SÉMINAIRE N. BOURBAKI

GABRIEL SABBAGH

Caractérisation algébrique des groupes de type fini ayant un problème de mots résoluble (théorème de Boone-Higman, travaux de B. H. Neumann et MacIntyre)

Séminaire N. Bourbaki, 1976, exp. n° 457, p. 61-80

<http://www.numdam.org/item?id=SB_1974-1975__17__61_0>

Séminaire BOURBAKI 457-01
27e année, 1974/75, n° 457 Novembre 1974

CARACTÉRISATION ALGÉBRIQUE DES GROUPES DE TYPE FINI AYANT UN PROBLÈME DE MOTS RÉSOLUBLE

[THÉORÈME DE BOONE-HIGMAN, TRAVAUX DE B. H. NEUMANN ET MACINTYRE]

par Gabriel SABBAGH

0. Introduction

On sait qu'il existe des groupes de présentation finie ayant un problème de mots non résoluble effectivement. Cela entraîne que nombre de problèmes "globaux" ne sont pas résolubles effectivement pour la classe des groupes de présentation finie ([24], [4]). En particulier, il n'y a pas d'algorithme permettant de décider si un groupe de présentation finie a un problème de mots résoluble (effectivement). Vers 1970, B. H. Neumann [22] et A. Macintyre [18] établirent le résultat suivant qui constitue une caractérisation algébrique, la première connue, des groupes de type fini ayant un problème de mots résoluble :

(I) Un groupe G de type fini a un problème de mots résoluble si et seulement si pour tout groupe S algébriquement clos il existe un homomorphisme injectif de G dans S.

Le caractère peu explicite de la notion de groupe algébriquement clos et le halo de logique qui l'entoure expliquent tout autant qu'un lapsus de [22] le peu de retentissement de ce résultat. En 1973, indépendamment de (I), Boone et Higman trouvèrent une autre caractérisation algébrique, sans doute plus spectaculaire, des groupes de type fini ayant un problème de mots résoluble :

(II) Un groupe G de type fini a un problème de mots résoluble si et seulement si il existe un homomorphisme injectif de G dans un sous-groupe simple d'un groupe de présentation finie.

Le but du présent exposé est de donner de (I) et (II) une démonstration que l'on puisse qualifier de self-contained. On se dispensera cependant des rappels de récursivité, ce qui suppose que la notion de procédé effectif n'est pas totale-

ment étrangère au lecteur (qui pourra se reporter aux premières pages de [1] et [15], pour ne citer que des sources orthodoxes).

1. Généralités

Après avoir défini les notions en présence, on établit dans ce paragraphe deux propositions très faciles. La première, conséquence triviale du résultat final et qui pourrait être omise sans créer de cercle vicieux, est là parce qu'elle semble avoir fourni l'étincelle initiale aux auteurs de (II) ; la seconde établit un lien direct entre (I) et (II).

On appelle présentation un couple de la forme (X, R) où X est un ensemble et R un sous-ensemble du groupe libre construit sur X, $F(X)$. Si X est dénombrable, ce que l'on suppose dorénavant, on peut énumérer effectivement et une fois pour toutes les éléments de X et de $F(X)$, ce qui permet de définir les sous-ensembles récursivement énumérables et les sous-ensembles récursifs de $F(X)$.

Soit $P = (X, R)$ une présentation ; on désigne par $N(P)$ le sous-groupe distingué de $F(X)$ engendré par R. On dit que P est une présentation finie si X et R sont finis, que P est une présentation récursive si $N(P)$ est récursivement énumérable et que P a un problème de mots résoluble si $N(P)$ est récursif. On définit de façon évidente les notions de groupe de présentation finie, de groupe récursivement présenté et de groupe ayant un problème de mots résoluble et on observe que, quand on se restreint à la classe des groupes de type fini, ces notions ont un caractère intrinsèque : autrement dit, soient G un groupe de type fini et $P_1 = (X_1, R_1)$, $P_2 = (X_2, R_2)$ des présentations de G où X_1 et X_2 sont finis ; si P_1 est une présentation finie (resp. est une présentation récursive, resp. a un problème de mots résoluble), il en est de même de P_2 (cf. [7], I.145, ex. 16 et [25]).

On dit qu'un groupe G est algébriquement clos ([29], [17]) si pour tout homomorphisme injectif f de G dans un groupe H et pour toute formule σ de la forme $(\exists\, x_1)\ldots(\exists\, x_m)\varphi(x_1,\ldots,x_m, g_1,\ldots,g_n)$ où φ est une formule sans quantificateurs de la théorie des groupes et où $g_1,\ldots,g_n$ sont des éléments de G, σ est satisfaisable dans G dès que la formule

$$\sigma^f = (\exists\, x_1)\ldots(\exists\, x_m)\varphi(x_1,\ldots,x_m, f(g_1),\ldots,f(g_n))$$

est satisfaisable dans H.

Avec force abus de langage, on dira que G est algébriquement clos si tout énoncé existentiel avec paramètres dans G vrai dans un "surgroupe" de G est vrai dans G. En utilisant uniquement le fait que tout groupe est isomorphe à un sous-groupe d'un groupe simple ([30], p. 316), il aisé de voir que pour définir les groupes algébriquement clos on peut se borner à considérer des systèmes finis d'équations avec paramètres (au lieu d'énoncés existentiels arbitraires), quitte à ajouter la condition : G non trivial, et que tout groupe algébriquement clos est simple (la démonstration "combinatoire" de ces résultats donnée dans [21] n'est pas inutilement compliquée puisqu'elle établit, sans l'énoncer - pour cela il faudra attendre [23] et [17] -, un résultat plus fin : pour tous éléments $x \neq e$ et y d'un groupe algébriquement clos, y est produit de deux conjugués de x).

On voit facilement que tout groupe se plonge dans un groupe algébriquement clos [29] (fabriquer par induction transfinie un surgroupe "presque" algébriquement clos, itérer ω fois et passer à la limite inductive). On trouve des variantes dans [26] et ([27], pp. 144-146).

PROPOSITION 1.- Tout groupe simple de type fini récursivement présenté a un problème de mots résoluble ([19], pp. 209-210 et [14] que je n'ai pu consulter).

