MÉMOIRES DE LA S. M. F.

WOLFGANG THOMAS

An application of the Ehrenfeucht-Fraisse game in formal language theory

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 11-21

<http://www.numdam.org/item?id=MSMF_1984_2_16__11_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p. 11-21

AN APPLICATION OF THE EHRENFEUCHT-FRAISSÉ GAME IN FORMAL LANGUAGE THEORY

Wolfgang Thomas

Abstract A version of the Ehrenfreucht-Fraissé game is used to obtain a new proof of a hierarchy result in formal language theory: It is shown that the concatenation hierarchy ("dot-depth hierarchy") of star-free languages is strict.

Résumé Une version du jeu de Ehrenfeucht-Fraissé est appliquée pour obtenir une nouvelle preuve d'un théorême dans la théorie des langages formels: On montre que la hiérarchie de concaténation ("dot-depth hierarchy") des langages sans étoile est stricte.

1. Introduction.

The present paper is concerned with a connection between formal language theory and model theory. We study a hierarchy of formal languages (namely, the dot-depth hierarchy of star-free regular languages) using logical notions such as quantifier complexity of first-order sentences. In this context we apply a form of the Ehrenfeucht-Fraissé game which serves to establish the elementary equivalence between structures with respect to sentences of certain prefix types.

The class of star-free regular languages is of a very basic nature: It consists of all languages (= word-sets) over a given alphabet A which can be obtained from the finite languages by finitely many applications of boolean operations and the concatenation product. (For technical reasons we consider only nonempty words over A , i.e.

0037-9484/84 03 11 11/$ 3.10/

languages $L \subset A^+$; in particular, the complement operation is applied w.r.t. A^+.) General references on the star-free regular languages are McNaughton-Papert (1971), Chapter IX of Eilenberg (1976), or Pin (1984b).

A natural classification of the star-free regular languages is obtained by counting the "levels of concatenation" which are necessary to build up such a language: For a fixed alphabet A, let

$$\mathcal{B}_0 = \{L \subset A^+ \mid L \text{ finite or cofinite}\},$$

$$\mathcal{B}_{k+1} = \{L \subset A^+ \mid L \text{ is a boolean combination of languages of the form } L_1 \cdot \ldots \cdot L_n (n \geq 1) \text{ with } L_1, \ldots, L_n \in \mathcal{B}_k\}.$$

The language classes $\mathcal{B}_0, \mathcal{B}_1, \ldots$ form the so-called dot-depth hierarchy (or: Brzozowski hierarchy), introduced by Cohen/Brzozowski (1971). In the framework of semigroup theory, Brzozowski/Knast (1978) showed that the hierarchy is infinite (i.e. that $\mathcal{B}_k \supsetneq \mathcal{B}_{k-1}$ for $k \geq 1$). The aim of the present paper is to give a new proof of this result, based on a logical characterization of the hierarchy that was obtained in Thomas (1982). The present proof does not rely on semigroup-theory; instead, an intuitively appealing model-theoretic technique is applied: the Ehrenfeucht-Fraissé game.

Let us first state the mentioned characterization result, taking $A = \{a,b\}$. One identifies any word $w \in A^+$, say of length n, with a "word model"

$$w = (\{1,\ldots,n\}, <, \min, \max, S, P, Q_a, Q_b)$$

where the domain $\{1,\ldots,n\}$ represents the set of positions of letters in the word w, ordered by $<$, where min and max are the first and the last position, i.e. $\min = 1$ and $\max = n$, S and P are the successor and predecessor function on $\{1,\ldots,n\}$ with the convention that $S(\max) = \max$ and $P(\min) = \min$, and Q_a, Q_b are unary predicates over $\{1,\ldots,n\}$ containing the positions with letter a, b respectively. (Sometimes it is convenient to assume that the position-sets of two words u,v are disjoint; then one takes any two nonoverlapping segments of the integers as the position-sets of u and v.) Let L be the first-order language with equality and nonlogical symbols $<, \min, \max, S, P, Q_a, Q_b$. Then the satisfaction of an L-sentence φ in a word w

(written: $w \models \varphi$) can be defined in a natural way, and we say that $L \subset A^+$ is defined by the L-sentence φ if $L = \{w \in A^+ \mid w \models \varphi\}$.

For example, the language $L = (ab)^+$ is defined by

$$Q_a\min \wedge Q_b\max \wedge \forall y(y < \max \rightarrow (Q_a y \leftrightarrow Q_b S(y))) .$$

As usual, a Σ_k-formula is a formula in prenex normal form with a prefix consisting of k alternating blocks of quantifiers, beginning with a block of existential quantifiers. A $B(\Sigma_k)$-formula is a boolean combination of Σ_k-formulas.

1.1 Theorem. (Thomas (1982)). Let $k > 0$. A language $L \subset A^+$ belongs to $\mathcal{B}_k$ iff L is defined by a $B(\Sigma_k)$-sentence of L.

For the formalization of properties of words the symbols min,max,S,P are convenient. But of course they are definable in the restricted first-order language L_0 with the nonlogical constants $<, Q_a, Q_b$ alone. Indeed, we have:

1.2 Lemma. Let $k > 0$. If $L \subset A^+$ is defined by a $B(\Sigma_k)$-sentence of L, then L is defined by a $B(\Sigma_{k+1})$-sentence of L_0.

Proof. The quantifier-free kernel of a Σ_k-formula φ of L can be expressed both by a Σ_2- and a Π_2-formula of L_0. For example, $Q_a S(\min)$ is expressible in the following two ways:

(+) $\exists y(y = S(\min) \wedge Q_a y)$, $\forall y(y = S(\min) \rightarrow Q_a y)$

where $y = S(\min)$ is rewritten as a Π_1-formula of L_0 using

$$x = \min \leftrightarrow \forall z(x = z \vee x < z), \quad x = \max \leftrightarrow \forall z(z = x \vee z < x)$$
$$S(x) = y \leftrightarrow (x = \max \wedge x = y) \vee (x < y \wedge \forall z \neg (x < z \wedge z < y)).$$

Hence we obtain a Σ_{k+1}-sentence of L_0 which is equivalent (in all word-models) to φ by applying one of the two definitions in (+), depending on the case whether the innermost quantifier-block of φ is existential or universal.

We mention without proof that (for $k > 0$) the $B(\Sigma_k)$-sentences of L_0 define exactly those languages $L \subset A^+$ which occur on the k-th level of another hierarchy of star-free regular languages, introduced by

Straubing (1981). For details concerning the Straubing hierarchy and its relation to the Brzozowski hierarchy cf. Pin (1984a,b). The proof to be given below also shows that the Straubing hierarchy is infinite.

2. The Example Languages

In order to show that $\mathcal{B}_k \supsetneq \mathcal{B}_{k-1}$ for $k \geq 1$, we introduce "example languages" L_k, L_k^+, L_k^- over $A = \{a,b\}$.

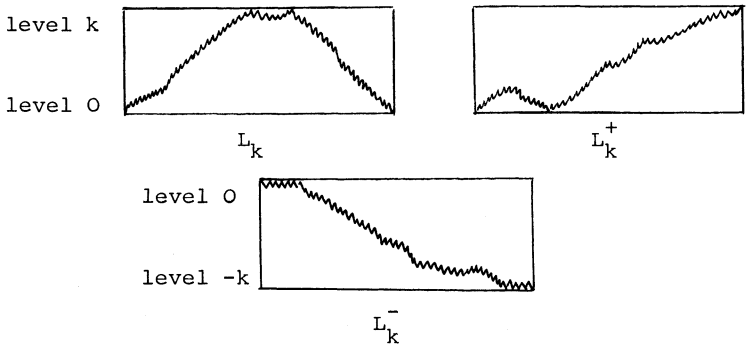
Let $|w|_a$ (resp. $|w|_b$) denote the number of occurrences of the letter a (resp. b) in w, and define the weight $\|w\|$ of a word w by

$$\|w\| = |w|_a - |w|_b \ .$$

In the sequel we write $v \sqsubseteq w$ if the word v is an initial segment (left factor) of w. Let

$$L_k = \{w \in A^+ \mid \|w\| = 0,\ \forall v \sqsubseteq w\ 0 \leq \|v\| \leq k,\ \exists v \sqsubseteq w\ \|v\| = k\} \ ,$$
$$L_k^+ = \{w \in A^+ \mid \|w\| = k,\ \forall v \sqsubseteq w\ 0 \leq \|v\| \leq k\} \ ,$$
$$L_k^- = \{w \in A^+ \mid \|w\| = -k,\ \forall v \sqsubseteq w\ -k \leq \|v\| \leq 0\} \ .$$

To obtain a more intuitive picture of these languages, it is useful to represent the letter a by the stroke ↗ and b by ↘. Then the word abababa, for example, is represented by ∧∧∧. Thus L_k contains all words whose "graph" has the following properties: It ends on the same level where it starts ("level 0"), it is confined to level 0 and the next k levels, and it assumes the k-th level at least once. Similarly for L_k^+, L_k^-. The "typical shape" of words in L_k, L_k^+, L_k^- is indicated in the following diagrams:



L_k L_k^+ L_k^-

We now state the main result:

2.1 Theorem. For all $k \geq 1$: $L_k \in \mathcal{B}_k - \mathcal{B}_{k-1}$.

The proof is split into lemmas 2.2 and 2.3.

2.2 Lemma. For all $k \geq 1$: $L_k \in \mathcal{B}_k$.

Proof. By induction on k we show that $L_k, L_k^+, L_k^- \in \mathcal{B}_k$. Concerning $k = 1$, it is clear that $L_1 = (ab)^+$, $L_1^+ = (ab)^*a$, $L_1^- = b(ab)^*$; hence we can define

$$L_1 \text{ by } (aA^* \cap A^*b) - (A^*aaA^* \cup A^*bbA^*),$$

$$L_1^+ \text{ by } (aA^* \cap A^*a) - (A^*aaA^* \cup A^*bbA^*),$$

$$L_1^- \text{ by } (bA^* \cap A^*b) - (A^*aaA^* \cup A^*bbA^*) .$$

Observing that, e.g., $A^*aaA^* = aa \cup aaA^+ \cup A^+aa \cup A^+aaA^+$, we see that all three languages belong to $\mathcal{B}_1$. - Similarly one obtains, for $k \geq 1$,

$$L_{k+1} = (L_k^+aA^* \cap A^*bL_k^-) - (A^*aL_k^+aA^* \cup A^*bL_k^-bA^*),$$

$$L_{k+1}^+ = (L_k^+aA^* \cap A^*aL_k^+) - (A^*aL_k^+aA^* \cup A^*bL_k^-bA^*),$$

$$L_{k+1}^- = (L_k^-bA^* \cap A^*bL_k^-) - (A^*aL_k^+aA^* \cup A^*bL_k^-bA^*).$$

By induction hypothesis, $L_k, L_k^+, L_k^- \in \mathcal{B}_k$; hence, using the elimination of A^* as above, we have $L_{k+1}, L_{k+1}^+, L_{k+1}^- \in \mathcal{B}_{k+1}$.

2.3 Lemma. For all $k \geq 1$: $L_k \notin \mathcal{B}_{k-1}$.

Proof. For $k = 1$, the result is clear since $(ab)^+$ is neither finite nor cofinite. By 1.1, it suffices to show for $k \geq 2$ that L_k is not defined by a $B(\Sigma_{k-1})$-sentence of L. Using 1.2, it is sufficient to prove:

(*) For every $k \geq 2$: L_k is not defined by a $B(\Sigma_k)$-sentence of L_0.

Let us write

$u \equiv_n^k v$ iff u and v satisfy the same $B(\Sigma_k)$-sentences of L_0 in which only prefixes with $\leq n$ quantifiers occur.

We shall verify, for $k \geq 1$, the claim

$(*)_k$ For every $n \geq k$ there are words $u \in L_k$, $v \notin L_k$ with $u \equiv_n^k v$.

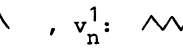
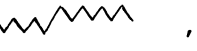
Then in particular for any $k \geqslant 2$ and $n \geqslant k$, a $B(\Sigma_k)$-sentence of L_0 in which only prefixes with $\leqslant n$ quantifiers occur cannot define L_k, and hence (*) is proved.

The words u,v required in $(*)_k$ for given n will be denoted u_n^k, v_n^k. Together with auxiliary words w_n^k they are defined as follows:

$$u_n^1 = (ab)^{2^n}, \quad v_n^1 = u_n^1 a u_n^1, \quad w_n^1 = u_n^1 b u_n^1,$$

$$u_n^{k+1} = \left(v_n^k w_n^k\right)^{2^n}, \quad v_n^{k+1} = u_n^{k+1} a u_n^{k+1}, \quad w_n^{k+1} = u_n^{k+1} b u_n^{k+1}.$$

(To distinguish superscripts from exponents, the latter are applied only to words in brackets.) The graphs of the first words look as follows (where n = 2):

u_n^1:  , v_n^1:  , w_n^1: 

u_n^2: 

From the definition it is immediate that $u_n^k \in L_k$, $v_n^k \notin L_k$. Hence the proof of the main theorem 2.1 is completed when we have shown

(**) $\qquad u_n^k \equiv_n^k v_n^k$

for $1 \leqslant k \leqslant n$. A proof is given in the next section.

3. The Ehrenfeucht-Fraissé Game $G_{\bar{m}}$.

For the proof that two words are $\equiv_n^k$-equivalent (as required in (**) above) it is convenient to consider a slight refinement of this notion.

For a sequence $\bar{m} = (m_1,\ldots,m_k)$ of positive integers, where $k \geqslant 0$, let length $(\bar{m}) = k$ and $\mathrm{sum}(\bar{m}) = m_1+\ldots+m_k$. The set of $\bar{m}$-formulas (of L_0) is defined by induction on length$(\bar{m})$: If length$(\bar{m}) = 0$, it is the set of quantifier-free L_0-formulas; and for $\bar{m} = (m,m_1,\ldots,m_k)$, an $\bar{m}$-formula is a boolean combination of formulas $\exists x_1 \ldots x_m \varphi$ where φ is an $(m_1,\ldots,m_k)$-formula. We write $u \equiv_{\bar{m}} v$ if u and v satisfy the same $\bar{m}$-sentences. Clearly we have:

3.1 Remark. If $u \equiv_{\bar{m}} v$ for all $\bar{m}$ with length $(\bar{m}) = k$ and $\mathrm{sum}(\bar{m}) = n$, then $u \equiv_n^k v$.

We now describe the Ehrenfeucht-Fraissé game $G_{\bar{m}}(u,v)$ which is useful for showing $\equiv_{\bar{m}}$-equivalence. (We restrict ourselves here to the case of word-models for L_0; however, all considerations could easily be adapted to arbitrary relational structures.)

The Game $G_{\bar{m}}(u,v)$, where $\bar{m} = (m_1,\ldots,m_k)$, is played between two players I and II on the word-models u and v; we assume that the position-sets of u and v are disjoint. We write $<^u$ to denote the $<$-relation in u; $Q_a^u, Q_b^u, <^v, Q_a^v, Q_b^v$ are used similarly. A play of the game consists of k moves. In the i-th move player I chooses, in u or in v, a sequence of m_i positions; then player II chooses, in the remaining word (v or u), also a sequence of m_i positions. Before each move, player I has to decide whether to choose his next elements from u or from v. After k moves, by concatenating the position-sequences chosen from u and chosen from v, two sequences $\bar{p} = p_1\ldots p_n$ from u and $\bar{q} = q_1\ldots q_n$ from v have been formed where $n = m_1+\ldots+m_k$. Player II has won the play if the map $p_i \mapsto q_i$ respects $<$ and the predicates Q_a, Q_b (i.e. $p_i <^u p_j$ iff $q_i <^v q_j$, $Q_a^u p_i$ iff $Q_a^v q_i$, $Q_b^u p_i$ iff $Q_b^v q_i$ for $1 \leq i,j \leq n$). Equivalently, the two subwords in u and v given by the position-sequences $\bar{p}$ and $\bar{q}$ should coincide. If there is a winning strategy for II in the game (to win each play) we say that II wins $G_{\bar{m}}(u,v)$ and write $u \sim_{\bar{m}} v$.

The standard Ehrenfeucht-Fraissé game is the special case of $G_{\bar{m}}(u,v)$ where $\bar{m} = (1,\ldots,1)$. (For a detailed discussion cf. Rosenstein (1982).) If $\text{length}(\bar{m}) = k$ and $\bar{m} = (1,\ldots,1)$ we write $G_k(u,v)$ instead of $G_{\bar{m}}(u,v)$ and $u \sim_k v$ instead of $u \sim_{\bar{m}} v$. Note that in this case the $\bar{m}$-formulas are (up to equivalence) just the formulas of quantifier-depth k. In the familiar form the Ehrenfeucht-Fraissé Theorem states (for the case of word-models) that u and v satisfy the same L_0-sentences of quantifier-depth k iff $u \sim_k v$. An analogous proof yields the result for $\bar{m}$-sentences and $\sim_{\bar{m}}$ (cf. Fraissé (1972), where the terminology of partial isomorphisms is used instead of game-theoretical notions):

3.2 Theorem. For all $\bar{m} = (m_1,\ldots,m_k)$ with $k > 0$ and $m_i > 0$ for $i = 1,\ldots,k$, we have $u \equiv_{\bar{m}} v$ iff $u \sim_{\bar{m}} v$.

Hence, in view of 3.1, we can prove the claim (**) of the preceding section (and thus the main result 2.1) by showing

3.3 Lemma. For $0 < k \leq n$ and any $\bar{m}$ with length $(\bar{m}) = k$ and $\mathrm{sum}(\bar{m}) = n$, $u_n^k \sim_{\bar{m}} v_n^k$ and $u_n^k \sim_{\bar{m}} w_n^k$.

As a preparation for the proof we state some basic properties of $\sim_{\bar{m}}$ and $\sim_n$:

3.4 Lemma.

(a) $\sim_{\bar{m}}$ is an equivalence relation.

(b) If $n \geq \mathrm{sum}(\bar{m})$ and $u \sim_n v$, then $u \sim_{\bar{m}} v$.

(c) If $u \sim_{\bar{m}} v$ and $u' \sim_{\bar{m}} v'$, then $uu' \sim_{\bar{m}} vv'$.

Parts (a), (b) are immediate from the definition of $G_n(u,v)$ and $G_{\bar{m}}(u,v)$. For the proof of (c) note that player II can combine the two given winning strategies on u,v and on u',v' in the obvious manner to obtain a winning strategy on uu',vv': As far as the initial segments u and v are concerned, the first given strategy is to be used, similarly for the final segments u',v' the second given strategy.

The following lemma is a familiar exercise on the game:

3.5 Lemma. If $m,m' \geq 2^n - 1$, then $(w)^m \sim_n (w)^{m'}$.

Proof. Consider the natural decomposition of $u = (w)^m$ and $v = (w)^{m'}$ into w-segments. Before each move we have in u and v certain w-segments in which positions have been chosen, and others where no positions have been chosen. Call a maximal segment of succeeding w-segments without chosen positions a gap. (A gap may be empty.) Before each move there is a natural correspondence between the gaps in u and v (given by their order). II should play according to what we call the 2^i-strategy, namely guarantee the following condition before each move: When i elements are still to be chosen by both players, two corresponding gaps should both consist of any number $\geq 2^i - 1$ of w-segments, or else should both consist of the same number $(< 2^i - 1)$ of w-segments. By induction on n-i it is easy to see that II always can choose his w-segment in this manner (cf. Rosenstein (1982), p. 99); of course, inside his w-segment, II should pick exactly that position which matches the position chosen by I in the corresponding w-segment.

Since any word u_n^k as defined in §2 is of the form $(w)^{2^n}$, we note as a consequence of 3.5:

3.6 Remark. For $1 \leq k \leq n$: $u_n^k \sim_n u_n^k u_n^k$.

We now turn to the

Proof of 3.3. By induction on k we show $u_n^k \sim_{\bar{m}} v_n^k$ and $u_n^k \sim_{\bar{m}} w_n^k$ for any $\bar{m}$ with $\text{length}(\bar{m}) = k$ and $\text{sum}(\bar{m}) \leq n$.

If $k = 1$ we deal with the game involving one move in which $\leq n$ elements are chosen by both players. Let us consider

$$u_n^1 = (ab)^{2^n} , \quad v_n^1 = (ab)^{2^n} a (ab)^{2^n} .$$

Since in both words u_n^1 and v_n^1 all possible words over $\{a,b\}$ of length n occur as subwords, any subword specified by I through his choice of n positions in one word can also be realized by II in the remaining word by n corresponding positions. Hence there is a winning strategy for II. The proof for u_n^1 and w_n^1 is analogous.

In the induction step we write u for u_n^k and consider the words

$$u_n^{k+1} = (uauubu)^{2^n} , \quad v_n^{k+1} = (uauubu)^{2^n} a (uauubu)^{2^n} .$$

Given a sequence $(m,\bar{m})$ with $\text{length}(m,\bar{m}) = k + 1$ and $\text{sum}(m,\bar{m}) \leq n$, we have to show $u_n^{k+1} \sim_{(m,\bar{m})} v_n^{k+1}$, using as induction hypothesis

$$\text{(a)} \quad u \sim_{\bar{m}} uau \ (= v_n^k) , \qquad \text{(b)} \quad u \sim_{\bar{m}} ubu \ (= w_n^k) .$$

(In an analogous manner it will be possible to show $u_n^{k+1} \sim_{(m,\bar{m})} w_n^{k+1}$.)

In order to verify $u_n^{k+1} \sim_{(m,\bar{m})} v_n^{k+1}$, it is convenient to apply 3.4(a), (b) and consider two different words instead which are $\sim_n$-equivalent to u_n^{k+1}, v_n^{k+1} respectively: Instead of u_n^{k+1} we take

(1) $\quad (uauubu)^{2^n} \ uauubu \ (uauubu)^{2^n}$

which is $\sim_n$-equivalent to u_n^{k+1} by 3.5. Concerning v_n^{k+1}, we use 3.6 in order to duplicate (several times) the u-segments next to the central letter a there; thus we obtain the $\sim_n$-equivalent word

(2) $\quad (uauubu)^{2^n} \ uau \ (u)^{m+1} (uauubu)^{2^n}$.

For the proof of (1) $\sim_{(m,\bar{m})}$ (2) we distinguish the two cases that I first picks m positions from (1) or I first picks m positions from (2).

Assume that I has chosen m positions from (1). Then in the first 2^n (uauubu)-segments of (1) there must occur a gap consisting of $\geq 2^{n-m}$ (uauubu)-segments (since $(2^n-m)/m \geq 2^{n-m}$). Let u_1 be the initial segment of (1) preceding the first such gap, v_1 the corresponding initial segment (of same length) in (2), and u_2 the final segment of (1) succeeding this gap. By 3.5, there is a final segment v_2 of (2) included in the last 2^n-1 (uauubu)-segments which is $\sim_n$-equivalent to u_2. Hence u_1, v_1 are isomorphic and u_2, v_2 are $(m,\bar{m})$-equivalent; so there is a winning strategy for II on these segments of (1) and (2). By 3.4(c) it now suffices to show that II has a winning strategy also on the remaining segments between u_1, u_2 and between v_1, v_2. II will pick no positions between v_1 and v_2 during the first move, since I picked no positions between u_1 and u_2. Hence a winning strategy for II in $G_{(m,\bar{m})}((1),(2))$ will emerge if these two "middle segments" are $\sim_{\bar{m}}$-equivalent:

$$(uauubu)^{m_1} \sim_{\bar{m}} (uauubu)^{m_2} uau\,(u)^{m+1} (uauubu)^{m_3} .$$

Note that $sum(\bar{m}) = n - m$, and $m_1 \geq 2^{n-m}$. But also $m_2 \geq 2^{n-m}$, since (according to definition of u_1) the gap after u_1 intersects the first 2^n (uauubu)-segments of (1) by at least 2^{n-m} such segments and hence the same holds for v_1. - Now by induction hypothesis (a) (and 3.4(c)) we may replace the critical segment uau on the right-hand side by u, and then, using 3.6 repeatedly, delete the extra u-segments there altogether. Hence it suffices to show

$$(uauubu)^{m_1} \sim_{\bar{m}} (uauubu)^{m_2+m_3} .$$

This is clear from 3.5 and 3.4(b), since $sum(\bar{m}) = n - m$ and $m_1 \geq 2^{n-m}$, $m_2 + m_3 \geq 2^{n-m}$ as seen above.

Assume now that I has picked his first m positions from (2). II will pick exactly corresponding positions in (1), except possibly for the segment uubuu around the b in the middle of (1), which corresponds to the segment $u(u)^{m+1}u$ in (2). It suffices to show that

(+) $\quad uubuu \sim_{(m,\bar{m})} u(u)^{m+1}u$.

Obviously, at least one of the $m+1$ central u-segments on the right-hand side of (+) is free of chosen positions after I's first move. Let us display such a free u-segment by writing

$$u(u)^{m+1}u = w_1 u w_2 .$$

Then, by 3.6, $w_1 \sim_{(m,\bar{m})} u$ and $w_2 \sim_{(m,\bar{m})} u$; hence II can pick corresponding positions in the outer u-segments of uubuu during his first move, leaving the central segment ubu free. Thus for (+) is suffices to have $u \sim_{\bar{m}} ubu$; but this is guaranteed by induction hypothesis (b).

References

J.A. Brzozowksi, R. Knast (1978): The dot-depth hierarchy of star-free languages is infinite, J.Comput.System Sci. 16, 37-55.

R.S. Cohen, J.A. Brzozowski (1971): Dot-depth of star-free events, J.Comput.System Sci. 5, 1-16.

S. Eilenberg (1976): "Automata, Languages, and Machines", Vol.B, Academic Press, New York.

R. Fraissé (1972): "Cours de Logique Mathématique", Tome 2, Gauthier-Villars, Paris.

R. McNaughton, S. Papert (1971): "Counter-free Automata", MIT Press, Cambridge, Mass.

J.E. Pin (1984a): Hierarchies de concaténation, RAIRO-Informatique Théorique (to appear).

J.E. Pin (1984b): "Variétés de langages formels", Masson, Paris (in press).

J.G. Rosenstein (1982): "Linear Orderings", Academic Press, New York.

H. Straubing (1981): A generalization of the Schützenberger product of finite monoids, Theor.Comput. Sci. 13, 107-110.

W. Thomas (1982): Classifying regular events in symbolic logic, J.Comput.System Sci. 25, 360-376.

Wolfgang Thomas
Lehrstuhl für Informatik II

Büchel 29-31
D-5100 Aachen

MÉMOIRES DE LA S. M. F.

CHRISTIAN U. JENSEN

Théorie des modèles pour des anneaux de fonctions entières et des corps de fonctions méromorphes

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 23-40

<http://www.numdam.org/item?id=MSMF_1984_2_16__23_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p. 23-40

THÉORIE DES MODÈLES POUR DES ANNEAUX DE FONCTIONS ENTIÈRES ET DES CORPS DE FONCTIONS MÉROMORPHES.

Christian U. Jensen

Résumé. Pour un sous-corps K de $\underline{\underline{C}}$ soit $E(K)$ le sous-anneau de $K[[X]]$ formé des séries formelles dont le rayon de convergence est infini. Si $\rho \in \underline{\underline{R}}^+$ ou $\rho = \infty$ on désigne par E_ρ l'anneau des fonctions entières d'ordre $< \rho$. On pose $E_\rho(K) = E_\rho \cap E(K)$. On montre entre autres choses que l'anneau des polynômes $K[X]$ est définissable dans $E_\rho(K)$ si $\rho < \infty$ ou $K = \underline{\underline{R}}$ ou $K = \underline{\underline{C}}$. En particulier, ces anneaux sont indécidables. De plus, si $K = \underline{\underline{R}}$ ou $K = \underline{\underline{C}}$, alors $E_\rho(K) \equiv E_\sigma(K)$ entraine $\rho = \sigma$. Soit $M_\rho(K)$ le corps des fractions de $E_\rho(K)$. Si $\rho > 0$ les corps $M_\rho(\underline{\underline{R}})$ sont indécidables, et l'on peut même interpréter l'arithmétique du second ordre dans ces corps. Si $\rho \leq 1$ et K est un sous-corps pythagoricien de $\underline{\underline{R}}$, les corps $M_\rho(K)$ sont indécidables. Si $\rho > 1$ le sous-anneau de $M_\rho(\underline{\underline{R}})$ formé des fonctions sans pôles réels est définissable dans $M_\rho(\underline{\underline{R}})$.

Summary. For a subfield K of $\underline{\underline{C}}$ let $E(K)$ be the subring of $K[[X]]$ consisting of all formal power series of infinite convergence radius. If $\rho \in \underline{\underline{R}}^+$ or $\rho = \infty$ we denote by E_ρ the ring of all entire functions of order $< \rho$. We set $E_\rho(K) = E_\rho \cap E(K)$. It is shown that the polynomial ring $K[X]$ is definable in $E_\rho(K)$ if $\rho < \infty$ or $K = \underline{\underline{R}}$ or $K = \underline{\underline{C}}$. In particular, these rings are undecidable. Moreover, if $K = \underline{\underline{R}}$ or $K = \underline{\underline{C}}$, then $E_\rho(K) \equiv E_\sigma(K)$ implies $\rho = \sigma$. Let $M_\rho(K)$ be the quotient field of $E_\rho(K)$. The fields $M(\underline{\underline{R}})$ are undecidable, and it is even possible to interpret second order number theory in these fields. If $\rho \leq 1$ and K is a Pythagorean subfield of $\underline{\underline{R}}$ the fields $M_\rho(K)$ are undecidable. If $\rho > 1$ the subring of $M_\rho(\underline{\underline{R}})$ consisting of all functions with no real poles is definable in $M_\rho(\underline{\underline{R}})$.

