DANIEL LACOMBE

Théorèmes de non-décidabilité

Séminaire N. Bourbaki, 1964, exp. n° 266, p. 323-363

<http://www.numdam.org/item?id=SB_1962-1964__8__323_0>

Séminaire BOURBAKI
16e année, 1963/64, n° 266

Février 1964

THÉORÈMES DE NON-DÉCIDABILITÉ (*)

par Daniel LACOMBE

TABLE DES MATIÈRES

(*) Le présent texte reproduit, après corrections, le tirage provisoire qui avait été multigraphié par l'Institut Blaise Pascal.

§ 1 - DÉFINITIONS GÉNÉRALES.

1.1 - $\mathbb{N}$ est l'ensemble des entiers naturels, $\mathbb{Z}$ l'ensemble des entiers rationnels, $\mathbb{Q}$ l'ensemble des nombres rationnels.

1.2 - A et B étant des ensembles quelconques, B^A est l'ensemble de toutes les applications de A dans B.

Nous assimilerons A^0 à $A^{\emptyset}$, c'est-à-dire à $\{\emptyset\}$.

Et nous assimilerons $A^{\{\emptyset\}}$ à A.

1.3 - Nous poserons $\mathfrak{F}^{(p)}(A) = A^{(A^p)}$ pour chaque $p \in \mathbb{N}$,

$$\text{et} \quad \mathfrak{F}(A) = \sum_{p \in \mathbb{N}} \mathfrak{F}^{(p)}(A) ,$$

où $\sum$ représente la somme directe (que dans la suite nous assimilerons sans vergogne à la réunion).

Pour $M \subset \mathfrak{F}(A)$, on posera $M^{(p)} = M \cap \mathfrak{F}^{(p)}(A)$.

1.4 - Nous poserons $\mathfrak{R}^{(p)}(A) = \mathfrak{P}(A^p)$,

$$\text{et} \quad \mathfrak{R}(A) = \sum_{p \in \mathbb{N}} \mathfrak{R}^{(p)}(A) .$$

Pour $M \subset \mathfrak{R}(A)$, on posera $M^{(p)} = M \cap \mathfrak{R}^{(p)}(A)$.

Pour $X \in \mathfrak{R}^{(p)}(A)$ et $(x_1, \ldots, x_p) \in A^p$, nous écrirons parfois "$X(x_1, \ldots, x_p)$" au lieu de "$(x_1, \ldots, x_p) \in X$".

1.5 - Soit B un sous-ensemble de A^p (avec éventuellement $B = A^p$), et soit φ une application de B dans A. Un sous-ensemble X de A est dit <u>clos</u> (ou "stable") <u>pour</u> φ si on a

$$\varphi(X^p \cap B) \subset X .$$

Dans le cas $p = 0$, $B = \{\emptyset\}$, cette condition devient $\varphi \in X$.

1.6 - Nous poserons $\mathbb{F} = \mathfrak{F}(\mathbb{N})$.

1.7 - Pour un sous-ensemble $\mathbb{M}$ de $\mathbb{F}$, considérons les conditions (a) et (b) suivantes:

(a) $\mathbb{M}$ contient les fonctions suivantes:

(1) la fonction (par ex. de 0 argument) identiquement nulle;

(2) la fonction successeur $x \to x + 1$;

(3) les fonctions projections $(x_1, \ldots, x_i, \ldots, x_p) \to x_i$.

(b) $\mathbb{M}$ est clos pour les opérations suivantes:

(1) les opérations de composition (ou "substitutions"), c'est-à-dire (pour chaque p , q) l'application $(\psi , \chi_1, \ldots, \chi_p) \to \varphi$ de $\mathbb{F}^{(p)} \times (\mathbb{F}^{(q)})^p$ dans $\mathbb{F}^{(q)}$, où φ est définie par:

$$\varphi(x_1, \ldots, x_q) = \psi[\chi_1(x_1, \ldots, x_q), \ldots, \chi_p(x_1, \ldots, x_q)] \quad ;$$

(2) les opérations de récurrence simple, c'est-à-dire (pour chaque p) l'application $(\chi , \psi) \to \varphi$ de $\mathbb{F}^{(p)} \times \mathbb{F}^{(p+2)}$ dans $\mathbb{F}^{(p+1)}$, où φ est définie par

$$\varphi(x_1, \ldots, x_p, 0) = \chi(x_1, \ldots, x_p)$$

$$\varphi(x_1, \ldots, x_p, y + 1) = \psi[x_1, \ldots, x_p, y, \varphi(x_1, \ldots, x_p, y)].$$

(3) les opérations " μ " , c'est-à-dire (pour chaque p) l'application $\psi \to \varphi$, avec

$\varphi(x_1, \ldots, x_p)$ = le plus petit y tel que $[\psi(x_1, \ldots, x_p, y) = 0]$,

application à valeurs dans $\mathbb{F}^{(p)}$ définie sur l'ensemble des éléments ψ de $\mathbb{F}^{(p+1)}$ qui satisfont à

$$\forall x_1 \ldots \forall x_p \; \exists y \, [\psi(x_1, \ldots, x_p, y) = 0] .$$

Nous désignerons par $\mathbb{F}_R$ le plus petit sous-ensemble de $\mathbb{F}$ qui satisfait aux conditions (a) et (b) (intersection complète de tous les sous-ensembles $\mathbb{M}$ qui satisfont à ces conditions).

Autrement dit, $\mathbb{F}_R$ est l'ensemble de toutes les fonctions qui peuvent s'obtenir à partir des fonctions initiales indiquées dans la condition (a) en appliquant (suivant un schéma fini quelconque) les opérations indiquées dans la condition (b) .

Les éléments de $\mathbb{F}_R$ sont appelés <u>fonctions récursives</u>.

1.8 - Un élément de $\mathfrak{R}^{(p)}(\mathbb{N})$ est dit <u>récursif</u> si sa fonction caractéristique appartient à $\mathbb{F}_R^{(p)}$.

Un élément X de $\mathfrak{R}^{(p)}(\mathbb{N})$ est dit <u>récursivement énumérable</u> s'il existe un élément récursif Y de $\mathfrak{R}^{(p+1)}(\mathbb{N})$ dont X soit la projection, c'est-à-dire un ensemble récursif Y tel qu'on ait

$$(\forall x_1,\dots,x_p \in \mathbb{N}) \; [\; X(x_1,\dots,x_p) \Leftrightarrow (\exists y \in \mathbb{N})\, Y(x_1,\dots,x_p,y) \;] .$$

Nous désignerons par (R) [resp. : (RE)] l'ensemble de tous les éléments récursifs [resp. : récursivement énumérables] de $\mathfrak{R}(\mathbb{N})$.

1.9 - $\mathbb{F}_R$, (R) et (RE) sont manifestement dénombrables. Et on a (R) $\subset$ (RE) .

D'autre part, on peut définir (R) et $\mathbb{F}_R$ à partir de (RE) , grâce aux résultats suivants:

PROPOSITION 1.1 - Pour qu'un élément de $\mathfrak{R}^{(p)}(\mathbb{N})$ soit récursif, il faut et il suffit que lui-même et son complémentaire (relativement à $\mathbb{N}^p$) soient récursivement énumérables.

PROPOSITION 1.2 - Pour qu'un élément de $\mathbb{F}^{(p)}$ soit récursif, il faut que son graphe [élément de $\mathfrak{R}^{(p+1)}(\mathbb{N})$] soit récursif, et il suffit que son graphe soit récursivement énumérable.

Enfin, on peut toujours se ramener aux fonctions d' 1 argument, car :

PROPOSITION 1.3 - Pour chaque $p \geq 1$, il existe une bijection récursive de $\mathbb{N}^p$ sur $\mathbb{N}$.

1.10 - A partir des définitions ci-dessus on obtient trivialement (à condition de suivre la filière adéquate) toute une collection de théorèmes "positifs" (ou "directs", ou encore "théorèmes de clôture") ayant la forme générale:

$\mathbb{F}_R$ [ou (R) , ou (RE)] est clos pour telle opération

dont un cas particulier (opération à 0 argument) est

$\mathbb{F}_R$ [ou (R) , ou (RE)] contient tel élément .

Les Prop. 1.1, 1.2, 1.3 appartiennent à cette collection. Citons encore les résultats fondamentaux suivants:

PROPOSITION 1.4 - $\mathbb{F}_R$, (R) et (RE) sont clos pour tous les changements de places portant sur les arguments (en particulier: permutation d'arguments, identification de deux arguments, adjonction d'un argument ineffectif).

PROPOSITION 1.5 - $\mathbb{F}_R$ contient la somme, le produit, l'exponentielle, le p. g. c. d. , etc.

PROPOSITION 1.6 - (R) contient les ensembles finis et leurs complémentaires, l'ensemble des nombres premiers, la relation d'ordre ordinaire, la relation de divisibilité, etc.

Désignons respectivement par $\cup^{(p)}$, $\cap^{(p)}$, $\complement^{(p)}$ l'union, l'intersection et le complémentation dans $\mathbb{N}^p$: ce sont des éléments particuliers de $\mathfrak{F}(\mathfrak{R}^{(p)}(\mathbb{N}))$.

Désignons par $\exists^{(p)}$ la quantification existentielle (ou projection, cf. 1.8) : c'est une application de $\mathfrak{R}^{(p+1)}(\mathbb{N})$ sur $\mathfrak{R}^{(p)}(\mathbb{N})$.

Désignons enfin par $\exists_{<}^{(p)}$ et $\forall_{<}^{(p)}$ les "quantifications (existentielle et universelle) bornées", c'est-à-dire les applications $X \to Y$ et $X \to Y'$ de $\mathfrak{R}^{(p+1)}(\mathbb{N})$ dans lui-même, où Y, Y' sont définies respectivement par:

$$Y(x_1,\ldots,x_p,y) \Longleftrightarrow (\exists i < y)\, X(x_1,\ldots,x_p,i),$$

$$Y'(x_1,\ldots,x_p,y) \Longleftrightarrow (\forall i < y)\, X(x_1,\ldots,x_p,i).$$

PROPOSITION 1.7 - (R) est clos pour les $\cup^{(p)}$, $\cap^{(p)}$, $\complement^{(p)}$, $\exists_{<}^{(p)}$, $\forall_{<}^{(p)}$.