En effet, soient F un groupe libre de type fini, X un système générateur fini de F, N un sous-groupe distingué maximal de F. Il s'agit d'établir que si N est récursivement énumérable, alors N est récursif. Puisqu'un élément x de F appartient au complémentaire de N si et seulement si tout élément de X appartient au sous-groupe distingué de F engendré par $N \cup \{x\}$, le complémentaire de N est récursivement énumérable dès que N est récursivement énumérable, ce qui donne le résultat cherché.

Remarque.- Jusqu'à une époque récente, on ne connaissait pas de groupe infini simple de type fini récursivement présenté. Depuis lors, R. Thompson et G. Higman ont établi l'existence de groupes infinis simples de présentation finie (cf. [20]). Le conférencier ignore si les groupes infinis simples de type fini d'exposant premier $p \geq 4381$ de Novikov-Adjan-Kostrikin ([27], pp. 143-144) ont un problème de mots résoluble.

PROPOSITION 2.- Soit H un sous-groupe simple d'un groupe K de présentation finie. Pour tout groupe S algébriquement clos il existe un homomorphisme injectif de H dans S.

En effet, soient $P = (X, R)$ une présentation finie de K et $\pi : F(X) \to K$ l'homomorphisme surjectif, de noyau $N(P)$, induit par la donnée de P. On pose $X = \{x_1,\ldots,x_n\}$. Désignons par $m_1(x_1,\ldots,x_n)$, ..., $m_p(x_1,\ldots,x_n)$ les éléments de R. Désignons par $m = m(x_1,\ldots,x_n)$ un élément de $F(X)$ vérifiant $\pi(m) \in H$ et $\pi(m) \neq e$. L'énoncé

$$(\exists\, x_1)\ldots(\exists\, x_n)\ \ (m(x_1,\ldots,x_n) \neq e \wedge \bigwedge_{1\leq i\leq p} m_i(x_1,\ldots,x_n) = e)$$

est satisfait dans $S \wr K$ par les éléments $\pi(x_1),\ldots,\pi(x_n)$. Il existe donc des éléments $s_1,\ldots,s_n$ de S qui vérifient cet énoncé. Il existe alors un homomorphisme φ et un seul de K dans S vérifiant $\varphi(\pi(x_i)) = s_i$ $(1 \leq i \leq n)$. On a évidemment $\varphi(\pi(m)) \neq e$, ce qui garantit que la restriction de φ à H est injective.

Compte tenu de la proposition 2, il suffit pour établir (I) et (II) de montrer que la condition de (I) est suffisante et que la condition de (II) est nécessaire (pour qu'un groupe de type fini ait un problème de mots résoluble). C'est ce à quoi nous allons nous attacher. La démonstration du premier résultat repose sur la méthode du forcing en théorie des modèles, celle du second résultat sur le grand théorème de Higman. Le lecteur qui s'intéresse uniquement à (I) ne verra pas pour autant son labeur sensiblement allégé ; celui qui s'intéresse uniquement à (II) modifiera la proposition 1 et sa démonstration pour montrer directement que la condition de (II) est suffisante.

2. Forcing à la Robinson et théorème de Macintyre

Pour la commodité du lecteur, nous exposons ci-dessous une version rudimentaire, mais suffisante pour nos besoins, du forcing d'Abraham Robinson ([2], [13]).

Soit L le langage du premier ordre construit sur une infinité dénombrable de variables $v_0, v_1, \ldots$ à l'aide des connecteurs $\vee$ (ou) et $\neg$ (non), du quantificateur existentiel $\exists$, du symbole d'égalité $=$, et d'un nombre dénombrable de symboles de relation, de fonction et de constante fixés une fois pour

toutes. On introduit la conjonction $\wedge$ et le quantificateur universel $\forall$ comme des abréviations (ici ce n'est pas une clause de style) : pour toutes formules φ et ψ ,

$$\varphi \wedge \psi \quad \text{abrège} \quad \neg(\neg\varphi \vee \neg\psi) \ ;$$
$$\forall x\, \varphi \quad \text{abrège} \quad \neg(\exists x \neg\varphi) \ .$$

Soit C un ensemble infini dénombrable fixé une fois pour toutes de symboles de constante dont aucun n'est dans L . Nous désignerons par $\tilde{L}$ le langage du premier ordre obtenu en adjoignant à L les symboles de constante de C . Les réalisations de $\tilde{L}$ sont les structures $(M, a_c)_{c \in C}$ où M est une réalisation de L et où chaque symbole de constante $c \in C$ est interprété dans M par l'élément a_c de M . On dit que la réalisation $(M, a_c)_{c \in C}$ est canonique si l'on a : $M = \{a_c \mid c \in C\}$.

Le langage (infinitaire) $L_{\omega_1\omega}$ est obtenu à partir de L en adjoignant à L un nouveau connecteur $\bigvee$ (disjonction dénombrable) et en élargissant à l'avenant les procédés usuels de formation des formules (seule "nouveauté" : pour tout ensemble dénombrable Φ de formules de $L_{\omega_1\omega}$, $\bigvee_{\varphi \in \Phi} \varphi$ est une formule de $L_{\omega_1\omega}$). Bien entendu, cela ne restreint pas la possibilité de raisonner par récurrence sur la complexité des formules. En particulier, pour toute formule φ de $L_{\omega_1\omega}$, on définit par récurrence l'ensemble $S(\varphi)$ des sous-formules de φ :

Si φ est atomique, on pose $S(\varphi) = \{\varphi\}$;
pour toutes formules φ_1 , φ_2 et tout ensemble dénombrable Φ de formules, on pose :

$$S(\varphi_1 \vee \varphi_2) = S(\varphi_1) \cup S(\varphi_2) \ ;$$
$$S(\neg\varphi_1) = S(\varphi_1) \cup \{\neg\varphi_1\} \ ;$$
$$S(\exists x\, \varphi_1) = S(\varphi_1) \cup \{\exists x\, \varphi_1\} \ ;$$
$$S(\bigvee_{\varphi \in \Phi} \varphi) = \bigcup_{\varphi \in \Phi} S(\varphi) \cup \{\bigvee_{\varphi \in \Phi} \varphi\} \ .$$

Il est clair que $S(\varphi)$ est un ensemble dénombrable.