0037-9484/84 03 23 18/$ 3.80/

C.U. JENSEN

1. ANNEAUX DES FONCTIONS ENTIÈRES.

1.1. Préliminaires. Soit E l'anneau des fonctions entières complexes d'une variable complexe. Pour un sous-corps K de $\mathbb{C}$ soit $E(K)$ l'anneau des fonctions entières à coefficients dans K, c.-à-d. le sous-anneau de $K[[X]]$ formé des séries formelles dont le rayon de convergence est infini. Évidemment $E = E(\mathbb{C})$.

$E(K)$ est un anneau intègre non-noethérien, mais $E(K)$ est un anneau de Bézout, c.-à-d. tout idéal de type fini est principal. Dans le cas $K = \mathbb{C}$ ce résultat est dû à Wedderburn (14) et dans le cas général il est dû a Helmer (5).

Nous allons esquisser la démonstration d'un résultat plus précis qui est dû à Rubel (12) dans le cas $K = \mathbb{C}$.

Proposition 1.1. Pour tout corps $K \subseteq \mathbb{C}$, $K \not\subseteq \mathbb{R}$, l'anneau $R = E(K)$ est un anneau de Bézout dont le rang stable est égal à 1, c.-à-d. pour tout couple (f,g) de fonctions de R il existe une fonction $h \in R$ telle que $Rf + Rg = R(f+gh)$[1].

Pour la démonstration on a besoin d'un lemme d'interpolation.

Lemme 1.2. Soit $\{\alpha_n\}_n$, $n \in \mathbb{N}$ une partie discrète de $\mathbb{C}$ et soit $p_n = \sum_{j=0}^{t_n} a_{nj}(x-\alpha_n)^j$ un polynôme en $(x-\alpha_n)$ à coefficients complexes. Si $\alpha_n = 0$ on suppose $a_{n,0},..,a_{n,t_n} \in K$. De plus, si $K \subseteq \mathbb{R}$, on suppose $p_n = \overline{p}_m$ lorsque $\alpha_n = \overline{\alpha}_m$. Alors, il existe $f \in E(K)$ telle que

$$f \equiv \sum_{j=0}^{t_n} a_{nj}(x-\alpha_n)^j \mod (x-\alpha_n)^{t_n+1}, \quad n \in \mathbb{N}.$$

En ce qui concerne la preuve du lemme nous remarquons que l'on procède comme dans le cas classique $K = \mathbb{C}$ en utilisant le fait suivant (cf. 5, 6).

Soit f une fonction entière et K un sous-corps de $\mathbb{C}$. Si $K \subseteq \mathbb{R}$ on suppose $f \in E(\mathbb{R})$. Alors, il existe une fonction entière g telle que $f \exp(g) \in E(K)$.

Retournons maintenant à la démonstration de la proposition 1.1. Ici et dans ce qui suit nous désignons par $Z(f)$, $f \in E$, l'ensemble des zéros de f.

Pour vérifier l'assertion de la proposition on peut se restreindre au cas où $Z(f) \cap Z(g) = \emptyset$.

Soit $Z(g) = \{\beta_n\}$ et soit t_n la multiplicité de β_n en tant que zéro de g. Puisque $f(\beta_n) \neq 0$ on construit - en considérant $\log f$ en β_n - un polynôme $u_n = \sum_{j=0}^{t_n-1} a_{j,n}(x-\beta_n)^j$ tel que

$$f - \exp(u_n) \equiv 0 \mod (x-\beta_n)^{t_n} .$$

Par le lemme 1.2 il existe une fonction $u \in E(K)$ telle que $f - \exp(u) \equiv 0 \mod g$; donc pour une fonction convenable $h \in E(K)$ la fonction $f + gh$ est inversible dans $E(K)$.

On dit qu'une fonction entière f est d'ordre fini s'il existe deux nombres réels a et c tels que

$$|f(x)| \leqq c \exp(|x|^a) \qquad (*)$$

pour tout $x \in \mathbb{C}$.

La borne inférieure ρ des nombres a pour lesquels (*) est satisfait pour une constante c (dépendante de a) est appelée l'ordre de la fonction f. (Pour de plus amples détails voir (3,13).)

On peut montrer qu'une fonction entière $f(x) = \sum_{n=0}^{\infty} a_n x^n$ est d'ordre fini ρ si et seulement $\liminf \log(1/|a_n|) / n \log n = 1/\rho$. (Si la borne ci-dessus est ∞ (resp. 0) la fonction f est d'ordre 0 (resp. ∞).)

Rappelons le théorème de factorisation de Hadamard. Soit f une fonction entière d'ordre $\rho < \infty$ et $Z(f) = \{\alpha_j\}$. Alors f est de la forme

$$f(x) = \exp(h(x))\, x^n \prod_{\alpha_j \neq 0} (1-x/\alpha_j)\exp\left(1+x/\alpha_j + \ldots + \frac{1}{[\rho]}(x/\alpha_j)^{[\rho]}\right),$$

où $[\rho]$ est le plus grand entier $\leq \rho$, $h(x)$ un polynôme de degré $\leq \rho$, et $n = 0$, si 0 n'est pas un zéro de f.

Pour une suite $\{\alpha_n\}$, $n \in \mathbb{N}$, de nombres complexes l'exposant de convergence est défini comme la borne inférieure des nombres positifs p tels que $\sum_{\alpha_n \neq 0} |\alpha_n|^{-p} < \infty$.

Alors, c'est un résultat classique qu'une partie discrète $\{\alpha_j\}$ de $\mathbb{C}$ est l'ensemble des zéros d'une fonction d'ordre $\leq \rho$ si et

seulement si l'exposant de convergence de la suite $\{\alpha_j\}$ est $\leqq \rho$.

Pour un nombre donné ρ les fonctions d'ordre $< \rho$ (resp. $\leqq \rho$) forment un sous-anneau E_ρ ($\overline{E}_\rho$) de E. L'anneau $E_\infty = \bigcup_{\rho<\infty} E_\rho$ est formé par toutes les fonctions entières d'ordre fini.

Pour un sous-corps K de $\mathbb{C}$ on définit $E_\rho(K) = E_\rho \cap E(K)$, $0 < \rho \leqq \infty$, et $\overline{E}_\rho(K) = \overline{E}_\rho \cap E(K)$, $0 \leq \rho < \infty$.

La structure des anneaux $E_\rho(K)$ et $\overline{E}_\rho(K)$ est plus compliquée que celle des anneaux $E(K)$. Comme $E(K)$ les anneaux $E_\rho(K)$ et $\overline{E}_\rho(K)$ ne sont pas noethériens, mais à la différence de $E(K)$ aucun des anneaux $E_\rho(K)$ et $\overline{E}_\rho(K)$ n'est un anneau de Bézout. (Il existe même deux fonctions f et g d'ordre zéro telles que l'idéal $E_\infty f + E_\infty g$ n'est pas principal dans E_∞.) De plus, c'est une question ouverte de savoir quel est le rang stable des anneaux $E_\rho(K)$ et $\overline{E}_\rho(K)$.

Cependant, c'est une conséquence facile du théorème de factorisation que chacun des anneaux $E_\rho(K)$ et $\overline{E}_\rho(K)$ est complètement intégralement clos dans son corps des fractions. La preuve s'appuie sur le fait suivant. Si R désigne un des anneaux $E_\rho(K)$ ou $\overline{E}_\rho(K)$, alors une fonction $f \in R$ divise une fonction $g \in R$ dans R si f divise g dans E. Ceci signifie que E/R est un R-module sans torsion.

Nous finissons cette section en mentionnant quelques résultats concernant la dimension globale et la dimension de Krull (notée K-dim) de ces anneaux.

Théorème 1.3. Soit R un sous-anneau de E contenant $E_0(\mathbb{R})$ et supposons que E/R soit un R-module sans torsion. Alors:

gl.dim $R \geqq 3$; de plus, l'énoncé "gl.dim $R = \infty$" est compatible avec ZFC + MA. (MA = l'axiome de Martin.)

K-dim $R \geqq 2^{\aleph_0}$; de plus, l'énoncé "K-dim $R = 2^{2^{\aleph_0}}$" est compatible avec ZFC + MA.

Si l'on suppose de plus que R est un anneau de Bézout, alors pour tout t, $3 \leqq t \leqq \infty$, l'énoncé "gl.dim $R = t$" est compatible avec ZFC + MA.

De même, dans le cas où R est un anneau de Bézout, soient P, Q et P' trois idéaux premiers de R tels que $P \subsetneqq Q \subsetneqq P'$.

Alors, les idéaux premiers entre P et P' forment une chaîne de longueur $\geq 2^{\aleph_0}$. Il est compatible avec ZFC + MA de supposer que cette chaîne est de longueur $2^{2^{\aleph_0}}$.

(Une partie de ces résultats se trouvent dans (7, 8), les détails seront publiés ultérieurement.)

1.2. Définissabilité et indécidabilité des anneaux $E_\rho(K)$ et $\overline{E}_\rho(K)$

Dans cette section on montre entre autres choses que $\underline{\mathbb{N}}$ est définissable dans $E_\rho(K)$ et $\overline{E}_\rho(K)$ pour tout $0 < \rho < \infty$ et tout sous-corps K de $\underline{\mathbb{C}}$. Il se trouve que même l'anneau de polynômes $K[X]$ est définissable dans $E_\rho(K)$, $\overline{E}_\rho(K)$ et $E(K)$.

D'abord nous donnons une caractérisation élémentaire des fonctions linéaires de ces anneaux.

Lemme 1.2.1. Pour chaque sous-corps K de $\underline{\mathbb{C}}$ et tout nombre ρ $0 < \rho \leq \infty$, les fonctions linéaires, $ax+b$, $a \in K \setminus 0$, $b \in K$, sont définissables (sans paramètre) dans $E_\rho(K)$ par une formule qui ne dépend ni de K ni de ρ. En effet, si $f \in E_\rho(K)$, alors f est linéaire ssi f est non-inversible et $E_\rho(K)(f-k)$ est un idéal premier de $E_\rho(K)$ pour tout $k \in K$.

Démonstration. Par le théorème de Picard les constantes sont définissables; donc, la description plus haut est une caractérisation élémentaire des fonctions linéaires.

Il suffit de montrer que f est linéaire si f est non-inversible et l'idéal principal engendré par f est un idéal premier. Mais cette assertion est une conséquence du lemme suivant.

Lemme 1.2.2. Soient A une partie discrète de $\underline{\mathbb{C}}$, f une fonction de E_ρ, $f(0) = 1$, et K un sous-corps de $\underline{\mathbb{C}}$. Si $K \subseteq \underline{\mathbb{R}}$ on suppose de plus que $f \in E_\rho(\underline{\mathbb{R}})$. Alors il existe une fonction $g \in E(K)$ telle que $f|g$ (dans E) et $Z(g/f) \cap A = \emptyset$.

Démonstration. (Esquissée) On construit g en ajoutant à $f(x) = \sum_n a_n x^n$ des facteurs $(1-x^n/b_n)$, où (b_n) est une suite "rapidement" croissante. Les nombres b_n sont construits par récurrence sur n tels que les coefficients du produit appartiennent à K.

Par la même méthode on montre

Lemme 1.2.3. Pour chaque sous-corps K de $\underline{\subseteq}$ et tout nombre ρ, $0 \leq \rho \leq \infty$ les fonctions linéaires de $\overline{E}_\rho(K)$ sont définissables (sans paramètre) dans $\overline{E}_\rho(K)$ par une formule qui ne dépend ni de K ni de ρ.

Proposition 1.2.4. Si f est une fonction linéaire de $E_\rho(K)$, $0 < \rho < \infty$, les $n^{\text{èmes}}$ puissances de f sont définissables dans $E_\rho(K)$ avec le seul paramètre f, où n parcourt les nombres naturels divisibles par $m = [\rho+1]p^2$, p étant un nombre premier plus grand que $\rho + 1$. La formule définissant ces puissances ne dépend que de ρ et est indépendante de K.

Démonstration. Sans restriction on peut supposer $f = x$.

L'ensemble suivant est définissable dans $E_\rho(K)$:

$$\mathcal{D} = \{g^m | x | g \,\&\, d | g \to d | 1 \vee x | d\}.$$

Par le théorème de Hadamard $\mathcal{D}$ est l'ensemble des fonctions de la forme $\exp(h(x))x^n$, où $m|n$ et $h(x)$ est un polynôme dans $K[X]$ de degré $\underline{\leq} \rho$.

Il est évident que x^m-1 divise x^n-1 si m divise n.

On prouve la proposition en établissant que réciproquement toute fonction H de $\mathcal{D}$ telle que $x^m-1 | H-1$ est forcément une puissance x^n, $m|n$.

En effet, considérons une fonction $\exp(h(x))x^n$, $h(x)$ étant un polynôme dans $K[X]$ de degré $\underline{\leq} \rho$, et supposons que

$$\exp(h(x))x^n \equiv 1 \text{ modulo } (x^m-1) \text{ dans l'anneau } E_\rho(K).$$

Nous allons en déduire que $h(x)$ est une constante $2\pi ib$, $b \in \underline{\mathbb{Z}}$. Posons $t = [\rho+1]$ et

$$h(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1},\ a_0, a_1, \ldots, a_{t-1} \in K .$$

Alors $h(\varepsilon) \equiv 0$ modulo $2\pi i\underline{\underline{Z}}$ si ε est une racine $m^{\text{ème}}$ de l'unité. En particulier, si ε_t est une racine primitive $t^{\text{ème}}$ de l'unité et si l'on pose $a_j = b_j(2\pi i)$, $0 \leq j < t$, alors

$$b_0 + b_1\varepsilon_t^k + \ldots + b_{t-1}(\varepsilon_t^k)^{t-1} \equiv 0 \text{ modulo } \underline{\underline{Z}},\ 0 \leq k < t .$$

Puisque le déterminant

$$\det_{0\leq k,j<t} (\varepsilon^k)^j = \prod_{0\leq k<j<t} (\varepsilon_t^j - \varepsilon_t^k) \neq 0$$

il s'ensuit que tout nombre b_j, $0 \leq j < t$, appartient au corps cyclotomique $\underline{\underline{Q}}(\varepsilon_t)$.

De plus, si l'on pose $\varepsilon = \varepsilon_p 2$, où $\varepsilon_p 2$ est une racine primitive $(p^2)^{\text{ème}}$ de l'unité, on obtient

$$b_0 + b_1\varepsilon_p 2 + \ldots + b_{t-1}\,\varepsilon_p 2^{t-1} \in \mathbb{Z} .$$

Puisque le degré de $\varepsilon_p 2$ par rapport à $\underline{\underline{Q}}(\varepsilon_t)$ est $\geq p > t$, on conclut que $b_1 = b_2 = \ldots = b_{t-1} = 0$ et $b_0 \in \underline{\underline{Z}}$, c.q.f.d.

Théorème 1.2.5. Pour tout sous-corps K de $\underline{\underline{C}}$ l'anneau de polynômes $K[X]$ est élémentairement définissable (sans paramètre) dans $E_\rho(K)$ $(0 < \rho < \infty)$ par une formule qui ne dépend que de ρ.

Démonstration. Il suffit de définir $K[X]$ dans $E_\rho(K)$ avec le paramètre x, puisque on peut éliminer ce paramètre grâce au lemme 1.2.1.

On remarque qu'une fonction $f \in E(K)$ est un polynôme si et seulement s'il existe une puissance x^n telle que $x^n f(1/x)$ soit une fonction entière.

En vertu de la proposition 1.2.4 les puissances x^n, n étant divisible par le nombre m de la proposition, forment un ensemble P définissable dans $E_\rho(K)$. On en déduit une définition élémentaire de $K[X]$ dans $E_\rho(K)$:

Une fonction $f \in E_\rho(K)$ appartient à $K[X] \Leftrightarrow \exists p \in P\ \exists g \in E_\rho(K)$ $(\forall \alpha \in K \setminus \{0\}, \exists \beta,\gamma \in K\ (x-\alpha^{-1}) \mid f-\beta \wedge (x-\alpha \mid p-\gamma) \wedge (x-\alpha) \mid g-\beta\gamma))$.

De façon analogue on montre

Théorème 1.2.6. Pour tout sous-corps K de $\underline{\underline{C}}$ l'anneau de polynômes $K[X]$ est élémentairement définissable (sans paramètre) dans $\overline{E}_\rho(K)$ $0 \leqq \rho < \infty$ par une formule que ne dépend que de ρ.

Remarque 1.2.7. La démonstration ci-dessus laisse voir qu'il existe pour tout couple ρ,σ de nombres réels une formule qui définit $K[X]$ dans $E_\rho(K)$, $E_\sigma(K)$, $\overline{E}_\rho(K)$ et $\overline{E}_\sigma(K)$. En vertu d'un résultat de Robinson (10) il s'ensuit que $\underline{\underline{N}}$ est définissable (sans paramètre) par la même formule dans $E_\rho(K)$, $E_\sigma(K)$, $\overline{E}_\rho(K)$ et $\overline{E}_\sigma(K)$.

Corollaire 1.2.8. Pour tout sous-corps K de $\underline{\underline{C}}$ les anneaux $E_\rho(K)$ $0 < \rho < \infty$, et $\overline{E}_\rho(K)$, $0 \leqq \rho < \infty$, sont indécidables.

Corollaire 1.2.9. Soient K et L deux sous-corps de $\underline{\underline{C}}$ et ρ un nombre positif réel. Alors $E_\rho(K) \equiv E_\rho(L)$ entraîne $K \equiv L$ (où "$\equiv$" désigne l'équivalence élémentaire.) De même, $\overline{E}_\rho(K) \equiv \overline{E}_\rho(L)$ entraîne $K \equiv L$ si $0 \leqq \rho < \infty$.

Remarque 1.2.10. Les implications réciproques ne subsistent pas. Par exemple, (de façon analogue à un résultat dans (7)) $E_\rho(K) \not\equiv E_\rho(\underline{\underline{C}})$ pour tout sous-corps propre K de $\underline{\underline{C}}$ et tout nombre réel positif ρ.

Remarque 1.2.11. Soit R un sous-anneau de $E_\rho = E_\rho(\underline{\underline{C}})$, $0 < \rho < \infty$, contenant l'anneau de polynômes $\underline{\underline{C}}[X]$. Supposons de plus que E_ρ/R soit un R-module sans torsion. En modifiant les arguments utilisés plus haut on trouve que $\underline{\underline{C}}[X]$ est définissable (sans paramètre) dans R par une formule qui ne dépend que de ρ.

Pour traiter le cas des anneaux $E_\infty(K)$ et $E(K)$ nous avons besoin du résultat suivant, dont la démonstration repose sur les arguments, légèrement modifiés, de l'analyse classique.

Lemme 1.2.12. Soit K un sous-corps de $\underline{\underline{C}}$. Toute partie infinie discrète de $\underline{\underline{C}}$ contient un sous-ensemble infini $\{\alpha_n\}$, $n \in \underline{\underline{N}}$, tel qu'il existe une fonction $f \in \overline{E}_0(K)$ pour laquelle $f(\alpha_n) = n$ pour tout $n \in \underline{\underline{N}}$.

Proposition 1.2.13. Soit K un sous-corps de $\underline{\underline{C}}$ et désignons par R un des anneaux $E_\rho(K)$, $0 < \rho \leqq \infty$, ou $E(K)$. Si $\underline{\underline{N}}$ est définis-

sable dans R, alors $K[X]$ est définissable par une formule qui ne dépend que de la formule qui définit $\underline{\underline{\mathbb{N}}}$ dans R.

Démonstration. Les constantes sont définissables dans R. $K[X]$ peut être défini comme suit. Si $f \in R$, alors:

$$f \in K[X] \Leftrightarrow \forall k \in K\ \forall g \in R(\exists n \in \mathbb{N}\ (R(f-k) + R(g-n) = R)$$

" $\Rightarrow$ " : Si $f \in K[X]$, f n'a qu'une nombre fini de zéros, et l'énoncé est une conséquence du fait que l'idéal $Rg+Rh$ est principal pour chaque polynôme h et un générateur est un plus grand commun diviseur de g et h.
" $\Leftarrow$ " : Si $f \notin K[X]$, alors f a une singularité essentielle dans ∞ et en vertu du second théorème de Picard il existe $k \in K$ telle que $f+k$ a un ensemble infini de zéros. Ensuite on applique le lemme 1.2.12.

Si $R = E(K)$ il est bien connu que $\underline{\underline{\mathbb{N}}}$ est définissable dans R. Donc, on obtient

Corollaire 1.2.14. Pour tout sous-corps K de $\underline{\underline{\mathbb{C}}}$ l'anneau de polynômes $K[X]$ est définissable (sans paramètre) dans $E(K)$ par une formule qui ne dépend pas de K.

Si $K = \underline{\underline{\mathbb{R}}}$ ou $K = \underline{\underline{\mathbb{C}}}$ une modification immédiate d'un argument de Robinson (10) montre que $\underline{\underline{\mathbb{N}}}$ est définissable dans $E_\rho(K)$, $\rho \geq 1$, par une formule qui ne dépend pas de ρ. Si $\rho < 1$, l'anneau $K[X]$ est définissable uniformément dans $E_\rho(K)$ grâce au théorème 1.2.5 (et la remarque 1.2.7). En combinant ces deux formules [2], on arrive à

Théorème 1.2.15. Si $K = \underline{\underline{\mathbb{R}}}$ ou $\underline{\underline{\mathbb{C}}}$ il existe une formule qui définit (sans paramètre) l'anneau des polynômes $K[X]$ dans chacun des anneaux $E_\rho(K)$, $0 < \rho \leq \infty$. En particulier, il existe une formule qui définit $\underline{\underline{\mathbb{N}}}$ dans chacun des anneaux $E_\rho(K)$, $0 < \rho \leq \infty$.

Nous en déduisons un résultat qui répond à une question posée par Becker, Henson et Rubel (2).

Théorème 1.2.16. Si $K = \underline{\underline{R}}$ ou $\underline{\underline{C}}$ et $0 < \rho \leq \infty$, $0 < \sigma < \infty$, alors $E_\rho(K) \equiv E_\sigma(K)$ entraîne $\rho = \sigma$.

Démonstration. Il existe des formules qui définissent uniformément $\underline{\underline{N}}$ dans $E_\rho(K)$ et $E_\sigma(K)$, le corps des constantes K dans $E_\rho(K)$ et $E_\sigma(K)$, et l'ensemble L des fonctions linéaires dans $E_\rho(K)$ et $E_\sigma(K)$.

Supposons $\rho < \sigma$ et soit p/q $(p,q \in \underline{\underline{N}})$ un nombre rationel tel que $\rho < p/q < \sigma$.

La suite $(n^{q/p})$, $n \in \underline{\underline{N}}$, est l'ensemble des zéros d'une fonction de E_σ, mais pas d'une fonction de E_ρ.

Considérons l'énoncé élémentaire suivant:

$$\varphi: (\exists f \in L \wedge \exists g \neq 0 (f \mid g \vee \forall \alpha \in K (f-\alpha \mid g) \rightarrow \exists \beta \in \underline{\underline{N}}, \gamma \in K$$

$$\beta^q = \alpha^p \wedge (\beta+1)^q = \gamma^p \wedge (f-\gamma) \mid g) .$$

L'énoncé φ est satisfait dans $E_\rho(K)$:

On peut choisir $f = x$, et puisque l'exposant de convergence de la suite $(n^{q/p})$, $n \in \underline{\underline{N}}$, est p/q il existe une fonction $g \in E_\sigma(K)$ dont l'ensemble des zéros est $(n^{q/p})$, $n \in \underline{\underline{N}}$.

L'énoncé φ n'est pas satisfait dans $E_\sigma(K)$:

Sans restriction on peut supposer que $f = x$. L'ensemble $Z(g)$ devait contenir 0 ainsi qu'une suite $z_1, z_2, .., z_n, ..$ où $z_n = n^{q/p} \varepsilon_n$, ε_n étant une racine $p^{\text{ème}}$ de l'unité. Puisque l'exposant de convergence de cette suite est égal à p/q, aucune fonction de E_ρ ne contient les nombres 0 et z_n, $n \in \underline{\underline{N}}$, dans son ensemble des zéros. Par conséquent φ n'est pas satisfait dans E_ρ. Ceci achève la démonstration du théorème 1.2.16.

Remarque 1.2.17. Avec une légère modification on montre que $\rho = \sigma$ si $\overline{E}_\rho(K) \equiv \overline{E}_\sigma(K)$, où $K = \underline{\underline{R}}$ ou $\underline{\underline{C}}$, $0 \leq \rho < \infty$. De même, $\overline{E}_\rho(K) \not\equiv \overline{E}_\sigma(K)$ pour tout nombre ρ rationnel.

2. CORPS DES FONCTIONS MÉROMORPHES.

Pour un sous-corps K de $\underline{\underline{C}}$ soit $M(K)$ le corps des fractions de $E(K)$. On appelle $M(K)$ le corps des fonctions méromorphes à coefficients dans K. De même, désignons par $M_\rho(K)$, resp. $\overline{M}_\rho(K)$, le corps des fractions de $E_\rho(K)$, resp. $\overline{E}_\rho(K)$.

Théorème 2.1. Soit ρ un nombre réel positif. L'ensemble $\underline{\underline{N}}$ des nombre naturels est définissable dans chaque corps F entre $M_\rho(\underline{\underline{R}})$ et $M(\underline{\underline{R}})$ par une formule qui ne dépend que de ρ. En particulier, un tel corps F est indécidable.

Démonstration. Puisque le genre de la courbe $X^4 = 1 + Y^4$ est plus grand que 1, le théorème d'uniformisation de Picard implique que $\underline{\underline{R}}$ est définissable dans F par la formule

$$\underline{\underline{R}} = \{\xi \in F \mid \exists \eta \in F\ (\eta^4 = 1 + \xi^4)\}.$$

En particulier, l'ensemble $\underline{\underline{R}}^+$ des nombres réels positifs est définissable dans F.

Par une modification facile de (9. prop.2) on prouve qu'une fonction $f = f(x) \in M_\rho(\underline{\underline{R}})$, $\rho > 0$, est une somme de deux carrés dans $M_\rho(\underline{\underline{R}})$ si (et seulement si) $f(x) \geq 0$ pour tout nombre réel x qui n'est pas un pôle de f.

Pour $\alpha \in \underline{\underline{R}}$ et $f,g \in F$ on définit la formule $\Phi(\alpha,f,g)$:

$$\exists c \in \underline{\underline{R}}^+\ \exists p,q \in F\left(c(g-\alpha)^2 - \frac{f^2}{1+f^2} = p^2 + q^2\right).$$

Soit t un entier tel que $t > \rho^{-1}$. Puisque $\underline{\underline{R}}$ et $\underline{\underline{R}}^+$ sont définissables dans F, la définissabilité de $\underline{\underline{N}}$ dans F est une conséquence de l'énoncé suivant:

Si $\alpha \in \underline{\underline{R}}^+$, alors $\alpha \in \underline{\underline{N}} \Leftrightarrow \forall f,g \in F$

$$(\Phi(1,f,g) \wedge [\forall \beta \in \underline{\underline{R}}^+(\Phi(\beta^t,f,g) \rightarrow \Phi((\beta+1)^t,f,g)]) \rightarrow \Phi(\alpha^t,f,g)\ .$$

L'implication " $\Rightarrow$ " est évidente.

" $\Leftarrow$ ": Posons $g = x$ et $f = f(x) = \prod_{n=1}^{\infty} (1-x/n^t)$, qui appartient à $E_\rho(\underline{\underline{R}}) \subset M_\rho(\underline{\underline{R}}) \subset F$, puisque l'exposant de convergence de la suite (n^t), $n \in \underline{\underline{N}}$, est $< \rho$. D'après la remarque plus haut on déduit

$$\Phi(\gamma,f(x),x) \Leftrightarrow f(\gamma) = 0 \Leftrightarrow \gamma = n^t \quad \text{où} \quad n \in \underline{\underline{N}}.$$

Nous en concluons que $\alpha^t = n^t$ pour un nombre $n \in \underline{\underline{N}}$, et, puisque $\alpha \in \underline{\underline{R}}^+$ nous obtenons $\alpha \in \underline{\underline{N}}$.

Théorème 2.2. Soit ρ un nombre réel positif. L'ensemble $\underline{\underline{N}}$ des nombres naturels est définissable dans chaque corps F entre $\underline{\underline{R}}(X)$ et $M_\rho(\underline{\underline{R}})$ par une formule que ne dépend que de ρ. En particulier, tout corps $\overline{M}_\rho(\underline{\underline{R}})$, $0 \leqq \rho < \infty$, est indécidable.

Démonstration. Comme plus haut $\underline{\underline{R}}$ est définissable dans F. D'abord nous définissons $\underline{\underline{N}}$ avec le paramètre X. Choisissons un entier t tel que $t > \rho$.