PROPOSITION 1.8 - (RE) est clos pour les $\cup^{(p)}$, $\cap^{(p)}$, $\exists^{(p)}$, $\exists_{<}^{(p)}$, $\forall_{<}^{(p)}$.

De même, $\mathbb{F}_R$ est clos pour des opérations de récurrence beaucoup plus générales que celles utilisées dans la définition (1.7).

PROPOSITION 1.9 - Si $\varphi \in \mathbb{F}_R^{(p)}$ et si φ est bijective, les p "fonctions inverses" (ou "coordonnées de l'inverse") de φ appartiennent à $\mathbb{F}_R^{(1)}$.

PROPOSITION 1.10 - Pour qu'un sous-ensemble de $\mathbb{N}$ appartienne à $(RE)^{(1)}$, il faut et il suffit qu'il soit ou bien vide, ou bien identique à l'ensemble de toutes les valeurs d'un élément de $\mathbb{F}_R^{(1)}$.

C'est de là que vient l'expression "récursivement énumérable".

PROPOSITION 1.11 - $(RE)^{(p)}$ est énumérable par un élément de $(RE)^{(p+1)}$; autrement dit

$$[\exists A \in (RE)^{(p+1)}][\forall U \in (RE)^{(p)}](\exists u \in \mathbb{N})(\forall x_1,\ldots,x_p \in \mathbb{N})[U(x_1,\ldots,x_p) \Longleftrightarrow A(u,x_1,\ldots,x_p)]$$

Tous ces théorèmes directs (à l'exeption de la Prop. 1.11 prise sous cette forme) restent vrais lorsqu'on remplace $\mathbb{F}_R$ par n'importe quel sous-ensemble de $\mathbb{F}$ satisfaisant aux conditions de clôture (a) et (b) de 1.7.

1.11 – De la Prop. 1.4 on déduit immédiatement (par le "procédé diagonal"):

[PROPOSITION 1.12 – Pour $p \geq 1$, $(R)^{(p)}$ n'est pas énumérable par un élément de $(R)^{(p+1)}$. De même pour $\mathbb{F}_R^{(p)}$.]

Des Propositions 1.11 et 1.12 on tire alors le résultat "négatif" fondamental suivant:

[THÉORÈME 1.I – Pour chaque $p \geq 1$, il existe un sous-ensemble de $\mathbb{N}^p$ qui est récursivement énumérable mais non récursif.]

[COROLLAIRE – Pour $p \geq 1$, $(RE)^{(p)}$ n'est pas clos pour $C^{(p)}$.]

Nous aurons besoin du résultat (un peu plus fort que le Th. 1.I mais obtenu par la même méthode) suivant:

Un couple (X, X') de sous-ensembles de $\mathbb{N}$ est dit <u>séparable</u> s'il existe un sous-ensemble récursif Y de $\mathbb{N}$ tel qu'on ait $X \subset Y$ et $X' \subset \complement Y$.

[THÉORÈME 1.II – Il existe un couple non-séparable de sous-ensembles récursivement énumérables disjoints de $\mathbb{N}$.]

La démonstration des Théorèmes 1.I et 1.II permet d'exhiber explicitement les schémas de définition des ensembles récursivement énumérables dont ces théorèmes affirment l'existence.

1.12 – Il existe de nombreuses définitions équivalentes à celles données en 1.7 et 1.8.

On définit par exemple (par une méthode très simple dans son principe, mais sans utilité ici) l'ensemble (T) des éléments de $\mathbb{F}$ qui sont "calculables par une machine de Turing".

THÉORÈME 1.III (TURING - POST) - $(T) = \mathbb{F}_R$.

De même, désignons par (G) le plus petit sous-ensemble de $\mathfrak{R}(\mathbb{N})$ qui

(1) contient $\{1\}$, le graphe de l'addition, et celui de la multiplication;

(2) est clos pour les $\cup^{(p)}$, $\cap^{(p)}$, $\exists^{(p)}$, $\forall_{<}^{(p)}$ (cf. 1.10) et pour les changements de place sur les arguments.

THÉORÈME 1.IV - (G) = (RE) .

Les inclusions $(T) \subset \mathbb{F}_R$ et $(G) \subset (RE)$ constituent des résultats "affirmatifs" de la forme indiquée en 1.10; leur démonstration n'est que l'aboutissement d'une succession (plus ou moins longue, mais triviale) de résultats analogues [pour (G) , cf. Prop. 1.4, 1.5, 1.8]. Ce sont les inclusions en sens inverse qui nécessitent des astuces.

Pour démontrer que $(RE) \subset (G)$, on considère l'ensemble $\mathbb{F}_G$ des éléments de $\mathbb{F}$ dont le graphe appartient à (G) , et on montre que $\mathbb{F}_G$ satisfait aux conditions de clôture (a) et (b) de 1.7 (la seule difficulté provient des opérations de récurrence, et se résout par une méthode due à GÖDEL) .

§ 2 - LA THÈSE DE CHURCH.

2.1 - Bien qu'elle soit d'ordre extra-mathématique (on peut la qualifier de "métamathématique" ou de "périmathématique"), la notion de fonction [élément de $\mathbb{F}$] effectivement calculable (ou "mécaniquement calculable") est en pratique parfaitement claire. Exemples de telles fonctions:

- $(x , y , z) \to (x + y^2)^z$;
- $x \to x^{\text{ième}}$ décimale du nombre π ;
- $(x , y) \to$ partie entière de $|$ partie réelle de e^{x+iy} $|$.

Il en est de même pour la notion d'ensemble [élément de $\mathfrak{R}(\mathbb{N})$] effectivement décidable. Exemples de tels ensembles:

- l'ensemble des nombres premiers;
- $\{ (x_1,\ldots,x_p) \mid \exists y, \in \mathbb{Q} , \varphi(x_1,\ldots,x_p , y) = 0 \}$, où φ est un polynôme de $(p + 1)$ arguments à coefficients dans $\mathbb{Z}$.

Toute aussi claire en pratique est la notion d'ensemble effectivement semi-décidable (dans le sens positif), en appelant ainsi tout sous-ensemble X de $\mathbb{N}^p$ tel qu'on dispose d'un procédé effectif (mécanique) uniforme [en $(x_1,\ldots,x_p)$] pour reconnaitre l'appartenance [d'un $(x_1,\ldots,x_p)$ quelconque] à X lorsque cette appartenance est réalisée, sans pour autant disposer nécessairement d'un procédé effectif uniforme permettant de reconnaitre la non-appartenance éventuelle. Exemple-type de tels ensembles:

- les ensembles diophantiens, c'est-à-dire de la forme
- $\{ (x_1,\ldots,x_p) \mid (\exists y_1,\ldots,y_q \in \mathbb{Z}) [\varphi (x_1,\ldots,x_p , y_1,\ldots,y_q) = 0] \}$

où φ est un polynôme de $(p + q)$ arguments à coefficients dans $\mathbb{Z}$.

2.2 - De la définition de $\mathbb{F}_R$, (R) et (RE) il résulte manifestement que:

Toute fonction récursive est effectivement calculable; tout ensemble récursif est effectivement décidable; tout ensemble récursivement énumérable est effectivement semi-décidable.

La <u>réciproque</u> de ces affirmations (ou de l'une quelconque d'entre elles, ce qui entraine le reste) constitue la "thèse de Church".

Bien qu'elle ne soit pas du tout évidente à première vue, cette thèse semble néanmoins pratiquement certaine. Sa justification est constituée par le fait expérimental suivant: pour chaque sous-ensemble mathématiquement défini M de $\mathbb{F}$ (jusqu'à présent rencontré ou inventé, et éventuellement réduit à un seul élément) dont les éléments sont effectivement calculables au sens intuitif, non seulement on a pu démontrer $M \subset \mathbb{F}_R$, mais de plus la démonstration de cette inclusion s'est toujours révélée <u>triviale</u>. Dans chaque cas, en effet, cette démonstration consiste à dérouler, sans aucune astuce, une chaîne plus ou moins longue (que nous baptiserons "filière de Church") de propositions "affirmatives" du type indiqué en 1.10 (cf. aussi ce qui a été dit à propos des Th. 1.III et 1.IV) .

§ 3 - NUMÉROTAGES.

3.1 - La plupart des questions d' "effectivité" qui se posent naturellement en mathématiques concernent des éléments de $\mathfrak{F}(E)$ ou de $\mathfrak{R}(E)$ (ou, plus généralement, de F^E), lorsque E (ou F, ou chacun d'eux) est un ensemble dénombrable déterminé, non nécessairement identique à $\mathbb{N}$. On peut se ramener à $\mathbb{N}$ (et, ce faisant, ramener l'effectivité en question à la récursivité) au moyen d'une correspondance bijective entre E et $\mathbb{N}$.

Pour que les résultats de récursivité ou de non-récursivité obtenus grâce à une telle correspondance soient intéressants, il faut évidemment que la bijection choisie "tienne compte" de la structure particulière considérée sur E ; mais cette dernière condition est en générale satisfaite par une infinité (dénombrable) de bijections. Le choix d'une bijection particulière risque donc de paraitre arbitraire, et sa définition exacte fastidieuse.

On peut essayer de réduire ce double inconvénient en employant la notion générale de "numérotage".

3.2 - Soit A un ensemble dénombrable [ou fini] quelconque. Nous appellerons <u>numérotation de</u> A toute application biunivoque de $\mathbb{N}$ [ou d'un segment initial de $\mathbb{N}$] sur A.

Nous appellerons <u>numérotage sur</u> A (ou encore "structure récursive sur A") chacune des classes d'équivalence déterminées dans l'ensemble des numérotations de A par <u>l'équivalence récursive</u>, c'est-à-dire par la relation

$$\{(\alpha, \alpha') \mid \alpha^{-1} \alpha' \in \mathbb{F}_R^{(1)} \}$$

[avec la convention, pour le cas où A est fini, que toute fonction, dont le domaine de définition est fini, est récursive] .

