonction définissable dans M . Nous disons qu'il existe n_F tel que quel que soit $m \geq n_F$, $a , b \in S_m$, $a < b \Longrightarrow \forall a_1 \ldots \forall a_k$ $[a_1 ,\ldots, a_k < a \Longrightarrow$ soit $F(a_1,\ldots,a_k) < b$, soit $F(a_1,\ldots,a_k) \geq \max S_m]$. En effet, posons $R(a,b,c) = *$ si $a_1,\ldots,a_k < a \Longrightarrow F(a_1,\ldots,a_k) \notin [b,c)$, $**$ sinon . Soit $n_F \geq n_{k+1}$ tel que $R = P_{n_F}$. Alors $s_1^{k+1} < s_2$ où $S_{n_F} = \{s_1,\ldots,s_\ell\}$; si R était constamment égale à $**$ sur S_{n_F} , on aurait $M \models \ell \leq s_1^k + 2 \leq s_1^{k+1} < s_2$, contredisant la densité de S_{n_F} .

Nous achèverons la preuve au moyen du

<u>Lemme de Vérité</u> (Z).- Il y a une application qui à toute formule $E = E(v_1,\ldots,v_k)$ du langage de $\mathcal{P}$ associe une formule $\bar{E} = \bar{E}(v_1,\ldots,v_k , u_1,\ldots,u_\ell)$ et une suite finie $B(E) = \langle b_1,\ldots,b_\ell\rangle$ d'éléments de M telles que

$$I \models E(a_1,\ldots,a_k) \Longleftrightarrow M \models \bar{E}(a_1,\ldots,a_k , b_1,\ldots,b_\ell)$$

quels que soient $a_1,\ldots,a_k \in I$.

<u>Démonstration du Lemme</u>. On définit $\bar{E}$ et $B(E)$ et on vérifie en même temps la conclusion du lemme par récurrence sur E . Pour E atomique, on pose $\bar{E} = E$, $B(E) = \emptyset$; on pose $\overline{E_1 \wedge E_2} = \bar{E}_1 \wedge \bar{E}_2$, $B(E_1 \wedge E_2) = B(E_1) \cup B(E_2)$ ordonnés selon les u_i , $\overline{\neg E} = \neg \bar{E}$, $B(\neg E) = B(E)$. Pour ces cas la conclusion du lemme est évidente. Supposons que $E = \forall v\, E_1(v_1,\ldots,v_k , v)$. Soient $\bar{E}_1 = \bar{E}_1(v_1,\ldots,v_k , v , u_1,\ldots,u_\ell)$, $B(E_1) = \langle b_1,\ldots,b_\ell\rangle$. Considérons la fonction $F : M^k \longrightarrow M$ qui est définie dans M par

$$F(a_1,\ldots,a_k) = b \Longleftrightarrow M \models b = \mu x(\neg \bar{E}_1(a_1,\ldots,a_k , x , b_1,\ldots,b_\ell))$$

où " $\mu x \ldots$ " abrège "le plus petit x tel que ..." . Soit n_F l'entier associé à la fonction définissable F , soit $m \geq n_F , n_1 , n_2 , n_k$, soit $S_m = \{s_1,\dots,s_t\}$ et soit $b_{\ell+1} = \max S_m = s_t$. Nous posons $\bar{E} = \forall v\ (v < u_{\ell+1} \longrightarrow \bar{E}_1(v_1,\dots,v_k , v , u_1,\dots,u_\ell))$ et $B(E) = \langle b_1,\dots,b_{\ell+1}\rangle$. Vérifions la conclusion du lemme : pour $a_1,\dots,a_k \in I$, soit $n \geq m$ tel que $a_1,\dots,a_k < \min S_n$. Alors nous avons $I \models \forall v\ E(a_1,\dots,a_k , v) \Longleftrightarrow \forall a \in I$,

$I \models E(a_1,\dots,a_k , a) \Longleftrightarrow$ (par l'hypothèse de récurrence) $\forall a \in I$,

$M \models \bar{E}_1(a_1,\dots,a_k , a , b_1,\dots,b_\ell) \Longleftrightarrow \forall s \in S_m \cap I , \forall a < s$,

$M \models \bar{E}_1(a_1,\dots,a_k , a , b_1,\dots,b_\ell) \Longleftrightarrow \forall s \in S_m \cap I$,

$M \models \forall a < s\ \bar{E}_1(a_1,\dots,a_k , a , b_1,\dots,b_\ell) \Longleftrightarrow (m \geq n_F , b_{\ell+1} = \max S_m)$

$M \models \forall a < b_{\ell+1}\ \bar{E}_1(a_1,\dots,a_k , a , b_1,\dots,b_\ell)$.