Si $\alpha_1,..,\alpha_n$ sont des nombres réels distincts deux à deux, il existe un nombre réel positif c tel que

$$f(x) = \frac{c(x-\alpha_1)\ldots(x-\alpha_n)}{1+(x-\alpha_1)^2\ldots(x-\alpha_n)^2}$$

satisfait aux conditions

$$f(x)^2 \leqq (x-\alpha_j)^2 \quad \text{pour tout} \quad x \in \underline{\underline{R}} \quad \text{et tout} \quad j,\ 1 \leqq j \leqq n.$$

Donc, $(x-\alpha)^2 - f(x)^2 = p^2 + q^2$ pour deux fonctions convenables, p et q, de $\underline{\underline{R}}(X)$. Pour $\alpha \in \underline{\underline{R}}$, $f,g \in F$ introduisons la formule

$$\varphi(\alpha,f,g): \exists p,q \in F \ ((g-\alpha)^2 - f^2 = p^2 + q^2).$$

La définition de $\underline{\underline{N}}$ se fait comme suit:

$$\beta \in \underline{\underline{N}} \Leftrightarrow \beta \in \underline{\underline{R}}^+ \wedge (\exists f \neq 0(\varphi(0,f,x) \wedge \forall \alpha \in \underline{\underline{R}}^+(\varphi(\alpha,f,x)$$

$$\rightarrow \alpha^t = \beta \vee \exists \gamma \in \underline{\underline{R}}^+ (\gamma^t = 1 + \alpha^t) \wedge \varphi(\gamma,f,x).$$

Vérifions d'abord " $\Rightarrow$ ": Si $\beta = n \in \underline{\underline{N}}$ prenons pour la fraction construit plus haut avec $j = n+1$ et $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = 2^{1/t},..,\alpha_{n+1} = n^{1/t}$. Alors, il est clair que f satisfait à la condition désirée.

Pour vérifier l'implication réciproque " $\Leftarrow$ " supposons $\beta \notin \underline{\underline{N}}$. Dans ce cas, il n'existe pas une fonction f satisfaisant à la condition ci-dessus, parce que l'ensemble $Z(f)$ devait alors con-

tenir les nombres $0, 1, 2^{1/t},..,n^{1/t},..$, dont l'exposant de convergence est $t > \rho$.

Finalement, un argument de Robinson (11) montre que $\underline{\underline{N}}$ est définissable sans paramètre.

Par une modification de la démonstration du théorème 2.2, et en utilisant un argument de (9) on obtient

Théorème 2.3. Il existe une formule qui définit $\underline{\underline{N}}$ dans chaque corps F intermédiaire entre $K(X)$ et $M_1(K)$, où K est un sous-corps pythagoricien quelconque de $\underline{\underline{R}}$.

Remarque 2.4. En utilisant des arguments de Becker, Henson, Rubel (2) et Delon (4) on déduit par une modification de la démonstration du théorème 2.2 que l'arithmétique du second ordre est interprétable dans la théorie élémentaire des corps $M_\rho(\underline{\underline{R}})$, $0 < \rho \leq \infty$, et $M(\underline{\underline{R}})$.

C'est une question ouverte (et vraisemblablement assez délicate) de savoir si E ou $E(\underline{\underline{R}})$ sont définissables dans leur corps des fractions. Dans cet ordre d'idées nous n'avons que des résultats fragmentaires.

Théorème 2.5. Soit F un des corps $M_\rho(\underline{\underline{R}})$, $1 < \rho < \infty$, $\overline{M}_\rho(\underline{\underline{R}})$, $1 \leq \rho < \infty$, ou $M(\underline{\underline{R}})$. Alors le sous-anneau A de F formé de toutes les fonctions $f \in F$ telles que $f_{res,\underline{\underline{R}}}$ soit une fonction continue de $\underline{\underline{R}}$ dans $\underline{\underline{R}}$ (c.-à-d. f n'a pas de pôles réels) est définissable (sans paramètre) dans F par une formule qui ne dépend pas de ρ.

Pour la démonstration nous aurons besoin du résultat suivant

Proposition 2.6. Retenons les notations du théorème 2.5, et soit S l'ensemble des fonctions $f \in F$, dont la restriction à $\underline{\underline{R}}$ est une fonction monotone ayant tout nombre réel comme valeur avec la multiplicité 1. Alors S est définissable dans F.

Puisque $\underline{\underline{R}}$ est définissable dans F il en est de même des sous-ensemble suivants:

$$P = \{f \mid \exists\ p_1, p_2 \in F,\ f = p_1^2 + p_2^2\}$$

$$A = \{f \mid \forall\ a,b \in \underline{\underline{R}},\ a \neq b,\ (f-a)(f-b) \notin P\}$$

$$B = \{f \mid f \in A \wedge (\forall g \in F,\ g \notin P, -g \notin P,\ 1-g^2 \in P)\ \exists \alpha,\ c \in \underline{R}$$

$$c(f-\alpha)^2 - g^2 \in P\}$$

Pour chaque $f \in A$ l'image $f(\underline{\underline{R}})$ est manifestement un sous-ensemble dense de $\underline{\underline{R}}$. Nous affirmons que $S = B$.

Si $g \notin P, -g \notin P$ et $1-g^2 \in P$ la fonction g a un zero réel β. Si $f \in S$, on a l'inégalité $(g(x))^2 \leqq c(f(x) - f(\beta))^2$ pour tout nombre réel x et un nombre positif c convenable. Par conséquent, $c(f(x) - f(\beta))^2 - (g(x))^2 \in P$. Ceci montre l'inclusion $S \subseteqq B$.

L'inclusion réciproque est vérifiée en trois étapes.

1. Toute fonction $f \in B$ est injective en tant que fonction de $\underline{\underline{R}}$ dans $\underline{\underline{R}}$.

Supposons que $f(x_1) = f(x_2)$ pour $x_1, x_2 \in \underline{\underline{R}}$, $x_1 \neq x_2$. La fonction $g = g(x) = \tanh(x-x_1)$ (où tanh désigne la tangente hyperbolique) appartient à $E_1(\underline{\underline{R}}) \subseteqq F$ et $g \notin P, -g \notin P, 1-g^2 \in P$. Donc, il existe deux nombres réels c et α tels que

$$(g(x))^2 \leq c(f(x) - \alpha)^2 \qquad (*)$$

pour tout nombre réel x qui n'est pas un pôle de f.

Parce que $f(\underline{\underline{R}})$ est dense dans $\underline{\underline{R}}$ il existe une suite (x_n) de nombres réels telle que $f(x_n) \to \alpha$. Puisque $(g(x))^2 \to 1$ si $|x| \to \infty$, la suite (x_n) est bornée et sans restriction on peut supposer que (x_n) a un point limite $\gamma \in \underline{\underline{R}}$; ici γ n'est pas un pôle de f et $f(\gamma) = \alpha$. De l'inégalite (*) on déduit $g(\gamma) = 0$; par conséquent $\gamma = x_1$ et $f(\gamma) = f(x_1) = f(x_2)$. En posant $x = x_2$ dans (*) on obtient la contradiction désirée.

2. Toute fonction $f \in B$ est surjective en tant que fonction de $\underline{R}$ dans $\underline{R}$.

En vertu de 1. il suffit de vérifier que f n'a pas de pôles réels. Supposons que β est un pôle réel de f ; d'après 1. β devrait alors être le seul pôle réel de f et $|\lim_{x\to\infty} f| < \infty$ et $|\lim_{x\to-\infty} f| < \infty$. Comme plus haut il devrait exister des nombres réels α et c tels que

$$(\tanh(x-\beta))^2 \leq c(f(x)-\alpha)^2 .$$

Puisque $(\tanh(x-\beta))^2 \to 1$ si $x \to \infty$ et $x \to -\infty$ il existe un nombre réel $\gamma \neq \beta$ tel que $f(\gamma) = \alpha$. On obtient une contradiction en posant $x = \gamma$.

3. Toute fonction $f \in B$ prend toute valeur dans $\underline{R}$ avec la multiplicité 1.

Si une valeur de f était prise au point $x = \beta$ avec une multiplicité > 1 l'inégalité $(\tanh(x-\beta))^2 \leq c(f(x)-\alpha)^2$ $(x \in \underline{R})$ ne serait satisfaite par aucun nombre c et $\alpha \in \underline{R}$.

Nous retournons maintenant à la démonstration du théorème 2.5.

La définition élémentaire de A dans F est la suivante:

$$A = \{g \in F \mid \forall f \in S\ \forall \alpha \in \underline{R}\ \exists \beta,\ c \in \underline{R}$$
$$(c(f-\alpha)^2 - \frac{(g-\beta)^2}{1+(g-\beta)^2} \in P)\} \qquad (\dagger)$$

Si $g \in A$ et $f \in S$ alors $\alpha = f(\gamma)$ pour un nombre $\gamma \in \underline{R}$. Pour une constante convenable $c \in \underline{R}$ on a l'inégalité

$$\frac{(g(x)-g(\gamma))^2}{1+(g(x)-g(\gamma))^2} \leq c(f(x)-\alpha)^2, \qquad x \in \underline{R}$$

et par conséquent $(\dagger)$ est satisfait avec $\beta = g(\gamma)$.

Réciproquement, supposons que g satisfait à la condition $(\dagger)$. En posant $f = x$ cette condition implique que pour tout $\alpha \in \underline{R}$ la fonction g n'a pas de pôle en α, et donc $g \in A$.

Ceci achève la démonstration du théorème 2.5.

En ce qui concerne l'inéquivalence des corps $M_\rho(\underline{\underline{R}})$, $\overline{M}_\rho(\underline{\underline{R}})$ et $M(\underline{\underline{R}})$ nous n'avons que des résultats fragmentaires.

Théorème 2.7. Le corps $M(\underline{\underline{R}})$ n'est élémentairement équivalent à aucun des corps $M_\rho(\underline{\underline{R}})$, $0 < \rho \leqq \infty$, ou $\overline{M}_\rho(\underline{\underline{R}})$, $0 \leqq \rho < \infty$.

Démonstration. Supposons que $M(\underline{\underline{R}}) \equiv F$ où $F = M_\rho(\underline{\underline{R}})$, $0 < \rho \leqq \infty$ ou $F = \overline{M}_\rho(\underline{\underline{R}})$, $0 \leqq \rho < \infty$.

La formule qui définit $\underline{\underline{N}}$ dans $M(\underline{\underline{R}})$ définit dans F un sous-ensemble ordonné N' de $\underline{\underline{R}}$ qui est $\equiv \underline{\underline{N}}$, et donc, puisque $\underline{\underline{R}}$ est archimédien, $N' = \underline{\underline{N}}$.

Si $F = M_\rho(\underline{\underline{R}})$, $1 < \rho \leqq \infty$, ou $F = \overline{M}_\rho(\underline{\underline{R}})$, $1 \leqq \rho < \infty$, l'ensemble défini dans la démonstration de la proposition 2.6 est égal à l'ensemble S des fonctions bijectives de $\underline{\underline{R}}$ dans $\underline{\underline{R}}$ telles que toute valeur réelle est prise avec la multiplicité 1.

Dans le cas $F = M_\rho(\underline{\underline{R}})$, $0 < \rho \leqq 1$ ou $F = \overline{M}_\rho(\underline{\underline{R}})$, $0 \leqq \rho < 1$ l'ensemble correspondant défini par la même formule contient manifestement les fonctions bijectives de $\underline{\underline{R}}$ dans $\underline{\underline{R}}$ pour lequelles toute valeur est prise avec la multiplicité 1.

L'énoncé

$$\Phi\colon \forall f \in \mathcal{B}\ \exists g \neq 0 (\forall n \in \underline{\underline{N}}\ \exists c \in \underline{\underline{R}}^+,\ c(f-n)^2 - \frac{g^2}{1+g^2} \in P)$$

est satisfait dans $M(\underline{\underline{R}})$.

En effet, chaque $f \in \mathcal{B}$ est une fonction continue monotone de $\underline{\underline{R}}$ dans $\underline{\underline{R}}$; la suite (a_n), $n \in \underline{\underline{N}}$, définie par $f(a_n) = n$ est une partie discrète de $\underline{\underline{R}}$ et par conséquent l'ensemble des zéros d'une fonction entière $g \in E(\underline{\underline{R}}) \subset M(\underline{\underline{R}})$. Maintenant, on vérifie aisément que la partie entre parenthèses de Φ est satisfaite par cette fonction g.

Cependant, Φ n'est satisfait dans aucun des corps F ci-dessus. Si $F = M_\rho(\underline{\underline{R}})$, $1 < \rho \leqq \infty$, ou $F = \overline{M}_\rho(\underline{\underline{R}})$, $1 \leqq \rho < \infty$, la fonction $f = f(x) = \sinh(x)$, (où sinh désigne le sinus hyperbolique) appartient à $\mathcal{B}$, mais il n'existe aucune fonction méromorphe g d'ordre fini dont l'ensemble des zéros est égal à la suite $\sinh^{-1}(n) = (\log(n + \sqrt{1+n^2}))$, $n \in \underline{\underline{N}}$, parce que l'exposant de convergence de cette suite est infini.

Si $F = M_\rho(\underline{\underline{R}})$, $0 < \rho \leqq 1$ ou $F = \overline{M}_\rho(\underline{\underline{R}})$, $0 \leqq \rho < 1$ on considère la fonction $f = x$ et on utilise le fait que la suite (n), $n \in \underline{\underline{N}}$, n'est pas l'ensemble des zéros d'une fonction méromorphe d'ordre < 1.

Remarque 2.8. On déduit facilement d'un résultat de Bauval (1) que tout corps infini K contient un sous-corps dénombrable K' tel que $K(X) \equiv K'(X)$. L'assertion correspondante pour les corps $M(K)$ n'est pas vraie: Pour tout sous-corps propre K de $\underline{\underline{R}}$ on a $M(K) \not\equiv M(\underline{\underline{R}})$. On peut distinguer $M(K)$ et $M(\underline{\underline{R}})$ en exprimant que l'ensemble B défini ci-dessus est vide si $K \subsetneq \underline{\underline{R}}$.

Bibliographie

1. A. BAUVAL, La théorie du premier ordre des anneaux de polynômes sur des corps, Thèse 3ème cycle, Univ. Paris VII, 1983.
2. J. BECKER, C.W. HENSON, L.A. RUBEL, First-order conformal invariants, Ann. of Math., 112 (1980), 123-178.
3. É. BOREL, Leçons sur les fonctions entières, Gauthier-Villars, Paris, 1921.
4. F. DELON, Indécidabilité de la théorie des anneaux de séries formelles à plusieurs indéterminées, Fund. Math., 112 (1981), 215-229.
5. O. HELMER, Divisibility properties of integral functions, Duke Math. J., 6 (1940), 38-47.
6. A. HURWITZ, Über beständig convergirende Potenzreihen mit rationalen Zahlencoefficienten und vorgeschriebenen Nullstellen, Acta Math., 14 (1890), 211-215.
7. C.U. JENSEN, Propriétés homologiques et logiques des anneaux de fonctions entières, C.R. Acad. Sci. Paris 291 (1980), 515-517.
8. C.U. JENSEN, La dimension globale de l'anneau des fonctions entières, C.R. Acad. Sci. Paris, 294 (1982), 385-386.
9. C.U. JENSEN, L'indécidabilité d'une classe de corps des fonctions méromorphes, C.R. Acad. Sci. Canada, 5 (1983), 69-74.
10. R. ROBINSON, Undecidable rings, Trans. Amer. Math. Soc., 70 (1951), 137-159.
11. R. ROBINSON, The undecidability of pure transcendental extensions of real fields, Z. Math. Logik Grundlagen Math., 10 (1964), 275-282.

12. L.A. RUBEL, Solution of Problem 6117, Amer. Math. Monthly, 85 (1978), 505-506.

13. E.C. Tichmarsch, The theory of functions, Oxford University Press, 1939.

14. J.H.M. WEDDERBURN, On matrices whose coefficients are functions of a single variable, Trans. Amer. Math. Soc., 16 (1915), 328-332.

Matematisk Institut
Universitetsparken 5
DK-2100 København Ø
DANEMARK

Notes

(1) Pour $K \subsetneq \underline{\mathbb{R}}$, l'anneau $E(K)$ est un anneau de Bézout de rang stable égal à 2 .

(2) Soit R l'anneau $E_\rho(K)$, $0 < \rho \leq \infty$, $K = \underline{\mathbb{R}}$ ou $K = \underline{\mathbb{C}}$; l'ensemble K des constantes et celui $\mathcal{L}$ des fonctions linéaires non nulles sont définissables dans R ; alors $\underline{\mathbb{N}}$ est définissable dans R par la formule en α

$$(\alpha \in K) \wedge \Big\{ (\forall u \in \mathcal{L})\ (\forall v)\ \Big[\lfloor (u \mid v) \wedge (\forall p \in K)\,((u+p \mid v) \rightarrow (u+p+1 \mid v))\rfloor \rightarrow (u+\alpha \mid v) \Big] \Big\}$$

$$\wedge \Big\{ (\exists f \in \mathcal{L})\ (\exists g \neq 0))\ (f \mid g) \wedge (\forall \gamma \in K)\ \Big[(f+\gamma \mid g) \rightarrow ((f+\gamma+1 \mid g) \vee (\gamma = \alpha)) \Big] \Big\}$$

Preuve: $\Rightarrow$ Clair (on prend $f = X$, $g = X(X+1)\ldots(X+\alpha)$).

$\Leftarrow$ Soit α vérifiant cette formule;

-pour $\rho \geq 1$, en prenant $u = X$ et v une fonction de R ayant $\underline{\mathbb{N}}$ pour ensemble de zéros, on voit que $\alpha \in \underline{\mathbb{N}}$.

-pour $\rho < 1$, supposons $\alpha \notin \underline{\mathbb{N}}$, alors il existerait $g \in R$, $g \neq 0$, ayant tous les entiers pour zéros; c'est impossible pour une fonction d'ordre 1 .

MÉMOIRES DE LA S. M. F.

HUGO VOLGER

The role of rudimentary relations in complexity theory

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 41-51

<http://www.numdam.org/item?id=MSMF_1984_2_16__41_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p. 41-51

THE ROLE OF RUDIMENTARY RELATIONS IN COMPLEXITY THEORY

Volger, Hugo

Résumé:

On étudie dans cet article les classes R et XR des relations rudimentaires et faiblement rudimentaires qui se reposent sur la relation de la concaténation bornée. On obtient RUD et XRUD, les classes correspondantes des langages, comme l'union d'une hiérarchie linéaire resp. polynômiale. Ces hiérarchies utilisent des quanteurs alternants aux longueurs bornés ou également des machines alternantes de Turing avec alternance constante. Nous allons introduire une autre description utilisant des quanteurs alternants pour des oracles. En plus on obtiendra une chaîne nouvelle des hiérarchies pour tous les niveaux exponentiels, dont l'union sera ERUD, l'analogue exponentiel de la classe RUD. Et on va montrer que ERUD est la classe E_3 des langages élémentaires.

Abstract:

We shall study the classes R resp. XR of rudimentary resp. extended rudimentary relations which are based on the relation of bounded concatenation. The associated classes RUD resp. XRUD of languages are the union of a linear - resp. polynomial time hierarchy. It can be described either by means of alternating length bounded quantifiers or by means of Turing machines with constant alternation. We shall introduce another description based on alternating quantifiers for oracle sets. Extending these results we obtain a chain of hierarchies for the iterated exponential time levels, whose union is the class ERUD, the exponential analogue of RUD. Moreover, it will be shown that ERUD coincides with the class of elementary recursive languages.

Table of contents:

0037-9484/84 03 41 11/$ 3.10/

Hugo Volger

1. Introduction:

This paper is a survey on the classes R, XR, ER of rudimentary resp. extended rudimentary resp. exponential rudimentary relations and the corresponding classes RUD, XRUD, ERUD of languages. R and XR were introduced by Smullyan in 1961 resp. Bennett in 1962 (cf.[19],[1]), whereas ER is a new class. As we shall see later, a relation is rudimentary if it is definable from the concatenation relation by means of a first order formula where all quantifiers have linear length bounds. XR resp. ER will be the polynomially resp. exponentially bounded analogue of R.

The associated classes RUD, XRUD, ERUD may be obtained as the union of certain hierarchies. In her thesis in 1975 Wrathall [27] has shown that there are length bounded quantification hierarchies which yield LH = RUD resp. PH = XRUD and have as first step NLTIME resp. NPTIME. As length bounded quantification is closely related to time bounded alternation, these hierarchies can also be described as constant alternation hierarchies for LH and PH (cf.Chandra,Stockmeyer [4],Kozen [10]).

Recently Orponen [16] has introduced a class EH as the union of an exponential time hierarchy involving oracle set quantification and having NEXPTIME as a first step. Extending his approach we are able to describe the hierarchies for LH and PH as oracle set quantification hierarchies. Moreover, we shall introduce classes $EH^{(i)}$ as the union of an analogous hierarchy involving the i-th iterate e_i of the exponential function, and we shall show that each of the three descriptions may be used. As a consequence we obtain that ERUD is the union of the classes $EH^{(i)}$ and coincides with the class of elementary recursive languages. In addition, the alternating logspace hierarchy of Chandra,Kozen and Stockmeyer [5] may be viewed as step -1 of this chain of hierarchies.

The class $EH^{(i)}$ which consists of languages requiring a constant number of alternations is contained in the class LA_i the corresponding class with a linear amount of alternation. Recently we have shown that the decision problem of the theory e_i-bounded concatenation is complete in the class LA_i w.r.t. polynomial time reductions for $i \geq 1$. In a certain sense these results for $EH^{(i)}$ and LA_i measure the power of e_i-bounded concatenation (cf.also Wilkie [24,25,26]). However, the question whether the inclusion $EH^{(i)} \subseteq LA_i$ is proper for some $i \geq 0$ remains open. A positive answer would imply that the inclusions $PH \subseteq APTIME$ and $LH \subseteq ALTIME$ are proper, thus solving important open problems in complexity theory.

2. Concatenation as a base of computability theory:

In 1946 Quine [17] suggested to use the concatenation relation rather than addition and multiplication as a base of computability theory. Thus in 1961 Smullyan [19] introduced the class R resp. R_s of rudimentary resp. strictly rudimentary relations on $\{1,2\}^*$. They consist of those relations which are definable from the concatenation relation by a first order formula where all quantifiers have a linear

bound resp. are subword quantifiers. Smullyan has shown that R_s is all we need to describe computations. Each language $L \subseteq \{1,2\}^*$ which is recursively enumerable i.e. accepted by some Turing machine M can be obtained from a relation Q in R_s as follows: $x \in L$ iff $\exists y: (x,y) \in Q$, where $(x,y) \in Q$ expresses the fact that y is an accepting computation sequence with input x. This shows that R_s is large enough to enable us to describe Turing machine computations by means of words consisting of sequences of configuration words. On the other hand R_s is quite small since the associated class RUD_s of languages is contained in LOGSPACE and does not contain $\{1^n 2^n : n \in N\}$ (cf. Nepomnjascii [15], Meloul [11]). In addition, the NPTIME-complete problem SAT(x) is of the form $\exists y: |y| \leq |x| \wedge Q(x,y)$ with Q in R_s as Meloul [11] has shown. This may explain why the class R_s and the related classes R and XR play an important role in complexity theory.

3. The rudimentary relations:

The class R resp. R_s of rudimentary resp. strictly rudimentary relations on $\{1,2\}^*$, introduced by Smullyan [19], is defined as the least class of relations which contains the concatenation relation Con and which is closed under the boolean operations, explicit transformations and linearly bounded resp. subword quantification. The class R^+ of positive rudimentary relations on $\{1,2\}^*$, introduced by Bennett [1], is defined as the least class of relations which contains the relation Con and which is closed under finite unions and intersections, explicit transformations, subword quantification and linearly bounded existential quantification.

$\exists y: y \subseteq x \wedge \ldots$, $\forall y: y \subseteq x \rightarrow \ldots$ subword quantification

$\exists y: |y| \leq k|x| \wedge \ldots$, $\forall y: |y| \leq k|x| \rightarrow \ldots$ linearly bounded quantification

Using the k-adic encoding words over $\{1,\ldots,k\}$ may be identified with natural numbers. Bennett [1] has shown that modulo the dyadic encoding R coincides with the class CA of constructive arithmetic relations on N, which is the analogue of R on N using + and × rather than Con. In addition, CA coincides with the class of bounded arithmetic relations of Harrow [6]. Moreover, the analogues of R resp. R_s resp. R^+ on $\{1,\ldots,k\}^*$ coincide with R resp. R_s resp. R^+ on $\{1,2\}^*$ modulo the k-adic encoding and the dyadic decoding. Using the sequential encoding $\theta(Q)$ of a relation Q one obtains the corresponding classes of languages on $\{1,2,\S\}$: RUD, RUD_s, RUD^+. It can be shown that these classes may be identified with the unary relations in R, R_s, R^+.

Replacing linearly bounded quantification by polynomially bounded quantification (i.e. $\exists y: |y| \leq |x|^k \wedge \ldots$ and $\forall y: |y| \leq |x|^k \rightarrow \ldots$) one obtains the classes of extended rudimentary resp. extended positive rudimentary relations, which were introduced by Bennett [1].

Going a step further we introduce the classes ER resp. ER^+ of exponential rudimentary resp. exponential positive rudimentary relations. They are obtained from

R resp. R^+ by replacing linearly bounded quantification by exponentially bounded quantification (i.e. $\exists y: |y| \leq e_1(|x|^k) \wedge \ldots$ and $\forall y: |y| \leq e_1(|x|^k) \rightarrow \ldots$ with $e_1(n) = 2^n$). Clearly, iterated exponential functions can be used as length bounds as well. - The corresponding classes of languages are denoted by XRUD, $XRUD^+$ resp. ERUD, $ERUD^+$. These classes are related as follows: $RUD_s \subseteq RUD^+ \subseteq RUD$, $XRUD^+ \subseteq XRUD$, $ERUD^+ \subseteq ERUD$ and $RUD^+ \subseteq XRUD^+ \subseteq ERUD^+$, $RUD \subseteq XRUD \subseteq ERUD$.

It should be mentioned that Jones [8] has introduced sublinear analogues of the class R resp. RUD. In particular, he considered a subclass RUD_{log} of LOGSPACE. It is not clear how this class fits into the above set up.

4. Turing machines with constant resp. linear alternation:

Chandra and Stockmeyer [4] and Kozen [10] have extended the concept of nondeterministic Turing machines (NTM's) to alternating Turing machines (ATM's). There is a close connection between alternation and quantification. In particular, hierarchies defined by bounded quantification are closely related to hierarchies defined by constant alternation using the same time bound.

An ATM M is a NTM which has 2 disjoint sets of states, the existential and universal states, and a distinguished accepting resp. rejecting state. Configurations and their successor relation are defined as for NTM's. An input w is accepted by M (i.e. $w \in L(M)$), if there exists a finite accepting subtree B of the computation tree of M for w. B is accepting, if (1) the root of B is labeled with the input configuration for w, (2) all leaves of B are labeled with accepting configurations, (3) if a node b of B is labeled with an existential (resp. universal) configuration C then at least one (resp. all) successor configurations C' of C must appear as labels of successors b' of b (cf. Berman [2]).

A language L belongs to the alternation class STA(s,t,a), if L is accepted by an ATM M such that each w in L posesses an accepting subtree B of depth $\leq t(n)$ and alternation depth $\leq a(n)$ and each configuration in B uses space $\leq s(n)$, where $n=|w|$. We shall use the notation $STA_\exists(s,t,a)$ resp. $STA_\forall(s,t,a)$ to indicate that the input configuration is required to be existential resp. universal. As special cases we obtain the alternating time class $ATIME(t) = STA(-,t,-)$ and the alternating space class $ASPACE(s) = STA(s,-,-)$. The time class with constant alternation CATIME(t) is defined as $\cup\langle STA_\exists(-,t,k): k \in N\rangle$. Similarly the time class with linear alternation LATIME(t) is defined as $STA_\exists(-,t,id)$.

Alternating time bridges the gap between nondeterministic time and deterministic space as Chandra, Kozen and Stockmeyer [5] have shown:

(*) $NTIME(t) \subseteq CATIME(t) \subseteq LATIME(t) \subseteq ATIME(t) \subseteq DSPACE(t)$ for $t \geq id$

(**) $ALOGSPACE = PTIME$, $APTIME = PSPACE$, $APSPACE = EXPTIME$

5.The linear - and polynomial time hierarchies:

Wrathall [27] has shown that the class XRUD is the union of the polynomial time hierarchy of Meyer and Stockmeyer [12], and that the class RUD is the union of a linear time analogue of this hierarchy. There are several descriptions of these two hierarchies as we shall see below.

Constant Alternation:

$APH = U\langle AP_k : k \in N\rangle$, $AP_k = U\langle STA_{\exists}(-, O(n^i), k) : i \in N\rangle$ for $k \geq 1$, $AP_0 = PTIME$,

$ALH = U\langle AL_k : k \in N\rangle$, $AL_k = STA_{\exists}(-, O(n), k)$ for $k \geq 1$, $AL_0 = LTIME$.

Hence we have $APH = U\langle CATIME(O(n^i)) : i \in N\rangle$, $ALH = CATIME(O(n))$

Length Bounded Quantification:

$PH = U\langle P\Sigma_k : k \in N\rangle$, $P\Sigma_0 = PTIME$,

$L \in P\Sigma_k$ iff there exists $L' \in P\Sigma_0$ and $m_1, \ldots, m_k$ such that:

$$x \in L \text{ iff } \exists y_1 : |y_1| \leq |x|^{m_1} \ldots Q_k y_k : |y_k| \leq |x|^{m_k} : (x, y_1, \ldots, y_k) \in L' .$$

$LH = U\langle L\Sigma_k : k \in N\rangle$, $L\Sigma_0 = LTIME$,

$L \in L\Sigma_k$ iff there exist $L' \in L\Sigma_0$ and $m_1, \ldots, m_k$ such that:

$$x \in L \text{ iff } \exists y_1 : |y_1| \leq m_1|x| \ldots Q_k y_k : |y_k| \leq m_k|x| : (x, y_1, \ldots, y_k) \in L' .$$

Oracle Set Quantification:

$OPH = U\langle OP_k : k \in N\rangle$, $OP_0 = U\langle STA_{\exists}(\log(n^i), -, k) : i, k \in N\rangle$,

$L \in OP_k$ iff there exists a constant alternation oracle TM $\underline{M}$ with k oracles working in space $\log(n^i)$ for some i such that:

$$x \in L \text{ iff } \exists A_1 \ldots Q_k A_k : \underline{M} \text{ accepts } x \text{ with the oracles } A_1, \ldots, A_k .$$

Iterated Nondeterministic Oracles:

$NP_* = U\langle NP_k : k \in N\rangle$, $NP_0 = PTIME$, $NP_{k+1} = \underline{NP}(NP_k)$,

$NL_* = U\langle NL_k : k \in N\rangle$, $NL_0 = LTIME$, $NL_{k+1} = \underline{NL}(NL_k)$,

where $\underline{NP}(\underline{A})$ resp. $\underline{NL}(\underline{A})$ is the class of languages accepted by a nondeterministic oracle TM with a polynomial resp. linear time bound and an oracle for a member of $\underline{A}$.