L'ensemble des numérotages sur A est réduit à un seul élément lorsque A est fini, et possède la puissance du continu lorsque A est dénombrable.

3.3 - Soient $A_1,\dots,A_p$, B des ensembles finis ou dénombrables, respectivement munis des numérotages $\mathcal{A}_1,\dots,\mathcal{A}_p$, $\mathcal{B}$. Soit X un sous-ensemble de $A_1\times\dots\times A_p$, et soit ξ une application de $A_1\times\dots\times A_p$ dans B. On définit de façon évidente (en considérant des numérotations, puis en passant au quotient) la propriété pour X d'être <u>récursif</u> [et de même la propriété d'être <u>récursivement énumérable</u>] <u>dans</u> $(\mathcal{A}_1,\dots,\mathcal{A}_p)$, ainsi que la propriété pour ξ d'être <u>récursive</u> <u>dans</u> $(\mathcal{A}_1,\dots,\mathcal{A}_p;\mathcal{B})$.

Bien entendu, si $A_1 = \dots = A_p = A$, et $\mathcal{A}_1 = \dots = \mathcal{A}_p = \mathcal{A}$, nous dirons "récursif dans $\mathcal{A}$" [resp. : "récursive dans $(\mathcal{A} ; \mathcal{B})$"] au lieu de "récursif dans $(\mathcal{A},\dots,\mathcal{A})$" [resp. : "récursive dans $(\mathcal{A},\dots,\mathcal{A};\mathcal{B})$"]. De même, sauf avis contraire, $\mathbb{N}$ sera toujours considéré comme muni du numérotage qui correspond à l'application identique, et nous sous-entendrons la référence à ce numérotage, etc.

3.4 - En mettant à part le cas trivial des numérotages finis, la théorie des numérotages est "univalente" : deux numérotages $\mathcal{A}$ et $\mathcal{A}'$ quelconques, établis respectivement sur des ensembles dénombrables A et A', sont toujours isomorphes entre eux (dans la définition des isomorphismes, on considère $\mathcal{A}$ et $\mathcal{A}'$ comme des structures sur A et A', $\mathbb{N}$ jouant dans cette définition le rôle d'un ensemble auxiliaire ponctuellement invariant).

Quant aux "morphismes" (en général) d'un numérotage $\mathcal{A}$ (sur A) dans un numérotage $\mathcal{B}$ (sur B), leur rôle est tenu par les applications de A dans B qui sont récursives dans $(\mathcal{A} ; \mathcal{B})$.

3.5 - Etant donné un numérotage $\mathcal{A}_1$ sur A_1 et un numérotage $\mathcal{A}_2$ sur A_2, il existe un numérotage $\mathcal{A}$ et un seul sur $A_1 \times A_2$ tel que l'application identique de $A_1 \times A_2$ sur lui-même soit récursive dans $(\mathcal{A}_1, \mathcal{A}_2; \mathcal{A})$. Ce numérotage $\mathcal{A}$ sera appelé le <u>produit direct</u> de $\mathcal{A}_1$ et de $\mathcal{A}_2$.

Etant donné un numérotage $\mathcal{A}$ sur A, et un sous-ensemble B de

A , pour qu'il existe un numérotage $\mathcal{B}$ sur B tel que l'application identique de B dans A soit récursive dans $(\mathcal{A} ; \mathcal{B})$, il faut et il suffit que B soit récursivement énumérable dans $\mathcal{A}$; dans ce cas le numérotage $\mathcal{B}$ satisfaisant à la condition ci-dessus est unique : on l'appellera le numérotage <u>induit</u> par $\mathcal{A}$ sur B , ou encore la <u>restriction</u> de $\mathcal{A}$ à B . Si B est non seulement récursivement énumérable, mais de plus récursif dans $\mathcal{A}$, certaines propriétés de "prolongement" sont vérifiées; en particulier, tout sous-ensemble de B, qui est récursif dans $\mathcal{B}$, est alors récursif aussi dans $\mathcal{A}$ (la réciproque est vraie dans le cas général).

On constate que les ensembles E sur lesquels on est amené à se poser des problèmes d'effectivité [concernant par exemple des éléments de $\mathfrak{F}(E)$ ou de $\mathfrak{R}(E)$] sont tous obtenus à partir de $\mathbb{N}$ et (éventuellement) de certains ensembles finis $A_1, \ldots, A_n$ en appliquant (suivant un schéma fini quelconque) les opérations de produit direct et de restriction. On peut donc, sur chacun de ses ensembles E , définir un <u>numérotage canonique</u>. En effet, lorsqu'un même ensemble E peut être obtenu (éventuellement à une bijection triviale près) par des schémas différents, les numérotages correspondants sont identiques (en vertu d'un certain nombre de propositions générales immédiates).

Parmi les opérations qui sont définissables à partir du produit direct et de la restriction, citons : la somme directe finie, ou infinie dans certains cas, le quotient par une relation d'équivalence récursive, l'image homomorphe par une application telle que l'équivalence associée soit récursive, etc.

3.6 - Un numérotage $\mathcal{A}$ sur A d'une part, et une "structure algébrique" $(R_1, \ldots, R_h, \varphi_1, \ldots, \varphi_k)$ sur A d'autre part, avec $R_i \in \mathfrak{R}^{(p_i)}(A)$ et $\varphi_j \in \mathfrak{F}^{(q_j)}(A)$, seront dits <u>compatibles</u> si chaque relation R_i et chaque fonction φ_j est récursive dans $\mathcal{A}$.

Une structure algébrique sur A sera dite <u>récursivisable</u> s'il existe un numérotage sur A compatible avec cette structure.

Dans beaucoup de cas, le numérotage canonique sur un ensemble E (de la famille ci-dessus considérée) peut être défini comme l'unique numérotage compatible avec certains éléments de $\mathfrak{F}(E)$.

On a par exemple:

PROPOSITION 3.1 - Sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, il existe un numérotage et un seul compatible avec l'addition (et ce numérotage se trouve être aussi compatible avec la multiplication).

Par contre, sur chacun de ces trois ensembles, il existe manifestement une infinité de numérotages compatibles avec la multiplication.

PROPOSITION 3.2 - Sur l'anneau des polynômes à coefficients dans $\mathbb{Z}$ (ou dans $\mathbb{Q}$) il existe un numérotage et un seul compatible avec l'addition et la multiplication.

PROPOSITION 3.3 - Sur le corps des nombres algébriques réels, il existe un numérotage et un seul compatible avec l'addition et la multiplication.

Dans ce dernier numérotage, les sous-ensembles $\mathbb{Q}$, $\mathbb{Z}$, l'ensemble des entiers algébriques réels, l'ensemble des nombres de Pisot, etc. sont récursifs.

Dans le même ordre d'idées, citons encore:

PROPOSITION 3.4 - Soit G un groupe dénombrable, A un système de générateurs de G , $\mathcal{A}$ un numérotage sur A . Il existe au plus un numérotage $\mathcal{G}$ sur G qui soit compatible avec l'opération du groupe et tel que l'injection canonique (identique) de A dans G soit récursive dans ($\mathcal{A}$; $\mathcal{G}$) .

COROLLAIRE - Sur un groupe à nombre fini de générateurs, il existe au plus un numérotage compatible avec l'opération du groupe.

§ 4 - RÉCURSIVITÉ SUR DES ENSEMBLES AUTRES QUE $\mathbb{N}$.

4.1 - Les expressions "numérotage canonique" et "numérotage canoniquement associé à un numérotage donné" sont chaque fois définies par la méthode indiquée en 3.5 .

4.2 - Soit $\mathbb{P}$ l'ensemble de tous les polynômes (d'un nombre quelconque d'arguments) à coefficients dans $\mathbb{Z}$; autrement dit:

$$\mathbb{P} = \bigcup_{p \in \mathbb{N}} \mathbb{Z}(\underline{x}_1, \ldots, \underline{x}_p) .$$

Soit $\mathbb{H}$ le sous-ensemble de $\mathbb{P}$ constitué par les polynômes qui admettent au moins un système de solutions (d'annulation) dans $\mathbb{Z}$; autrement dit:

$$\varphi \in \mathbb{H}^{(\mathbb{P})} \Longleftrightarrow (\exists\, x_1, \ldots, x_p \in \mathbb{Z})\ [\ \varphi(x_1, \ldots, x_p) = 0\ ].$$

$\mathbb{P}$ possède un numérotage canonique. Et, dans ce numérotage, on a trivialement (par la filière de Church) :

PROPOSITION 4.1 - $\mathbb{H}$ est récursivement énumérable.

4.3 - Pour chaque ensemble A , désignons par $\mathfrak{L}A$ le groupe libre engendré par A .

A tout numérotage sur A on associe canoniquement un numérotage sur $\mathfrak{L}A$. En particulier, si A est fini, $\mathfrak{L}A$ possède un numérotage canonique unique et bien déterminé.

U étant un sous-ensemble quelconque de A , désignons par $\mathfrak{D}U$ le plus petit sous-groupe distingué de $\mathfrak{L}A$ qui contient U .

Dans le numérotage sur $\mathfrak{L}A$ canoniquement associé à un numérotage quelconque sur A , on a:

PROPOSITION 4.2 - Pour qu'un sous-groupe distingué D de $\mathfrak{L}A$ soit récursivement énumérable, il suffit qu'il existe un sous-ensemble récursivement énumérable U de $\mathfrak{L}A$ tel que $D = \mathfrak{D}U$, et il faut qu'il existe un sous-ensemble récursif U' tel que $D = \mathfrak{D}U'$.

La première partie de cette Proposition est triviale, la seconde s'obtient par une méthode simple utilisant des "redondances" (analogues aux "pléonasmes" employés pour la Prop. 8.6 ci-dessous).