Le lemme prouvé, quelques remarques termineront la démonstration. Le segment $I < M$ est clos pour l'addition et la multiplication de M ; les axiomes sur les fonctions primitives de $\mathcal{P}$ sont universels et donc automatiquement satisfait dans I . Le schéma d'induction ou ce qui lui est équivalent, le principe de l'élément minimal, est satisfait dans I parce que d'après le Lemme de Vérité, toute partie X définissable de I est la restriction à I d'une partie définissable $\bar{X}$ de M ; l'élément minimum de $\bar{X}$ est donc l'élément minimum de X . C.Q.F.D.

Démonstration (W). Cette démonstration est fort analogue à celle pour (Z), mais elle utilise plus d'outils "Logiques". Soit $i \longmapsto \varphi_i$ une énumération récursive des formules de $\mathcal{P}$ (identifiées avec leurs nombres de Gödel) à quantification bornée (tout quantificateur $\forall v$ se trouvant dans le contexte $\forall v\ (v < u \longrightarrow \dots)$). La relation $S(i,\langle n_1,\dots,n_k\rangle) \equiv$ la suite $\langle n_1,\dots,n_k\rangle$ satisfait $\varphi_i = \varphi_i(v_1,\dots,v_k)$ est une relation récursive. Soit M un modèle non-standard de $\mathcal{P}$ et soient α , β , γ des entiers infinis de M tels que $M \models [\alpha,\beta] \underset{*}{\rightarrow} (2\gamma)^{\gamma}_{\gamma}$. L'énumération φ_i et la relation de satisfaction S se prolongent canoniquement à M . Or, pour $i , k \in \mathbb{N}$ et $a_1,\dots,a_k \in M$, on a

$$M \models \varphi_i(a_1,\dots,a_k) \Longleftrightarrow M \models S(i,\langle a_1,\dots,a_k\rangle).$$

Soit $\delta > \mathbb{N}$ tel que $M \models \delta < \log_2(\gamma)$. Travaillant dans M , posons pour $i < \delta$ et $x = \{x_1,\dots,x_\gamma\} \in [\alpha,\beta]^\gamma$, $f(i,x) = 0$ si $S(i,\langle x_1,\dots,x_\gamma\rangle)$, 1 sinon. Ceci donne lieu à une partition P de $[\alpha,\beta]^\gamma$ dans 2^δ classes : $P(x) = \langle f(0,x),\dots,f(\delta - 1 , x)\rangle$. Soit H' une partie homogène dense pour P de cardinalité $\geq 2\gamma$, $H' = \{e_1,\dots,e_{\ell'}\}$. Soit ℓ la partie entière de $\frac{1}{2}\ell'$ et soit $H = \{e_1,\dots,e_\ell\}$. Revenant à l'extérieur de M , nous notons que H est un

<u>ensemble d'indiscernables simples</u> pour les φ_i , $i \in \mathbb{N}$: pour toute $\varphi_i = \varphi_i(v_1,\dots,v_k)$ et toutes suites $e_{i_1} < \dots < e_{i_k}$, $e_{j_1} < \dots < e_{j_k}$ d'éléments de H , on a

$$M \models \varphi_i(e_{i_1},\dots,e_{i_k}) \Longleftrightarrow \varphi_i(e_{j_1},\dots,e_{j_k}) .$$

Pour ce voir, on remarque que les suites $e_{i_1},\dots,e_{i_k}$ et $e_{j_1},\dots,e_{j_k}$ se prolongent dans M en des suites $x = \langle e_{i_1},\dots,e_{i_k},\dots\rangle$, $y = \langle e_{j_1},\dots,e_{j_k},\dots\rangle$, de longueur γ d'éléments de H' et que $M \models f(i,x) = f(i,y)$.