The following 2 propositions show that the union of these hierarchies is XRUD resp. RUD and that all descriptions yield the same hierarchies.

Prop.1: (1) $NP_k = P\Sigma_k$ for k in N ; $NP_* = PH$

(2) $PH = XRUD$; $NP_1 = NPTIME = XRUD^+$

(3) $NL_k = L\Sigma_k$ for k in N ; $NL_* = LH$

(4) $LH = RUD$; $NL_1 = NLTIME \subseteq RUD^+$

The proofs of (1) - (4) except $NL_1 \subseteq RUD^+$ can be found in Wrathall [28,29]. An application of a result of Book and Greibach [3] to the inclusion $CFL \subseteq RUD^+$ in Yu [30] yields the desired inclusion (cf.Meloul [11]).

The proof of the next proposition will be given in some detail since the result will be generalized later on.

Prop.2: (1) $AP_k = P\Sigma_k$ for k in N ; APH = PH
(2) $AL_k = L\Sigma_k$ for k in N ; ALH = LH
(3) $OP_k = AP_k$ for $k \geq 1$ in N ; $OP_0 \subseteq AP_0$; OPH = APH .

The result in (1) was mentioned in Chandra , Kozen and Stockmeyer [5] and the analogous result in (2) can be found in Volger [23] . (3) is a new result which constitutes an analogue of a result of Orponen [16] for EH , the union of an exponential time hierarchy .

(1) and (2) can be proved by the same method . Given the syntactic description of L which uses at most k alternations of length bounded quantifiers , it is easy to construct an ATM accepting L with the corresponding time bound and at most k alternations . This proves $P\Sigma_k \subseteq AP_k$ resp. $L\Sigma_k \subseteq AL_k$. - Conversely , given an ATM accepting L with at most k alternations , one constructs a deterministic TM accepting a language L' and having k additional tapes with the following property . Simulating the i-th alternation phase the machine controls the choice of moves to be simulated by reading the i-th tape as long as necessary going from left to right . Hence L can be obtained from L' by an appropriate length bounded quantification with at most k alternations , as desired . This should be compared with the incremental stack automata in Yu [30] . This proves $AP_k \subseteq P\Sigma_k$ resp. $AL_k \subseteq L\Sigma_k$.

To prove (3) we adapt Orponen's proof in [16] . The oracle free part of the constant alternation oracle TM $\underline{M}$ for L can be simulated by a DTM $\underline{M}'$ working in polynomial time because of $STA_{\exists}(\log(n^i),-,k) \subseteq ASPACE(\log(n^i)) \subseteq DTIME(O(n^j))$ for some j . This inclusion can be found in Chandra , Kozen and Stockmeyer [5] . The k quantifiers concerning the oracle sets $A_1, \ldots, A_k$ will be replaced by k alternations of an ATM $\underline{M}''$ extending $\underline{M}'$, where each branch in the j-th alternation phase corresponds to an oracle set $A_j' = A_j \wedge \{1,2\}^{\leq \log(n^1)}$. Because of the space bound of $\underline{M}$ it suffices to consider A_j' instead of A_j . Moreover , each set A_j' can be specified in n^1 steps . Thus $\underline{M}''$ works in polynomial time . This shows $OP_k \subseteq AP_k$.

Conversely , let L be accepted by a constant alternation TM $\underline{M}$ working in polynomial time . The idea is to code a computation sequence α of configurations of $\underline{M}$ by an oracle set $C(\alpha)$ which is coded characterwise . A sequence α of $d = n^1$ configurations of length n^1 is a word of length $\leq d^2$. It can be coded as follows : $C(\alpha) = \{(i,j,\alpha_{i,j}) : i,j \leq d^2\}$, where $\alpha_{i,j}$ is the j-th character in the i-th configuration of α . The indices i , j are short because of $|i|, |j| \leq 2\log(n^1)$. Given (i,j) $\alpha_{i,j}$ can be recovered from $C(\alpha)$ by at most a fixed number of queries . Since the successor relation is local , it is possible to construct a constant alternation oracle TM $\underline{M}'$ working on space $\log(n^i)$ for some i such that (u,v) is accepted by $\underline{M}'$ with oracle C iff C codes a computation sequence of $\underline{M}$ starting with u and ending with v and having no alternation except at the last step . Similarly , the input configurations and the

accepting configurations can be handled by appropriate machines. In order to express acceptance by the given ATM $\underline{M}$ note that each alternation phase i gives rise to a quantification over an oracle C_i corresponding to it. By this method one obtains a constant alternation oracle TM $\hat{\underline{M}}$ working on space $\log(n^i)$, which does the required job. It should be noted that $\hat{\underline{M}}$ can be chosen to be universal. This shows $AP_k \subseteq OP_k$.

The inclusion $OP_o = U<STA_\exists(\log(n^i),-,k):i,k \in N> \subseteq AP_o = PTIME$ follows from PTIME = ALOGSPACE which was proven in Chandra, Kozen and Stockmeyer [5].

6. A chain of exponential time hierarchies:

As mentioned above, Orponen [16] introduced a class EH as the union of an exponential time analogue of the hierarchy for APH = PH. More generally, we shall consider iterated exponential time analogues of the hierarchy for PH and obtain a chain of classes $EH^{(i)}$ whose union is the class $\tilde{E}$ of elementary recursive languages.

Let e_i be the i-th iterate of the exponential function, i.e. $e_o(n) = n$ and $e_{i+1}(n) = \exp(2, e_i(n))$, where $\exp(2,m) = 2^m$. As before there are several ways of describing the hierarchies for $EH^{(i)}$.

The constant alternation hierarchy $AEH^{(i)} = U<AE_k^{(i)}:k \in N>$ is obtained from APH by replacing everywhere $O(n^1)$ by $e_i(O(n^1))$. The length bounded quantification hierarchy $EH^{(i)} = U<E\Sigma_k^{(i)}:k \in N>$ is obtained from PH by replacing everywhere $O(n^1)$ by $e_i(O(n^1))$. The oracle set quantification hierarchy $OEH^{(i)} = U<OE_k^{(i)}:k \in N>$ is obtained from OPH by replacing everywhere the space bound $\log(n^1)$ by the time bound $e_{i-1}(O(n^1))$ and defining $OE_o^{(i)} = AE$

Orponen [16] considered the hierarchies for $AEH^{(1)}$ and $OEH^{(1)}$ and proved $AEH^{(1)} = OEH^{(1)}$. The hierarchy for $EH^{(1)}$ and all the other hierarchies for $i \geq 2$ seem to be new. In the case i = 0 we obtain the hierarchies for APH, PH and OPH discussed earlier. The following proposition extends the results in proposition 2.

Prop.3: For $i \geq 1$ we have:

(1) $AE_k^{(i)} = E\Sigma_k^{(i)}$ for k in N; $AEH^{(i)} = EH^{(i)}$

(2) $OE_k^{(i)} = AE_k^{(i)}$ for $k \geq 1$ in N; $OE_o^{(i)} \subseteq AE_o^{(i)}$; $OEH^{(i)} = AEH^{(i)}$.

This can be proved by the same method which was used to prove (1) and (3) in proposition 2. To prove $OE_o^{(i)} = AEH^{(i-1)} \subseteq AE_o^{(i)}$ we use $STA_\exists(-,e_{i-1}(O(n^1)),k) \subseteq ASPACE(e_{i-1}(O(n^1))) \subseteq DTIME(e_i(O(n^{1'})))$ proved in [5]. Moreover, an oracle set of words of length $e_{i-1}(O(n^1))$ can be specified in $e_i(O(n^{1'}))$ steps, whereas the code of a computation sequence of $e_i(O(n^1))$ configurations of length $e_i(O(n^1))$ uses words of length $\leq e_{i-1}(O(n^{1'}))$. This shows that (1) and (2) can be proved as before.

The next proposition shows that $\tilde{E}$, the class of elementary recursive languages, coincides with ERUD and that the classes $EH^{(i)}$ form a new hierarchy for $\tilde{E}$.

We shall use the following abbreviations : $LA_i = U<LATIME(e_i(O(n^l))):l \in N>$ and $AS_i = U<ASPACE(e_i(O(n^l))):l \in N>$.

Prop.4: (1) $AEH^{(i)} \subseteq LA_i \subseteq AS_i \subseteq AE_o^{(i+1)} \subseteq AEH^{(i+1)}$ for i in N

(2) $U<AE_o^{(i)}:i \in N> = U<AEH^{(i)}:i \in N> = U<LA_i:i \in N> = U<AS_i:i \in N> = \tilde{E}$

(3) For each $L \in AEH^{(i)}$ there exists $L' \in LH$ and l in N such that $x \in L$ iff $\exists y:|y| \leq e_i(O(n^l)):(x,y) \in L'$

(4) $\tilde{E} = ERUD = ERUD^+$

(5) $AEH^{(i)} \neq AEH^{(i+2)}$; $AE_o^{(i)} \neq AEH^{(i)}$ implies $AEH^{(i)} \neq AEH^{(i+1)}$.

The inclusions needed for (1) can again be found in [5] . (2) is a consequence of (1) because of the well known fact $\tilde{E} = U<AE_o^{(i)}:i \in N>$. To prove the representation result in (3) which represents elements of $EH^{(i)}$ with the help of elements of LH we show (cf.Wrathall [27] in the case i = 0) :

(*) For each $L \in STA_\exists(-,e_i(O(n^l)),k)$ there exists $L' \in STA_\exists(-,O(n),k)$ such that : $x \in L$ iff $\exists y:|y| \leq e_i(|x|^l) \wedge (x,y) \in L'$.

$L' = \{(x,y):|y| \leq e_i(|x|^l) \wedge x \in L\}$ or $\{xc^m:x \in L \wedge |xc^m| = e_i(|x|^l)\}$ will do the job .

ERUD is contained in $\tilde{E}$ since $\tilde{E}$ contains Con and has the necessary closure properties . To prove the converse note that ERUD as well as $\tilde{E}$ are closed under length bounded quantification where any e_i is used as a length bound . Then the inclusion $\tilde{E} \subseteq ERUD$ follows by an application of (3) because of $LH \subseteq LSPACE \subseteq \tilde{E}$. This proves $ERUD = \tilde{E}$. To prove the equality $ERUD^+ = \tilde{E}$ it suffices to show $DTIME(e_i(O(n^l))) \subseteq ERUD^+$ because of $U<AE_o^{(i)}:i \in N> = \tilde{E} = ERUD$. However , for each L in $DTIME(e_i(O(n^l)))$ there exists L' in LOGSPACE such that : $x \in L$ iff $\exists y:|y| \leq e_i(O(n^l)) \wedge (x,y) \in L'$. $(x,y) \in L'$ states that y is an accepting computation sequence with input x . This proves (4) . (5) follows from (1) and the well known fact $AE_o^{(i)} \neq AE_o^{(i+1)}$.

It should be mentioned that the representation result in (3) can be used to lift equalities between complexity classes at the linear time level to higher levels, e.g. LH = LSPACE implies $EH^{(i)} = U<DSPACE(e_i(O(n^l))):l \in N>$.

7.Two logspace hierarchies:

In [5] Chandra , Kozen and Stockmeyer considered indexing ATM's , a variant of the ATM's which permits the use of sublinear time bounds . An indexing ATM has an index tape whose content may be interpreted as position of the input which can be accessed. Let $e_{-1}(n)$ be log(n) . The two logspace hierarchies defined below might both be considered as step -1 of the chain of hierarchies discussed earlier . The first hierarchy was introduced in [5] .

$\overline{AEH}^{(-1)} = U<\overline{AE}_k^{(-1)}:k \in N>$, $\overline{AE}_o^{(-1)} = LOGSPACE$, $\overline{AE}_k^{(-1)} = U<STA_\exists(\log(n^i),-,k):i \in N>$

$AEH^{(-1)} = U<AE_k^{(-1)}:k \in N>$, $AE_o^{(-1)} = LOGTIME$, $AE_k^{(-1)} = U<STA_\exists(-,\log(n^i),k):i \in N>$

We obtain another description of these logspace hierarchies if we replace in the definition of PH the bounds $O(n^1)$ by $\log(n^1)$ and PTIME by LOGSPACE resp. LOGTIME. This yields the hierarchies $\overline{EH}^{(-1)} = U\langle \overline{E\Sigma}_k^{(-1)} : k \in N\rangle$ and $EH^{(-1)} = U\langle E\Sigma_k^{(-1)} : k \in N\rangle$.

The following proposition shows that $\overline{AEH}^{(-1)}$ is contained in the class RUD = LH whereas $AEH^{(-1)}$ contains the class RUD_{log} of Jones [8]:

Prop.5: (1) $RUD_s \subseteq LOGSPACE \subseteq \overline{AEH}_1^{(-1)} \subseteq RUD^+$, $\overline{AEH}^{(-1)} \subseteq RUD$

(2) $\overline{AE}_k^{(-1)} = \overline{E\Sigma}_k^{(-1)}$ for k in N , $\overline{AEH}^{(-1)} = \overline{EH}^{(-1)}$

(3) $RUD_{log} \subseteq AEH^{(-1)} \subseteq LOGSPACE$

(4) $AE_k^{(-1)} = E\Sigma_k^{(-1)}$ for k in N , $AEH^{(-1)} = EH^{(-1)}$

(1) was proved in Volger [23]. (3) follows since $AEH^{(-1)}$ has the closure properties of RUD_{log}. (2) and (4) can be proved as (1) resp. (2) in proposition 2.

8. The theories of bounded concatenation:

The question whether linear alternation is more powerful than constant alternation, i.e. whether the inclusions $CATIME(e_i) \subseteq LATIME(e_i)$ and $EH^{(i)} \subseteq LA_i$ are proper, remains open. The classes $LA_i = U\,STA(\,,e_i(O(n^1)),n) : 1 \in N\rangle$ are closely related to the theories of bounded concatenation. They were introduced by A.R.Meyer in 1975 (cf. [22]) as a uniform method for proving lower bounds for the complexity of first order theories.

The t-bounded concatenation relation Con_t for a given function $t:N \to N$ is defined as follows: $(u,v,w,x) \in Con_t$ iff $uv = w \wedge |w| \leq t(|x|)$. $BCT(\{1,2\}|t)$, the theory of t-bounded concatenation, is the theory $Th((\{1,2\}^*, Con_t, 1, 2))$. Viewed in this context the equality $AEH^{(i)} = EH^{(i)}$ implies that each L in $AEH^{(i)}$ is first order definable in the structure $(\{1,2\}^*, Con_t, 1, 2)$. Recently, we have proved a completeness result for the classes LA_i which in some sense measures the power of bounded concatenation (cf.[22]).

Prop.6: (1) for all L in $EH^{(i)}$ there is a uniform polynomial time reduction to the decision problem of $BCT(\{1,2\}|e_i)$.

(2) For each L in LA_i there is a polynomial time reduction to the decision problem of $BCT(\{1,2\}|e_i)$.

(3) The decision problem of $BCT(\{1,2\}|e_i)$ belongs to LA_i, whenever $i \geq 1$. In the case $i = 0$ i.e. $LA_0 = ATIME(O(n))$ the problem remains open.

9. Conclusion:

The results presented in this paper show that the bounded concatenation relation as well as the different classes of rudimentary languages which are based on it play an important role in that part of complexity theory concerned with the classes LOGSPACE, PTIME, NPTIME etc.. There is also a close connection with time classes

with constant resp. linear alternation which should be studied in more detail.

10. References:

[1] Bennett,J.H.: On spectra, Ph.D.Thesis, Princeton Univ.,Princeton N.J. 1962, 135 pp.

[2] Berman,L.: The complexity of logical theories, Theoret.Comp.Sci.11(1980), 71-77

[3] Book,R.,Greibach,S.: Quasirealtime languages, Math.Systems Theory 4(1970), 97-111

[4] Chandra,A.K.,Stockmeyer,L.J.: Alternation, in: Proc.17th IEEE Symp.Found. of Comp.Sci.(1976), 98-108

[5] Chandra,A.K.,Kozen,D.C.,Stockmeyer,L.J.: Alternation, J.ACM 28(1981), 114-133

[6] Harrow,K.: The bounded arithmetic hierarchy, Information and Control 36(1978), 102-117

[7] Jones,N.D.: Context-free languages and rudimentary attributes, Math.Systems Theory 3(1969), 102-109, 11(1977/8), 379-380

[8] Jones,N.D.: Space-bounded reducibility among combinatorial problems, J.Comp. System Sci.11(1975), 68-85, 15(1977), 241

[9] King,K.N.,Wrathall,C.: Stack languages and log n space, J.Comp.System Sci.17 (1978), 281-299

[10] Kozen,D.C.: On parallelism in Turing machines, in: Proc.17th IEEE Symp.Found. of Comp.Sci.(1976), 89-97

[11] Meloul,J.: Rudimentary predicates, low level complexity classes and related automata, Ph.D.Thesis, Oxford Univ.,Oxford 1979, 210 pp.

[12] Meyer,A.R.,Stockmeyer,L.J.: The equivalence problem for regular expressions with squaring requires exponential space, in: Proc.13th IEEE Symp. Switching and Automata Theory (1972), 125-129

[13] Nepomnjascii,V.A.: Rudimentary predicates and Turing computations, Soviet Math.Dokl.11(1970),1462-1465

[14] Nepomnjascii,V.A.: Rudimentary interpretation of two-tape Turing computations, Kibernetika (1970) 2, 29-35

[15] Nepomnjascii,V.A.: Examples of predicates not expressible by S-Rud formulae, Kibernetika (1978) 2, 44-46

[16] Orponen,P.: Complexity classes of alternating machines with oracles, in: Proc. 10th Coll. Automata,Languages and Programming (1983),Lecture Notes in Comp. Sci.154,Springer Verlag 1983, 573-584

[17] Quine,W.V.: Concatenation as a basis for arithmetic, J.Symb.Logic 11(1946), 105-114

[18] Simon,J.: Polynomially bounded quantification over higher types and a new hierarchy of the elementary sets, in: Non-classical Logic,Model Theory and Computability, North-Holland Publ.Comp.1977, 267-281

[19] Smullyan,R.: Theory of formal systems, Annals of Math.Studies 47, Princeton Univ.Press 1961, 147 pp.

[20] Stockmeyer,L.J.: The polynomial-time hierarchy, IBM Res.Report RC5379(1975)

[21] Stockmeyer,L.J.: The polynomial-time hierarchy, Theoret.Comp.Sci.3(1977), 1-22

[22] Volger,H.: Turing machines with linear alternation, theories of bounded concatenation and the decision problem of first order theories, Theoret.Comp.Sci. 23(1983), 333-338

[23] Volger,H.: Rudimentary relations and Turing machines with linear alternation, to appear in: Proc.Conf.Recursive Combinatorics,Münster 1983, 6 pp.

[24] Wilkie,A.J.: Applications of complexity theory to Σ_0-definability problems in arithmetic, in: Model Theory of Algebra and Arithmetic, Lecture Notes in Math. 834,Springer Verlag 1980, 363-369

[25] Wilkie,A.J.: On core structures for Peano arithmetic, in: Logic Coll.'80, North-Holland Publ.Comp. 1982, 311-314

[26] Wilkie,A.J.,Paris,J.B.: Models of arithmetic and the rudimentary sets, Bull. Math.Soc.Belg.Sér.B 33(1981), 157-169

[27] Wrathall,C.: Subrecursive predicates and automata , Ph.D.Thesis , Harvard Univ., Cambridge Mass. 1975 , 156 pp.
[28] Wrathall,C.: Complete sets and the polynomial-time hierarchy , Theoret.Comp. Sci.3(1977),23-33
[29] Wrathall,C.: Rudimentary predicates and relative computation , SIAM J.Computing 7(1978) , 194-209
[30] Yu,Y.Y.: Rudimentary relations and formal languages , Ph.D.Thesis , Univ. of California,Berkeley Cal. 1970 , 47 pp.
[31] Yu,Y.Y.: Rudimentary relations and stack languages , Math.Systems Theory 10 (1977) , 337-343

Hugo Volger
Mathematisches Institut
Universität Tübingen
Auf den Morgenstelle 10
D 7400 TÜBINGEN

MÉMOIRES DE LA S. M. F.

ALEXANDER PRESTEL

Model theory of fields : an application to positive semidefinite polynomials

Mémoires de la S. M. F. 2e série, tome 16 (1984), p. 53-65

<http://www.numdam.org/item?id=MSMF_1984_2_16__53_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p.53-65

MODEL THEORY OF FIELDS:

AN APPLICATION TO POSITIVE SEMIDEFINITE POLYNOMIALS

Alexander Prestel

Abstract: Using some model theoretic arguments, we will settle the following problem raised by E. Becker: Which polynomials $f \in \mathbb{R}[X_1,\ldots,X_n]$ can be written as a finite sum of 2m-th powers of rational functions in $X_1,\ldots,X_n$ over $\mathbb{R}$?

INTRODUCTION

From Artin's solution of Hilbert's 17-th Problem, it is clear that polynomials $f \in \mathbb{R}[X_1,\ldots,X_n]$ which can be written as a sum of squares of rational functions in $\bar{X} = (X_1,\ldots,X_n)$ over $\mathbb{R}$ are exactly the positive semidefinite ones, i.e. those satisfying $f(\bar{a}) \geq 0$ for all $\bar{a} = (a_1,\ldots,a_n) \in \mathbb{R}^n$. In view of this result, the question naturally arises under what conditions such an f can be even written as a sum of 2m-th powers of rational functions in $\bar{X}$ over $\mathbb{R}$.

Denoting for a ring R, by ΣR^s the set of finite sums of s-th powers of elements from R, the question then is: When does $f \in \Sigma\, \mathbb{R}(\bar{X})^{2m}$ hold? For odd exponents the answer is trivial, since $\mathbb{R}(\bar{X}) = \Sigma\, \mathbb{R}(\bar{X})^{2m+1}$ by a result of Joly (see [J], Théorème (2.8)).

0037-9484/84 03 53 13/$ 3.30/

We will give the following answer for homogeneous*) polynomials f :

THEOREM 1 *Let* $f \in \mathbb{R}[X_1,\ldots,X_n]$ *be homogeneous and positive semi-definite. Then* $f \in \Sigma\mathbb{R}(\bar{X})^{2m}$ *if and only if* $2m \mid \deg f$ *and* $2m \mid \operatorname{ord} f(p_1,\ldots,p_n)$ *for all polynomials* $p_1,\ldots,p_n \in \mathbb{R}[t]$ *with at least one* p_i *having a non-vanishing absolute term.*

Here ord $h(t)$ is the order of $h(t)$ at the place $t = 0$, i.e. the maximal r such that t^r divides $h(t)$. The proof of this theorem ultimately makes use of the Ax-Kochen - Ershov Theorem on the model completeness of certain classes of henselian fields.

Clearly, one is tempted to ask the corresponding question for polynomials $f \in K_o[X_1,\ldots,X_n]$ where K_o is some other formally real field. The main theorem of this note refers to a fixed archimedean ordering on K_o . Thus, in particular, if R is some *archimedean* real closed field, we will have the same situation as in Theorem 1 . All attempts to generalize this result to non-archimedean real closed fields failed, and, as it finally turned out, must fail.

In case Theorem 1 would hold for all real closed fields R and for $n = 2$, by the Compactness Theorem one could conclude that for each $d \in \mathbb{N}$, there were some formula $\varphi(a_o,\ldots,a_d)$, in the language of rings, such that for all real closed fields R we could get (after dehomogenizing)

$$R \models \varphi(a_o,\ldots,a_d) \quad \text{iff} \quad a_o+\ldots+a_dX^d \in \Sigma R(X)^{2m} .$$

Equivalently, one could find bounds N and s , depending only on d and m such that, for all $a_o,\ldots,a_d \in R$, $f = a_o+\ldots+a_dX^d \in \Sigma R(X)^{2m}$

---

*) This is no restriction of the generality.

implies

$$f = \sum_{i=1}^{N} \frac{g_i(X)^{2m}}{h_i(X)^{2m}} \quad \text{and} \quad \deg g_i \,,\ \deg h_i \leq s \,.$$

This, however, turns out to be wrong in general. Using a simple non-standard argument (i.e. an application of the Compactness Theorem), we will prove

THEOREM 2 *For all* $m \geq 2$ *and all* $n \geq 0$,

$X^{2m} + nX^2 + 1 = h^{(n)}(X)^{-2m} \sum_{i=1}^{N(n)} g_i^{(n)}(X)^{2m}$. *Moreover, if* n *tends to infinity, so does* $N(n)$ *or* $\deg h^{(n)}$.

By this theorem and the remarks above, Theorem 1 cannot hold for arbitrary real closed fields R . In fact, Theorem 2 shows that, for $m \geq 2$, the property '$f \in \Sigma R(\bar{X})^{2m}$' is not elementary in the coefficients of f . This should be seen in contrast to the case $m = 1$. In this case, $f \in \Sigma R(\bar{X})^2$ can be expressed by the formula

$$\forall a_1,\ldots,a_n \ \exists b \quad f(a_1,\ldots,a_n) = b^2 \,,$$

saying that f is positive semidefinite.

1. On Theorem 1

In [1] Becker developed a general theory of sums of $2m$-th powers in formally real fields. From this theory ([1],Satz 2.14) one obtains the following characterization: Let K be formally real. Then for any $a \in K$:

$$a \in \Sigma K^{2m} \text{ iff } \begin{cases} a \in \Sigma K^2 \text{ and } 2m \mid v(a) \text{ for all} \\ \text{valuations } v \text{ of } K \text{ with formally} \\ \text{real residue field } \bar{K}_v \,. \end{cases}$$

A valuation here and in what follows may have an arbitrary ordered abelian group Γ as group of values. By $2m|v(a)$ we then mean that there is some $b \in K$ satisfying $2m\, v(b) = v(b^{2m}) = v(a)$. Concerning the theory of valuations we refer the reader to [3] and [4].

The first lemma will be a slight generalization of the above equivalence. For its proof we need some notations and results from [1].

A subset S of K is called a preordering of level $2m$ if

(i) $S + S \subset S$, $S \cdot S \subset S$, $K^{2m} \subset S$, $-1 \notin S$.

In case $m = 1$, we obtain the usual notion of preordering (cf. [7]). A preordering S of level $2m$ is called complete if

(ii) $a^2 \in S$ implies $a \in S \cup -S$.

In what follows, complete preorderings will always be denoted by P. If $m = 1$, completeness of P just means $P \cup -P = K$. Thus in this case, P is an ordering in the usual sense. In general,

$$a \leq_P b \quad \text{iff} \quad b - a \in P$$

defines a partial ordering on K, which for level 2 is linear. By [1], Section 1, for any preordering S of level $2m$ we have

(iii) $$S = \bigcap_{S \subset P} P$$

where P ranges over complete preorderings of level $2m$. From [1], Section 2, we further obtain that for every complete preordering P of level $2m$,

(iv) $A_P = \{x \in K \mid -n \leq_P x \leq_P n \text{ for some } n \in \mathbb{N}\}$ defines a valuation ring on K such that $1 + M_P \subset P$ and $\overline{P \cap A_P}$ is an ordering (of level 2) of the residue field $\bar{K}_P$.

Here M_p denotes the maximal ideal of A_p and $\bar{a}$ the residue of a, i.e. $\bar{a} = a + M_p$.

LEMMA 1 Let P_o be an archimedean ordering of the subfield K_o of K . Then $a \in K$ belongs to $\Sigma P_o \cdot K^{2m}$ if and only if $a \in \Sigma P_o \cdot K^2$ and $2m | v(a)$ for every valuation v , real over P_o .

Let v have valuation ring A and residue field $\bar{K}$. We call v real over P_o , if $\overline{P_o \cap A}$ is an ordering of $\overline{K_o}$ which extends to some ordering of $\bar{K}$. Since P_o is archimedean, it follows that v must be trivial on K_o , i.e. $v(K_o) = \{0\}$ or, equivalently, $K_o \subset A$. Moreover, it follows that the set $\Sigma P_o \cdot K^{2m}$ of sums of $2m$-th powers with coefficients from P_o , actually is a preordering of level $2m$ on K .

Proof: First assume that $a \in \Sigma P_o \cdot K^{2m}$. Then clearly $a \in \Sigma P_o \cdot K^2$. But also $2m | v(a)$ is easily seen for valuations v , real over P_o . Indeed, for such a valuation we have

$$(v) \qquad v(\sum_i p_i x_i^2) = \min_i \{v(p_i x_i^2)\}.$$

In fact, if $v(p_1 x_1^2)$ is of minimal value, then $\sum_i (p_1 x_1^2)^{-1} (p_i x_i^2)$ belongs to A_v and yields a non-vanishing residue class in $\bar{K}_v$ by the assumption on v .Thus its value is 0 . This proves (v). Now (v) and $a = \Sigma p_i a_i^{2m}$ clearly imply $2m | v(a)$.