On rappelle qu'un énoncé est une formule sans variable libre. Toute sous-formule d'un énoncé n'a qu'un nombre fini de variables libres.

On appelle fragment de $L_{\omega_1\omega}$ tout ensemble A de formules de $L_{\omega_1\omega}$ qui vérifie :

(1) toute formule atomique appartient à A ;

(2) A est stable pour $\vee$, $\neg$ et $\exists$;

(3) si $\varphi(x)$ appartient à A et si t est un terme, alors $\varphi(t)$ appartient à A ;

(4) toute sous-formule d'un élément de A appartient à A.

Il résulte de cette définition que tout fragment de $L_{\omega_1\omega}$ contient l'ensemble des formules de L (qui constitue le plus petit fragment de $L_{\omega_1\omega}$) et que tout ensemble Φ de formules de $L_{\omega_1\omega}$ est contenu dans un plus petit fragment de cardinal égal à $\mathrm{Sup}(\mathrm{card}\,\Phi, \aleph_0)$.

Soit A un fragment dénombrable, fixé une fois pour toutes, de $L_{\omega_1\omega}$. On désigne par $\tilde{A}$ le plus petit fragment de $\tilde{L}_{\omega_1\omega}$ contenant A. Il est clair qu'une formule de $\tilde{L}_{\omega_1\omega}$ appartient à $\tilde{A}$ si et seulement si elle est obtenue à partir d'une formule de A en remplaçant toutes les occurrences libres d'un nombre fini de variables par des symboles de constante $c \in C$ (toutes les occurrences libres d'une même variable étant évidemment remplacées par des occurrences d'un même $c \in C$).

Pour définir la notion de forcing, nous aurons besoin des deux définitions suivantes :

DÉFINITION 1.- On dit qu'une formule est basique si elle est de la forme φ ou $\neg\varphi$ où φ est une formule atomique.

DÉFINITION 2.- Etant donnée une classe $\mathfrak{M}$ de réalisations de L, on appelle $\mathfrak{M}$-condition tout ensemble fini d'énoncés basiques de $\tilde{L}$ qui soit satisfaisable dans un élément M de $\mathfrak{M}$.

Exemple 1.- Soit L le langage du premier ordre n'ayant aucun symbole de relation, ayant deux symboles de fonction, l'un binaire et noté $.$, l'autre unaire et noté Inv , et un symbole de constante noté e. Soit $\mathfrak{M}$ la classe des groupes. Posons $p_1 = \{c_1^2 = e\,,\ \neg(c_1 = e)\,,\ c_2^3 = e\}$, $p_2 = \{c_1 c_3 = c_3 c_2\}$

avec $c_1, c_2, c_3 \in C$. Il est immédiat que p_1 et p_2 sont des conditions et que $p_1 \cup p_2$ n'est pas une condition.

Etant donnée une classe $\mathfrak{M}$ de réalisations de L fixée une fois pour toutes, la notion de forcing se définit par récurrence comme suit :

DÉFINITION 3.- Etant donnés une $\mathfrak{M}$-condition p et un énoncé φ de $\tilde{A}$, on dit que p force φ et on note $p \Vdash \varphi$ si l'une des conditions suivantes est réalisée :

φ est atomique et $\varphi \in p$;

φ est de la forme $\neg\varphi_1$ et aucune condition contenant p ne force φ_1 ;

φ est de la forme $\bigvee_{\psi \in \Phi} \psi$ et p force l'un des éléments de Φ ;

φ est de la forme $\varphi_1 \vee \varphi_2$ et p force φ_1 ou φ_2 ;

φ est de la forme $\exists x \varphi_1$ et il existe un élément $c \in C$ tel que p force $\varphi(c)$.

On dit que p force faiblement φ et on note $p \Vdash^f \varphi$ si l'on a $p \Vdash \neg\neg\varphi$.

Avec les notations précédentes, on a le lemme suivant dont la démonstration ne présente aucune difficulté et est laissée au soin du lecteur.

Lemme 1.- Soient p une condition et φ un énoncé de $\tilde{A}$.

(i) p force faiblement φ si et seulement si pour toute condition q contenant p il y a une condition r contenant q qui force φ .

(ii) Si p force φ et si q est une condition contenant p , alors q force φ .

(iii) Si φ est de la forme $\forall x \psi(x)$, alors p force φ si et seulement si pour tout $c \in C$ et toute condition q contenant p il y a une condition r contenant q telle que r force $\psi(c)$.

(iv) On ne peut avoir à la fois $p \Vdash \varphi$ et $p \Vdash \neg\varphi$.

(v) Si $p \Vdash \varphi$ alors $p \Vdash^f \varphi$.

(vi) $p \Vdash^f \neg\varphi$ si et seulement si $p \Vdash \neg\varphi$.

(vii) Si φ est basique et si p force φ, alors $p \cup \{\varphi\}$ est une condition.

(viii) p force tous les éléments de p.

Ce qui précède porte à croire (à juste titre) que l'équivalence logique des formules ($\varphi_1 \sim \varphi_2$ si φ_1 et φ_2 ont les mêmes modèles) n'est pas compatible avec le forcing ; cela explique l'introduction des réalisations génériques.

DÉFINITION 4.- Un ensemble G de conditions est dit <u>générique</u> si l'on a :

(1) tout sous-ensemble d'un élément de G est un élément de G ;

(2) la réunion de deux éléments quelconques de G est un élément de G ;

(3) pour tout énoncé φ de $\tilde{A}$ il y a un élément $p \in G$ tel que $p \Vdash \varphi$ ou $p \Vdash \neg\varphi$.

DÉFINITION 5.- Etant donnés une réalisation canonique $(M, a_c)_{c \in C}$ de $\tilde{L}$, un ensemble générique G et une condition p, on dit que G <u>engendre</u> $(M, a_c)_{c \in C}$ si tout énoncé de $\tilde{A}$ forcé par un élément de G est vrai dans $(M, a_c)_{c \in C}$ (et réciproquement) ; on dit que $(M, a_c)_{c \in C}$ est <u>générique pour</u> p si $(M, a_c)_{c \in C}$ est engendré par un ensemble générique dont p est élément.