Un groupe G est dit <u>décidable</u> [resp. : <u>récursivement présentable</u>] s'il existe un ensemble A, un numérotage $\mathcal{A}$ sur A, un sous-groupe distingué D de ΩA qui soit récursif [resp. : récursivement énumérable] dans l'énumérage sur ΩA canoniquement associé à $\mathcal{A}$, et un isomorphisme de G sur le groupe quotient $\Omega A / D$.

On démontre aisément:

PROPOSITION 4.3 - Pour qu'un groupe soit décidable, il faut et il suffit qu'il soit récursivisable (cf. 3.6).

PROPOSITION 4.4 - Tout groupe à nombre fini de générateurs qui est plongeable dans (c.à d. isomorphe à un sous-groupe d') un groupe décidable [resp. : récursivement présentable] est lui-même décidable [resp. : récursivement présentable].

Un groupe G est dit <u>finiment présentable</u> s'il existe un ensemble fini A et un sous-ensemble fini U de ΩA tel que G soit isomorphe à $\Omega A / \mathfrak{D} U$.

On obtient immédiatement:

PROPOSITION 4.5 - Tout groupe finiment présentable est récursivement présentable.

4.4 - Choisissons une fois pour toutes une suite d'ensembles $(A_n)_{n \in \mathbb{N}}$ telle que, pour chaque n, A_n ait exactement n éléments.

Nous désignons par Pf l'ensemble de tous les couples (A, U) tels que A appartienne à $\{A_n \mid n \in \mathbb{N}\}$ et que U soit un sous-ensemble fini de ΩA. Les éléments de Pf seront appelés des <u>présentations finies</u>.

Pour chaque élément $P = (A, U)$ de Pf, le groupe quotient (finiment présentable par définition) $\Omega A / \mathfrak{D} U$ sera désigné par $\mathfrak{G} P$.

On définit sur Pf un numérotage canonique. Et dans ce numérotage on a (entre autres) :

PROPOSITION 4.6 - Le sous-ensemble $\{(P, P') \mid \mathfrak{G}P$ isomorphe à $\mathfrak{G}P'\}$ de Pf^2 est récursivement énumérable.

COROLLAIRE - Le sous-ensemble $\{P \mid \mathfrak{G}P$ trivial$\}$ de Pf est récursivement énumérable.

en appelant trivial tout groupe qui est réduit à son élément neutre.

PROPOSITION 4.7 - Il existe un certain élément pl de $\mathfrak{F}^{(2)}(Pf)$ qui est récursif et tel que, pour tout (P, P') dans Pf^2, $\mathfrak{G}[pl(P, P')]$ est isomorphe au produit libre de $\mathfrak{G}P$ et de $\mathfrak{G}P'$.

4.5 - Soit $\mathbb{K}_p$ l'ensemble de tous les complexes simpliciaux finis (abstraits) de dimension p.

Soit Hm_p le sous-ensemble de $\mathbb{K}_p^2$ constitué par tous les couples (C, C') tels que (les réalisations de) C et C' soient homéomorphes.

Une application σ de $\mathbb{K}_p \times \mathbb{N}$ dans $\mathbb{N}$ (ou dans $\mathbb{Z}$) sera dite un système d'invariants d'homéomorphie (en dimension p) si on a, quels que soient C et C' dans $\mathbb{K}_p$:

$$(C, C') \in Hm_p \Rightarrow [\forall n \in \mathbb{N},\ \sigma(C, n) = \sigma(C', n)] .$$

Si l'implication inverse est aussi vérifiée, le système σ sera dit complet.

On définit sur $\mathbb{K}_p$ un numérotage canonique. Et dans ce numérotage on a (de façon immédiate) :

PROPOSITION 4.8 - S'il existe en dimension p un système d'invariants d'homéomorphie qui soit complet et récursif, alors $\complement Hm_p$ est récursivement énumérable.

6 - Considérons un ensemble E muni d'une part d'une certaine structure, et d'autre part d'un numérotage canonique (associé à la structure considérée). Il arrive parfois que la récursivité sur E [c'est-à-dire par exemple l'ensemble des éléments de $\mathfrak{R}(E)$ qui sont récursivement énumérables dans le numérotage canonique] puisse se définir directement, en ne faisant appel qu'à des opérations [portant par exemple sur les éléments de $\mathfrak{R}(E)$] qui ont une signification intrinsèque simple relativement à la structure considérée.

On a entre autres le résultat suivant, qui est intéressant en lui-même et dont nous verrons par ailleurs une application très importante:

Soit $\mathbb{E}$ le sous-ensemble de $\mathbb{Z}^{\mathbb{Z}}$ constitué par toutes les fonctions à support fini (c'est-à-dire prenant la valeur 0 en dehors d'un sous-ensemble fini de $\mathbb{Z}$).

On définit sur $\mathbb{E}$ un numérotage canonique (unique et bien déterminé). Par abus de langage, nous désignerons par $(R\ E)^{(1)}$ l'ensemble des éléments de $\mathfrak{P}(E)$ qui sont récursivement énumérables dans le numérotage canonique.

Pour chaque $i \in \{1, 2, 3, 4\}$, considérons l'élément θ_i de $\mathbb{Z}^{\mathbb{Z}}$ ainsi défini :

$$\theta_1(x) = -x \ .$$

$$\theta_2(x) = x-1 \ .$$

$$\theta_3(0) = 1 \ ; \quad \theta_3(1) = 0 \ ; \quad \theta_3(x) = x \quad \text{pour} \quad x < 0 \text{ et pour } x > 1.$$

$$\theta_4(x) = 2x \ .$$

Pour chaque $j \in \{1,2\}$, soit A_j le sous-ensemble de $\mathbb{Z}$ ainsi défini:

$$A_1 = \{0\} \ .$$

$$A_2 = \mathbb{N} - \{0\} \ .$$

Pour $\xi \in E$, $m \in \mathbb{N} -\{0\}$, $p \in \mathbb{Z}$, considérons l'élément ξ_m^p de $\mathbb{E}$ ainsi défini :

$$\xi_m^p(x) = \xi(pm+x) \quad \text{pour} \quad 0 \leqslant x < m \ ;$$

$$\xi_m^p(x) = 0 \qquad \text{pour} \quad x < 0 \text{ et pour } x \geqslant m \ .$$

Pour $X \subset \mathbb{E}$, $i \in \{1,2,3,4\}$, $j \in \{1,2\}$, $m \in \mathbb{N} - \{0\}$, posons :

$$\Theta_i(X) = \{\xi\theta_i \mid \xi \in X\} \; ;$$
$$\Phi_j(X) = \{\xi \in \mathbb{E} \mid (\exists\eta \in X)\ (\forall x \notin A_j)\ (\xi x = \eta x)\} \; ;$$
$$\Psi_m(X) = \{\xi \in \mathbb{E} \mid (\forall p \in \mathbb{Z})\ (\xi_m^p \in X)\} \; .$$

Soit enfin $0^{(1)}$ l'élément identiquement nul de $\mathbb{E}$, et soit S le sous-ensemble de $\mathbb{E}$ ainsi défini :

$$\xi \in S \iff [(\xi 1 = 1 + \xi 0) \text{ et } (\xi x = 0 \text{ pour } x < 0 \text{ et } x > 1)]$$

Nous désignerons par (Hig) le plus petit sous-ensemble de $\mathfrak{P}(\mathbb{E})$ qui contient $\{0^{(1)}\}$ et S et est clos pour $\cup$, $\cap$, les Θ_i , les Φ_j et les Ψ_m .

THÉORÈME 4.I (HIGMAN) - (Hig) = $(\mathrm{RE})^{(1)}$.

L'inclusion (Hig) $\subset$ $(\mathrm{RE})^{(1)}$ s'obtient trivialement par la filière de Church. Pour l'inclusion inverse, le principe général de la démonstration est analogue à celui employé pour le Th. 1.IV .

§ 5 - PROBLÈMES ET PROCÉDÉS GÉNÉRAUX

5.1 - Appelons (pour abréger) <u>questionnaire</u> tout ensemble (Q), fini ou infini, dont les éléments sont des triplets $(A, \mathcal{A}, X)$ où $\mathcal{A}$ est un numérotage sur A et X un sous-ensemble de A. Il peut arriver que A et $\mathcal{A}$ soient les mêmes pour tous les éléments de (Q), voire que (Q) soit réduit à un seul élément.

Un questionnaire (Q) sera dit <u>décidable</u> si, quel que soit l'élément $(A, \mathcal{A}, X)$ de (Q), X est récursif dans $\mathcal{A}$.

Appelons <u>questionnaire fondamental</u>, et désignons par (Q_0), l'ensemble de tous les triplets $(N, \mathcal{N}, X)$ où $\mathcal{N}$ est le numérotage canonique (identique) sur N, et X un élément quelconque de (RE)[1]. le Th. 1.I donne:

[PROPOSITION 5.1 - (Q_0) n'est pas décidable.]

5.2 - Un "théorème de non-décidabilité" (relatif à un questionnaire donné) est donc un énoncé de la forme générale :

[Dans telle famille d'ensembles, il existe un élément non-récursif]

un cas particulier de cette forme étant;

[Tel ensemble n'est pas récursif.]

En fait, dans tous les exemples que nous examinerons, la forme générale se ramène à la forme particulière, car on peut chaque fois exhiber explicitement (par son "schéma de définition") un élément non-récursif particulier de la famille considérée.

Dans le langage courant, on qualifie souvent d' "indécidable" toute formule (ou "proposition", ou "énoncé formel") F telle que ni F ni sa négation ne soient démontrables dans une théorie formelle donnée (cf. § 8). Il s'agit là, non pas de non-décidabilité (au sens que nous avons défini), mais de non-démonstrabilité. Bien que techniquement reliées (cf. § 8), ces deux notions sont néanmoins essentiellement différentes.

5.3 - Soient A et B deux ensembles dénombrables, munis respectivement des numérotages $\mathcal{A}$ et $\mathcal{B}$. Soient X et X' deux sous-ensembles de A , Y et Y' deux sous-ensembles de B . Le couple (X , X') sera dit <u>biréductible à</u> (Y , Y') <u>dans</u> $(\mathcal{A} ; \mathcal{B})$ s'il existe une application ξ de A dans B qui soit récursive dans $(\mathcal{A} ; \mathcal{B})$ et telle qu'on ait: $\xi(X) \subset Y$ et $\xi(X') \subset Y'$.