Next assume the conditions on the RHS of the lemma. If $a \notin \Sigma P_o \cdot K^{2m}$, then by (iii) there is a complete preordering P such that $a \notin P$. By (iv), P defines the valuation ring A_p . Let v_p denote a valuation corresponding to A_p . Note that $K_o \subset A_p$ since P_o is archimedean. Thus v_p is trivial on K_o . Moreover, $\overline{P \cap A_p}$ is an ordering of the residue field which clearly extends $\overline{P_o \cap A_p}$.

Hence we know that $2m|v_p(a)$. Let $b \in K$ be such that $v(ab^{-2m}) = 0$. Then ab^{-2m} is a unit. Since $ab^{-2m} \in \Sigma P_o \cdot K^2$, the residue class $\overline{ab^{-2m}}$ belongs to the ordering $\overline{P \cap A_p}$ of $\bar{K}$. Therefore we can find $p \in P$ such that

$$ab^{-2m} p^{-1} \in 1 + M_p .$$

Since $1 + M_p \subset P$, this implies $a \in P$, a contradiction.

q.e.d.

We will now apply Lemma 1 to the situation where P_o is an archimedean ordering of K_o and $K = K_o(X_1,\ldots,X_n)$, the field of rational functions in $\bar{X} = (X_1,\ldots,X_n)$ over K_o. By R_o we denote the real (algebraic) closure of K_o with respect to P_o. Moreover, $R_o((t))$ denotes the field of formal Laurent series

$$\rho = \sum_{i=r}^{\infty} a_i t^i \quad \text{with} \quad a_i \in R_o , \; r \in \mathbb{Z} .$$

The canonical valuation on $R_o((t))$ is denoted by ord. We have

$$\operatorname{ord}\Big(\sum_{i=r}^{\infty} a_i t^i\Big) = r \quad \text{if} \quad a_r \neq 0 .$$

If almost all coefficients a_i vanish, ρ is called a finite Laurent series.

MAIN THEOREM *With the above notations, the following are equivalent for all* $f \in K_o[\bar{X}]$:

(1) $f \in \Sigma P_o \cdot K_o(\bar{X})^{2m}$,

(2) f *is positive semidefinite over* R_o *and* $2m|\operatorname{ord} f(\rho_1,\ldots,\rho_n)$ *for all* $\rho_1,\ldots,\rho_n \in R_o((t))$,

(3) *the same as in* (2) *except that* $\rho_1,\ldots,\rho_n$ *are finite Laurent series*.

Proof: (1)⇒(2): Clearly, f is positive semidefinite over R_o. Next observe that the substitutions $x_i \to \rho_i$ define a homomorphism from $K_o[\bar{X}]$ to $R_o((t))$ which can be easily extended to some place from $K_o(\bar{X})$ to $R_o((t))$. Lifting the valuation ord from $R_o((t))$ through this place, we obtain a valuation v on $K = K_o(\bar{X})$ with residue field contained in R_o. Thus v is real over P_o. By Lemma 1 we therefore have $2m|v(f)$. From the construction of v, this implies $2m|\text{ord } f(\rho_1,\ldots,\rho_n)$.

Since (2)⇒(3) is trivial, it remains to prove (3)⇒(1), which is the main point of this theorem. From the positive semidefiniteness of f over R_o it follows by well-known arguments that $f \in \Sigma P_o \cdot K_o(\bar{X})^2$. Thus in view of Lemma 1, it remains to prove $2m|v(f)$ for every valuation v of K, real over P_o. As explained after Lemma 1, v is trivial on K_o. Thus v is a place of the function field K/K_o in the usual sense. (We may consider K_o as a subfield of $\bar{K}_v$.) Let us assume $2m \nmid v(f)$.

By the result of [6] we know that we may replace the valuation v by some other valuation v', trivial on K_o, still satisfying $2m \nmid v'(f)$, but having additional properties*) like

(a) value group of v' is $\mathbb{Z}$,

(b) residue field of v' is a subfield of $\bar{K}_v$ finitely generated over K_o.

Since v is real over P_o, the residue field $\bar{K}_v$ admits an ordering extending that of K_o. Hence the well-known theory of function fields

---

*) The proof of this 'density' theorem for places on function fields makes essential use of the Ax-Kochen - Ershov Theorem mentioned in the introduction.

over real closed fields yields a place from the residue field $\bar{K}_{v'}$ of v' to the real closure R_o of K_o with respect to P_o ; i.e. a valuation $\bar{w}$ of $\bar{K}_{v'}$, trivial on K_o, with residue field contained in R_o. The valuation $\bar{w}$ of $\bar{K}_{v'}$ can be lifted through v' to some refinement w of v'. Then, the value group $\bar{w}(\bar{K}_{v'})$ is an isolated subgroup of the value group $w(K)$, the quotient being isomorphic to $v'(K)$. Thus w is a valuation of K, trivial on K_o, with residue field contained in R_o and still satisfying $2m \nmid w(f)$. Applying once more the above mentioned result of [6], we finally obtain a valuation w', trivial on K_o, such that $2m \nmid w'(f)$ and

(a) value group of w' is $\mathbb{Z}$,

(b) residue field of w' is a subfield of $\bar{K}_w$, finitely generated over K_o.

Thus, in particular $\bar{K}_{w'}$ is contained in R_o.

We now pass from K to the completion $\hat{K}_{w'}$ of K with respect to the valuation w'. From the above properties of w' we conclude that $\hat{K}_{w'}$ and hence also K may be identified with some subfield of $R_o((t))$ such that ord induces w' on K. Hence $X_1,\ldots,X_n$ are identified with some Laurent series $\rho_1,\ldots,\rho_n \in R_o((t))$ and thus $2m \nmid \operatorname{ord} f(\rho_1,\ldots,\rho_n)$.

Finally, we observe that in the topology induced by the valuation ord on $R_o((t))$,

$$\sum_{i=r}^{\infty} a_i t^i = \lim_{s\to\infty} \sum_{i=r}^{s} a_i t^i \quad .$$

By the continuity of f and the fact that the set $\{\rho \in R_o((t)) \mid 2m \nmid \operatorname{ord} \rho\}$ is open, we may assume that $\rho_1,\ldots,\rho_n$ are finite Laurent series satisfying $2m \nmid f(\rho_1,\ldots,\rho_n)$. This contradiction to the assumptions of (3) proves (1).

q.e.d.

Proof of Theorem 1: Assume first $f \in \Sigma\, \mathbb{R}(\bar{X})^{2m}$. We may assume that f actually is a polynomial in X_1. Applying now condition (3) of the Main Theorem to $\rho_1 = a\,t$ and $\rho_n = t, \ldots, \rho_n = t$ and choosing $a \in \mathbb{R}$, such that $f(at,t,\ldots,t) \neq 0$, we conclude that $2m \mid \deg f$. Since every polynomial in t in particular is a finite Laurent series, (3) yields the necessity of the condition in Theorem 1.

Conversely, let $2m \mid \deg f = d$ and $2m \mid \operatorname{ord}(p_1,\ldots,p_n)$ for all $p_i \in \mathbb{R}[t]$ such that $\operatorname{ord} p_i = 0$ for at least one p_i. Let $\rho_1,\ldots,\rho_n$ be finite Laurent series in t. If $r = \min_i \{\operatorname{ord} \rho_i\}$, clearly all $p_i = \rho_i t^{-r}$ are polynomials, one having $\operatorname{ord} = 0$. Thus it follows from the condition in Theorem 1 that $2m \mid \operatorname{ord} f(p_1,\ldots,p_n)$. From

$$f(p_1,\ldots,p_n) = f(\rho_1 t^{-r},\ldots,\rho_n t^{-r}) = t^{-dr} f(\rho_1,\ldots,\rho_n)$$

and $2m \mid d$ we therefore conclude $2m \mid \operatorname{ord} f(\rho_1,\ldots,\rho_n)$ as asserted in (3) of the Main Theorem. Now the equivalence of (3) and (1) yields the result $f \in \Sigma\, \mathbb{R}(\bar{X})^{2m}$.

q.e.d.

It should be observed that there is no restriction in considering homogeneous polynomials only. One easily checks the following

Remark: Let $f(X_1,\ldots,X_n)$ be a polynomial of degree d over a formally real field K_o. Then $f \in \Sigma\, K_o(X_1,\ldots,X_n)^{2m}$ if and only if

$$X_o^d \cdot f\left(\frac{X_1}{X_o},\ldots,\frac{X_n}{X_o}\right) \in \Sigma\, K_o(X_o,X_1,\ldots,X_n)^{2m}.$$

The following corollary is an immediate consequence of the equivalence of the Main Theorem, observing that a polynomial $f \in \mathbb{Q}[\bar{X}]$ is positive semidefinite over $\mathbb{R}$ if it is so over $\mathbb{Q}$. With a little

more effort, this corollary can already be deduced from Lemma 1 .

COROLLARY Let $f \in \mathbb{Q}[X_1,\ldots,X_n]$. Then $f \in \Sigma\, \mathbb{R}(\bar{X})^{2m}$ if and only if $f \in \Sigma\, \mathbb{Q}(\bar{X})^{2m}$.

2. On Theorem 2

Let us now consider the case $n = 1$, i.e. $K = K_o(X)$. As before we assume that P_o is an archimedean ordering of K_o . The valuations v of K , real over P_o , are trivial on K_o . The totality of these valuations is well-known. Such a valuation is either the 'degree'-valuation of $K_o(X)$ or corresponds one-to-one to a pair consisting of an irreducible polynomial $p \in K_o[X]$ and a zero of p in R_o , the real (algebraic) closure of K_o with respect to P_o . Thus the following lemma is already a consequence of Lemma 1 .

LEMMA 2 With the notations from above, a polynomial $f \in K_o[X]$ belongs to $\Sigma\, P_o \cdot K_o(X)^{2m}$ if and only if f is positive semidefinite over R_o , $2m \mid \deg f$ and, in the factorization of f , 2m divides the exponent of every prime polynomial p having a zero in R_o .

Specializing K_o to $\mathbb{R}$ and P_o to the unique ordering of $\mathbb{R}$, we proceed to the

Proof of Theorem 2: Note first of all that the polynomial $X^{2m} + nX^2 + 1$ is positive definite, has no real zero and its degree is divisible by 2m . Hence by Lemma 2 we can find a natural number $N(n)$ and polynomials $g_i^{(n)}$, $h^{(n)} \in \mathbb{R}[X]$ $(1 \le i \le N(n))$ such that

$$X^{2m} + n X^2 + 1 = \sum_{i=1}^{N(n)} \frac{g_i^{(n)}(X)^{2m}}{h^{(n)}(X)^{2m}} \cdot$$

Assume that there are bounds N and d, independent of n, such that for all n

$$N(n) \leq N \quad \text{and} \quad \deg h^{(n)} \leq d .$$

Then we also have

$$\deg g_i^{(n)} \leq d + 1 \qquad \text{for all} \quad i \leq N(n) .$$

By this assumption, it is possible to express the phrase

$$(\forall n \in \mathbb{N})(\exists g_1,\ldots,g_N,h)(X^{2m} + nX^2 + 1)h^{2m} = \sum_{i=1}^{N} g_i^{2m}$$

by a formula φ in the first order language of fields, involving some unary predicate for $\mathbb{N}$. Thus

$$(\mathbb{R}, \mathbb{N}) \models \varphi .$$

Let $(\mathbb{R}^*, \mathbb{N}^*)$ be a proper elementary extension of $(\mathbb{R}, \mathbb{N})$. Then, as it is well-known $\mathbb{N}^*$ contains elements which are bigger than every $n \in \mathbb{N}$. Let ω be such a non-standard natural number. Since φ also holds in $(\mathbb{R}^*, \mathbb{N}^*)$, we conclude that

$$(*) \qquad X^{2m} + \omega X^2 + 1 \in \Sigma\, \mathbb{R}^*(X)^{2m} .$$

This will lead us to a contradiction.

Let v^* be a valuation on $\mathbb{R}^*$ which corresponds to the valuation ring

$$A = \{x \in \mathbb{R}^* \mid -n \leq x \leq n \quad \text{for some} \quad n \in \mathbb{N}\} .$$

Note that v^* has a formally real residue field; in fact, $\overline{\mathbb{R}}_{v^*} = \mathbb{R}$. Moreover, $v^*(\omega) < 0$ if we write the valuation additively. Now by [3],Ch.VI,§10,Proposition 1, v^* can be extended to a valuation v of $\mathbb{R}^*(X)$ by setting

$$v(a_n X^n + \ldots + a_o) = \min_i \{(v^*(a_i), i)\} \quad ,$$

where the value group is $v^*(\mathbb{R}^*) \times \mathbb{Z}$, ordered lexicographically such that the first component dominates. This extension has the same residue field as v^*, hence is a valuation of $\mathbb{R}^*(X)$ to which the condition of Lemma 1 applies. From (*) we therefore conclude

$$2m \mid v(X^{2m} + \omega X^2 + 1) = (v^*(\omega), 2) \quad .$$

This is a contradiction, since $2m$ does not divide 2 , except for $m = 1$.

q.e.d.

Using a result of Becker ([2], Theorem 2.9), we can find a bound N in Theorem 2 depending only on m . (In fact, if $m = 2$, we may take $N = 36$.) Then the assertion of Theorem 2 may be modified, saying that for this fixed N , deg $h^{(n)}$ tends to infinity, if n does.

REFERENCES

[1] BECKER, E.: Summen n-ter Potenzen in Körpern. J.reine angew. Math. 307/308 (1979), 8-30

[2] BECKER, E.: The real holomorphy ring and sums of 2n-th powers. Lecture Notes in Math. 959 (Springer, 1982), 139-181

[3] BOURBAKI, N.: Elements of mathematics, commutative algebra. Paris 1972

[4] ENDLER, O.: Valuation theory. Berlin-Heidelberg-New York 1972

[5] JOLY, R.J.: Sommes de puissance d-ièmes dans un anneau commutatif. Acta arithmetica 17 (1970), 37-114

[6] KUHLMANN, F.V. - PRESTEL, A.: On places of algebraic function fields. (To appear)

[7] PRESTEL, A.: Lectures on formally real fields. Monografías de matematica 22, IMPA, Rio de Janeiro 1975

Alexander Prestel
Fakultät für Mathematik
Universität, Postfach 5560
7750 Konstanz
West-Germany

MÉMOIRES DE LA S. M. F.

PETER H. SCHMITT

Undecidable theories of valuated abelian groups

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 67-76

<http://www.numdam.org/item?id=MSMF_1984_2_16__67_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p. 67-76

UNDECIDABLE THEORIES OF VALUATED ABELIAN GROUPS

Peter H. Schmitt - Heidelberg

INTRODUCTION

Since their first appearence in [5] valuated abelian groups have quickly developed into a popular and promising area of research in abelian group theory. For information on the goals and achievments of this theory we refer to the survey articles [4] and [2]. All we need about valuated abelian groups for the purpose of this paper will be explained in section 1 below.

We are interested in a modeltheoretic investigation of the class of valuated abelian groups. Ideally we would wish to obtain a complete classification upto elementary equivalence. Experience has shown that this problem can be attacked with hope for success only if the theory under consideration is decidable. (It is ofcourse possible to construct theories with a complete system of elementary invariants, where the question , which finite combinations of these are consistent is undecidable; but this situation is unlikely to occur for the "natural" theories arising from mathematical practise) Consequently the first step in the pursuit of our ideal goal is to ask: Is the theory of valuated abelian groups decidable ?

We consider valuated abelian groups as two-sorted structures and restrict attention to abelian groups with a p-valuation for just one prime p. The main results are:

Theorem: *The theory of p-valuated abelian groups is hereditarily undecidable.*

We will even show that the class of all p-valuated abelian groups, where the underlying group is a direct sum of copies of $\mathbb{Z}(p^9)$ is hereditarily undecidable.

Theorem: *The theory of p-valuated torsionfree abelian groups is hereditarily undecidable.*

It is possible to trace back the reasons for undecidability and arrive at classes of valuated p-groups and valuated torsionfree groups respectively for which a relative quantifier elimination procedure can be obtained (i.e. quantifiers over

0037-9484/84 03 67 10/$ 3.00/

group elements are eliminated in favor of quantifiers over the linearly ordered set of values). These results together with the accompanying decidability results will appear elsewhere.

We assume that the reader is familiar with the basic facts about undecidability, abelian groups and ordinal arithmetic. All groups considered are assumed to be abelian.

§1 P-VALUATED GROUPS

Let G be a group, p a prime.

Definition: A p-valuation on G is a mapping v from G onto a successor ordinal $\alpha+1$ satisfying the following axioms:

(V1) $v(g-h) \geq \min\{v(g), v(h)\}$

(V2) $v(pg) > v(g)$ if $v(g) < \alpha$.

(V3) $v(g) = \alpha$ iff $g = 0$

We will follow established notation and write ∞ for α, the greatest possible value. Axiom (V3) is usually not counted among the axioms for a p-valuation, but including it here gives stronger undecidability results.

A p-valuated group is a group G together with a p-valuation. A valuated group is a group with a p-valutation for every prime p.

Lemma 1.1: *Every p-valuated group (G,v) satisfies for all $g,h \in G$:*

(i) *if $v(g) < v(h)$ then $v(g+h) = v(g)$*

(ii) *if $m \in \mathbb{Z}$ is not divisible by p then $v(mg) = v(g)$.*

Proof: Easy.

Definition: A p-filtration on G is a sequence G_β, $\beta \leq \alpha$ of subgroups of G such that: (F0) $G_0 = G$

(F1) $G_\beta \supset G_\gamma$ for $\beta < \gamma \leq \alpha$

(F2) $pG_\beta \subseteq G_{\beta+1}$

(F3) $G_\alpha = \{0\}$

There is a one-one correspondence between p-filtrations and p-valuations on G.

Lemma 1.2:

(i) *If* $v:G \longrightarrow \alpha+1$ *is a p-valuation then* $G_\beta = \{g\in G : v(g)\geq\beta\}$ *defines a p-filtration on* G.

(ii) *If* G_β, $\beta\leq\alpha$ *is a p-filtration then*

$$v(g) = \begin{cases} \text{the smallest } \beta<\alpha \text{ with } g \notin G_{\beta+1}, & \text{if there exists one} \\ \infty & \text{otherwise} \end{cases}$$

defines a p-valuation .

Proof: Obvious.

Definition: The direct product (sum) of a family (G_i,v_i), $i\in I$ of p-valuated groups consists of the direct product $\prod(G_i : i\in I)$ (resp. direct sum $\Sigma(G_i : i\in I)$) of the underlying groups with the valuation v given in both cases by $v(g) = \min\{ v_i(g(i)) : i \in I\}$.

Definition : For given p-valuation v on G and integer $s \geq 1$ we denote by $v_{p,s}$ the function given by :

$$v_{p,s}(g) = \min\{ \beta : \text{there is no } h \in G \text{ such that } v(g+p^sh)\geq \beta \}$$

To make this definition work also for $g \in p^sG$ we add a new element ∞^+ on top of ∞. We thus have by definition for all $g \in G$: $g \in p^sG$ iff $v_{p,s}(g) = \infty^+$.

Let L be the two-sorted first-order language with one sort of variables denoted by $x,y,z,..$, the group variables, and the other sort of variables denoted by $\alpha,\beta,\gamma,...$, the value variables; furthermore L contains a symbol for the group operations $+,-$, a constant symbol 0 , a symbol for the order relation $\leq$ between values, a constant symbol ∞ and a symbol v for the valuation.
It is straightforward how p-valuated groups are regarded as L-structures.
Let $TV(p)$ denote the L-theory of the class of all p-valuated groups. There will certainly be models (M,v) of $TV(p)$ where the ordered set $Im(v)$ of values, while still a model of the theory of well-orderings is not a well-ordered set. These generalised p-valuated groups as we might call them will play no particular rôle in the following.

§2 THE UNDECIDABILITY RESULTS

Theorem 2.1: *TV(p) is hereditarily undecidable.*

This theorem is an obvious corollary to the following result:

Theorem 2.2: *The L-theory $T(p^9)$ of the class of p-valuated groups (G,v) with:*

(i) G is a direct sum of copies of $\mathbb{Z}(p^9)$

(ii) $card(Im(v)) \leq 28$

is hereditarily undecidable.

In the proof of theorem 2.2. we will use the following lemma :

Lemma 2.3: *The class of all groups G with two distinguished subgroups C_1, C_2 such that :*

(1) $C_2 \subsetneq C_1 \subseteq G$

(2) G is a direct sum of copies of $\mathbb{Z}(p^9)$

is hereditarily undecidable.

This lemma is obtained in turn from the following:

Lemma 2.4: *The class of all groups G satisfying $p^9G = \{0\}$ with one distinguished subgroup C is hereditarily undecidable.*

To derive lemma 2.3. from lemma 2.4. we note that any pair (G,C) with $p^9G = \{0\}$ can be interpreted as $(G/C_2, C_1/C_2)$ using a triple (G,C_1,C_2) subject to the conditions of lemma 2.3. Lemma 2.4. itself was proved in [6] with 12 in place of 9 . This latter improvement is due to W.Baur , [1] .

It seems to be an open question wether 9 is the best possible exponent in lemma 2.4.

Proof of Theorem 2.2.

Let L^* be obtained from L by adding two constant symbols γ_1, γ_2 for values and let $T^* = T(p^9) + \gamma_2 \geq \gamma_1$ .Because of $T^* \vdash \varphi(\gamma_1,\gamma_2)$ iff $T \vdash \forall\alpha,\beta(\alpha \leq \beta \longrightarrow \varphi(\alpha,\beta))$ it suffices to show that T^* is hereditarily undecidable. To achieve this we have to construct for every given triple (G,C_1,C_2) subject to the conditions of lemma 2.3. a p-valuation v on G such that

$C_j = \{g \in G : v(g) \geq \gamma_j\}$ for $j=1,2$.

Consider the following sequence H_n of subgroups of G :

$$H_n = p^n G + C_1 \quad \text{for } 0 \leq n < 9$$

$$H_{9+n} = p^n C_1 + C_2 \quad \text{for } 0 \leq n < 9$$

$$H_{18+n} = p^n C_2 \quad \text{for } 0 \leq n < 9$$

We get a p-filtration H'_n from H_n by dropping repetitions. Finally γ_1, γ_2 are chosen such that $H'_{\gamma_1} = H_9$ and $H'_{\gamma_2} = H_{18}$.

The undecidability theorem 2.2. did not use the full strenth of the language L; quantifiers over values were not used. This will change when we now consider the torsionfree case.

Theorem 2.5: *The theory T_{tf} of p-valuated torsionfree groups is hereditarily undecidable.*

We will prove the following stronger result:

Theorem 2.6: *The L-theory T^1_{tf} of the class of all p-valuated torsionfree groups (G,v) satisfying: (i) and (ii) is hereditarily undecidable .*

(i) G is divisible by any prime q , $q \neq p$.

(ii) for all $g \in G$, $g \neq 0$: $v(pg) = v(g) + 1$.

Proof: We will interpret in T^1_{tf} the theory of two equivalence relations which by [3 , p.295] is hereditarily undecidable (even finitely inseperable).

We first list the formulas needed in this interpretation. Let $s \geq 2$ be an integer fixed for the remainder of this proof.

$$\varphi_0(\alpha) = \exists x(v_{p,s}(x)=\alpha) \;\&\; "\alpha = \omega n \text{ for some } n, 0 < n < \omega"$$

$$\chi_1(\alpha,\gamma) = \varphi_0(\alpha) \;\&\; "\gamma > \omega^2 \cdot 2" \;\&\; \exists x(v_{p,s}(x)=\alpha \;\&\; v_{p,s}(px)=\gamma) \;\&\; \forall x(v_{p,s}(x)=\alpha \rightarrow v_{p,s}(px) \leq \gamma)$$

$$\varphi_1(\alpha,\beta) = \varphi_0(\alpha) \;\&\; \varphi_0(\beta) \;\&\; [\exists\gamma(\chi_1(\alpha,\gamma) \;\&\; \chi_1(\beta,\gamma)) \vee \alpha=\beta].$$

$$\chi_2(\alpha,\gamma) = \varphi_0(\alpha) \;\&\; "\omega^2 < \gamma < \omega^2 \cdot 2" \;\&\; \exists x(v_{p,s}(px)=\alpha \;\&\; v_{p,s}(p^2x)=\gamma) \;\&\; \forall x(v_{p,s}(px)=\alpha \rightarrow v_{p,s}(p^2x) \leq \gamma)$$

$$\varphi_2(\alpha,\beta) = \varphi_0(\alpha) \;\&\; \varphi_0(\beta) \;\&\; [\exists\gamma(\chi_2(\alpha,\gamma) \;\&\; \chi_2(\beta,\gamma)) \vee \alpha = \beta\,]$$

By definition of χ_i there can be for every α at most one γ with $\chi_i(\alpha,\gamma)$. Thus we see that forevery model (G,v) of T^1_{tf} φ_i^G defines an equivalence relation on φ_0^G for $i=1,2$.

Now let V be a countable set and E_1,E_2 equivalence relations on V. We shall construct a p-valuated torsionfree group (G,v) satisfying conditions (i),(ii) such that $(\varphi_0^G,\varphi_1^G,\varphi_2^G) \cong (V,E_1,E_2)$.

For this purpose let $f:V \to \omega-\{0\}$ be an injection and $\{C_{m,i} : 1 \leq m < k_i\}$ enumerations of all E_i-equivalence classes, $i = 1,2$; $k_i \leq \omega$.

As a preparation we introduce groups (G_α,v_α) for all α, $0 \leq \alpha \leq \omega^2\cdot 3$ by

$G_\alpha \cong \mathbb{Z}_p$ = the subgroup of the rationals consisting of all fractions z_0/z_1 with z_1 prime to p.

and
$$v_\alpha(z) = \begin{cases} \infty = \omega^2\cdot 3 & \text{if } z = 0 \\ \alpha + k & \text{if } z = p^k z_0/z_1 \text{ with } (p,z_0) = 1 . \end{cases}$$

Let $(G^*,v^*) = \prod_\alpha (G_\alpha,v_\alpha)$ and $(G^0,v^0) = \sum_\alpha (G_\alpha,v_\alpha)$

We observe the following easy facts:

(o) for $g \in G^*$, $g\neq 0$: $v^*(pg) = v^*(g) + 1$

(1) for $g \in G^0$ $v^0_{p,s}(g)$ is never a limit

(2) if for $g \in G^*$ $v^*(g) \geq \alpha$ and α is a limit, then for all $\gamma<\alpha$ $g(\gamma)=0$.

(3) if for $g \in G^*$ $v^*_{p,s}(g) \geq \alpha$ and α is a limit ordinal, then for all $\gamma < \alpha$ $g(\gamma) \in p^s Z_p$.

Fix $x \in V$.

Let $C_{m_i,i}$ be the E_i-equivalence class of x. We define elements $a_{x,i},b_{x,i}$ of G^* as follows:

$$a_{x,1}(\gamma) = a_{x,2}(\gamma) = \begin{cases} p & \omega\cdot(f(x)-1) \leq \gamma < \omega\cdot f(x) \\ 0 & \text{otherwise} \end{cases}$$

$$b_{x,1}(\gamma) = \begin{cases} p^{s-1} & \omega^2\cdot 2 + \omega(m_1-1) \leq \gamma < \omega^2\cdot 2 + \omega\cdot m_1 \\ 0 & \text{otherwise} \end{cases}$$

$$b_{x,2}(\gamma) = \begin{cases} p^{s-2} & \text{if } \omega^2 + \omega(m_2-1) \leq \gamma < \omega^2 + \omega\cdot m_2 \\ 0 & \text{otherwise} \end{cases}$$

Let $G_{(x,i)}$ be the $\mathbb{Z}_p$-submodule of G^* generated by $G^0 \cup \{ a_{x,i}, b_{x,i}\}$ and $v^{(x,i)}$ the restriction of v^* to $G_{(x,i)}$.

The following properties of these groups are easily verified:

(4) If for $g \in G_{(x,1)}$ $v_{p,s}^{(x,1)}(g)$ is a limit ordinal, then it is equal to $\omega\cdot f(x)$ or $\omega^2\cdot 2 + \omega\cdot m_1$

(5) $v_{p,s}^{(x,1)}(p^{s-1}a_{x,1} + b_{x,1}) = \omega\cdot f(x)$

$v_{p,s}^{(x,1)}(p^s a_{x,1} + pb_{x,1}) = v_{p,s}^{(x,1)}(pb_{x,1}) = \omega^2\cdot 2 + \omega\cdot m_1$

(6) If for $g \in pG_{(x,1)}$ $v_{p,s}^{(x,1)}(g)$ is a limit , then $v_{p,s}^{(x,1)}(g) = \omega^2\cdot 2 + \omega\cdot m_1$

(7) If for $g \in G_{(x,2)}$ $v_{p,s}^{(x,2)}(g)$ is a limit ordinal then it is equal to $\omega\cdot f(x)$ or $\omega^2 + \omega\cdot m_2$.

(8) $v_{p,s}^{(x,2)}(p^{s-1}a_{x,2} + pb_{x,2}) = \omega\cdot f(x)$

$v_{p,s}^{(x,2)}(p^s a_{x,2} + p^2 b_{x,2}) = v_{p,s}^{(x,2)}(p^2 b_{x,2}) = \omega^2 + \omega\cdot m_2$.