DÉFINITION 6.- Etant donnée une réalisation M de L, on dit que M est <u>générique</u> si l'on peut trouver une interprétation $(a_c)_{c \in C}$ des éléments c de C dans M qui fasse de $(M, a_c)_{c \in C}$ une réalisation canonique (de $\tilde{L}$) générique pour la condition vide.

THÉORÈME FONDAMENTAL.- Pour toute condition p, il y a une réalisation générique pour p.

Le théorème résulte immédiatement des deux lemmes suivants :

<u>Lemme</u> 2.- Toute condition p appartient à un ensemble générique.

En effet, soit $(\varphi_n)_{n \geq 1}$ une énumération de l'ensemble des énoncés de $\tilde{A}$. On définit par récurrence une suite $(p_n)_{n \geq 1}$ de conditions : on pose $p_1 = p$; si p_n force $\neg\varphi_n$, on pose $p_{n+1} = p_n$; sinon on prend pour p_{n+1} une condi-

tion qui contient p_n et qui force φ_n .

L'ensemble $\{q \mid q$ est une condition et il y a un $n < \omega$ tel que $q \subset p_n\}$ fait l'affaire.

Lemme 3.- Tout ensemble générique G engendre une réalisation.

Principe de la démonstration : soit T l'ensemble $\{\varphi$ énoncé de $\tilde{A} \mid$ il y a un $p \in G$ tel que $p \Vdash \varphi\}$. Il est facile de voir que pour tout terme t sans variable de $\tilde{A}$ il y a un élément c de C tel que $(t = c)$ soit un élément de T .

On construit un modèle $(M, a_c)_{c \in C}$ de T par la technique de Henkin, i.e. comme suit : pour tous éléments $c, d \in C$ on pose $c \sim d$ si $(c = d)$ est un élément de T . Il est immédiat que $\sim$ est une relation d'équivalence. On prend pour ensemble sous-jacent à M l'ensemble des classes d'équivalence de $\sim$ et on pose $a_c = \text{classe}(c)$. On interprète dans M les symboles de L de la façon suivante :

pour tout symbole R de relation on a $\bar{R}(a_{c_1}, \ldots a_{c_m})$ si et seulement si $R(c_1, \ldots, c_m)$ est un élément de T ;

pour tout symbole F de fonction on a $\bar{F}(a_{c_1}, \ldots, a_{c_n}) = a_c$ si et seulement si l'énoncé $F(c_1, \ldots, c_n) = c$ est un élément de T ;

pour tout symbole E de constante on a $\bar{E} = a_c$ si et seulement si l'énoncé $E = c$ est un élément de T .

La remarque initiale sur les termes sans variable de $\tilde{A}$ montre que les éléments a_c dont on a besoin pour définir $\bar{F}$ et $\bar{E}$ existent. En utilisant les propriétés élémentaires du forcing, on voit sans peine que les $\bar{R}$, $\bar{F}$, $\bar{E}$ sont bien définis, donc que $(M, a_c)_{c \in C}$ constitue une réalisation canonique de $\tilde{L}$. On montre ensuite en raisonnant par récurrence que pour tout énoncé φ de $\tilde{A}$ on a : φ est vrai dans $(M, a_c)_{c \in C}$ si et seulement si $\varphi \in T$, d'où le résultat.

COROLLAIRE 1.- Soit p une condition.

(i) Pour tout énoncé φ de $\tilde{A}$, $p \Vdash^{f} \varphi$ si et seulement si φ est vrai

dans toutes les réalisations génériques pour p .

(ii) p force faiblement tout énoncé de $\widetilde{A}$ qui est conséquence de $\{$énoncés φ de $\widetilde{A} \mid p \Vdash^{f} \varphi\}$.

<u>Démonstration</u> : il suffit d'établir (i). Soit $(M, a_c)_{c \in C}$ une réalisation générique pour p . Si $p \Vdash^{f} \varphi$ alors $p \Vdash \neg\neg\varphi$; donc les formules $\neg\neg\varphi$ et φ sont vraies dans $(M, a_c)_{c \in C}$. Si p ne force pas faiblement φ , alors il y a une condition p' contenant p qui force $\neg\varphi$. Soit $(M', a'_c)_{c \in C}$ une réalisation générique pour p' ; alors $\neg\varphi$ est vraie dans $(M', a'_c)_{c \in C}$ qui est une réalisation générique pour p .

PROPOSITION 3.- Soit φ un énoncé de A de la forme

$$\forall x_1 \ldots \forall x_m \ \psi(x_1,\ldots,x_m) = \forall x_1 \ldots \forall x_m \bigvee_{n<\omega} \varphi_n(x_1,\ldots,x_m)$$

où les φ_n sont des formules basiques. L'énoncé φ est vrai dans toutes les réalisations génériques si et seulement si pour toute condition p et tout m-uple (c_i) de C^m l'ensemble $p \cup \{\psi(c_i)\}$ est satisfaisable dans un élément de $\mathfrak{M}$.

En effet, considérons les assertions suivantes :

(1) φ est vrai dans toutes les réalisations génériques ;

(2) pour tout m-uple (c_i) de C^m , $\psi(c_i)$ est vrai dans toutes les réalisations génériques ;

(3) pour tout m-uple (c_i) de C^m , la condition vide force faiblement $\psi(c_i)$;

(4) pour tout m-uple (c_i) de C^m et pour toute condition p , il y a une condition q contenant p telle que q force $\psi(c_i)$;

(5) pour tout m-uple (c_i) de C^m et pour toute condition p , il y a une condition q contenant p et un entier n tel que q force $\varphi_n(c_i)$;

(6) pour tout m-uple (c_i) de C^m et pour toute condition p , il y a un entier n tel que $p \cup \{\varphi_n(c_i)\}$ est une condition ;

(7) pour toute condition p et tout m-uple (c_i) de C^m , l'ensemble $p \cup \{\psi(c_i)\}$ est satisfaisable dans un élément de $\mathfrak{M}$.