Nous dirons que X est <u>réductible à</u> Y <u>dans</u> $(\mathcal{A} ; \mathcal{B})$ si $(X , \complement_A X)$ est biréductible à $(Y, \complement_B Y)$ dans $(\mathcal{A} ; \mathcal{B})$.

On obtient immédiatement les résultats suivants (où nous sous-entendons les mots "dans $\mathcal{A}$ ", "dans $\mathcal{B}$ ", "dans $(\mathcal{A} ; \mathcal{B})$" :

PROPOSITION 5.2 - Si Y est récursif [resp. récursivement énumérable] et si X est réductible à Y , alors X est récursif [resp. récursivement énumérable] .

PROPOSITION 5.3 - Si (Y , Y') est séparable, et si (X , X') est biréductible à (Y , Y') , alors (X , X') est séparable (cf. 1. 11).

Indiquons d'autre part, à titre d'exemple, que la Prop. 4.4 ci-dessus est une conséquence immédiate du résultat suivant:

PROPOSITION 5.4 - Si A est fini et si $\mathfrak{L} A/D$ est plongeable dans $\mathfrak{L} A'/D'$, alors D est réductible à D' dans tout couple $(\mathcal{L} , \mathcal{L}')$ où $\mathcal{L}$ est le numérotage canonique sur $\mathfrak{L} A$ et $\mathcal{L}'$ le numérotage sur $\mathfrak{L} A'$ canoniquement associé à un numérotage quelconque sur A'.

5.4 - (Q) et (R) étant des questionnaires, nous dirons que (Q) est <u>réductible à</u> (R) si, pour tout élément $(A , \mathcal{A} , X)$ de (Q) , il existe un élément $(B , \mathcal{B} , Y)$ de (R) tel que X soit réductible à Y dans $(\mathcal{A} ; \mathcal{B})$.

PROPOSITION 5.5 - La réductibilité est réflexive et transitive.

PROPOSITION 5.6 - Si (Q) est réductible à (R) et si (R) est décidable, alors (Q) est décidable.

Dans les paragraphes précédents et suivants, nous indiquons (explicitement ou implicitement) un certain nombre de méthodes et de résultats concernant la réductibilité entre divers questionnaires particuliers. Un cas particulier de réductibilité (dont nous avons vu des exemples non triviaux) est celui où les deux questionnaires considérés se révèlent identiques.

5.5 - Les théorèmes de non-décidabilité s'obtiennent en chaîne à partir de la Prop. 5.1 en utilisant la Prop. 5.6.

Pour passer de la non-décidabilité du questionnaire (Q_i) à celle du questionnaire (Q_{i+1}), on prouve que (Q_i) est réductible à (Q_{i+1}) en définissant une fonction (ou une famille de fonctions) ξ dont le caractère effectivement calculable est manifeste, et en démontrant des équivalences de la forme

$$(1) \qquad (\forall x)(x \in X \iff \xi x \in Y) \quad ;$$

il suffit ensuite (on se donne d'ailleurs rarement la peine d'expliciter cette dernière étape) de transformer, par la filière de Church, l'effectivité intuitive de ξ en une récursivité démontrée.

Le passage de (Q_0) à (Q_1) est réalisé:

dans le cas du § 6 par le Th. 1.IV ,
dans le cas du § 7 par le Th. 4.I ,
dans le cas du § 8 par le Th. 8.IV .

Les Th. 1.IV, 4.I et 8.IV (ainsi, bien entendu, que le Th. 1.I qui sert de point de départ) nécessitent une certaine connaissance - d'ailleurs assez sommaire - de la théorie des fonctions récursives. Pour les autres réductions [passage de (Q_i) à (Q_{i+1}) pour $i \geq 1$] , on constate que la définition des fonctions ξ utilisées et la démonstration des équivalences (1) s'effectuent par des procédés qui relèvent uniquement des domaines mathématiques (théorie des groupes, etc...) correspondant aux questionnaires considérés; en particulier, les Lemmes 7.A et 7.B, ainsi que la définition de la fonction-test du Lemme 7.C et celle de la fonction markovienne du Lemme 7.D, ne font appel à aucune notion relevant de la récursivité, et de même pour la Prop. 8.1 (base du Lemme 8.A). Et cette indépendance à l'égard de la récursivité est valable a fortiori pour des démonstrations comme celle de la Prop. 7.8 à partir du Th. 7.V.

5.6 - Les recherches concernant la non-décidabilité offrent souvent des "sous-produits" qu'on peut considérer comme aussi intéressants (voire plus) que les résultats de non-décidabilité eux-mêmes.

Ainsi, dans le Th. 7.II, la récursivité intervient pour formuler la solution d'un problème ("dans quels cas un groupe à nombre fini de générateurs est-il plongeable dans un groupe finiment présentable ?") dont l'énoncé ne fait appel à aucune notion récursive. De même pour le Th. 8.II.

Ainsi encore, lorsqu'on applique le Th. 7.IV à des groupes particuliers, la récursivité intervient comme outil pour démontrer un résultat ("tel groupe est plongeable dans un groupe finiment présentable") où ne figure aucune notion récursive. De même lorsqu'on applique le Th. 8.VI à des théories formelles particulières. De même encore pour la Prop. 6.1.

5.7 - On remarquera l'analogie entre:

la Prop. 4.2 et la Prop. 8.6,
la Prop. 4.4 et la Prop. 8.9,
la Prop. 4.5 et la Prop. 8.8,
la Prop. 7.4 et la Prop. 8.10,
le Th. 7.II et le Th. 8.II,
le Th. 7.IV et le Th. 8.III,

et aussi, dans une moindre mesure, entre:

la Prop. 7.3 et le Th. 8.IV,
le Th. 7.III et le Th. 8.V,
le Lemme 7.C et la conjonction des Lemmes 8.A et 8.B,
le Th. 7.V et le Th. 8.VII .

§ 6 - PROBLÈMES ET THÉORÈMES DE NON-DÉCIDABILITÉ EN ARITHMÉTIQUE

6.1 - Le "dixième problème de Hilbert" peut s'énoncer ainsi (cf. 4.2) :

[H est-il récursif ?]

On obtiendrait une réponse -négative- à ce problème si on pouvait démontrer l'hypothèse suivante (cf. 2.1) :

[Tout ensemble récursivement énumérable est diophantien.]

Pour essayer de démontrer cette hypothèse, les méthodes actuellement utilisées reposent (en gros) sur le principe suivant:

Puisque, d'après le Th. 1.IV, on a (RE) = (G) , chaque élément de (RE) est définissable par un certain "schéma" qui exprime comment cet élément est obtenu à partir de $1, +, \times$ en utilisant $\cup$, $\cap$, $\exists$, $\forall_{<}$. On peut donc chercher à construire une suite finie $(G_o), \ldots, (G_n)$ de sous-ensembles de (G), avec $(G_o) = (G)$ et (G_n) = la famille des ensembles diophantiens, chaque (G_i) correspondant à un certain ensemble plus ou moins restreint de schémas, et cela de telle façon que (G_i) soit réductible à (G_{i+1}) pour chaque i.

6.2 - La méthode ci-dessus définie n'a pas jusqu'à présent abouti au résultat désiré. Mais le processus de réduction a été poussé suffisamment loin pour obtenir un certain nombre de théorèmes de non-décidabilité, tels le suivant:

Soit H_1 le sous-ensemble de P constitué par les polynômes dont la valeur décrit $\mathbf{Z}$ tout entier lorsque les arguments décrivent $\mathbf{Z}$; autrement dit:

$$\varphi \in H_1^{(p)} \Longleftrightarrow (\forall y \in Z)(\exists x_1, \ldots, x_p \in Z)[\varphi(x_1, \ldots, x_p) = y].$$

[THÉORÈME 6.I (PUTNAM) - H_1 n'est pas récursif.]

D'autre part. du Th. 1.IV lui-même on déduit sans difficulté certains résultats amusants, comme le suivant:

PROPOSITION 6.1 (DAVIS) - Pour chaque $p \geqslant 1$, il existe un sous-ensemble diophantien de $\mathbb{N}^p$ dont le complémentaire n'est pas diophantien.

Contrairement à ce qui se produit pour les autres théorèmes d'existence cités dans cet exposé, l'état actuel des connaissances ne permet pas d'exhiber explicitement un ensemble diophantien à complémentaire non diophantien.

§ 7 - THÉORÈMES DE NON-DÉCIDABILITÉ EN THÉORIE DES GROUPES ET EN TOPOLOGIE.

7.1 - Considérons le groupe libre à 2 générateurs ΩA, avec $A = \{a,b\}$. Associons à chaque élément n de Z l'élément

$$n^* = a^n b^2 a^{-n} b a^n b^{-2} a^{-n} b^{-1}$$

de ΩA, et à chaque sous-ensemble X de $\mathbf{Z}$ le sous-ensemble $X^* = \{n^* \mid n \in X\}$ de ΩA.

On démontre aisément le Lemme suivant (amélioration triviale d'un résultat analogue dû à HIGMAN) :

LEMME 7.A - Quels que soient $X \subset \mathbf{Z}$ et $n \in \mathbf{Z}$,

$$n^* \in \mathfrak{D}\, X^* \Longleftrightarrow (n \in X \text{ ou } n = 0).$$

COROLLAIRE - X est réductible à $\mathfrak{D}\, X^*$.

(car l'application $n \to n^*$ est manifestement récursive).

De ce Corollaire et du Th. 1.I on déduit immédiatement, à l'aide de la Prop. 5.4 :

THÉORÈME 7.I (BRITTON - HIGMAN) - Il existe un groupe à deux générateurs qui est récursivement présentable mais non décidable.

7.2 - Soit maintenant G un groupe à nombre fini de générateurs, et soit H un sous-groupe de G. Nous dirons (d'après Higman) que H est <u>bénin</u> s'il existe un groupe finiment présentable K, un sous-groupe à nombre fini de générateurs L de K, et un plongement φ de G dans K tel que $\varphi(H) = L \cap \varphi(G)$.