Finally we set : $(G,v) = \bigoplus \sum_X [(G_{(x,1)}, v^{(x,1)}) \oplus (G_{(x,2)}, v^{(x,2)})]$

By definition we have :

(9) $v_{p,s}(g) = \min\{ v_{p,s}^{(x,i)}(g(x,i)) : x \in V , i=1,2 \}$

From this :

(10) $\varphi_o^G = \{\omega\cdot f(x) : x \in V \}$

We claim for all $x \in V$:

(11) If for $g \in G$ $v_{p,s}(g) = \omega\cdot f(x)$ and $V_{p,s}(pg)$ is a limit $< \infty$,then $v_{p,s}(pg) \leq \omega^2\cdot 2 + \omega\cdot m_1$ where $C_{m_1,1}$ is the E_1-equivalence class of x.

Let $g = \sum_{y\in V} \sum_{i=1,2} g(y,i)$ with $g(y,i) \in G_{(y,i)}$. By (10) $v_{p,s}(g) = \omega\cdot f(x)$ implies $v_{p,s}^{(x,i)}(g(x,i)) = \omega\cdot f(x)$ for i=1 or i=2 . Now the claim follows from (7) and (4) .

By (11) and (5) we get for $x,y \in V$:

(12) If xE_1y then $(G,V) \models \varphi_1(\omega\cdot f(x), \omega\cdot f(y))$

Furthermore we claim for all $x \in V$:

(13) If for $g \in G$ $v_{p,s}(pg) = \omega\cdot f(x)$ and $v_{p,s}(p^2g)$ is a limit $< \infty$,then $v_{p,s}(pg) \leq \omega^2 + \omega\cdot m_2$ where $C_{m_2,2}$ is the E_2-equivalence class of x.

To see this let g again be given in the form $\sum_{y\in V} \sum_{i=1,2} g(y,i)$. By (10) and (6) we must have $v_{p,s}^{(x,2)}(g(x,2)) = \omega\cdot f(x)$ which yields the desired result by (12)

By (13) and (8) we get for all $x,y \in V$:

(14) If xE_2y then $(G,v) \models \varphi_2(\omega\cdot f(x), \omega\cdot f(y))$

The reverse implications of (12) and (14) follow simply from the fact that $\chi_1(\omega\cdot f(x),\gamma)$ (resp. $\chi_2(\omega\cdot f(x),\gamma)$) implies $\gamma = \omega^2\cdot 2 + \omega\cdot m_1$ ($\gamma = \omega^2 + \omega\cdot m_2$)

Complementary to theorem 2.6. we have the following undecidability result:

Theorem 2.7. *The L-theory T^2_{tf} of the class of all p-valuated torsionfree groups (G,v) satisfying :*

(i) for all $s \geq 1$ and all $g \in G$ $v_{p,s}(g)$ is not a limit number

(ii) for all $g \in G, g\neq 0$ $v(pg) = v(g) + 1$.

is hereditarily undecidable.

The proof of Theorem 2.7. follows along the very same lines as that of the previous theorem. So we will only give a sketch.

Fix a prime number q, $q\neq p$ and an integer $s \geq 2$. Again we will interpret the theory of two equivalence relations in T^2_{tf} , this time using $v_{q,s}$ rather than $v_{p,s}$ .Since $v_{q,s}(g)$ can never by a successor ordinal $\neq \infty^+$, we have to consider higher powers of ω. We use the following formulas :

$$\varphi_0(\alpha) = \exists x(v_{q,s}(x)=\alpha) \;\&\; \text{"}\alpha = \omega^2\cdot n \text{ for some } n\text{ , } 0 < n < \omega\text{"}$$

$$\chi_1(\alpha,\gamma) = \varphi_0(\alpha) \;\&\; \text{"}\gamma > \omega^3\cdot 2\text{"} \;\&\; \exists x(v_{q,s}(x)=\alpha \;\&\; v_{q,s}(qx)=\gamma) \;\&\; \forall x(v_{q,s}(x)=\alpha \rightarrow v_{q,s}(qx) \leq \gamma))$$

$$\chi_2(\alpha,\gamma) = \varphi_0(\alpha) \;\&\; \text{"}\omega^3 < \gamma < \omega^3\cdot 2\text{"} \;\&\; \exists x(v_{q,s}(qx)=\alpha \;\&\; v_{q,s}(q^2x)=\gamma) \;\&\; \forall x(v_{q,s}(qx)=\alpha \rightarrow v_{q,s}(q^2x)\leq \gamma))$$

φ_1,φ_2 arise from φ_0, χ_1, χ_2 as in the proof of theorem 2.6.

VALUATED ABELIAN GROUPS

Given two equivalence relations E_1, E_2 on a countable set V we construct a p-valuated torsionfree group satisfying (i),(ii) such that $(\varphi_o^G, \varphi_1^G, \varphi_2^G) \simeq (V, E_1, E_2)$. For α, $0 \leq \alpha < \omega^3 \cdot 3$ we define p-valuated groups (G_α, v_α) by :

$$G_\alpha \simeq \mathbb{Z} \quad \text{for all } \alpha$$

$$v_\alpha(z) = \begin{cases} \infty = \omega^3 \cdot 3 & \text{if } z = 0 \\ \alpha + k & \text{if } z = p^k z_o \text{ with } (p, z_o) = 1 . \end{cases}$$

(G^*, v^*) , (G^o, v^o) denote the direct product , direct sum of the family (G_α, v_α) $0 \leq \alpha < \omega^3 \cdot 3$ .We observe :

(1) Let $g \in G^*$, $g \in q^s G^*$, $\alpha = \min\{ \gamma : g(\gamma) \in q^s Z\}$ and β the smallest limit ordinal $> \alpha$, then $v^*_{q,s}(g) = \beta$.

Fix $x \in V$ and let $m_1 . m_2$ be defined as in the proof of theorem 2.6. . We define elements $a_{x,i}$, $b_{x,i}$ of G^* by :

$$a_{x,1}(\gamma) = a_{x,2}(\gamma) = \begin{cases} q & \text{if } \omega^2(f(x)-1) \leq \gamma < \omega^2 \cdot f(x) \\ 0 & \text{otherwise} \end{cases}$$

$$b_{x,1}(\gamma) = \begin{cases} q^{s-1} & \text{if } \omega^3 \cdot 2 + \omega^2(m_1 - 1) \leq \gamma < \omega^3 \cdot 2 + \omega^2 \cdot m_1 \\ 0 & \text{otherwise} \end{cases}$$

$$b_{x,2}(\gamma) = \begin{cases} q^{s-2} & \text{if } \omega^3 + \omega^2(m_2 - 1) \leq \gamma < \omega^3 + \omega^2 \cdot m_2 \\ 0 & \text{otherwise} \end{cases}$$

From this data we obtain $(G_{(x,i)}, v^{(x,i)})$ and (G, v) as before. The verification that $x \to \omega^2 \cdot f(x)$ is an isomorphism from (V, E_1, E_2) onto $(\varphi_o^G, \varphi_1^G, \varphi_2^G)$ now parallels the corresponding argument in the proof of theorem 2.6.

REFERENCES

[1] Baur,W. Undecidability of the theory of abelian groups with a subgroup
Proc.AMS 55 (1976) 125-128

[2] Hunter,R. & Walker,E.
Valuated p-groups
in: Abelian group theory , Proc.Oberwolfach 1981, Spinger LN in Math. vol.874 , R.Göbel , E.Walker (eds.) pp 350-373

[3] Monk,J.D. Mathematical Logic
Graduate Texts in Mathematics , Springer Verlag , 1976

[4] Richman,F. A guide to valuated groups
in: Abelien Group Theory , Proc. 2.New Mexica State Univ.Conf. 1976 , Springer LN in Math. vol. 616 , pp 73-86

[5] Richman,F. & Walker,E.A.
Valuated abelian groups
Journal of Algebra 56 (1979) 145-167

[6] Slobodskoi,A.M. & Fridman,E.I.
Theories of abelien groups with predicates specifying a subgroup
Algebra and Logic 14 (1975) 353-355

Peter H. Schmitt
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 294
6900 Heidelberg
RFA

MÉMOIRES DE LA S. M. F.

ANNE BAUVAL

La théorie d'un anneau de polynômes

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 77-84
<http://www.numdam.org/item?id=MSMF_1984_2_16__77_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p. 77-84

LA THÉORIE D'UN ANNEAU DE POLYNOMES

Anne BAUVAL, Université de Paris 7

0. INTRODUCTION

Pour tout corps F et tout ensemble non vide I, la théorie du premier ordre de l'anneau $F[X_i]_{i\in I}$ détermine la théorie faible du second ordre de F. Avant de détailler nos résultats, dont le théorème est le principal, précisons ce que nous entendons par "théorie faible du second ordre".

DÉFINITIONS

A tout modèle $M = (A ; \mathcal{J})$ d'un langage du premier ordre L, on peut associer

- $Pf(M) = (A, Pf(A) ; \mathcal{J}, \epsilon)$, modèle du langage du premier ordre étendant L par adjonction d'une seconde sorte de variables, parcourant l'ensemble Pf(A) des parties finies de A, et d'un symbole d'appartenance ϵ,

- $Sf(M) = (A, Sf(A) ; \mathcal{J}, \epsilon, \cap)$, modèle du langage du premier ordre étendant L par adjonction d'une seconde sorte de variables, parcourant l'ensemble Sf(A) des suites finies dans A, d'un symbole d'appartenance ϵ, et d'un symbole de concaténation $\cap$,

- $Sf'(M) = (A, \mathbf{N}, Sf(A) ; \mathcal{J}, +, ., t, \ell)$, modèle du langage du premier ordre étendant L par adjonction de deux sortes de variables, l'une parcourant l'ensemble $\mathbf{N}$ des entiers naturels, l'autre parcourant Sf(A), de symboles + et . interprétés par l'addition et la multiplication dans $\mathbf{N}$, d'un symbole de fonction ℓ interprété par l'application de Sf(A) dans $\mathbf{N}$ qui à toute suite associe sa longueur, et d'un symbole de fonction t interprété par l'application de $Sf(A) \times \mathbf{N}$ dans A qui à $(S,n) = (x_0 \ldots x_{\ell(S)}, n)$ associe x_n si $n < \ell(S)$ et e si $n \geq \ell(S)$, e étant une constante fixée de M,

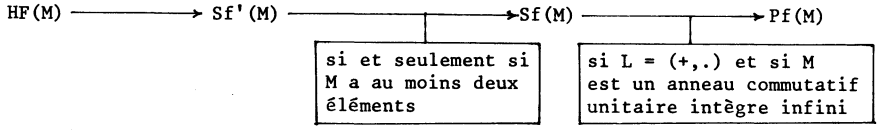
- $HF(M) = (HF(A) ; \mathcal{J}, A, \epsilon)$, modèle du langage du premier ordre étendant L par adjonction d'un prédicat unaire A et d'un symbole d'appartenance ϵ, HF(A) étant l'ensemble des ensembles héréditairement finis au-dessus de A et les éléments de A étant considérés comme atomiques.

La théorie de ce dernier modèle peut être baptisée "théorie faible du second ordre de M".

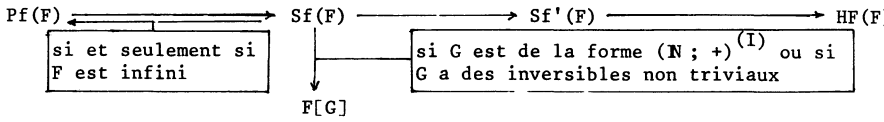
0037-9484/84 03 77 08/$ 2.80/

PRINCIPAUX RÉSULTATS

La notation "... → ..." signifiant "... est définissable dans ..., uniformément en tout modèle M de L", la séquence Pf(M) → Sf(M) → Sf'(M) → HF(M) est triviale, et réciproquement,



De plus, si L = (+,.) et si M est un corps F, ce diagramme peut être complété ainsi, les définissabilités étant uniformes en tout corps F et tout monoïde commutatif totalement ordonnable non trivial G :



ce qui généralise des résultats antérieurs ([R] § 4, [P] théorème 2.1, [Ba]).

En outre, pour tout monoïde arithmétique G, l'anneau A[G]est définissable dans HF(A), uniformément en tout anneau A, (en particulier si G est égal à la somme directe $(\mathbb{N};+)^{(I)}$ avec I au plus dénombrable ; A[G] est alors isomorphe à $A[X_i]_{i\in I}$).

Le langage de Sf peut être assimilé à un fragment de $L_{\omega_1\omega}$. La théorie faible du second ordre d'un corps ne détermine pas toujours sa théorie dans $L_{\omega_1\omega}$, car il existe des corps dénombrables non isomorphes ayant même théorie faible du second ordre ; nous montrerons même qu'il existe $2^{\aleph_0}$ corps dénombrables non isomorphes ayant même théorie faible du second ordre que $\mathbb{R}$.

Nous démontrerons enfin quelques résultats annexes sur les modèles de la théorie d'un anneau de polynômes.

Tous les résultats ci-dessus sont démontrés de façon plus détaillée dans [B2] et [B3].

THÉORIE D'UN ANNEAU DE POLYNOMES

TABLE DES MATIÈRES

I. DÉFINITION DE HF(M) DANS Sf'(M), UNIFORMEMENT EN M

Pour tout entier naturel N, soit E_N la relation binaire sur $\mathbb{N}$ définie par $m E_N n$ si et seulement si $n > N$ et le coefficient de 2^m dans l'écriture de $n - N$ en binaire est 1 ; $HF(\{1,2,\ldots,N\})$ est isomorphe à $(\mathbb{N};\{1,2,\ldots,N\},E_N)$.

Soient $(S,m) \in Sf(A) \times \mathbb{N}$, $N = \ell(S)$, et $a_1,\ldots,a_N \in A$ tels que $S = a_1 \ldots a_N$. Nous dirons que (S,m) représente un élément a de HF(A) si et seulement si $a_1,\ldots,a_N$ sont distincts et l'isomorphisme de $(\mathbb{N};\{1,\ldots,N\},E_N)$ sur $HF(\{a_1,\ldots,a_n\})$ qui envoie i sur a_i pour tout $i \in \{1,\ldots,N\}$ envoie m sur a.

L'ensemble des représentants d'éléments de HF(A), la relation liant deux représentants d'un même élément, l'ensemble des représentants d'éléments de A, et la traduction, en termes de représentants, de l'appartenance dans HF(M) et de l'interprétation $\mathfrak{I}$ dans M des symboles non logiques de L, sont définissables dans Sf'(M).

II.- DÉFINITION DE Sf'(M) DANS Sf(M), UNIFORMEMENT EN M AYANT AU MOINS DEUX ÉLÈMENTS

Si M a moins de deux éléments, Sf(M) est définissable dans $(\mathbb{N};+)$, donc sa théorie est décidable, alors que celle de Sf'(M) ne l'est jamais.

Une suite finie S dans A sera représentée dans Sf(M) par la même suite S. Un entier naturel n sera représenté par la suite ee...e (n fois) ; l'ensemble des représentants d'entiers naturels est définissable dans Sf(M).

Des formules assez compliquées permettent de définir les relations $\ell(S) = \ell(S')$ et $\ell(S) \mid \ell(S')$ dans Sf(M). On en déduit une définition dans Sf(M), en termes de représentants, de ℓ, t, +, et ..

III.- DÉFINITION DE Sf(M) DANS Pf(M), UNIFORMEMENT EN M ANNEAU COMMUTATIF UNITAIRE INTÉGRÉ INFINI

Pour tout modèle fini M, Pf(M) est fini, donc sa théorie est décidable, tandis que d'après le paragraphe précédent, celle de Sf(M) ne l'est pas, dès que M a au moins deux éléments, donc dans ce cas, non seulement Sf(M) n'est pas définissable dans Pf(M), mais sa théorie n'est même pas interprétable dans celle de Pf(M).

Un élément x de A sera représenté dans Pf(M) par le même élément x. Soit $S = a_0 a_1 \ldots a_{n-1} \in Sf(A)$ (ou $S = \emptyset$ et $n = 0$) ; nous dirons qu'un élément (y,B,C,D) de $AXPf(A)^3$ est un représentant de S si et seulement si les quatre conditions suivantes sont satisfaites :

1. $y \neq 0$, $1,y,\ldots,y^{n-1}$ sont distincts, et $B = \{1,y,\ldots,y^{n-1}\}$
2. $C = \{a_k / k \in \mathbb{N}, k < n, a_k \neq 0\}$

3. $D = \{a_k y^k / k \in \mathbb{N}, k < n, a_k \neq 0\}$

4. Pour tout entier naturel $k < n$ et pout tout $a \in C\backslash\{a_k\}$, $ay^k \notin D$.

Toute suite a une infinité de représentants.

L'ensemble des représentants d'éléments de Sf(A), la relation liant deux représentants d'une même suite, et la traduction en termes de représentants de ϵ et $\cap$ dans Sf(M) sont définissables dans Pf(M).

IV.- DÉFINITION DE Pf(F) DANS F[G], UNIFORMEMENT EN TOUT CORPS F ET TOUT MONOIDE COMMUTATIF TOTALEMENT ORDONNABLE NON TRIVIAL G

F est définissable dans F[G] par la formule $x = 0 \vee x = 1 \vee (x$ et $x - 1$ sont inversibles). On utilise un paramètre $P \in F[G]$ tel que pour tout $x \in F$, $P - x$ soit non inversible dans F[G] ; il existe de tels P, par exemple $P = g^2 + g$ avec $g \in G\backslash\{1\}$.

Un élément x de F sera représenté dans F[G] par le même élément x. Un élément non nul Q de F[G] représentera la partie finie $\{x \in F / F[G] \models P - x | Q\}$. Toute partie finie A de F a des représentants (par exemple $Q = \prod_{x \in A} (P - x)$).

La relation liant deux représentants d'une même partie finie de F et la traduction de ϵ dans Pf(F) en termes de représentants sont définissables dans F[G].

V. DÉFINITION DE Sf(F) DANS F[G], UNIFORMEMENT EN TOUT CORPS F ET TOUT MONOIDE COMMUTATIF TOTALEMENT ORDONNABLE NON TRIVIAL G QUI EST DE LA FORME $(\mathbb{N};+)^{(I)}$ OU QUI A DES INVERSIBLES NON TRIVIAUX

La propriété "F est fini" s'exprime par un énoncé dans Pf(F) donc aussi dans F[G] d'après le paragraphe précédent, uniformément en tout corps F et tout monoïde commutatif totalement ordonnable non trivial G. D'après les § III et IV, Sf(F) est définissable dans F[G], uniformément en tout corps F infini et tout monoïde commutatif totalement ordonnable non trivial G. Il reste donc à traiter le cas où F est fini et où G est de la forme $(\mathbb{N};+)^{(I)}$ ou a des inversibles non triviaux.

Pour tout corps fini F, soient N le nombre d'éléments de F, Ω_F l'ensemble des générateurs du groupe cyclique $(F\backslash\{0\}; .)$, $w \in \Omega_F$, f la bijection de $\{0,1,\ldots,N-1\}$ dans F qui à k associe 0 si $k = 0$ et w^k sinon, et $*$ l'opération sur $\{0,1,\ldots,N-1\}$ tranformée par f^{-1} de l'addition sur F.

Soit $p_0 = 2$, $p_1 = 3,\ldots$ la liste croissante des entiers naturels premiers. En représentant un élément a de F par l'entier $f^{-1}(a)$ et une suite finie $a_0 \ldots a_{n-1}$ dans F par le couple $(\prod_{k_0} f^{-1}(a_0)_{x \ldots x p_{n-1}} f^{-1}(a_{n-1}), n)$ on montre que Sf(F) est définissable dans $(\mathbb{N}; +, ., N, *)$, uniformément en tout corps fini F et tout $w \in \Omega_F$.

On peut également définir $(\mathbf{N}\ ;+,.,N,*)$ dans $F[G];+,.,w)$, uniformément en F corps fini, $w \in \Omega_F$, et G monoïde commutatif totalement ordonnable non trivial et définir Ω_F dans $(F[G];+,.)$ uniformément en F corps fini et G monoïde commutatif totalement ordonnable non trivial, grâce aux formules de R. Robinson [R] dans le cas où G est de la forme $(\mathbf{N}\ ;+)^{(I)}$, et grâce à la propriété suivante dans le cas où G a des inversibles non triviaux : pour tous I,J inversibles dans F[G] tels que $I \notin F$, $F[G] \models I - 1 \mid J - 1$ si et seulement s'il existe un entier relatif m tel que $J = I^m$.

VI.- DÉFINITION DE A[G] DANS HF(A) UNIFORMEMENT EN TOUT ANNEAU A, POUR TOUT MONOIDE ARITHMÉTIQUE G

$(\mathbf{N}\ ;+,.)$ est définissable dans HF(M), uniformément en tout modèle M, donc G est définissable dans HF(A), uniformément en tout anneau A, comme un quotient $(G'\ ;.)/\sim$.

Un élément P de A[G] sera représenté dans HF(A) par toute fonction f d'une partie finie de G' dans A telle que pour tout $g \in G$, si le coefficient de g dans P est non nul, il existe $h \in \mathrm{dom}(f)$ tel que la classe de h modulo $\sim$ soit g, et pour tout $h \in \mathrm{dom}(f)$, f(h) est égal au coefficient dans P de la classe de h modulo $\sim$.

L'ensemble des représentants d'éléments de A[G], la relation liant deux représentants d'un même élément, et la traduction de l'addition et de la multiplication dans A[G] en termes de représentants sont définissables dans HF(A).

REMARQUE.- Pour tout ensemble non vide I et pour tous corps F et F', si $F[X_i]_{i\in I} \equiv F'[X_i]_{i\in I}$, alors pour tout ensemble J, $F[X_j]_{j\in J} \equiv F'[X_j]_{j\in J}$. En effet, d'après les § I, II, V, HF(F) est définissable dans $F[X_i]_{i\in I}$, uniformément en tout corps F ; d'après le présent paragraphe, si J est fini ou dénombrable, $F[X_j]_{j\in J}$ est définissable dans HF(F), uniformément en tout corps F ; enfin, si J est infini, pour tout corps F, $F[X_j]_{j\in J} \equiv F[X_n]_{n\in\omega}$.

VII.- EXISTENCE DE $2^{\aleph_o}$ CORPS DÉNOMBRABLES NON ISOMORPHES AYANT MÊME THÉORIE FAIBLE DU SECOND ORDRE QUE $\mathbf{R}$

Nous allons construire une famille $(F_\lambda)_{\lambda<2^{\aleph_o}}$ de sous-corps dénombrables de $\mathbf{R}$, distincts et sous-structures élémentaires au sens du second ordre faible de $\mathbf{R}$, (donc réel-clos).

De tels corps sont non isomorphes, car si f est un isomorphisme entre deux sous-corps réel-clos F et F' de $\mathbf{R}$, f fixe 1, donc f fixe tout élément de $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$; de plus, f transforme tout carré en un carré donc f préserve l'ordre, et comme

$\mathbb{Q}$ est dense dans $\mathbb{R}$, f est l'identité sur F, donc F' = F.

Pour construire cette famille, nous utiliserons la propriété suivante : pour tout modèle M = (A ; $\mathcal{J}$) et pour toute sous-structure élémentaire N' de HF(M), il existe une partie B de A telle que N' = HF(B ; $\mathcal{J}_{\restriction B}$). Donc pour tout $a \in \mathbb{R}$, par le théorème de Löwenheim-Skolem descendant, il existe un sous-corps dénombrable F de $\mathbb{R}$ tel que $a \in F$ et $HF(F) \prec HF(\mathbb{R})$.

On construit la famille $(F_\lambda)_{\lambda<2^{\aleph_o}}$ par induction. Il existe un sous-corps dénombrable F_o de $\mathbb{R}$ tel que $HF(F_o) \prec HF(\mathbb{R})$. Soit μ un ordinal inférieur à $2^{\aleph_o}$ et supposons les F_λ construits pour tout $\lambda < \mu$. $\text{card}(\bigcup_{\lambda<\mu} F_\lambda) \leq (\text{card}(\mu) . \aleph_o) < 2^{\aleph_o}$, donc il existe $a \in \mathbb{R}$ tel que $a \notin \bigcup_{\lambda<\mu} F_\lambda$. On prend pour F_μ un sous-corps dénombrable de $\mathbb{R}$ contenant a et tel que $HF(F_\mu) \prec HF(\mathbb{R})$. Ainsi pour tout $\lambda < \mu$, $F_\lambda \neq F_\mu$.

VIII.- MODÈLES DE LA THÉORIE D'UN ANNEAU DE POLYNOMES

THÉORÈME.- Soit B un anneau commutatif intègre définissable dans $B[X_1,\ldots,X_n]$ par une formule Con. 1) Pour tout anneau A élémentairement équivalent à $B[X_1,\ldots,X_n]$, si B' est le sous-anneau défini dans A par Con et si $(B'^*)^{-1}A$ est factoriel ou noethérien (en particulier si A l'est), alors A est isomorphe à $B'[X_1,\ldots,X_n]$.

2) Pour tout sous-anneau élémentaire A de $B[X_1,\ldots,X_n]$, il existe $Y_1,\ldots,Y_n \in B[X_1,\ldots,X_n]$ et B' sous-anneau élémentaire de B tels que $A = B'[Y_1,\ldots,Y_n]$ et $B[X_1,\ldots,X_n] = B[Y_1,\ldots,Y_n]$.

En utilisant les formules de R. Robinson [R] et en analysant les propriétés de la fonction "degré en une indéterminée d'un polynôme", on parvient à construire des formules E_k, G_k (pour $k < n$) telles que sous les hypothèses du théorème, $B[X_1,\ldots,X_k] \models E_k(X_1,\ldots,X_k)$ et pour tous $Y_1,\ldots,Y_k \in A$ tels que $A \models E_k(Y_1,\ldots,Y_k)$, et pour tout $Q \in A$, $A \models C_k(Y_1,\ldots,Y_k,Q)$ si et seulement si $Q \in B'[Y_1,\ldots,Y_k]$, et $Y_1,\ldots,Y_k$ sont algébriquement indépendants sur B'. D'où le théorème.

COROLLAIRE.- Soient n un entier naturel non nul, et B l'un des anneaux suivants $\mathbb{Z}$, $\mathbb{Q}$, tout corps algébriquement clos de degré de transcendance fini sur son sous-corps premier, le corps des réels algébriques, ou tout corps fini.

1) Tout anneau factoriel ou noethérien élémentairement équivalent à $B[X_1,\ldots,X_n]$ est isomorphe à $B[X_1,\ldots,X_n]$.

2) $B[X_1,\ldots,X_n]$ n'a pas de sous-anneau élémentaire strict.

Pour tout ensemble non vide I, tout corps F est définissable dans $F[X_i]_{i\in I}$, et on peut définir $\mathbb{Z}$ dans $\mathbb{Z}[X_i]_{i\in I}$, car $\mathbb{N}$ est définissable par la formule sui-

vante, qui utilise les formules Pri et Pow de R. Robinson [R] :
$N(R) : \forall P \exists Q [(Pri(P) \wedge P \neq 2 \wedge P \neq 3) \rightarrow (Pow(P,Q) \wedge (P-1)^2 | Q - R(P-1) - 1)]$.
Chacun des anneaux du corollaire vérifie donc les hypothèses du théorème, et ces anneaux sont déterminés à isomorphisme près par leur théorie faible du second ordre, et n'ont pas de sous-structure élémentaire (au sens du second ordre faible) stricte, d'où le corollaire.

$0^0 0$

REFERENCES

[B1] A. BAUVAL : Une condition nécessaire d'équivalence élémentaire entre anneaux de polynômes sur des corps, C.R. Acad. Sc., Paris, t. 295 (1982), série I, pp. 31-33.

[B2] A. BAUVAL : La théorie du premier ordre des anneaux de polynômes sur des corps, thèse de 3° cycle, Université de Paris VII, 1983.

[B3] A. BAUVAL : Polynomial rings and weak second order logic, soumis au J.S.L.

[P] P.C. PAPPAS : The model theoretic structure of group rings, Ph. D. Thesis, Pennsylvania State University, 1982.

[R] R. ROBINSON : Undecidable rings, Transactions A.M.S. 1951, pp. 181-203.

Anne Bauval
Université de Paris 7
U.E.R. de Mathématiques
Tour 45-55 - 5ème étage
2, Place Jussieu
75251 PARIS CEDEX 05

MÉMOIRES DE LA S. M. F.

HELMUT WOLTER

Some results about exponential fields (survey)

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 85-94
<http://www.numdam.org/item?id=MSMF_1984_2_16__85_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p.85-94

SOME RESULTS ABOUT EXPONENTIAL FIELDS (SURVEY)

by Helmut Wolter in Berlin (G.D.R.)

Summary
In the present paper, a survey about some results from the theory of exponential fields is given. The investigations are motivated by Tarski's decidability problem of the field of real numbers with an additional exponential function. For solving Tarski's problem it seems to be useful to have more information about special exponential fields and classes of such structures. So different axiomatic classes of exponential fields and their theories are investigated. Especially, the solution of the "dominance problem" and the "problem of the last root" for exponential terms are given here.

§ 1 Introduction

In the present paper, a survey about some results from the theory of exponential fields is given. The investigations of this theory are motivated by A. Tarski's decidability problem of the field of real numbers with an additional exponential function. In recent years several people have been concerned with exponential fields and rings and obtained interesting results (see e.g. [Dr], [HR], [M], [R], [Wi], [DW1], [DW2], [Da], [Wo]), but Tarski's problem is still open and a solution is not in sight for the time being. However independent of the mentioned problem, the class of exponential fields is a very interesting subject of investigation. Only the interplay of analytical and algebraic means yields fundamental results, where the algebraic methods have often to be developed first.

0037-9484/84 03 85 10/$ 3.00/

H. Wolter

In the papers [DW1], [DW2], [Da], [Wo] B.I. Dahn and I investigated different classes of exponential fields with the intention to get more information on such structures and classes and their theories in order to give perhaps a contribution to the solution of Tarski's decidability problem. The most important results from our papers are presented here in a survey and without proofs.