Les équivalences (1) $\Leftrightarrow$ (2) et (6) $\Leftrightarrow$ (7) sont triviales. L'équiva-

lence (2) $\Leftrightarrow$ (3) résulte du corollaire 1 (i). L'équivalence (3) $\Leftrightarrow$ (4) résulte du lemme 1 (i). L'équivalence (4) $\Leftrightarrow$ (5) résulte de la définition du forcing. L'équivalence (5) $\Leftrightarrow$ (6) résulte du lemme 1 (vii) et (viii). On obtient finalement (1) $\Leftrightarrow$ (7), qui est le résultat cherché.

A partir de maintenant, on prend pour L le langage de la théorie des groupes explicité dans l'exemple 1, pour $\mathfrak{M}$ la classe des groupes. En mettant les axiomes de groupe sous forme universelle et en leur appliquant la proposition 3, on obtient immédiatement le

COROLLAIRE 2.- Toute réalisation $\mathfrak{M}$-générique est un groupe.

On pourra donc employer l'expression "groupe générique".

PROPOSITION 4.- Tout groupe générique est algébriquement clos.

En effet, soit M un groupe générique. Soient G un ensemble générique et $(a_c)_{c \in C}$ une interprétation des éléments de C dans M tels que G engendre $(M, a_c)_{c \in C}$. Pour montrer que M est algébriquement clos, il suffit, modulo une manipulation triviale ("forme prénexe des formules sans quantificateurs"), de montrer que tout énoncé σ de la forme $(\exists x_1)\ldots(\exists x_m)\varphi(x_1,\ldots,x_m, g_1,\ldots,g_n)$ vrai dans un surgroupe de M est vrai dans M, où φ est une conjonction finie de formules basiques et où $g_1,\ldots,g_n$ sont des éléments de M. Désignons par p l'ensemble des formules basiques intervenant dans φ. Désignons par $c_1,\ldots,c_n$ des éléments de C tels que $g_i = a_{c_i}$ $(1 \leq i \leq n)$. Soit q un élément arbitraire de G et soient $d_1,\ldots,d_m$ des éléments de C n'ayant pas d'occurrence dans q et n'appartenant pas à $\{c_1,\ldots,c_n\}$. Comme q est satisfaisable dans M et que σ est vrai dans un surgroupe de M, $p(d_1,\ldots,d_m, c_1,\ldots,c_n) \cup q$ est une condition. Un calcul facile donne

$$p(d_1,\ldots,d_m, c_1,\ldots,c_n) \cup q \Vdash (\exists x_1)\ldots(\exists x_m)\varphi(x_1,\ldots,x_m, c_1,\ldots,c_n) .$$

D'où il résulte que q ne force pas $\neg(\exists x_1)\ldots(\exists x_m)\varphi(x_1,\ldots,x_m, c_1,\ldots,c_n)$. Comme G est générique, l'énoncé $(\exists x_1)\ldots(\exists x_m)\varphi(x_1,\ldots,x_m, c_1,\ldots,c_n)$ est vrai dans $(M, a_c)_{c \in C}$, ce qui signifie que σ est vrai dans M.

THÉORÈME DE MACINTYRE [18].- Soit M un groupe de type fini. Si pour tout groupe S algébriquement clos M est isomorphe à un sous-groupe de S, alors M a un problème de mots résoluble.

En effet, soit $(a_i)_{1 \leq i \leq m}$ une famille génératrice finie d'éléments de M. Supposons que le problème des mots pour M ne soit pas résoluble. Soit $\Phi(x_1,\ldots,x_m)$ l'ensemble des formules basiques $\varphi(x_1,\ldots,x_m)$ telles que l'on ait $\neg\varphi(a_1,\ldots,a_m)$ dans M. On a alors :

(1) Pour tout groupe N, M n'est isomorphe à aucun sous-groupe de N si et seulement si l'énoncé $\sigma = \forall x_1 \ldots \forall x_m \bigvee_{\varphi \in \Phi} \varphi(x_1,\ldots,x_m)$ est vrai dans N.

(2) Pour chaque formule atomique $\varphi(x_1,\ldots,x_m)$, une et une seule des formules φ et $\neg\varphi$ appartient à Φ.

(3) Φ n'est pas un ensemble récursivement énumérable : en effet si Φ était récursivement énumérable, son complémentaire dans l'ensemble des formules basiques de la forme $\gamma(x_1,\ldots,x_m)$ serait également récursivement énumérable d'après (2) et donc Φ serait récursif, ce qui contredit le fait que le problème des mots pour M n'est pas résoluble effectivement.

Prenons alors pour A un fragment (dénombrable) de $L_{\omega_1\omega}$ qui contient la formule σ de (1). Nous allons montrer que σ est vrai dans tous les groupes génériques (pour le fragment A considéré !). Soient $c_1,\ldots,c_m$ des éléments de C et p une condition. On désigne par $\Gamma(x_1,\ldots,x_m)$ l'ensemble des formules basiques $\gamma(x_1,\ldots,x_m)$ telles que $p \cup \{\gamma(c_1,\ldots,c_m\}$ n'est pas une condition. Il résulte du théorème de complétude (le lecteur non logicien pourra consulter par exemple [9], p. 66 et (ou) observer l'analogie avec notre lemme 3 et s'en inspirer) que $\gamma \in \Gamma$ si et seulement si $\neg\gamma(c_1,\ldots,c_m)$ est démontrable à partir de p et des axiomes de groupe. On en déduit

(4) Pour chaque formule atomique $\gamma(x_1,\ldots,x_m)$, au plus une des deux formules γ, $\neg\gamma$ appartient à Γ.

(5) Γ est un ensemble récursivement énumérable.

[Alternativement, on pourrait bien entendu utiliser le théorème de Herbrand.]

On déduit de (3) et (5) que l'on a $\Phi \neq \Gamma$. En utilisant (2) et (4) il est alors clair que Φ n'est pas un sous-ensemble de Γ . Si φ est un élément de $\Phi - \Gamma$, $p \cup \{\varphi(c_1,\ldots,c_m)\}$ est une condition. La proposition 3 entraîne alors que σ est vrai dans tous les groupes génériques, qui sont tous algébriquement clos (Proposition 4). D'après (1), M n'est alors isomorphe à aucun sous-groupe de ces groupes.