Les sous-groupes bénins possèdent un certain nombre de propriétés intéressantes, et en particulier la suivante:

PROPOSITION 7.1 (HIGMAN) - Si A est fini, et si D est un sous-groupe distingué bénin de ΩA, alors $\Omega A/D$ est plongeable dans un groupe finiment présentable.

On obtient d'autre part trivialement (par la filière de Church) :

PROPOSITION 7.2 - Tout sous-groupe bénin de ΩA (avec A fini) est récursivement énumérable.

Considérons maintenant le groupe libre à 3 générateurs ΩB, avec $B = \{a, b, c\}$. A chaque $n \in \mathbb{Z}$ associons l'élément $b_n = c^{-n} b c^n$ de ΩB, et à chaque élément ξ de $\mathbb{E}$ (cf. 4.6) associons les éléments u_ξ et a_ξ de ΩB ainsi définis:

$$u_\xi = \ldots b_{-1}^{\xi(-1)} b_0^{\xi(0)} b_1^{\xi(1)} \ldots \qquad ; \qquad a_\xi = u_\xi^{-1} a u_\xi \quad .$$

Puis, à chaque sous-ensemble X de $\mathbb{E}$ associons le sous-groupe A_X de ΩB engendré par $\{ a_\xi \mid \xi \in X \}$.

LEMME 7.B (HIGMAN) - Si $X \in (\mathrm{Hig})$, alors A_X est bénin.

La démonstration de ce Lemme s'effectue en prouvant que l'ensemble de tous les sous-ensembles X de $\mathbb{E}$ qui sont tels que A_X soit bénin satisfait aux conditions de clôture utilisées dans la définition de (Hig) (cf. 4.6).

Du Lemme 7.B, du Th. 4.I, de la Prop. 7.2 et du fait que la correspondance $\xi \to a_\xi$ est manifestement récursive, on tire immédiatement:

PROPOSITION 7.3 - Pour que A_X soit bénin, il faut et il suffit que X soit récursivement énumérable.

De ce dernier résultat on déduit, par une manipulation algébrique relativement aisée (comparée à celles qui conduisent au Lemme 7.B) :

PROPOSITION 7.3^{bis} (HIGMAN) - Pour qu'un sous-groupe H de ΩA, avec A fini, soit bénin, il faut et il suffit que H soit récursivement énumérable.

Des Prop. 7.1 et 7.3^{bis} d'une part, et des Prop. 4.4 et 4.5 d'autre part, on tire alors:

THÉORÈME 7.II (HIGMAN) - Pour qu'un groupe à nombre fini de générateurs soit plongeable dans un groupe finiment présentable, il faut et il suffit qu'il soit récursivement présentable.

Enfin, des Th. 7.I et 7.II et de la Prop. 4.4 on déduit immédiatement:

THÉORÈME 7.III (NOVIKOV) - Il existe un groupe finiment présentable non décidable.

La méthode de démonstration (cf. 1.12) permet d'exhiber explicitement l'un des éléments de Pf (cf. 4.4) dont ce Th. 7.III affirme l'existence.

7.3 - Par ailleurs, on a le résultat suivant (forme "effective" d'un théorème de Higman - Neuman - Neuman concernant les groupes dénombrables):

PROPOSITION 7.4 (HIGMAN) - Tout groupe récursivement présentable peut être plongé dans un groupe récursivement présentable à 2 générateurs.

Du Th. 7.II et de la Prop. 7.4, on tire:

THÉORÈME 7.IV (HIGMAN) - Tout groupe récursivement présentable peut être plongé dans un groupe finiment présentable.

L'intérêt de ce Th. 7.IV vient de ce que, pour beaucoup de groupes dénombrables "usuels", le fait d'être récursivement présentable résulte immédiatement (par la filière de Church) de leur définition.

7.4 - Soit Rab l'ensemble de tous les triplets (A, U, x) où (A, U) est un élément quelconque de Pf (cf. 4.4) et x un élément quelconque de $\mathfrak{L} A$.

Une application τ de Rab dans Pf sera appelée une <u>fonction-test</u> si, pour tout (A, U, x) dans Rab, on a

$$x \in \mathfrak{D}\, U \Rightarrow \mathfrak{G}\, \tau(A, U, x) \text{ est trivial;}$$

$$x \notin \mathfrak{D}\, U \Rightarrow \mathfrak{G}(A, U) \text{ est plongeable dans } \mathfrak{G}\, \tau(A, U, x).$$

[LEMME 7.C (RABIN) - Il existe une fonction test récursive.]

Nous dirons qu'un sous-ensemble H de Pf possède la <u>propriété de Rabin</u> s'il existe deux éléments P_0, P_1 de Pf tels qu'on ait, quel que soit P dans Pf :

$\mathfrak{G}\, P_0$ plongeable dans $\mathfrak{G}\, P \Rightarrow P \notin H$;

$\mathfrak{G}\, P_1$ isomorphe à $\mathfrak{G}\, P \Rightarrow P \in H$.

[THÉORÈME 7.V (RABIN) - Tout sous-ensemble de Pf qui possède la propriété de Rabin est non-récursif.]

Ce Th. 7.V est une conséquence quasi-immédiate du Lemme 7.C et du Th. 7.III. Soient en effet H, P_0, P_1 comme ci-dessus; soit τ une fonction-test récursive; et soit pl une fonction satisfaisant aux conditions de la Prop. 4.7. Soit alors P un élément quelconque de Pf ; et soit $\mathrm{pl}(P_0\,,\,P) = (\mathbb{B}\,,\,V)$. On voit aisément que, pour tout $x \in \Omega\, \mathbb{B}$, on a

$$x \in \mathfrak{D}\,[\mathrm{pl}(P_0,P)] \iff \mathrm{pl}[P_1\,,\,\tau(\mathrm{pl}(P_0,P),x)] \in H\,.$$

Et par conséquent, si H était récursif, $\mathfrak{G}\,[\mathrm{pl}(P_0\,,\,P)]$ serait décidable pour chaque élément P de Pf. Mais de la Prop. 4.4 il résulte que, si $\mathfrak{G}\,[\mathrm{pl}(P_0\,,\,P)]$ est décidable, il en est de même pour $\mathfrak{G}\, P$; tous les groupes finiment présentables seraient donc décidables, contrairement au Th. 7.III.

7.5 - Un sous-ensemble H de Pf sera dit <u>héréditaire</u> si on a, quels que soient P et P' dans Pf,

$(P \in H$ et $\mathfrak{G}\, P'$ plongeable dans $\mathfrak{G}\, P) \Rightarrow P' \in H$.

Pour chacune des propriétés suivantes, l'ensemble des éléments P de Pf tels que $\mathfrak{G}\, P$ possède cette propriété est héréditaire:

- être trivial,
- être fini,
- être abélien,

- être métabélien,
- être localement fini,
- être localement infini,
- être périodique,
- être cyclique,
- être un p-groupe,
- être nilpotent,
- être libre (d'après le théorème de Nielsen - Schreier),
- être décidable (d'après la Prop. 5.4).

Du Th. 7.V résulte immédiatement

THÉORÈME 7.VI (RABIN) - Tout sous-ensemble héréditaire de Pf non-vide et différent de Pf est non-récursif.

Du Th. 7.VI appliqué à la propriété d'être trivial, on tire entre autres les deux résultats suivants (le premier de façon immédiate, le second par une réduction algébrique facile) :

PROPOSITION 7.5 (RABIN) - Le sous-ensemble

$$\{(P , P') \mid \circledast P \text{ est isomorphe à } \circledast P'\}$$

de Pf^2 n'est pas récursif.

PROPOSITION 7.6 (RABIN) - Le sous-ensemble $\{ P \mid \circledast P \text{ est simple} \}$ de Pf n'est pas récursif.

Du Th. 7.V on déduit directement, en montrant que les sous-ensembles considérés possèdent la propriété de Rabin (ce qui revient à construire un P_0 adéquat) :

PROPOSITION 7.7 (RABIN) - Le sous ensemble

$$\{ P \mid \circledast P \text{ est un produit libre de groupes finis} \}$$

de Pf n'est pas récursif.

PROPOSITION 7.8 (STALLINGS) - Soit $\mathcal{V}$ une famille non-vide (mais par ailleurs quelconque) de variétés de dimension 3. Le sous-ensemble

$$\{ P \mid (\exists V \in \mathcal{V}) [\circledast P \text{ est isomorphe à } \pi_1(V)]\}$$

de Pf n'est pas récursif.

7.7 - Soit Si_p le sous-ensemble de $\mathbb{K}_p$ constitué par tous les éléments C tels que (la réalisation de) C soit homéomorphe au simplexe de dimension p. Une application φ de Pf dans $\mathbb{K}_p$ sera dite <u>markovienne</u> si on a, pour tout $P \in Pf$:

$$\mathfrak{G}P \text{ trivial} \iff \varphi(P) \in Si_p .$$

LEMME 7.D (MARKOV) - Pour chaque $p \geq 4$, il existe une application markovienne récursive.

De ce Lemme et du Th. 7.VI (appliqué à la propriété d'être trivial) on tire immédiatement:

THÉORÈME 7.VII (MARKOV) - Pour $p \geq 4$, Si_p n'est pas récursif.

COROLLAIRE - Pour $p \geq 4$, Hm_p n'est pas récursif.

Du Lemme 7.D et des Prop. 4.6 (Corollaire) et 4.8, résulte:

THÉORÈME 7.VIII (MARKOV - RABIN) - En dimension ≥ 4, il n'existe aucun système d'invariants d'homéomorphie qui soit à la fois récursif et complet.

En fait, la fonction φ construite par Markov est telle que, lorsque $\mathfrak{G}P$ est trivial, $\varphi(P)$ est homéomorphe <u>par décomposition simpliciale</u> au simplexe de dimension p. Il en résulte, sans faire appel à la "Hauptvermutung", que le Th. 7.VII, son Corollaire et le Th. 7.VIII restent vrais quand on y substitue l'homéomorphie par décomposition simpliciale à l'homéomorphie ordinaire.