Definition. If F is a field and E a unary function from F into F, then (F,E) is said to be an exponential field if for all $x,y \in F$ it holds that $E(x+y) = E(x)E(y)$ and $E(o) = 1$, $E(1) \neq 1$. In this case E is said to be an exponential function on F.

In the following let L be a language for exponential fields, i.e. L contains the usual symbols $+, -, \cdot, ^{-1}$ and an additional unary function symbol E for an exponential function. Further, let E_{ax} be the set of axioms $E(x+y) = E(x)E(y)$, $E(o) = 1$, $E(1) \neq 1$ and let EF be an $\forall$-axiom system for fields of characteristic o augmented by E_{ax}. Then EF determines the theory of exponential fields. The most important models of EF are (R,e) and (C,e), where R and C are the fields of real and complex numbers, respectively, and e is the usual exponential function in these fields.
We could also regard exponential fields of characteristic p, p a $1 = E(o) = E(px) = E(x)^p$ and finally we get $E(x) = 1$ for all x.
in the set of the p-th roots of 1.
In the following Q denotes the field of rational numbers, Z the set of integers, F an arbitrary field of characteristic o and unless stated otherwise m,n,k,l,i,j denote natural numbers. i can also be $\sqrt{-1}$, the actual meaning of i will be clear from the context. If F is an ordered field and $a,b \in F$, then $|a|$ is the absolute value of a and $a \sim b$ means that $|a-b|$ is smaller than all positive rational numbers. Notions and denotations not specially explained in this paper are used as usual.
Our aim is now to give a contribution to finding a recursive and complete axiom system of $Th(R,e)$ if such a system exists. So we try to approximate this theory by appropriate and natural axioms.

§ 2 Unordered exponential fields

First of all we want to provide some easy, well-known facts.

Fact 1. In (F,E) E is not uniquely determined by F and EF. Indeed, if f is an additive function from F into F and $E(f(1)) \neq 1$, then $E^*(x) = E(f(x))$ is an exponential function on F, too.

Fact 2. (C,e) is strongly undecidable.

The field of rationals is definable in (C,e) by the formula $\varphi(x) := \exists y \exists z(E(y) = E(z) = 1 \wedge z \neq o \wedge x = y/z)$. In fact, $(C,e) \models e^y = 1$ iff $y = 2q\pi i$, where $q \in Z$ and $i = \sqrt{-1}$. Since Q is strongly undecidable (see e.g. [Sh]), we have the claim and, moreover, we obtain

Fact 3. EF is undecidable.

The next lemma shows that the range of the exponential function in every EF-existentially complete model is the whole field, excepting o.

Lemma 4. [DW1]

Let $\mathbf{F} = (F,E)$.

(i). If $a \in F$ and $a \neq o$, then there is an extension $\mathbf{F}^* = (F^*,E^*)$ of $\mathbf{F}$ such that $\mathbf{F}^* \models EF$ and $\mathbf{F}^* \models \exists x(E^*(x) = a)$.

(ii). If $\mathbf{F}$ is EF-existentially complete, then $\mathbf{F} \models \exists x(E(x) = a)$ for all $a \in F$, $a \neq o$.

Similar as for (C,e), there exists a formula $\Psi(x)$ which defines the field of rationals in all EF-existentially complete models.

Theorem 5. [DW1]

Let $\mathbf{F} = (F,E)$ be EF-existentially complete. Then, for all $a \in F$, $a \notin Q$ iff $\mathbf{F} \models \exists x(E(x) = 1 \wedge E(ax) = 2) := \neg\Psi(a)$.

Since $\Psi(x)$ does not define Q in (C,e), we get

Corollary 6. [DW1]

(C,e) is not existentially complete.

By compactness arguments and the strong undecidability of Q we

finally obtain from the above theorem:

Corollary 7. [DW1]

(i). EF is not companionable (and hence EF has no model completion).

(ii). Every existentially complete exponential field is strongly undecidable.

Theorem 8. [DW1]

(R,e) has no existential closure, i.e. there is no EF-existentially complete extension of (R,e) that is embeddable in every existentially complete extension of (R,e).

Our results show that the theory of EF is rather complicated and since EF has models with quite different properties, EF is not a good approximation of Th(R,e). Therefore, in the following, we confine ourselves to more special classes of such fields, namely to ordered exponential fields.

§ 3 Ordered exponential fields

Now we are going to study some parts of the universal theory of the ordered field of real numbers with exponentiation.
Let OF be an $\forall$-axiom system for ordered fields and
$T = OF \cup E_{ax} \cup \{(1 + 1/n)^n \leq E(1) \leq (1 + 1/n)^{n+1} : n > 0\}$.
Since the statement $\forall x > 0 \, \forall y (E(y) = 1 + 1/x \longrightarrow E(xy) < E(1))$ is true in (R,e) but not in some non-archimedean T-models, the $\forall$-theory of T is weaker than $Th_{\forall}(R,e)$.
Hence we regard the better approximation
$OEF = OF \cup E_{ax} \cup \{E(x) \geq 1 + x\}$.
The following theorem, which can be proved by standard arguments, shows that the theory of ordered exponential fields OEF is sufficiently strong to characterize the exponential function uniquely in the standard model (R,e).

Theorem 9. [DW1]

In OEF the following formulas can be proved.

(i). $E(0) = 1$, $E(x) \geq 0$.

(ii). $x \neq 0 \longrightarrow E(x) > 1 + x$, and hence E is strictly monotonously increasing.

(iii). $x > o \wedge E(y) = 1 + 1/x \longrightarrow E(xy) < E(1) < E((x+1)y)$.

(iv). E is continuous.

(v). E is differentiable and $E'(x) = E(x)$.

Here, the derivation is defined by means of the ε-δ-technique. For proving the next results some special algebraic tools were necessary, especially we need so-called partial exponential fields. These are fields with a partial exponential function. Suitable extensions of the fields and the corresponding exponential functions finally yield

Theorem 1o. [DW1]

(i). OEF-existentially complete models are real closed fields.

(ii). In every OEF-existentially complete model the statement $\forall x > o \, \exists y(E(y) = x)$ is true, i.e. in such models E has the intermediate value property.

OEF is not sufficiently strong to prove the $\forall$-theory of (R,e).

Theroem 11. [DW1]

$OEF \not\vdash \forall x > o(E(x) \geqslant 1 + x + x^2/2)$.

On the other hand, $OEF \vdash \forall x > 1/n(E(x) \geqslant 1 + x + x^2/2)$ for all $n > o$. Now we regard a stronger axiom system OEF'.
For this let $E_k(x) = \sum_{i \leq k} x^i/i!$ and
$OEF' = OEF \cup \{E(x) \geqslant E_k(x)\colon k \text{ odd}\}$.
Similar as above, OEF'-existentially complete models are real closed fields. Furthermore, in such models the intermediate value property is true for all terms without iterated exponential function. It is an open question whether this property is true for all terms and it is also open whether OEF' proves $Th_\forall(R,e)$.

Remark. One can prove that $Th(OEF') =$
$Th(OEF \cup \{\forall x(|x| < 1/n \longrightarrow E(x) \geqslant E_k(x)\colon$ for arbitrary fixed $n > o$ and all odd $k \geqslant 3\}$.

§ 4 A method for constructing new exponential functions

Now we want to investigate how well OEF' describes the

exponential function in exponential fields. First we are going to show that in archimedean ordered OEF'-models the exponential function is uniquely determined. For this purpose let L_2 be the language L augmented by a symbol E^* for a second exponential function and $OEF'_2 = OEF'(E) \cup OEF'(E^*)$ be the union of the theories OEF' formulated with E and E^*, respectively.

Theorem 12. [DW2]
Let (F,E,E^*) be a model of OEF'_2.
(i). For all $a \in F$, if $|a|$ is bounded by some natural number, then $E(a)$, $E^*(a)$ are bounded and $E(a) \sim E^*(a)$.
(ii). If F is archimedean, then $E^* = E$.

Now we regard an arbitrary model (F,E,E^*) of OEF'_2 and investigate the connections between E and E^*. Theorem 9 implies that E, E^* are continuous, strictly monotonously increasing (hence injective), and that E, E^* take only positive but arbitrarily small and large values. Moreover, let E take all positive values in F. Then, for every $a \in F$ there is exactly one $b \in F$ such that $E^*(a) = E(b)$.
Defining $h(a) = b-a$ we obtain a function h from F into F such that $E^*(a) = E(a + h(a))$.

Lemma 13. (partially contained in [DW2])
h is additive and differentiable (hence continuous) and the derivation h' is o everywhere.

Of course, if F is non-archimedean, then h has not to be constant. Now let h be an arbitrary additive map from F into F and E an exponential function on F.
If $E^*(x) = E(x + h(x))$ and $E^*(x) \geq E_k(x)$ for all $x \in F$ and all k odd, then E^* is an exponential function on F in the sense of OEF' too.

Theorem 14. [DW2]
Let $(F,E) \models OEF' \cup \{\forall x > o\, \exists y (E(y) = x)\}$.
Then $E^*(x) = E(x + h(x))$ is an exponential function on F in the sense of OEF' if h is an additive map from F into F and h has the following properties:

(i). If $x \sim o$, then $|h(x)| < |x|^n$ for all n.
(ii). If x is finite, then $h(x) \sim o$.
(iii). If x is infinite and $x > o$, then $h(x) \geq o$ arbitrary.

Corollary 15.

(i). If OEF' has a prime model (in the sense of A. Robinson), then e^e is trancendental where e^e is $E(E(1))$ in the standard model.
(ii). There is a model (F,E) of OEF' such that $R \subseteq F$ and $E(a)$ is transcendental for each $a \in F \cap R$ with $a \neq o$.

If we regard the additive group of a non-archimedean exponential field (F,E) as a Q-vector space with a base B, then we can define, by means of Theorem 14, at least card(F) different functions $h: B \longrightarrow B$ with the desired properties. Hence, these functions h yield card(F) different exponential functions on the same field F.
By some suitable variations of a given exponential function (in the sense of Theorem 14) one can prove

Theorem 16. [DW2]
In every OEF'_2-existentially complete model the rationals are definable by the formuly
$\varphi(x) := \forall y(E(y) = E^*(y) \longrightarrow E(xy) = E^*(xy))$.

Corollary 17. [DW2]

(i). OEF'_2 is not companionable.
(ii). Every OEF'_2-existentially complete model is strongly undecidable.
(iii). The theory of all OEF'_2-existentially complete models is undecidable.
(iv). OEF'_2 is undecidable.

Now we do not regard $\forall$-axiom systems any longer, because we need stronger axioms if we want to investigate more interesting analytical properties of exponential fields.
Let OEF^* = OEF $\cup$ {Intermediate value property for terms with one variable} $\cup$ {Rolle's Theorem for terms with one variable}.
By OEF^* the inequalities $E(x) \geq E_k(x)$ can be proved if k is

odd and $k \geqslant 3$.
By means of Wilkie's and Richardson's results, B.I. Dahn was able to solve the following dominance problem for terms.

Theorem 18. [Da]
Let $\mathbf{F} \models \mathrm{OEF}$, $\mathbf{F} \subseteq \mathbf{F}^* \models \mathrm{OEF}^*$ and let $t(x)$, $t'(x)$ be terms with parameters from $\mathbf{F}$. Then
$\mathbf{F}^* \models \exists y \forall x (x \geqslant y \longrightarrow t(x) \geqslant t'(x))$ iff
$\mathrm{Diagram}(\mathbf{F}) \cup \mathrm{OEF}^* \vdash \exists y \forall x (x \geqslant y \longrightarrow t(x) \geqslant t'(x))$.

This theorem finally implies

Theorem 19. [Da]
If $\mathbf{F}$, $\mathbf{F}^* \models \mathrm{OEF}^*$, $\mathbf{F} \subseteq \mathbf{F}^*$ and $\varphi(x)$ is a quantifier-free formula with one variable and parameters from F, then
$\mathbf{F} \models \exists x \varphi(x)$ iff $\mathbf{F}^* \models \exists x \varphi(x)$.

This result is a little hint that OEF^* could be model complete.

Theorem 2o. [Da]
Let $\mathbf{F} \models \mathrm{OEF}^*$, $a \in \mathbf{F}$ and let $t(x)$ be a term with one variable and parameters from $\mathbf{F}$.
If $\mathbf{F} \models \lim_{x \to \infty} t(x) = a$, then there is a constant term t^* (with the same parameters and the same number of iteration steps of E as t) such that $\mathbf{F} \models t^* = a$.

The latter theorem implies that the limit of a term t belongs already to the exponential field generated by the parameters from t.
We now want to investigate the "Problem of the last root" for exponential terms, which is induced by the following question of A. Macintyre (see [Dr]).
Let $p(x)$ be a non-zero exponential polynomial over R.
Is there an intelligible function which depends only on the real parameters of $p(x)$ and which bounds the absolute values of the real roots of $p(x)$?
The next theorems answer this question positively not only for exponential polynomials in the standard model but also for all non-zero exponential terms with one variable in all OEF^*-models.
Let $\mathbf{F} \models \mathrm{OEF}^*$ and let T be the theory OEF^* augmented by the

diagram of $\mathbf{F}$.

Theorem 21. [Wo]

If $t(x)$ is a non-zero term with one variable and with parameters from $\mathbf{F}$, then there exists a c in $\mathbf{F}$ such that:

(i). If $\mathbf{F} \models \exists y \forall x > y(t(x) > o)$, then $T \vdash \forall x(x > c \longrightarrow t(x) > o)$.

(ii). If $\mathbf{F} \models \exists y \forall x > y(t(x) < o)$, then $T \vdash \forall x(x > c \longrightarrow t(x) < o)$.

(iii). $T \vdash \forall x(t(x) = o \longrightarrow |x| \leq c)$.

Now we want to sharpen this result in some sense.

Theorem 22. [Wo]

If $t(x)$ is a non-zero term with one variable and with parameters from $\mathbf{F}$, then one can compute a constant term t^* (depending only on the parameters of $t(x)$) such that $\mathbf{F} \models \forall x(t(x) = o \longrightarrow |x| \leq t^*)$.

Finally I want to present some problems that have arisen in discussions with B.I. Dahn and which are still open in my opinion.

1. Is $Th_\forall(OEF') = Th_\forall(R,e)$?
2. Is the intermediate value property for terms with one variable true in all OEF'-existentially complete models ?
3. Is $E(E(1)) = E^*(E^*(1))$ if (F,E), (F,E^*) are models of OEF^* ?
4. Is there a prime model (in the sense of A. Robinson) for one of the regarded theories ?
5. Is one of the theories model complete ?
6. Is $OEF' \cup \{$Intermediate value property for terms with one variable$\}$ complete (analogous to the theory of ordered fields) ?

References

[Da] Dahn, B.I., The limit behaviour of exponential terms. Preprint 48 (1982) der Sekt. Math. der Humboldt-Universität zu Berlin.

[DW1] Dahn, B.I. and H. Wolter, On the theory of exponential fields. ZML, Band 29 (1983), 465-480. Paper presented at the International Logic Colloquium at Marseille, July 1981.

[DW2] Dahn, B.I. and H. Wolter, Ordered fields with several

exponential functions. To appear in ZML.
Preprint 42 (1982) der Sekt. Math. der Humboldt-Universität zu Berlin.

[Dr] van den Dries, L., Exponential rings, exponential polynomials and exponential functions. Preprint of the Department of Mathematics, Stanford University, December 1981.

[HR] Henson, C.W. and L.A. Rubel, Some applications of Nevanlinna theory to mathematical logic: Identities of exponential functions. Preprint.

[M] Macintyre, A., The laws of exponentiation. Preprint.

[R] Richardson, D., Solution of the identity problem for integral exponential functions. ZML, Band 15 (1969), 333-340.

[Sh] Shoenfield, J.R., Mathematical Logic. Addison-Wesley, Reading, Mass. 1967.

[Wi] Wilkie, A.J., On the exponential fields. Preprint.

[Wo] Wolter, H., On the 'Problem of the last root' for exponential terms. To appear in ZML. Preprint 58 (1983) der Sekt. Math. der Humboldt-Universität zu Berlin.

Helmut Wolter
Humbolt Universität
Sektion Mathematik
1086 Berlin P.S.F. 1297
RDA

MÉMOIRES DE LA S. M. F.

FRANÇOISE DELON

Corps équivalents à leur corps de séries

Mémoires de la S. M. F. 2e série, tome 16 (1984), p. 95-103
<http://www.numdam.org/item?id=MSMF_1984_2_16__95_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p.95-103

CORPS ÉQUIVALENTS A LEUR CORPS DE SÉRIES

Françoise Delon

Les équivalences élémentaires qui suivent se réfèrent au langage $\{0,1,+,.\}$. Si K est un corps de caractéristique nulle, dès qu'on a $K \equiv K((X))$, le théorème d'Ax-Kochen-Eršov implique $K \equiv K((X_1))...((X_p))$ pour tout entier $p \geq 1$. Nous montrons ici la réciproque de ce résultat:

Théorème. Si K est un corps de caractéristique 0 et si pour un entier $p \geq 1$, on a $K((X_1))...((X_p)) \equiv K$, on a alors $K \equiv K((X))$.

On montre aussi que, sous les mêmes hypothèses, si on considère K comme corps de constantes de son corps de séries K((X)), K est existentiellement clos dans K((X)).

Des résultats de même nature et plus complets sont exposés dans [D] mais le cadre plus général y complique sensiblement les preuves; au contraire on a essayé de donner ici des démonstrations élémentaires, ne faisant appel qu'à peu de connaissances extérieures. Ainsi on n'utilise des travaux de Gurevič sur les groupes abéliens ordonnés qu'un corollaire, dont on donne une preuve directe - qui m'a été indiquée par Peter Schmitt - et on fait sur la théorie des valuations les rappels nécessaires à la compréhension de cet exposé.

1. Groupes abéliens ordonnés (g.a.o.)

Dans cette catégorie, les sous-groupes convexes jouent un rôle essentiel (une partie A d'un ordre I est convexe lorsque $a,b \in A$, $i \in I$ et $a < i < b$ impliquent $i \in A$): si H est un sous-groupe convexe d'un g.a.o. G, les classes modulo H sont convexes et sont donc naturellement ordonnées par la relation

$$x/H < y/H \text{ ssi } (x \not\equiv y \text{ (modulo H) et } x < y).$$

Si G_1 et G_2 sont deux g.a.o. on appelle produit lexicographique de G_1 et G_2 le

0037-9484/84 03 95 09/$ 2.90/

groupe produit $G_1 \times G_2$ muni de l'ordre

$$(x_1,x_2) < (y_1,y_2) \quad \text{ssi } x_1 < y_1 \quad \text{ou} \quad (x_1 = y_1 \text{ et } x_2 < y_2)$$

pour $x_1,y_1 \in G_1$ et $x_2,y_2 \in G_2$; le plongement canonique de G_2 dans le g.a.o. $G_1 \times G_2$ en fait un sous-groupe convexe et on a un isomorphisme de g.a.o. entre G_1 et $(G_1 \times G_2)/G_2$; ce produit lexicographique est associatif. Plus généralement, pour un bon ordre I et des g.a.o. G_i , $i \in I$, le produit lexicographique $\prod_{i \in I} G_i$ s'obtient en munissant le groupe produit de l'ordre

$$(x_i)_{i \in I} < (y_i)_{i \in I} \quad \text{ssi} \quad x_{i_o} < y_{i_o}$$

où i_o est le premier indice i tel que $x_i \neq y_i$; si les I_j , $j \in J$, recouvrent I, sont disjoints, convexes pour l'ordre de I et vérifient $I_j < I_{j'}$ ssi $j < j'$, alors (J et les I_j sont bien ordonnés et) on a un isomorphisme de g.a.o.

$$\prod_{i \in I} G_i \cong \prod_{j \in J} \left(\prod_{i \in I_j} G_i \right) .$$

Les sous-groupes convexes d'un produit $\prod_{i \in I} G_i$ sont les sous-groupes de la forme $\prod_{i<i_o} \{0\} \times H_{i_o} \times \prod_{i>i_o} G_i$, pour un $i_o \in I$ et un sous-groupe convexe H_{i_o} de G_{i_o} . Le produit lexicographique est un cas simple du produit de Hahn explicitement donné par Feferman et Vaught comme exemple de produit auquel s'applique leur principe de transfert d'équivalence élémentaire ([FV] exemple 4.9); en conséquence $G_i \equiv G'_i$ pour tout $i \in I$, implique $\prod_{i \in I} G_i \equiv \prod_{i \in I} G'_i$, ces équivalences étant dans le langage des groupes ordonnés.

Lemme 1.[Gu]. Soit H un sous-groupe convexe d'un g.a.o. G ; alors les g.a.o. G et $(G/H) \times H$ sont élémentairement équivalents.

Démonstration. Il est connu que, dès qu'un groupe abélien est ω_1-saturé, il est facteur direct dans toute extension où il est pur (H pur dans G signifie ici $nG \cap H = nH$ pour tout entier n), voir [Sa] ou [Sh] . Dans un g.a.o. un sous-groupe convexe est toujours pur, donc si on prend un couple $H' \subset G'$ équivalent au couple $H \subset G$ dans le langage $\{0,+,<,H\}$ et ω_1-saturé, les groupes $(G'/H') \times H'$ et G' sont isomorphes; on vérifie immédiatement que cet isomorphisme respecte aussi l'ordre si l'on munit G'/H' de l'ordre quotient (H' reste convexe dans G') puis $(G'/H') \times H'$ de l'ordre produit. Par notre choix de G' et H', H et H' d'une part, G/H et G'/H' d'autre part, sont des g.a.o. équivalents; par Feferman et Vaught, on en déduit $(G/H) \times H \equiv (G'/H') \times H'$; ce dernier g.a.o. est isomorphe à G', lui-même équivalent à G, d'où $(G/H) \times H \equiv G$.

Définition. Pour $i \leq \omega$, appelons i-groupe un g.a.o. G admettant une famille $(G_n)_{n \leq i}$ de sous-groupes convexes vérifiant

$$G_o = G \ , \ G_i = \{0\}$$

pour chaque $n \in i$, $G_n \supset G_{n+1}$ et $G_n/G_{n+1} \cong \mathbb{Z}$

. si $i = \omega$, alors $\bigcap_{n\in i} G_n = \{0\}$.

Exemple. $\mathbb{Z}^i$.

Lemme 2. Pour $i \in \omega$, G est un i-groupe ssi $G \equiv \mathbb{Z}^i$; les i-groupes constituent donc une classe élémentaire complète.

Démonstration. Soient $(G_n)_{0\le n\le i}$ les sous-groupes convexes de $\mathbb{Z}^i$, avec $G_n \cong \mathbb{Z}^{i-n}$; nous montrons d'abord que chaque G_n est définissable dans $\mathbb{Z}^i$. Considérons le sous-ensemble G(a) définissable avec le paramètre a

$$G(a) = \{ x ; -a < 2x < a \}$$

et le prédicat H

$$H(a) \leftrightarrow [\ G(a) \text{ est un groupe }]$$

Prenons $a \in \mathbb{Z}^i$, $\mathbb{Z}^i \models H(a)$ (par exemple $a \equiv 1$ (modulo G_{n+1}) pour un $n<i$); soit $n \in \{0,\dots i-1\}$ tel que $a \in G_n - G_{n+1}$; G(a) est alors un sous-groupe convexe propre de G_n contenant G_{n+1} donc $G(a) = G_{n+1}$. L'élimination des paramètres se fait sans difficulté: on a l'équivalence, pour $1 \le n \le i$, $x \in G_n$ ssi $\mathbb{Z}^i \models \psi_n(x)$ où $\psi_n(x)$ est la formule

$$\exists\, a_1,\dots a_i \bigwedge_{j=1}^{i} H(a_j) \wedge [\ G(a_1) \supsetneq G(a_2) \supsetneq \dots \supsetneq G(a_i)\ ] \wedge [\ x \in G(a_n)\ ].$$

Soit maintenant $G \equiv \mathbb{Z}^i$; alors G contient i+1 sous-groupes convexes définissables, lui-même et les sous-groupes définis par les ψ_n , $1 \le n \le i$; si $G_n = \{ x ; G \models \psi_n(x) \}$, on a $G_{n+1}/G_n \equiv \mathbb{Z}$, ce qui prouve que G est un i-groupe.

La réciproque se montre par récurrence sur i,

- si $i = 1$, par définition, un i-groupe est un g.a.o. équivalent à $\mathbb{Z}$,
- si $i > 1$, G_1 est un (i-1)-groupe, donc équivalent à $\mathbb{Z}^{i-1}$ par hypothèse d'induction; par le lemme 1 on a $G \equiv (G/G_1)\times G_1 \equiv \mathbb{Z}\times G_1$ (par Feferman-Vaught) $\equiv \mathbb{Z}^i$.

Remarque. Cette propriété ne s'étend pas aux ω-groupes: deux ω-groupes ne sont en général pas équivalents et un g.a.o. équivalent à un ω-groupe n'en est pas nécessairement un. On peut néanmoins faire la remarque suivante: si G est un ω-groupe et $(G_n)_{n\in\omega}$ ses sous-groupes convexes correspondants ordonnés comme précédemment, chaque G_n est définissable: $x \in G_n$ ssi $G \models \chi_n(x)$ où $\chi_n(x)$ est la formule

$(0 < n < \omega)$

$$\exists\, a_1,\dots a_n \left\{ \bigwedge_{i=1}^{n} H(a_i) \wedge [\ G \supsetneq G(a_1) \supsetneq \dots \supsetneq G(a_n)\ ] \right.$$
$$\wedge\ \forall a \left[\left[H(a) \wedge [G(a) \supset G(a_n)] \right] \rightarrow \bigvee [G(a) = G(a_i)] \right]$$
$$\left. \wedge\ [x \in G(a_n)] \right\}$$

et pour un g.a.o. G' équivalent à G, si $\chi_n(G')$ est l'interprétation de χ_n dans G', les χ_n constituent une famille de sous-groupes convexes emboîtés, le quotient de deux termes successifs étant équivalent à $\mathbb{Z}$; donc si on pose $H = \bigcap_{n\in\omega} \chi_n(G')$, G'/H est un ω-groupe.

Proposition 1. [O]. Si G est un g.a.o. vérifiant $\mathbb{Z}^p \times G \equiv G$ pour un entier $p > 0$, on a $\mathbb{Z} \times G \equiv G$.

Démonstration. Avec ces hypothèses, il existe un ultrafiltre U qu'on peut prendre dénombrablement incomplet, pour lequel on a un isomorphisme de g.a.o. entre $(\mathbb{Z}^p \times G)^U$ et G^U, c'est-à-dire entre $(\mathbb{Z}^p)^U \times G^U$ et G^U. Cela permet de construire une chaîne $(G_n)_{n\in\omega}$ de sous-groupes convexes de G^U et des sous-groupes Z_n de G^U vérifiant, en tant que g.a.o.

$$G_n \cong G^U$$
$$G_n = Z_n \times G_{n+1}$$
$$Z_n \cong (\mathbb{Z}^p)^U .$$

Chaque G_n est définissable: on a $G_n = G(a)$ pour un $a \in G$ comme dans la preuve du lemme 2; $\bigcap_{n\in\omega} G_n$ est un sous-groupe convexe de G et, par le lemme 1, on a

$$G^U \equiv (G^U/\cap G_n) \times (\cap G_n) ;$$

l'application qui à $g \in G^U$ associe $(g_n)_{n\in\omega} \in \Pi Z_n$ définie par les relations, pour tout entier n,

$$g \equiv g_1 + g_2 + \ldots + g_n \text{ (modulo } G_n)$$

est surjective par ω_1-saturation de G^U et définissabilité des G_n ; elle a pour noyau $\cap G_n$, donc

$$G^U/\cap G_n \equiv \Pi Z_n \cong ((\mathbb{Z}^p)^U)^\omega \equiv (\mathbb{Z}^p)^\omega \cong \mathbb{Z}^\omega$$
$$G^U \equiv \mathbb{Z}^\omega \times (\cap G_n) \cong \mathbb{Z} \times (\mathbb{Z}^\omega \times (\cap G_n)) \equiv \mathbb{Z} \times G^U$$

et enfin $G \equiv \mathbb{Z} \times G$.

2. Application aux corps valués

Une référence agréable est le livre de P. Ribenboim [R].

a) Si (K,v) est un corps valué, la connaissance de l'anneau de valuation A_v permet de récupérer v : le groupe vK est le quotient du groupe multiplicatif K^* de K par le sous-groupe des unités U_{A_v} de A_v et v est la projection canonique de K^* sur K^*/U_{A_v}. On définit sur l'ensemble V(K) des valuations sur K un ordre: pour u,v dans V(K), on pose

$$v \leq w \quad (\text{"w plus fine que v"}) \text{ ssi } A_v \supset A_w .$$

Dans une telle situation, si on note M_v l'idéal maximal de A_v, on a

$$M_v \subset M_w \subset A_w \subset A_v ,$$

M_v est un idéal premier de A_w et A_v est le localisé de A_w en M_v. Réciproquement si P est un idéal premier de A_w, le localisé de A_w en P est l'anneau d'une valua-

tion w_P sur K plus grossière que w . On met ainsi en bijection les ensembles ordonnés suivants, si $w \in V(K)$ est fixée:

- l'ensemble des valuations sur K moins fines que w , muni de l'ordre de finesse
- les idéaux premiers de A_w ordonnés par l'inclusion.