<u>Lemme d'Indiscernabilité Forte</u>.- Soient $\bar{e}_i = \langle e_{i_1},\dots,e_{i_k}\rangle$ et $\bar{e}_j = \langle e_{j_1},\dots,e_{j_k}\rangle$ deux suites croissantes d'éléments de H et soit $e \in H$ tel que $e < e_{i_1}, e_{j_1}$. Supposons que $\varphi_n = \varphi_n(v_1,\dots,v_k, u_1,\dots,u_r)$ et que $a_1,\dots,a_r \leq e$. Alors $M \models \varphi_n(e_{i_1},\dots,e_{i_k}, a_1,\dots,a_r) \Longleftrightarrow \varphi_n(e_{j_1},\dots,e_{j_k},a_1,\dots,a_r)$.

<u>Démonstration du lemme</u>. Par l'indiscernabilité simple, il suffit de démontrer le lemme pour $e = e_1$. Le lemme se vérifie par induction sur r ; pour $r = 0$, on retrouve l'indiscernabilité simple. Pour alléger les notations pour le passage de r à $r + 1$, nous supprimerons les $a_1,\dots,a_r$ et nous noterons $a_{r+1} = a$. Nous supposons aussi, sans perte de généralité, que $a \leq {}^{e_1}/_{5k}$. On écrit $\bar{e}_i < \bar{e}_j$ si $e_{i_k} < e_{j_1}$. Pour trouver une contradiction, nous supposons qu'il existe $a \leq {}^{e_1}/_{5k}$, $\bar{e}_i$, $\bar{e}_j$ et $\Phi = \varphi_n$ tels que

$$M \models \Phi(a,e_{i_1},\dots,e_{i_k}) \wedge \neg\Phi(a,e_{j_1},\dots,e_{j_k}) .$$

On voit aisément que l'on peut supposer $\bar{e}_i < \bar{e}_j$. On définit pour $\bar{e}_i < \bar{e}_j$ une fonction $F(\bar{e}_i , \bar{e}_j)$ dans M par

$$F(\bar{e}_i , \bar{e}_j) = c \Longleftrightarrow M \models c = \mu x \left[x \leq \frac{e_1}{5k} \wedge [\Phi(x,\bar{e}_i) \not\Longleftrightarrow \Phi(x,\bar{e}_j)]\right] .$$

Cette fonction est définie au moyen d'une formule à quantification bornée ; par l'hypothèse de récurrence (l'indiscernabilité simple si $r = 1$), on a <u>soit</u>

pour tout quadruplet $\bar{e}_i < \bar{e}_j < \bar{e}_s < \bar{e}_t$, $F(\bar{e}_i , \bar{e}_j) = F(\bar{e}_s , \bar{e}_t)$

<u>soit</u>

pour tout quadruplet $\bar{e}_i < \bar{e}_j < \bar{e}_s < \bar{e}_t$, $F(\bar{e}_i , \bar{e}_j) \neq F(\bar{e}_s , \bar{e}_t)$.

Parce que $M \models |H| \geq \frac{1}{2} \min H - 1$, seule la première alternative est possible. Soit donc b_o la valeur constante de $F(\bar{e}_i , \bar{e}_j)$. Prenons alors $\bar{e}_i < \bar{e}_j < e_s$: on arrive à une contradiction parce qu'on ne peut avoir simultanément

$$M \models \Phi(b_o, \bar{e}_i) \not\Leftrightarrow \Phi(b_o, \bar{e}_j) ,$$

$$M \models \Phi(b_o, \bar{e}_i) \not\Leftrightarrow \Phi(b_o, \bar{e}_s) ,$$

$$M \models \Phi(b_o, \bar{e}_j) \not\Leftrightarrow \Phi(b_o, \bar{e}_s) .$$

Le lemme étant établi, posons $I = \{a \in M : \text{il existe } n \in \mathbb{N} , a < e_n\}$; nous disons que $I \models \mathcal{P}$. Tout d'abord remarquons que I est clos pour la multiplication et donc pour l'addition : si $e_n^2 \geq e_{n+1}$, on aurait $e_{n+1} = e_n \cdot \mu + \lambda$ avec $\mu , \lambda \leq e_n$ et $e_{n+2} \neq e_n \cdot \mu + \lambda$, contrairement à l'indiscernabilité forte des e_k , $k \in \mathbb{N}$.