C.Q.F.D.

3. Théorème de Boone-Higman [5, théorème I]

On veut établir que tout groupe de type fini G ayant un problème de mots résoluble est isomorphe à un sous-groupe simple d'un groupe de présentation finie. Le principe de la démonstration est le suivant :

On montre que G admet un homomorphisme injectif effectif dans un groupe G^+ qui est "presque" simple, au sens que le sous-groupe distingué engendré dans G^+ par un élément de G différent de e contient G , on itère ω fois cette construction et on passe à la limite inductive à laquelle on applique le théorème de Higman. Cette construction sort de la catégorie des groupes de type fini ayant un problème de mots résoluble (cf. (g), p. 18 de cet exposé), d'où la nécessité, peut-être temporaire, de considérer des présentations ayant un problème de mots résoluble et d'établir le résultat suivant :

Soient (X, R) une présentation ayant un problème de mots résoluble et G le groupe défini par (X, R) . Alors on peut construire une présentation d'un groupe simple H , une présentation finie d'un groupe K ayant un problème de mots résoluble, un homomorphisme injectif de G dans H et un homomorphisme injectif de H dans K .

Nous allons commencer par quelques rappels sur les groupes introduits dans [12].

Soit (X, R) une présentation arbitraire d'un groupe G . On désignera par $M \longmapsto \bar{M}$ l'homomorphisme canonique de $F(X)$ sur G . Soit $(J_v)_{v \in V}$ une famille d'ensembles. Pour tout élément $v \in V$, soient $(A_i)_{i \in J_v}$ et $(B_i)_{i \in J_v}$ des

familles d'éléments de $F(X)$ et soit f_v un isomorphisme du sous-groupe de G engendré par $\{\bar{A}_i \mid i \in J_v\}$ sur le sous-groupe de G engendré par $\{\bar{B}_i \mid i \in J_v\}$ tel que $f_v(\bar{A}_i) = \bar{B}_i$ $(i \in J_v)$. On montre dans [12] qu'il y a un surgroupe de G dans lequel tous les f_v deviennent des automorphismes intérieurs [esquisse de démonstration empruntée à [31], pp. 12-13 : se ramener au cas où V a un seul élément v_o , fabriquer par un argument de "back and forth" une limite inductive $\hat{G}$ de sommes amalgamées dans laquelle f_{v_o} devient un automorphisme, prendre un produit semi-direct de $\hat{G}$ et de Z pour rendre f_{v_o} intérieur. Alors que la première partie de cette démonstration - fabrication de $\hat{G}$ et d'un automorphisme de $\hat{G}$ prolongeant f_{v_o} - est codifiée dans les exposés qui traitent des modèles homogènes universels, personne ne semble avoir approfondi le fait que les automorphismes de certaines espèces de structures - groupes, corps (non nécessairement commutatifs),... - sont définissables dans des "surstructures"] . Il est immédiat que la présentation

$$(X \amalg \{p_v \mid v \in V\}, R \cup \{p_v^{-1} A_i p_v B_i^{-1} \mid (v,i) \in V \times J_v\})$$

définit un groupe $G^\times$ qui est la solution du problème universel qui consiste à transformer les f_v en automorphismes intérieurs. Il est alors clair que l'homomorphisme canonique de G dans $G^\times$ est injectif. On désignera encore par $M \mapsto \bar{M}$ l'homomorphisme canonique du groupe libre $F(X \amalg \{p_v \mid v \in V\})$ sur $G^\times$. Avec ces notations on a le lemme fondamental suivant (voir [8] pp. 20-22 pour la démonstration) :

Lemme de Britton.- Tout élément M de $F(X \amalg \{p_v \mid v \in V\})$ qui vérifie $\bar{M} = e$ et dans lequel l'une des lettres p_v de V intervient contient un sous-mot ayant l'une des deux formes suivantes :

(1) $p_v^{-1} C p_v$ où C appartient au sous-groupe de $F(X)$ engendré par $\{A_i \mid i \in J_v\}$;

(2) $p_v C p_v^{-1}$ où C appartient au sous-groupe de $F(X)$ engendré par $\{B_i \mid i \in J_v\}$.

Il résulte du lemme de Britton qu'il y a une application ρ du groupe $F(X \amalg \{p_v \mid v \in V\})$ dans lui-même ayant les propriétés suivantes :

(i) $\rho(M)$ est obtenu en remplaçant dans la forme normale de M ([7], I.84) tous les sous-mots de la forme (1) $p_v^{-1} C p_v$ (resp. (2) $p_v C p_v^{-1}$) par D, où D est obtenu à partir de C en remplacant chaque A_i par B_i (resp. chaque B_i par A_i) ; à chaque étape on remplace un seul sous-mots, le premier que l'on rencontre en allant de gauche à droite.

(ii) $\overline{\rho(M)} = \bar{M}$

(iii) pour tout élément $\bar{g}$ de G (et en particulier pour e), on a

$$\bar{M} = \bar{g} \Leftrightarrow (\rho(M) \in F(X) \text{ et } \overline{\rho(M)} = \bar{g}) .$$

Nous pouvons maintenant établir le résultat annoncé. Soit $P = (X, R)$ une présentation ayant un problème de mots résoluble d'un groupe G que l'on supposera non trivial. Soient $(M_i)_{1 \leq i}$ une énumération effective de tous les éléments de $F(X)$ et $(N_j)_{1 \leq j}$ une énumération effective de tous les éléments de $F(X)$ qui vérifient $\bar{N}_j \neq e$. Soit P^+ la présentation

$$(X \amalg \{t\} \amalg \{u_i \mid i \geq 1\} \amalg \{v_j \mid j \geq 1\} , R \cup \{u_i^{-1} t u_i (t M_i)^{-1} , v_j^{-1} t v_j (t, N_j)^{-1} \mid i \geq 1 , j \geq 1\})$$

où (t,N_j) désigne le commutateur $t^{-1} N_j^{-1} t N_j$. On désigne par G^+ le groupe défini par P^+ et par I l'homomorphisme canonique de G dans G^+ . Le lemme suivant est central :

Lemme 5.- (a) Pour tout élément $x \neq e$ de G , le sous-groupe distingué engendré par $I(x)$ dans G^+ contient G .