§ 8 - THÉORÈMES DE NON-DÉCIDABILITÉ EN LOGIQUE.

8.1 - Appelons base de prédicats tout couple (P, π) où P est un ensemble non-vide quelconque, et π une application quelconque de P dans $\mathbb{N}$. Chaque élément r de P sera appelé un prédicat (formel), et $\pi(r)$ sera appelé le nombre de places de r.

La base (P, π) sera dite finie si P est fini.

A chaque base de prédicats $A = (P, \pi)$ on associe un certain ensemble $\mathbb{L}_A$ (nous n'avons pas besoin ici de sa définition exacte) dont les éléments sont appelés formules sans variable libre du premier ordre en A (ce sont des suites finies particulières formées suivant certaines règles à partir d'un certain ensemble de "symboles" comprenant entre autres les éléments de P ; la plupart des résultats de ce paragraphe s'étendent d'ailleurs aux "formules d'ordre > 1").

Si P est fini ou dénombrable, $\mathbb{L}_A$ est dénombrable.

On définit d'autre part (soit "syntaxiquement", soit "sémantiquement") une certaine application Cs_A de $\mathfrak{P}(\mathbb{L}_A)$ dans lui-même, qui possède (entre autres) les quatre propriétés suivantes:

(1) $X \subset Cs_A X$.

(2) $Y \subset X \Rightarrow Cs_A Y \subset Cs_A X$.

(3) $Cs_A Cs_A X = Cs_A X$.

(4) $(\forall x \in Cs_A X)(\exists Y \subset X)(Y \text{ fini et } x \in Cs_A Y)$.

Les éléments de $Cs_A X$ s'appellent les conséquences de X (dans $\mathbb{L}_A$).

Nous posons $\mathbf{T}_A = Cs_A \emptyset$.

On définit enfin un certain élément $\sim$ de $\mathfrak{F}^{(1)}(\mathbb{L}_A)$ et un certain élément $\supset$ de $\mathfrak{F}^{(2)}(\mathbb{L}_A)$, respectivement appelés négation et implication (formelles). Nous écrirons "$x \supset y$" au lieu de "$\supset(x,y)$".

On a le résultat suivant (généralement baptisé "théorème de la déduction") :

PROPOSITION 8.1 - Pour tout $X \subset \mathbb{L}_A$ et tout $x \in \mathbb{L}_A$, on a :

$$x \in Cs_A X \Longleftrightarrow (\exists n \in \mathbb{N})(\exists y_1, \ldots, y_n \in X)[y_1 \succ (y_2 \succ (\ldots (y_{n-1} \succ (y_n \succ x)) \ldots)) \in \mathbb{T}_A] ,$$

La propriété (4) ci-dessus se déduit immédiatement de cette Prop. 4.1 .

8.2 - Nous appellerons <u>théorie</u> (<u>basée sur</u> A) tout sous-ensemble T de $\mathbb{L}_A$ tel qu'on ait $T = Cs_A T$.

$\mathbb{T}_A$ est une théorie particulière, et toute théorie basée sur A contient $\mathbb{T}_A$.

Pour chaque théorie T , on posera $T^{\sim} = \sim^{-1}(T)$.

Une théorie T sera dite:

<u>à nombre fini de prédicats</u> si elle est basée sur une base A finie;

<u>consistante</u> (ou "non-contradictoire") si $T \cap T^{\sim} = \emptyset$;

<u>saturée</u> (ou "complète") si $T \cup T^{\sim} = \mathbb{L}_A$;

<u>finiment axiomatisable</u> si elle est basée sur une base A finie et s'il existe un sous-ensemble U fini de $\mathbb{L}_A$ tel que $T = Cs_A U$.

8.3 - A et B étant des bases quelconques, on définit certaines applications de $\mathbb{L}_A$ dans $\mathbb{L}_B$ que (pour simplifier) nous appellerons des <u>traductions</u>. On peut dire (en gros) que ces applications s'obtiennent en "traduisant" chaque prédicat à p places de A par une "formule en B à p variables libres", et en "relativisant" de plus toutes les variables par une formule en B à 1 variable libre.

Toute traduction θ de $\mathbb{L}_A$ dans $\mathbb{L}_B$ possède (entre autres) les propriétés suivantes:

(1) $\theta(\sim x) = \sim \theta(x)$.

(2) $\theta(x \succ y) = \theta(x) \succ \theta(y)$.

(3) $\theta(Cs_A X) \subset Cs_B \theta(X)$.

(4) $\theta(\mathbb{T}_A) \subset \mathbb{T}_B$.

Dans (1) et (2), en toute rigueur, l'égalité devrait être remplacée par "l'équivalence formelle dans $\mathbb{L}_B$ "

D'autre part, les propriétés (3) et (4) se déduisent l'une de l'autre si on a (2) .

Un cas particulier de traduction est celui où on a $A = (P , \pi)$ et $B = (P_1 , \pi_1)$ avec $P \subset P_1$ et π_1 prolongeant π , et où θ est l'application identique de $\mathbb{L}_A$ (qui est alors un sous-ensemble de $\mathbb{L}_B$) dans $\mathbb{L}_B$. Dans ce cas, les inclusions qui figurent en (3) et (4) peuvent être remplacées par des égalités.

Soit T une théorie basée sur A , S une théorie basée sur B , et θ une traduction de $\mathbb{L}_A$ dans $\mathbb{L}_B$. Nous dirons que S est une <u>extension</u> de T <u>par</u> θ si on a $\theta(T) \subset S$
[d'où $\theta(T^\sim) \subset S$] .

Si on a de plus $\theta(T) = S \cap \theta(\mathbb{L}_A)$
[d'où $\theta(T^\sim) = S^\sim \cap \theta(\mathbb{L}_A)$] , alors S sera dite une extension <u>conservative</u> (ou "inessentielle") de T par θ .

Si S est une extension (non nécessairement conservative) de T et si S est consistante, alors T est consistante.

Une théorie T basée sur A sera dite <u>plongeable</u> dans une théorie S basée sur B s'il existe une traduction θ de $\mathbb{L}_A$ dans $\mathbb{L}_B$ telle que S soit une extension conservative de T par θ .

8.5 - Dans ce qui suit, nous ne considérerons plus que des bases $A = (P , \pi)$ où P est fini ou dénombrable. Nous appellerons, par abus de langage, numérotage sur A tout numérotage $\mathcal{P}$ sur P tel que π soit récursive dans $\mathcal{P}$

A chaque numérotage sur A on associe canoniquement un certain numérotage sur $\mathbb{L}_A$ (d'où la notion de "numérotage canonique" lorsque A est fini).

Quel que soit le numérotage choisi sur A , on a, dans le numérotage sur $\mathbb{L}_A$ canoniquement associé, les propriétés suivantes:

PROPOSITION 8.2 - $\sim$ et $>$ sont récursives.

PROPOSITION 8.3 - $\mathbb{T}_A$ est récursivement énumérable.

PROPOSITION 8.4 - Si A ne contient que des prédicats à 0 ou 1 place, alors $\mathbb{T}_A$ est récursif.

La Prop. 8.2 est triviale (à partir des définitions exactes).

La Prop. 8.3 est immédiate si la fonction Cs_A est définie syntaxiquement. Si Cs_A est définie sémantiquement, cette Prop. 8.3 se déduit d'un lemme de SKOLEM - GÖDEL - HERBRAND.

La Prop. 8.4 s'obtient aisément à partir de certains lemmes concernant les prédicats à 1 place.

D'autre part, de la définition exacte des traductions on déduirait aisément:

PROPOSITION 8.5 - Si A est fini, toute traduction de $\mathbb{L}_A$ dans $\mathbb{L}_B$ est récursive (dans le numérotage sur $\mathbb{L}_B$ canoniquement associé à n'importe quel numérotage sur B) .

Des Prop. 8.1, 8.2, 8.3 d'une part, et d'autre part d'un procédé (dû à EHRENFEUCHT) utilisant des "pléonasmes", on tire:

PROPOSITION 8.6 - Pour qu'une théorie T basée sur A soit récursivement énumérable (dans le numérotage sur $\mathbb{L}_A$ canoniquement associé à un numérotage donné sur A), il suffit qu'il existe un sous-ensemble récursivement énumérable U de $\mathbb{L}_A$ tel que $T = Cs_A\ U$, et il faut qu'il existe un sous-ensemble récursif U' tel que $T = Cs_A\ U'$.

Une théorie T basée sur A est dite décidable [resp. récursivement axiomatisable] s'il existe un numérotage sur A tel que, dans le numérotage sur $\mathbb{L}_A$ canoniquement associé, l'ensemble T soit récursif [resp. récursivement énumérable] .

De cette définition et de la Prop. 8.2 on déduit que, si T est décidable [resp. récursivement énumérable] , alors l'ensemble $T^{\sim}$ est lui-aussi récursif , [resp. récursivement énumérable] dans le numérotage considéré.

De cette remarque et de la Prop. 1.1 on tire:

PROPOSITION 8.7 - Toute théorie récursivement axiomatisable saturée est décidable.

D'autre part la Prop. 8.6 (première partie) donne:

PROPOSITION 8.8 - Toute théorie finiment axiomatisable est récursivement axiomatisable.

Et la Prop. 8.5 donne:

PROPOSITION 8.9 - Toute théorie à nombre fini de prédicats qui est plongeable dans une théorie décidable [resp. récursivement axiomatisable] est elle-même décidable [resp. récursivement axiomatisable] .

Enfin, des Prop. 8.1 et 8.2 on déduit:

LEMME 8.A - Si la base A est finie, et s'il existe une théorie finiment axiomatisable non décidable basée sur A , alors T_A n'est pas récursif.

8.6 - Une théorie est dite p-<u>unitaire</u> si sa base ne contient qu'un unique prédicat, et si ce prédicat est à p places.

Par diverses méthodes (dont aucune n'est triviale), on peut démontrer:

THÉORÈME 8.I (KALMAR) - Toute théorie à base dénombrable est plongeable dans une théorie p-unitaire , pour chaque $p \geq 2$.