<u>Lemme de Vérité</u>.- Soit $E(y_1,\ldots,y_m) = Qv_n \ldots Qv_1 F(x_1,\ldots,x_n , y_1,\ldots,y_m)$ où F est sans quantificateur et Qv_i est soit $\forall v_i$, soit $\exists x_i$, $1 \leq i \leq n$. Alors, pour tous $a_1,\ldots,a_m \in I$, pour tous $e_{i_1} > \ldots > e_{i_n} > I$, on a

$$I \models E(a_1,\ldots,a_m) \Longleftrightarrow M \models Qv_n < e_{i_n} \ldots Qv_1 < e_{i_1} F(x_1,\ldots,x_n , a_1,\ldots,a_m) .$$

<u>Démonstration</u>. Par récurrence sur n . Pour fixer les idées, supposons $Qv_{n+1} = \forall v_{n+1}$ et que $a_1,\ldots,a_m < e_k$. Alors

$\forall b \in I$, $I \models Qv_n \ldots Qv_1 F(v_1,\ldots,v_n , b , a_1,\ldots,a_m)$

$\Longleftrightarrow$ pour tout $s \geq k$, $s \in \mathbb{N}$,

$$I \models \forall b < e_{s+1} Qv_n \ldots Qv_1 F(v_1,\ldots,v_n , b , a_1,\ldots,a_m)$$

$\Longleftrightarrow$ (par l'hypothèse de récurrence) pour tout $s \geq k$,

$$M \models \forall v_{n+1} < e_{s+1} Qv_n < e_{i_n} \ldots Qv_1 < e_{i_1} F(v_1,\ldots,v_n , v_{n+1} , a_1,\ldots,a_m)$$

$\Leftrightarrow$ (indiscernabilité forte) pour tout $e_{i_{n+1}}$, $e_k < e_{i_{n+1}} < e_{i_n}$

$$M \models \forall v_{n+1} < e_{i_{n+1}} Qv_n < e_{i_n} \ldots Qv_1 < e_{i_1} F(v_1,\ldots,v_{n+1} , a_1,\ldots,a_m) .$$

Le Lemme de Vérité étant établi, la démonstration se termine comme dans le cas de l'indicatrice Z . C.Q.F.D.

En fin de compte ces "nouveautés" peuvent être réintégrées dans l'analyse Gödelienne. Une variante bien connue de "la formule" de Gödel est celle qui exprime la 1-consistance de $\mathcal{P}$: "Toute formule universelle vraie est consistante avec $\mathcal{P}$ ", que l'on notera $\mathrm{Cons}(T_1 + \mathcal{P})$. Si l'on pose $\mathcal{J}_1 = \{F : F$ une formule close universelle telle que $\mathbb{N} \models F\}$, on a alors que $\mathrm{Cons}(T_1 + P)$ n'est pas démontrable dans $\mathcal{P} + \mathcal{J}_1$, bien que satisfait dans $\mathbb{N}$; ceci n'est qu'une forme relativisée du Théorème de Gödel. Nous énonçons

THÉORÈME (Harrington, Mc Aloon).- Soient Z et W les indicatrices pour P introduites ci-dessus. Alors

$$\mathcal{P} \vdash \mathrm{Cons}(T_1 + \mathcal{P}) \longleftrightarrow \forall x \forall z \exists y \ (Z(x\cdot y) \geq z) \longleftrightarrow \forall x \forall z \exists y \ (W(x,y) \geq z) .$$

Notons finalement que $\mathrm{Cons}(T_1 + \mathcal{P})$ et ces autres énoncés sont équivalents dans $\mathcal{P}$ à un énoncé de la forme

$$\forall v_1 , \ldots \forall v_n \ \exists u_1 \ldots \exists u_m \ P(v_1,\ldots,v_n , u_1,\ldots,u_m) = Q(v_1,\ldots,v_n , u_1,\ldots,u_m)$$

pour une certaine équation diophantienne $P = Q$.

§ 3. Remarques

Posons $D(n) = \ell$ si ℓ est le premier entier tel que $\ell \underset{*}{\longrightarrow} (2n)^n_n$ et $E(n) = \ell$ si ℓ est le premier entier tel que $[n,\ell]$ est n-dense (3,2) . Alors D et E sont des fonctions récursives de $\mathbb{N}$ dans $\mathbb{N}$. Une fonction récursive $f : \mathbb{N} \longrightarrow \mathbb{N}$ est dite prouvable s'il existe une formule existentielle $F(u,v)$ telle que

(a) $f(m) = n \Longleftrightarrow \mathcal{P} \vdash F(m,n)$

(b) $\mathcal{P} \vdash \forall u \exists ! v \ F(u,v)$.

Le résultat suivant est un corollaire à la démonstration du fait que Z et W sont des indicatrices pour $\mathcal{P}$.