(b) P^+ a un problème de mots résoluble et I est un homomorphisme injectif effectif de G dans G^+ .

Démonstration. (a) est évident. Pour démontrer (b) posons $G(t) = G * \langle t \rangle$ = produit libre de G et du groupe libre sur $\{t\}$. Il est clair que I est composée des applications canoniques $G \to G(t) \to G^+$. Montrons que G^+ est un surgroupe de $G(t)$ du type $G(t)^\times$. Il suffit pour cela de s'assurer que les iso-

morphismes requis f_v existent, ce qui est clair compte tenu du fait que le théorème de la forme normale ([7], I.83) garantit que chacun des éléments suivants de $G(t)$ engendre dans $G(t)$ un sous-groupe infini (monogène) : t , tM_i $(1 \leq i)$, (t,N_j) $(1 \leq j)$. On en déduit que I est injectif et on exploite ensuite le lemme de Britton et les propriétés de ρ . Il est essentiel de remarquer que ρ est une application effective (cf. [3], pp. 58-59, lemme 1, auquel nous ne faisons pas appel et dont il faut sans doute amender l'énoncé en exigeant que les f_v soient des isomorphismes effectifs, ce qui est apparemment implicite dans la notation de [3]) : pour cela, comme les isomorphismes f_v sont certainement effectifs, il y a lieu seulement de montrer que l'on peut déterminer effectivement les sous-mots que l'on remplace (cf. (i)), autrement dit, qu'il y a un algorithme permettant de déterminer pour tout élément M de $G(t)$ si M appartient au sous-groupe $\langle t \rangle$ (de $G(t)$), au sous-groupe $\langle tM_i \rangle$ $(1 \leq i)$, au sous-groupe $\langle\langle (t,N_j) \rangle\rangle_{(1 \leq j)}$. Le théorème de la forme normale réduit aisément chacun de ces problèmes au problème des mots pour P , qui est effectivement résoluble par hypothèse. La propriété (iii) entraîne alors que P^+ a un problème de mots résoluble et que I est effectif.

C.Q.F.D.

On peut alors construire par récurrence une suite (P_n , G_n) de présentations de groupes G_n en posant : $(P_o , G_o) = (P , G)$, $(P_{n+1} , G_{n+1}) = (P_n^+ , G_n^+)$. On obtient avec des morphismes injectifs évidents un système inductif filtrant dont on désigne la limite par $(\varinjlim P_n , \varinjlim G_n = H)$. Il y a une fonction effective de H dans $\mathbb{N}$ qui à tout élément x de H associe un entier n tel que x "provient" de G_n . La partie (a) du lemme 5 entraîne que H est simple et la partie (b) (loc. cit.) entraîne que la présentation $\varinjlim P_n$ de H a un problème de mots résoluble. On termine en appliquant la version suivante du théorème de Higman :

(A) tout groupe H récursivement présenté admet un homomorphisme injectif dans un groupe K de présentation finie ;

(B) si en outre H a un problème de mots résoluble, K a la même propriété.

Pour (B) voir [10]. (A) est établi dans [11] (et [28]) pour les groupes de type fini, ce qui suffit puisque, comme remarqué dans [11], on peut se ramener à

à ce cas en inspectant la démonstration de [12] qui établit que tout groupe dénombrable est isomorphe à un sous-groupe d'un groupe engendré par 2 éléments.

Remarque.- Quitte à améliorer la proposition 2, on peut établir la nécessité de I dès que l'on dispose de G^+ (sans itération, cf. [22]).

4. Compléments

(a) Le lecteur n'aura aucune peine à établir tous les résultats des paragraphes 1 et 2 dans un cadre beaucoup plus général. En particulier, il pourra unifier les propositions 3 et 4 et s'assurer que le théorème de Macintyre est vrai dans les structures algébriques usuelles. L'analogue de II est vrai pour les monoïdes [5] et trivialement faux pour les groupes commutatifs et les anneaux commutatifs.

(b) On trouvera dans [5] une version "uniforme" de (II). On ne peut pas pousser trop loin ce genre de résultats : comme rappelé dans les premières lignes de cet exposé, la classe des présentations finies de groupe ayant un problème de mots résoluble n'est pas récursive [24], ni même récursivement énumérable [6]. On montre également dans [6] qu'il n'y a aucun algorithme partiel qui permette, quand on l'applique à un groupe de présentation finie ayant un problème de mots résoluble, de résoudre le problème de mots pour ce groupe. On en déduit aisément (imiter la preuve classique du fait qu'un groupe de présentation finie résiduellement fini a un problème de mots résoluble) qu'il n'y a aucun groupe de présentation finie ayant un problème de mots résoluble "universel" pour tous les groupes de présentation finie ayant un problème de mots résoluble (une conséquence facile du grand théorème de Higman est qu'il existe un groupe de présentation finie universel pour tous les groupes de présentation finie).

(c) Un résultat à comparer avec le préambule du paragraphe 3 : d'après P. Hall, tout groupe dénombrable est isomorphe à un sous-groupe d'un groupe simple engendré par 9 éléments (pour une application intéressante, voir [17]).

(d) Il est facile de voir (modulo l'existence d'un groupe simple infini de présentation finie !) qu'être simple est une propriété de Markov (au sens de [4] et [24]). Il s'ensuit que la classe des présentations finies de groupes simples n'est pas récursive et plus généralement que le résultat 1 de ([4], p. 16)

s'étend à la propriété d'être simple (cf. [4], p. 17).

(e) Il est facile de voir qu'un groupe algébriquement clos n'admet pas de présentation récursive [17].

(f) La tradition orale (Kreisel ?) et écrite ([15], pp. 23 et [16]) a relevé certaines analogies non triviales entre des résultats spécifiques à la théorie des groupes et des résultats de logique (e.g. entre le grand théorème de Higman et le théorème de Kleene-Craig-Vaught). Le présent exposé suggère d'autres analogies, somme toute peu significatives :

théorie complète	groupe simple
toute théorie récursivement énumérable complète est décidable	proposition 1
toute théorie décidable a une extension complète décidable	tout groupe ayant un problème de mots résoluble est isomorphe à un sous-groupe d'un groupe simple ayant un problème de mots résoluble.