Ce théorème se laisse "effectiviser" en:

PROPOSITION 8.10 - Pour $p \geq 2$, toute théorie récursivement [resp. finiment] axiomatisable est plongeable dans une théorie récursivement [resp. finiment] axiomatisable p-unitaire .

On a d'autre part le résultat suivant (dont la démonstration utilise comme point de départ le Lemme 8.B ci-dessous):

THÉORÈME 8.II (KLEENE) - Pour qu'une théorie à nombre fini de prédicats soit récursivement axiomatisable, il faut et il suffit qu'elle soit plongeable dans une théorie finiment axiomatisable.

Du Th. 8.II et de la Prop. 8.10 on tire:

THÉORÈME 8.III - Toute théorie récursivement axiomatisable est plongeable dans une théorie finiment axiomatisable.

8.7 - Une théorie T basée sur A sera dite <u>représentative</u> s'il existe un numérotage sur A tel que, dans le numérotage sur $\mathbb{L}_A$ canoniquement associé, tout couple de sous-ensembles récursivement énumérables disjoints de $\mathbb{N}$ soit biréductible à $(T , T^{\sim})$ (cf. 5.3).

Une théorie T à nombre fini de prédicats sera dite <u>essentiellement non-décidable</u> si elle est consistante et si toute extension consistante (mais pas nécessairement conservative) de T est non-décidable.

Du Th. 1.II et des Prop. 5.3 et 8.5, on déduit:

PROPOSITION 8.11 - Toute théorie à nombre fini de prédicats qui est représentative et consistante est essentiellement non-décidable.

Soit A_0 une base particulière constituée par deux prédicats à 3 places (qui seront "interprétés" comme représentant respectivement les graphes de l'addition et de la multiplication sur $\mathbb{N}$) . On définit une certaine théorie récursivement axiomatisable T_0 basée sur A_0 (T_0 est parfois appelée "arithmétique de Peano"), et on démontre:

THÉORÈME 8.IV (GÖDEL - ROSSER) - T_0 est représentative.

La démonstration de ce théorème s'obtient en "représentant" chaque couple (X , X') de sous-ensembles récursivement énumérables disjoints de $\mathbb{N}$ par une "formule à 1 variable libre en A_0" x construite de façon à avoir, pour tout $n \in \mathbb{N}$:

$$n \in X \Rightarrow x(\overline{n}) \in T_0 ,$$

$$n \notin X \Rightarrow x(\overline{n}) \in T_0^{\sim},$$

où $\overline{n}$ est une "constante formelle" canoniquement associée à n, et où $x(\overline{n})$ est l'élément de $\mathbb{L}_A$ obtenu en "substituant" $\overline{n}$ à la variable libre de x.

L'outil essentiel pour la construction de x est le Th. 1.IV.

D'autre part, avec des moyens "ensemblistes" très restreints on démontre sans peine la consistance de T_0.

Du Th. 8.IV et de la Prop. 8.11 on déduit alors:

[THÉORÈME 8.V (CHURCH) - Toute extension consistante de T_0 (et en particulier T_0 elle-même) est non-décidable.]

Enfin, du Th. 8.V et de la Prop. 8.7 on tire:

[THÉORÈME 8.VI (GÖDEL - ROSSER) - Toute extension consistante et récursivement axiomatisable de T_0 (et en particulier T_0 elle-même) est non-saturée.]

L'intérêt des Th. 8.V et 8.VI provient de ce que la plupart des théories formelles "usuelles" sont des extensions récursivement axiomatisables (souvent même finiment axiomatisables) de T_0, et sont consistantes (du moins on le suppose).

8.8 - Sur la même base A_0 que T_0 on définit une certaine théorie finiment axiomatisable T_0^*, dont T_0 est une extension (non conservative). Et on démontre (en raffinant quelque peu la méthode employée pour le Th. 8.IV):

[LEMME 8.B (MOSTOWSKI - ROBINSON - TARSKI) - T_0^* est représentative.]

Quant à la consistance de T_0^* elle se démontre immédiatement par des moyens purement arithmétiques.

On peut donc renforcer les Th. 8.V et 8.VI en y remplaçant T_0 par T_0^*.

Mais alors, en utilisant le Lemme 8.A et la Prop. 8.10, on obtient le résultat suivant (qui constitue la réciproque de la Prop. 8.4):

THÉORÈME 8.VII (CHURCH) - Si A contient au moins un prédicat à plus d'1 place, alors T_A est non récursif (dans le numérotage sur $\mathbb{L}_A$ associé à un numérotage quelconque sur A).

8.9 - Pour chaque théorie particulière T satisfaisant aux conditions du Th. 8.VI (et explicitement donnée par un "schéma de définition" de l'ensemble de ses axiomes), on peut explicitement exhiber une formule f qui n'appartient ni à T ni à $T^{\sim}$. Mais cette formule f n'offre en général aucun intérêt "mathématique" intrinsèque.

Tout ce qu'on peut dire de f, c'est qu'elle appartient à un certain sous-ensemble L_0 (qu'il est inutile de définir ici) de $\mathbb{L}_{A_0}$.

Or il existe divers sous-ensembles L_i de $\mathbb{L}_{A_0}$ dont les éléments présentent un certain intérêt intrinsèque. Par exemple les ensembles L_1 et L_2 constitués respectivement par les "formalisations dans T_0" des énoncés ayant respectivement la forme (1) et la forme (2) suivantes:

(1) "tel élément de $\mathbb{P}$ appartient à $\mathbb{H}_1$ (cf. 6.2)",

(2) "pour tel élément (A, U, x) de Rab (cf. 7.3), $x \notin \mathfrak{D}U$".

Un sous-ensemble L de $\mathbb{L}_{A_0}$ sera dit <u>génératif</u> (c'est une notion dérivée du concept général de réductibilité) s'il existe une application γ de L_0 dans L telle que, pour tout $x \in L_0$, les formules $x > \gamma(x)$ et $\gamma(x) > x$ appartiennent à T_0.

De cette définition il résulte que, pour tout sous-ensemble génératif L de $\mathbb{L}_{A_0}$, et toute extension récursivement axiomatisable consistante T de T_0 , il existe un élément g de L (explicitement exhibable si la fonction γ qui correspond à L est récursive et explicitement définie) qui n'appartient ni à T ni à $T^{\sim}$.

Or les Théorèmes 6.1 et 7.IV (ou plus exatement les méthodes employées pour leur démonstration) conduisent au résultat suivant:

PROPOSITION 8.12 - Les sous-ensembles particuliers L_1 et L_2 ci-dessus définis sont génératifs.

D'où la construction, pour chaque théorie formelle usuelle, d'une formule "mathématiquement intéressante" (ou tout au moins "mathématiquement décente") qui n'est ni démontrable ni réfutable dans cette théorie.

8.10 - Considérons les théories S_0 , ... , S_3 suivantes :

$S_0 = T_0$;

S_1 = la théorie des ensembles de Zernelo ;

S_2 = la théorie des ensembles de Zernelo-Fraenkel (ou de Neuman-Bernays, ou de Bourbaki) ;

S_3 = la théorie obtenue en ajoutant à S_2 un "axiome des univers" plus ou moins fort, ou encore un axiome affirmant l'existence d'un cardinal "fortement inaccessible".

Pour $j = 0 , 1 , 2 , 3$, S_{j+1} est une extension de S_j (directement ou moyennant une traduction adéquate). Et on suppose que S_j est non-contradictoire.

Soit s_j la formalisation dans T_0 de l'énoncé affirmant la non-contradiction de S_j . On sait que s_j (ou sa traduction) n'est pas démontrable dans S_j . On démontre par contre aisément que s_j est démontrable dans S_{j+1} . Or $s_j \in L_0$ (cf. 8.9). D'où :

PROPOSITION 8.13 - Pour chaque j , il existe un élément de L_i ($i = 1 , 2$) , qui est démontrable dans S_{j+1} , mais non dans S_j .

BIBLIOGRAPHIE SOMMAIRE

- Sur les § 1 et § 8 :

DAVIS (Martin). - Computability and unsolvability. - New York, McGraw-Hill Book Company, 1958 (McGraw-Hill Series in Information Processing and Computers).

GRZEGORZYK (Andrzej). - Fonctions récursives. - Paris, Gauthier-Villars, 1961 (Collection de Logique mathématique, Série A, 17).

KLEENE (S. C.). - Introduction to metamathematics. - Amsterdam, North-Holland publishing Company ; Groningen, Noordhoff, 1952 (Bibliotheca Mathematica, 1).

SMULLYAN (Raymond M.). - Theory of formal systems. - Princeton, Princeton University Press, 1961 (Annals of Mathematics Studies, 47).

- Sur le § 6 :

PUTNAM (Hilary). - An unsolvable problem in number theory, J. of symb. Logic, t. 25, 1960, p. 220-232.

- Sur le § 7 :

HIGMAN (G.). - Subgroups of finitely presented groups, Proc. Royal Soc. London, Series A, t. 262, 1961, p. 455-475.

MARKOV (A. A.). - The problem of homeomorphy [en russe], Proc. Intern. Congr. of Math. [1958. Edinburgh], p. 300-306. - Cambridge, at the University Press, 1960.

RABIN (Michael O.). - Recursive unsolvability of group theoretic problems, Annals of Math., Series 2, t. 67, 1958, p. 172-194.

STALLINGS (J. R.). - On the recursiveness of sets of presentations of 3-manifold groups, Fund. Math., t. 51, 1962, p. 191-194.

- Sur le § 8 :

TARSKI (A.), MOSTOWSKI (A.) and ROBINSON (R. M.). - Undecidable theories. - Amsterdam, North-Holland publishing Company, 1953 (Studies in Logic and the Foundations of Mathematics).

- Généralités, renseignements complémentaires, bibliographie moins sommaire :

LACOMBE (Daniel). - La théorie des fonctions récursives et ses applications (Exposé d'information générale), Bull. Soc. math. France, t. 88, 1960, p. 393-468.