THÉORÈME (Paris).- Pour toute fonction f récursive prouvable, il existe $n = h_f$ tel que $f(m) \leq E(m)$, $D(m)$ quel que soit $m \geq n$.

Le théorème démontre donc que E et D sont à croissance extrêmement rapide dépassant à la limite toute fonction récursive prouvable. Une démonstration directe de ce théorème a été donnée par Solovay utilisant au lieu de Théorie des Modèles une analyse des fonctions récursives prouvables en termes de la hierarchie de Grzegorczyk-Wainer. Ce travail a été simplifié ensuite par Ketonen de façon à mettre encore plus en évidence l'utilisation au niveau de la combinatoire finie des intuitions provenant de la combinatoire infinie des grands cardinaux.

Notons enfin quelques extensions des résultats de Kirby-Paris-Harrington à des théories autres que $\mathcal{P}$. D'abord, comme nous l'avons déjà remarqué, Kirby et Paris prouvent que toute théorie axiomatisable non-contradictoire a une indicatrice admissible, ce qui établit un théorème d'incomplétude fort général sans utiliser l'astuce d'autoréférence de Gödel. Cette méthode permet de voir aussi que pour tout modèle non-standard M de $\mathcal{P}$, il existe I , $\mathbb{N} < I < M$ tel que $I \models \mathcal{T}$ quel que soit la théorie axiomatisable $\mathcal{T}$ telle que $\mathbb{N} \models \mathcal{T}$; ceci permet de croire à l'existence d'indicatrices "combinatoires" pour des théories beaucoup plus puissantes que $\mathcal{P}$.

De premiers résultats dans ce sens sont de nous ; à titre d'exemple,

Soit $\mathcal{P}^+$ l'extension de $\mathcal{P}$ par le schéma de Réflection Complète, où l'on rajoute pour chaque n , la formule "Toute formule vraie a n-changements de quantificateurs est consistante avec $\mathcal{P}$ " .

Soit $\mathcal{P}^*$ l'extension de $\mathcal{P}$ où l'on rajoute le schéma : "Pour toute fonction f définie par une formule à k-changements de quantificateurs,

$$\forall m , n , r \ \exists \ell \ (\ell \xrightarrow[f(*)]{} (m)^r_n) \text{ "}$$

où $f(*)$ signifie que la partie homogène H doit satisfaire $|H| \geq f(\min H)$.

Ecrivons $\ell \xrightarrow[**]{} (m)^r_n$ si toute partition de P_2 de $[1,\ell]^r$ en n-classes a une partie homogène H telle que $H \xrightarrow[*]{} (2 \min^2 H)^{\min^2 H}_{\min^2 H}$, $\min^2 H = \min H^{\text{ième}}$ élément de H.

THÉORÈME (Mc Aloon).- Les systèmes $\mathcal{P}^+$ et $\mathcal{P}^*$ axiomatisent la même théorie et

$$\mathcal{P} \vdash \mathrm{Cons}(T_1 + P^*) \longleftrightarrow \forall m , n , r \ \exists \ell \ (\ell \xrightarrow[**]{} (m)^r_n) \ .$$

BIBLIOGRAPHIE

[F] H. FRIEDMAN - Higher set theory and mathematical practice, Ann. Math. Logic, 1971,

[G] K. GÖDEL - Philosophy of Mathematics, recueil de Benacareff et Putmann, Prentice-Hall, 1964.

[H,P] L. HARRINGTON-J. PARIS - A mathematical incompleteness in Peano arithmetic, Handbook of Mathematical Logic, North-Holland, 1977.

[Ke] J. KETONEN - Set theory for a small universe, manuscrit.

[Ki] L. KIRBY - Initial segment of models of arithmetic, Thèse, Manchester, 1976.

[K,P] L. KIRBY-J. PARIS - Initial segments of models of arithmetic, Lecture Notes in Math., vol. 619, Springer-Verlag.

[M] D. MARTIN - Borel Determinacy, Ann. Math., 1976.

[Mc] K. MC ALOON - Iterating the new "true, unprovable" formulas, manuscrit.

[P] J. PARIS - Independence results in Peano arithmetic using miner models, à paraître.

[Sc] J. SCHLIPF - Scribblings on papers of Kirby and Paris and Paris and Harrington, Notices de l'A.M.S., Avril 1978.

[S] R. SOLOVAY - Rapidly growing Ramsey functions, manuscrit.