Peut-on "expliquer" ces analogies ? Les techniques de [13] semblent inopérantes.

(g) Les problèmes suivants sont apparemment ouverts :

- La classe des présentations finies de groupes simples est-elle récursivement énumérable ?

- Tout groupe de type fini ayant un problème de mots résoluble est-il isomorphe à un sous-groupe d'un groupe simple de présentation finie ? Par (B), on ne gagne rien à se restreindre aux groupes de présentation finie (une rumeur non confirmée dit que tout groupe de type fini ayant un problème de mots résoluble est isomorphe à un sous-groupe d'un groupe simple récursivement présenté et de type fini).

- Y a-t-il un analogue pour le problème de la conjugaison des résultats de cet exposé ?

- Y a-t-il un groupe infini de présentation finie ayant un nombre fini de classes de conjugaison (Lachlan) ?

- On sait [18] que la classe des groupes algébriquement clos dans lesquels un groupe G récursivement présenté et de type fini admet un homomorphisme injectif détermine le degré de Turing du problème des mots de G. Cette classe dépend-elle seulement de ce degré de Turing ?

BIBLIOGRAPHIE

[1] J.-P. AZRA - Relations diophantiennes et la solution négative du dixième problème d'Hilbert, Séminaire Bourbaki, exposé 383 (Novembre 1970), Lecture Notes in Math. n° 244, Springer-Verlag, 1971.

[2] J. BARWISE et A. ROBINSON - Completing theories by forcing, Ann. Math. Logic, Vol. 2 (1970), 119-142.

[3] W. W. BOONE - Word problems and recursively enumerable degrees of unsolvability. A sequel on finitely presented groups, Annals of Maths., Vol. 84 (1966), 49-84.

[4] W. W. BOONE - Decision problems about algebraic and logical systems as a whole and recursively enumerable degrees of unsolvability, in Contributions to Mathematical Logic (Hannover 1966), 13-36, North-Holland, Amsterdam, 1968.

[5] W. W. BOONE et G. HIGMAN - An algebraic characterization of groups with soluble word problem, Journal Austral. Math. Soc., à paraître.

[6] W. W. BOONE et H. ROGERS Jr. - On a problem of J. H. C. Whitehead and a problem of Alonzo Church, Math. Scand., Vol. 19 (1966), 185-192.

[7] N. BOURBAKI - Algèbre I, chapitres 1 à 3, Hermann, Paris, 1970.

[8] J. L BRITTON - The word problem, Annals of Maths., Vol. 77 (1963), 16-32.

[9] C. C. CHANG et H. J. KEISLER - Model theory, North-Holland, Amsterdam, 1973.

[10] C. R. J. CLAPHAM - An embedding theorem for finitely generated groups, Proc. London Math. Soc., Vol. 17 (1967), 419-430.

[11] G. HIGMAN - Subgroups of finitely presented groups, Proc. of the Royal Society, A, Vol. 262 (1961), 455-475.

[12] G. HIGMAN, B. H. NEUMANN et H. NEUMANN - Embedding theorems for groups, J. London Math. Soc., Vol. 24 (1949), 247-254.

[13] H. J. KEISLER - The omitting types theorem, à paraître dans un recueil édité par Morley (Carus).

[14] A. V. KUZNECOV - dans Akad. Nauk S.S.S.R. (1956), 145-146.

[15] D. LACOMBE - Théorèmes de non-décidabilité, Séminaire Bourbaki, exposé 266 (février 1964), W. A. Benjamin, New York, 1966.

[16] R. C. LYNDON - Metamathematics and Algebra : An example in Proc. Int. Congress Phil. Sci., Stanford, 1960.

[17] A. MACINTYRE - On algebraically closed groups, Annals of Maths., Vol. 96 (1972), 53-97.

[18] A. MACINTYRE - Omitting quantifier-free types in generic structures, Journ. of Symbolic Logic, Vol. 37 (1972), 512-520.

[19] A. MALCEV - The metamathematics of algebraic systems, North-Holland, Amsterdam, 1971.

[20] R. MCKENZIE et R. J. THOMPSON - Unsolvable word problems, in Word problems : decision problems and the Burnside problem in group theory, North-Holland, Amsterdam, 1973, 457-478.

[21] B. H. NEUMANN - A note on algebraically closed groups, J. London Math. Soc., Vol. 27 (1952), 247-249.

[22] B. H. NEUMANN - The isomorphism problem for algebraically closed groups, in Word problems : decision problems and the Burnside problem in group theory, North-Holland, Amsterdam, 1973, 553-562.

[23] B. H. NEUMANN et S. YAMAMURO - Boolean powers of simple groups, Journ. Austral. Math. Soc., Vol. 5 (1965), 315-324.

[24] M. O. RABIN - Recursive unsolvability of group theoretic problems, Annals of Maths., Vol. 67 (1958), 172-194.

[25] M. O. RABIN - Computable algebra, general theory and theory of computable fields, Trans. Amer. Math. Soc., Vol. 95 (1960), 341-360.

[26] M. O. RABIN - Non-standard models and independence of the induction axiom, in Essays on the foundations of Mathematics, Jerusalem, 1961, 287-299.

[27] D. J. S. ROBINSON - Finiteness conditions and generalized soluble groups, Part I, Springer, Berlin, 1972.

[28] J. J. ROTMAN - The theory of groups : an introduction, second edition, Allyn and Bacon, Boston, 1973.

[29] W. R. SCOTT - Algebraically closed groups, Proc. Amer. Math. Soc., Vol. 2 (1951), 118-121.

[30] W. R. SCOTT - Group theory, Prentice-Hall, 1964.

[31] J.-P. SERRE - Groupes discrets, Collège de France, 1968/1969.

[32] H. SIMMONS - The word problem for absolute presentations, J. London Math. Soc., Vol. 6 (1973), 275-280. [explicite le fait que les présentations "absolues" récursives de [22] ont un problème de mots résoluble ; notre exposé a utilisé implicitement la réciproque qui est triviale.]