Dans un anneau de valuation les idéaux sont totalement ordonnés par l'inclusion; en conséquence, dans $(V(K),\leq)$ l'ensemble des minorants d'un élément est totalement ordonné, on dit que $(V(K),\leq)$ est un arbre. Remarquons aussi que dans cet ensemble il y a des bornes inférieures: soient $v_i \in V(K)$ pour $i \in I$; alors l'anneau engendré par les A_{v_i} dans K est un anneau de valuation. A l'opposé, deux éléments de V(K) admettent un majorant commun ssi ils sont comparables.

b) On peut préciser la correspondance établie ci-dessus: si P est un idéal premier de A_w , $w(A_w - P) \cup [-w(A_w - P)]$ est un sous-groupe convexe T_P de wK , et w_P est la composée de w avec la projection de wK sur wK/T_P (Notation: $w_P = w/T_P$). Le a) exprime que toute valuation plus grossière que w est ainsi obtenue à partir de w par passage au quotient modulo un sous-groupe convexe de wK .

En résumé, les ensembles ordonnés mis en correspondance sont les suivants, pour $w \in V(K)$ fixée:

- les valuations sur K moins fines que w
- les idéaux premiers de A_w ordonnés par l'inclusion
- les sous-groupes convexes de wK ordonnés par l'ordre inverse de l'inclusion.

c) Soit $u,v \in V(K)$, $u \leq v$, r_v le passage au reste $A_v \twoheadrightarrow K/v$ (Notation: $K/v = A_v/M_v$); on a $A_v \subset A_u$ donc $r_u(A_v) \subset r_u(A_u) = K/u$ et il est facile de vérifier que $r_u(A_v)$ est un anneau de valuation de K/u ; on note v/u la valuation associée; si $x \in A_u$, v/u vérifie $v/u(x/u) = v(x)$ et est donc à valeurs dans le sous-groupe convexe de vK associé à u . Inversement, soit $u \in V(K)$ et $\bar{v} \in V(K/u)$; alors $r_u^{-1}(A_{\bar{v}})$ est un anneau de valuation de K ; on note $u \times \bar{v}$ la valuation associée; on a pour $x \in K$, $u \times \bar{v}(x) \geq 0$ ssi [$u(x) > 0$ ou $u(x) = 0$ et $\bar{v}(x/u) \geq 0$] ; trivialement $u \times \bar{v} \geq u$. Ces deux constructions sont inverses l'une de l'autre en ce sens que $(u \times \bar{v})/u = \bar{v}$ et $u \times (v/u) = v$. Il est classique que, pour $u \leq v$ sur K , (K,v) est henselien ssi (K,u) et (K/u, v/u) le sont.

d) Si G est un g.a.o. et k un corps, on note k((G)) le corps de séries formelles généralisées à exposants dans G et coefficients dans k (voir par exemple [F] p.134)

$$k((G)) = \{ \sum_{g \in I} a_g X^g \ ; \ I \text{ partie bien ordonnée de } G \ , \ a_g \in k \ \}$$

avec la somme et le produit habituels sur les séries et la valuation $v(\Sigma a_g X^g) =$ le premier g tel que $a_g \neq 0$. Si G_1 et G_2 sont deux g.a.o., il y a un isomorphisme de corps valués entre $k((G_1 \times G_2))$ muni de la valuation associée à $G_1 \times G_2$ et

$(k((G_2)))((G_1))$ muni du produit de la valuation associée à G_1 et de la valuation associée à G_2 sur le corps de restes par rapport à G_1 .

e) Pour finir donnons un résultat qui va nous être utile:

Proposition 2. Soit $i \in \omega+1$; alors un corps K porte au plus une valuation henselienne à valeurs dans un i-groupe. Si $i \in \omega$, une telle valuation est définissable dans la seule structure de corps de K .

Démonstration. Elle se fait par induction sur i ;
1) $i = 1$; c'est un résultat d'Ax [A] : si T est un élément de K de valuation 1 et si la caractéristique résiduelle ne divise pas l'entier m , on a

$$x \in A_v \quad \text{ssi} \quad \exists y\ (1+Tx^m=y^m)$$

Pour éliminer le paramètre T et le problème de caractéristique, on définit les prédicats $A_m(t)$

$$x \in A_m(t) \quad \text{ssi} \quad \exists y\ (1+tx^m=y^m) \ .$$

On a alors, si (K,v) est henselien

$$x \in A_v \quad \text{ssi} \quad \exists t\ [\ \forall y\ (t \neq y^2)\ ] \wedge \Big\{ [(A_2(t) \text{ est stable par multiplication}) \wedge (x \in A_2(t))] \vee [(A_3(t) \text{ est stable par multiplication}) \wedge (x \in A_3(t))] \Big\}$$

2) pour $i \in \omega$, soit v à valeurs dans un $(i+1)$-groupe G . Alors G contient un sous-groupe convexe H qui est un i-groupe; il lui correspond une valuation $w < v$ sur K , à valeurs dans $G/H \equiv Z$, et une valuation v/w sur K/w à valeurs dans $H \equiv Z^i$; pour $x \in K$ on a

$$v(x) \geq 0 \quad \text{ssi} \quad w(x) > 0 \quad \text{ou} \quad w(x) = 0 \wedge v/w(x/w) \geq 0$$

ce qui se dit au premier ordre dans la seule structure de corps par hypothèse de récurrence et par le cas $i = 1$.
3) Si v est à valeurs dans un ω-groupe G , G contient les sous-groupes convexes $(G_n)_{n\in\omega}$, auxquels sont associées des valuations v_n , v_n à valeurs dans $G/G_n \equiv Z^n$; pour chaque n , v_n est henselienne donc unique, les v_n sont croissantes et v est leur borne supérieure, définie par $A_v = \bigcap_{n\in\omega} A_{v_n}$.

3. Démonstration du théorème

Le principe d'Ax-Kochen-Eršov nous dit que, pour des corps valués henseliens (K,v) et (K',v') de caractéristique résiduelle nulle, on a $(K,v) \equiv (K',v')$ ssi $K/v \equiv K/v'$ en tant que corps et $vk \equiv v'k'$ en tant que g.a.o., et que dans le cas où $(K,v) \subset (K',v')$, on a $(K,v) \prec (K',v')$ ssi $K/v \prec K'/v'$ et $vK \prec vK'$. Supposons que K est un corps de caractéristique 0, équivalent à $K((X_1))\ldots((X_p))$ c'est-à-dire

à $K((\mathbb{Z}^p))$; par itération, en appliquant le théorème d'Ax-Kochen-Eršov, on a $K \equiv K((\mathbb{Z}^{pn}))$ pour tout entier $n \geq 1$; $K((\mathbb{Z}^{pn}))$ porte naturellement une valuation henselienne à valeurs dans $\mathbb{Z}^{pn}$ et donc par la proposition 2 cette propriété se transporte par équivalence élémentaire: K porte une valuation v_n henselienne et à valeurs dans $H_n \equiv \mathbb{Z}^{pn}$; à cause de l'unicité d'une telle valuation à n fixée, ces valuations sont nécessairement de plus en plus fines, et elles admettent pour borne supérieure la valuation v définie par $A_v = \bigcap_{n\in\omega} A_{v_n}$; chaque v_n est plus grossière que v et $G = vK$ contient donc une famille de sous-groupes convexes décroissants $(G_n)_{n\in\omega}$ de façon à ce qu'on ait, pour tout $n\in\omega$, $G/G_n = H_n$. Parce que chaque v_n est henselienne, v l'est aussi et parce que tous les K/v_n sont de caractéristique 0 (parce qu'équivalents à K), K/v l'est aussi (K/v_n de carac. 0 $\Leftrightarrow$ $M_{v_n} \cap \mathbb{Q} = \{0\}$ et $M_v \cap \mathbb{Q} = (\cup M_{v_n}) \cap \mathbb{Q} = 0$). Par le théorème d'Ax-Kochen-Eršov, on a $K \equiv k((G))$ si on a posé $k = K/v$; mais par hypothèse, $K \equiv K((\mathbb{Z}^p))$ donc $K \equiv k((G))((\mathbb{Z}^p))$; grâce à l'isomorphisme entre $k((G))((\mathbb{Z}^p))$ et $k((\mathbb{Z}^p\times G))$, nous arrivons à l'équivalence (des corps) $k((G)) \equiv k((\mathbb{Z}^p\times G))$. Prenons un ultrafiltre U tel que $[k((G))]^U \cong [k((\mathbb{Z}^p\times G))]^U$; soit L ce corps; L porte deux valuations henseliennes, v à valeurs dans G^U et w à valeurs dans $(\mathbb{Z}^p\times G)^U \cong (\mathbb{Z}^p)^U \times G^U$; G^U n'est pas un ω-groupe mais contient un sous-groupe convexe $H = \cap(G_n^U)$ tel que G^U/H en soit un (voir la remarque finale du 1.); à H est associée la valuation v/H sur L à valeurs dans G^U/H ; de même pour un certain sous-groupe convexe de wL qu'on note aussi H parce qu'il lui est isomorphe, wL/H est un ω-groupe, et w/H est à valeurs dans wL/H ; on en déduit l'égalité v/H = w/H donc vL/H = wL/H et $(vL/H)\times H = (wL/H)\times H$; or le premier g.a.o. est équivalent à vL et le deuxième à wL ; donc $G^U \equiv (\mathbb{Z}^p\times G)^U$ et $G \equiv \mathbb{Z}^p\times G$. La proposition 1 nous dit qu'alors $G \equiv \mathbb{Z}\times G$; par Ax-Kochen-Eršov on a $k((G)) \equiv k((\mathbb{Z}\times G)) \cong k((G))((X))$, soit $K \equiv K((X))$.

4. Étude de l'inclusion de K dans K((X))

Considéré comme corps de constantes de K((X)) , K n'en est jamais sous-structure élémentaire: on a vu dans la proposition 2 que K[[X]] est définissable sans paramètre dans K((X)), disons par une formule E ; si K était sous-structure élémentaire de K((X)), l'interprétation de E dans K serait la trace de son interprétation dans K((X)), ce qui est contradictoire avec les relations $K \subset K[[X]] \not\subset K((X))$. En général K n'est même pas existentiellement clos dans K((X)), par exemple l'équation de Fermat

$$\exists x,y,z,t\ (x^3+y^3=1) \wedge (xz=1) \wedge (yt=1)$$

admet une solution dans $\mathbb{Q}((X))$ et non dans $\mathbb{Q}$. Mais pour $K \equiv \mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}_p$, K est

existentiellement clos dans K((X)): en effet, pour un tel corps, K est sous-structure élémentaire de son corps de séries de Puiseux $K((X^{\frac{1}{\infty}})) = \bigcup_{n\in\mathbb{N}} K((X^{(\frac{1}{n!})}))$ (voir par exemple [C]) et il est trivial que, pour un corps quelconque, K est existentiellement clos dans K((X)) ssi il l'est dans $K((X^{\frac{1}{\infty}}))$. C'est, plus généralement, le cas des corps que nous avons considérés:

Proposition 3. Si K est de caractéristique nulle et élémentairement équivalent à k((G)) pour un corps k et un g.a.o. $G \neq 0$, alors K est existentiellement clos dans K((X)).

Démonstration. On étudie d'abord le cas K = k((G)) avec G ω_1-saturé, on achèvera la démonstration en prouvant que le fait d'être existentiellement clos dans son corps de séries est une propriété du premier ordre.

Soit donc K = k((G)), G ω_1-saturé et G^U une ultrapuissance $|G|^+$-saturée; on considère le plongement diagonal de G dans G^U et on prend un sous-groupe H de G^U isomorphe à $\mathbb{Z}$, tel que les groupes G·H et G×$\mathbb{Z}$ soient isomorphes, et vérifiant $\{ h\in H ; h > 0 \} > G$; les g.a.o. H.G et $\mathbb{Z}$×G sont alors isomorphes au-dessus de G, et les corps valués k((H.G)) et k((G))(($\mathbb{Z}$)) sont isomorphes au-dessus de k((G)) (on utilise 2.d). Or $k((G)) \prec k((G^U))$ par le principe d'Ax-Kochen-Eršov. Si un système d'équations et d'inéquations à coefficients dans K admet une solution dans K((X)), il en admet une dans k((H.G)), donc dans $k((G^U))$ et enfin dans k((G)) = K.

Nous cherchons maintenant à traduire au premier ordre sur un corps L le fait qu'il est existentiellement clos dans L((X)); d'abord L est existentiellement clos dans L((X)) ssi il l'est dans L[[X]]; ensuite si E est un système de n équations en m variables et de degré d , si s est un entier, Greenberg a prouvé dans [Gr] qu'il existe un entier N, ne dépendant que de n, m, d et s tel que E admet une solution $\vec{y}$ dans L[[X]] ssi il en admet une $\vec{x}$ modulo X^N, et qu'on peut alors choisir $\vec{y}$ coïncidant avec $\vec{x}$ modulo X^s. Donc L est existentiellement clos dans L((X)) ssi, pour tous entiers m, n, d, r et s, il satisfait l'énoncé

$\forall$ (les coefficients d'un système E borné en nombre de variables, d'équations et en degré respectivement par m, n et d)

$\forall (Q \in L[X_1,\ldots X_n]$ de degré $\leq r)$

$\{ [$E admet dans L[[X]] une solution $\vec{x}$ modulo X^N avec $Q(\vec{x}) \neq 0$ (modulo X^S)$]$

$\rightarrow [\ \exists \vec{x}\ E(\vec{x}) \wedge Q(\vec{x})\neq 0\ ] \}$.

La réciproque de cette proposition est fausse: un corps K pseudo-algébriquement clos (appelé aussi régulièrement clos, voir [CDM]) est existentiellement clos dans toute extension régulière, donc dans K((X)); s'il est, en tant que corps,

élémentairement équivalent à k((G)) avec $G \neq 0$, il a, par le théorème de Keisler-Shelah, une ultrapuissance portant une valuation henselienne non triviale et est donc algébriquement clos [D]; un corps pseudo-algébriquement clos et non algébriquement clos fournit ainsi un contre-exemple à cette réciproque.

Bibliographie

[A] J. Ax, On the undecidability of power series fields, Proc. AMS 16^2(1965), p. 846.

[AK] J. Ax et S. Kochen, Diophantine problems over local fields III, Ann. of Math. 83 (1966), pp. 437-456.

[C] G. Cherlin, Model Theoretic Algebra-Selected Topics, Springer Verlag, Berlin-Heidelberg-New York 1976, LNM n° 521.

[CDM] G. Cherlin, L. van den Dries et A. Mac Intyre, The Elementary Theory of Regularly Closed Fields, à paraître.

[D] F. Delon, Périodicité des théories élémentaires des corps de séries formelles itérées, à paraître.

[E] J. L. Eršov, On the elementary theory of maximal normed fields, English translation, Soviet Math. Dokl. 6^2 (1965), pp. 1390-1393.

[F] L. Fuchs, Partially ordered systems, Pergamon Press, Oxford London New-York Paris 1963.

[FV] S. Feferman et R. Vaught, The first-order properties of products of algebraic systems, Fund. Math. XLVII (1959), pp. 57-103.

[Gr] M. Greenberg, Lectures on forms in many variables, IHES Publications Mathématiques 31 (1966), pp. 59-64.

[Gu] Y. Gurevič, Elementary properties of ordered abelian groups, AMS Translations 46 (1965), pp. 165-192.

[O] F. Oger, Produits lexicographiques de groupes ordonnés, isomorphisme et équivalence élémentaire, à paraître.

[R] P. Ribenboim, Théorie des valuations, Les Presses de l'Université de Montréal, Montréal 1964.

[Sa] G. Sabbagh, Aspects logiques de la pureté dans les modules, C.R.A.S. Paris, t. 271 (9 nov. 1970), Série A, pp. 909-912.

[Sh] S. Shelah, The lazy model-theorician's guide to stability, in Six Days of Model Theory /.../, ed. P. Henrard, Castella, Albeuve 1977.

Françoise Delon

Université de Paris 7
U.E.R. de Mathématiques
Tour 45-55 - 5ème étage
2, Place Jussieu
75251 PARIS CEDEX 05

MÉMOIRES DE LA S. M. F.

WILFRID HODGES

Groupes nilpotents existentiellement clos de classe fixée

Mémoires de la S. M. F. 2^e série, tome 16 (1984), p. 1-10
<http://www.numdam.org/item?id=MSMF_1984_2_16__R1_0>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p. 1-10

GROUPES NILPOTENTS EXISTENTIELLEMENT CLOS DE CLASSE FIXEE

Wilfrid Hodges

Résumé. *Nous démontrons que pour chaque $k \geqslant 2$, il y a une famille continupotente de groupes existentiellement clos nilpotents de classe k, telle que si* G *et* H *sont deux groupes distincts dans la famille, alors il existe une proposition du 1er ordre et de la forme* $\exists\forall\exists$, *qui est vraie dans* G *mais pas dans* H. *La forme* $\exists\forall\exists$ *est la meilleure possible.*

Summary. *We show that if $k \geqslant 2$, then there is a family of existentially closed nilpotent groups of class k which has the cardinality of the continuum, such that if* G *and* H *are two distinct groups in the family, then there is an* $\exists\forall\exists$ *first-order sentence which is true in* G *but not in* H. *The form* $\exists\forall\exists$ *is best possible.*

Soit $\mathcal{N}_k$ la classe des groupes nilpotents de classe k. On dit qu'un groupe $G \in \mathcal{N}_k$ est e.c. (pour existentiellement clos) dans $\mathcal{N}_k$ si pour tout groupe $H \in \mathcal{N}_k$ avec $G \subseteq H$, et tout système fini E d'équations et d'inéquations avec paramètres dans G, si E est satisfait dans H alors E est satisfait dans G.

THEOREME. Pour tout $k \geqslant 2$, il y a 2^{ω} groupes e.c. dans $\mathcal{N}_k$, G_α $(\alpha < 2^{\omega})$, tels que si $\alpha \neq \beta$, alors il existe une proposition ϕ de la forme $\exists\forall\exists$ qui est vraie dans G_α mais pas dans G_β. (La forme $\exists\forall\exists$ est $\exists\bar{x}\forall\bar{y}\exists\bar{z}\psi$ avec ψ sans quanteurs.)

On sait déjà: (1) Le théorème est vrai avec 2 pour 2^{ω} (Saracino [10]). (2) Il y a 2^{ω} groupes e.c. dans $\mathcal{N}_k$, G_α $(\alpha < 2^{\omega})$, tels que si $\alpha \neq \beta$ alors $G_\alpha \not\cong G_\beta$ (Hodges [6]). (3) Si G, H sont e.c. dans $\mathcal{N}_k$, alors pour toute proposition ϕ de la forme $\forall\exists$, ϕ est vraie ou bien dans G et H, ou bien dans aucun des deux (cf. Prop. 1.14 dans Hirschfeld & Wheeler [5]). (Voir aussi Maier [9].) Le théorème remplit la lacune entre ces résultats. Au même temps sa démonstration

0037-9484/84 03 01 10/$ 3.00/

donne quelque substance algébrique au résultat (2).

Pour les groupes e.c., au lieu des groupes e.c. dans $\mathcal{N}_k$, le théorème au-dessus est un résultat bien connu de Belegradek [3] et Ziegler [12]. Pour les groupes e.c. dans $\mathcal{N}_k$ qui sont périodiques, le théorème est tout à fait faux. Il n'y a qu'un groupe dénombrable et périodique qui soit e.c. dans $\mathcal{N}_2$ (Theorem 3.5 de Saracino & Wood [11], cf. aussi Apps [1].

Nous procédons en deux coups. La première étape, c'est de bâtir 2^ω groupes e.c. dans $\mathcal{N}_k$ qui "représentent" différents ensembles d'entiers. Et puis au second coup nous trouvons des formules ϕ_X qui expriment qu'un ensemble X est représenté dans un groupe e.c. Nous écrivons G' pour le sousgroupe dérivé de G. $[x_1,\ldots,x_n]$ est le commutateur $[\ldots[x_1,x_2],x_3\ldots,x_n]$ de poids n. G*H est le produit libre de G et H dans le sens de $\mathcal{N}_k$. Pour plusiers détails je renvoie à Hodges [6]. Nous fixons $k \geqslant 2$.

1. Construction d'un ensemble continupotent de groupes e.c. dans $\mathcal{N}_k$

LEMME 1. Soient p un nombre premier, $G \in \mathcal{N}_k$ et b un élément de G. Alors (a), (b) sont équivalents:

(a) Il y a un groupe $H \supseteq G$, $H \in \mathcal{N}_k$, avec des éléments $h_2, \ldots, h_k$ tels que $[b,h_2,\ldots,h_k] \neq 1$ et $h_k^p = 1$.

(b) Dans G il n'y a pas d'élément a tel que $a^p b^{-1} \in G'$.

Démonstration. Soit F le groupe k-nilpotente libre de générateurs $x_2, \ldots, x_{k-1}$. Considérons $K = G*F*Z_p$, où x_k engendre le groupe cyclique Z_p d'ordre p. La condition (a) est équivalente à

(1) $\qquad [b,x_2,\ldots,x_k] \neq 1.$

Supposons d'abord que (b) soit fausse. Prenant a tel que $a^p b^{-1} = c \in G'$, nous avons par les lois de $\mathcal{N}_k$:

$$[b,x_2,\ldots,x_k] = [c^{-1}a^p,x_2,\ldots,x_k] = [a,x_2,\ldots,x_{k-1},x_k^p] = 1,$$

qui contredit (1). Puis supposons que (1) soit fausse. Alors d'après des faits connus sur $\mathcal{N}_k$, puisque aucun des $x_2, \ldots, x_k$ n'est de la forme y^p modulo K', b est de cette forme modulo G'. (Cf. Lemma 2(a) de Hodges [6].) □

D'après le lemme 1, nous avons:

LEMME 2. Soit G e.c. dans $\mathcal{N}_k$, soit b un élément de G et soit p un nombre premier. Alors les conditions suivantes sont équivalents:

(a) b est de la forme a^p modulo G'.

(b) $G \models \forall x_2 \ldots x_k (x_k^p = 1 \rightarrow [b, x_2, \ldots, x_k] = 1)$. □

Maintenant soient $G \in \mathcal{N}_k$, b un élément de G et X un ensemble de nombres premiers. Nous disons que b <u>représente</u> X dans G si pour tout nombre premier p,

(2) $p \in X \Rightarrow$ b est de la forme a^p modulo G', et

(3) $p \notin X \Rightarrow$ il y a $h_2, \ldots, h_k \in G$ avec $h_k^p = 1$ et $[b, h_2, \ldots, h_k] \neq 1$.

Puisque les seconds membres de (2), (3) sont existentielles, il est clair que si b représente X dans G, alors b représente X aussi dans chaque $H \supseteq G$, $H \in \mathcal{N}_k$.

L'ensemble X de nombres premiers étant donné, nous construisons un groupe G_X avec un élément g_1^X qui représente X, comme suit. Soit Q_X le groupe des nombres rationnels q tels que si un nombre premier p divise le dénominateur de q, alors $p \in X$. Soit g_1^X le nombre 1 dans Q_X. Soit F le groupe libre $\in \mathcal{N}_k$ sur k-1 générateurs $g_2^X, \ldots, g_k^X$. (Les éléments $g_2^X, \ldots, g_{k-1}^X$ suffisent ici, mais on a besoin de g_k^X plus tard.) Soit B_X le groupe $\bigoplus\{Z_p : p \text{ premier } \notin X\}$. Alors G_X sera $Q_X * F * B_X$. On voit que g_1^X représente X dans G_X (c'est le Lemma 5 de Hodges [6]).

Notre but est de construire un groupe e.c. dans $\mathcal{N}_k$, dans lequel certains ensembles récursifs de nombres premiers sont représentés, et certains autres ne le sont pas. Pour ceci nous employons le forcing fini de Abraham Robinson (Barwise & Robinson [2]), pour omettre les ensembles que nous voulons laisser. Il faut ajouter quelques items aux définitions de Barwise & Robinson. Par exemple, dans le forcing correspondant à une théorie T, si ϕ_i $(i < \omega)$ sont des propositions universelles du premier ordre, alors une condition π force $\bigwedge_{i<\omega} \phi_i$ ssi $T \cup \pi \vdash \phi_i$ pour tout $i < \omega$. (Pour justifier cela, et pour d'autres faits sur le forcing que nous ne démontrons pas ici, voir Hodges [7] ou Ziegler [12].) Nous écrivons A pour le modèle construit par forcing.

Soit E un ensemble dénombrable d'ensembles infinis de nombres premiers. Nous écrivons G_E pour la somme directe $\bigoplus\{G_X : X \in E\}$. Alors G_E est dénombrable. Soit Δ_E le diagramme de G_E, et soit T la théorie de $\mathcal{N}_k$.

LEMME 3. Dans le forcing correspondant à $T \cup \Delta_E$, la condition $\emptyset$ force que le modèle A construit soit un groupe e.c. dans $\aleph_k$ contenant G_E comme sousgroupe. □

Or, grâce aux lemmes 2, 3, la propriété "c est de la forme a^p modulo A'" équivaut (pour A) à

(4) $\quad \forall x_2 \ldots x_k (x_k^p = 1 \to [c, x_2, \ldots, x_k] = 1).$

On remarque que (4) est une proposition universelle, et de là, si π est une condition de forcing qui force (4), alors $T \cup \Delta_E \cup \pi$ l'implique. Le même est vrai pour la propriété "c n'est pas de la forme a^p modulo A'", utilisant un nombre infini de propositions universelles.

LEMME 4. Dans le forcing correspondant à $T \cup \Delta_E$, soit c une constante de forcing (un témoin), soit π une condition, et soit Y un ensemble infini de nombres premiers, tel qu'il existe une infinité de nombres premiers $\notin Y$. Alors si π force "c représente Y", il y a $X \in E$ tel que $Y \setminus X$ soit fini.

Démonstration. Soient $c, d_1, \ldots, d_m$ les constantes de forcing qui apparaissent dans π. Soit K le groupe $\in \aleph_k$ présenté par l'ensemble d'equations dans $\Delta_E \cup \pi$. Puisque π est une condition, $T \cup \Delta_E \cup \pi$ a un modèle, d'où $\Delta_E \cup \pi$ toute entière est vérifiée dans K. Alors $G_E \subseteq K$ sans perte de généralité, et K est engendré sur G_E par $c, d_1, \ldots, d_m$. Or pour chaque $p \in Y$, soit θ_p la proposition (4). Alors $T \cup \Delta_E \cup \pi \vdash \theta_p$, d'ou nous deduirons que si $H \supseteq K$, $H \in \aleph_k$, alors $H \models \theta_p$ aussi. D'après le lemme 1 il suit que c est de la forme a^p modulo K' pour chaque $p \in Y$. Mais pareillement si q est un nombre premier $\notin Y$, alors c n'est pas de la forme a^q modulo K'.

Passons maintenant à K/K'. Soit a^* l'image dans K/K' d'un élément a de K. Alors K/K' est un groupe abélien finiment engendré sur G_E/G'_E par les generateurs $c^*, d_1^*, \ldots, d_m^*$. Puisqu'il y a une infinité de nombres premiers qui ne divisent pas c^* dans K/K', c^* est d'ordre infini. Dans $(K/K')/(G_E/G'_E)$, qui est une somme directe finie de groupes cycliques, l'image de c^* est divisible par une infinité de nombres premiers. Alors il existe j tel que $jc^* \in G_E/G'_E$.

Or, par la construction de G_E, il y a des ensembles $X_{i_1}, \ldots, X_{i_n}$, des entiers $\ell_1, \ldots, \ell_n \leq k$, et un element t d'ordre fini, tels que

(5) $\quad jc^* = \alpha_1 g_{\ell_1}^{X_{i_1}} + \ldots + \alpha_n g_{\ell_n}^{X_{i_n}} + t \quad (\alpha_1, \ldots, \alpha_n \in \mathbb{Z}).$

Puisque jc^* est d'ordre infini, $n \geq 1$; nous prenons n aussi petit que possible. Considérons $p \in Y$ tel que p ne divise pas l'ordre de t. Si $p \notin X_{i_1}$, alors par la construction de G_E, il y a des éléments $h_2, \ldots, h_k$ tels que $h_k^p = 1$ et $[c^j, h_2, \ldots, h_k] \neq 1$. Par le lemme 1, ce contredit le fait que p divise jc^* dans K/K'. On déduit que $p \in X_{i_1}$. Donc $Y \setminus X_{i_1}$ est fini. □

Soit $\{P_n : n < \omega\}$ une partition de l'ensemble des nombres premiers en ensembles recursifs infinis. On sait qu'il existe une famille $\{S_\alpha : \alpha < 2^\omega\}$ de sous-ensembles S_α de ω, telle que si $\alpha \neq \beta$ alors $S_\alpha \setminus S_\beta \neq \emptyset$. Pour chaque $\alpha < 2^\omega$, soit E_α l'ensemble de tous P_n avec $n \in S_\alpha$. Dans le forcing relatif à $T \cup \Delta_{E_\alpha}$, il résulte des lemmes 3, 4 (et de faits standards sur le forcing) que nous avons un groupe G_α e.c. dans $\mathcal{N}_k$, qui contient G_{E_α} comme sousgroupe, et dans lequel aucun des ensembles P_n ($n \notin S_\alpha$) n'est représenté par un élément.

On peut ajouter: les groupes G_α ($\alpha < 2^\omega$) sont dénumerables, et si $\alpha \neq \beta$ alors G_α n'est pas isomorphe à aucun sousgroupe de G_β.

2. Propositions exprimant la différence entre les groupes

Il nous faut trouver, pour chaque ensemble récursif Y de nombres premiers, une proposition ϕ_Y qui exprime que "L'ensemble Y est représenté dans le groupe". Nous réussirons à le faire pour les groupes e.c. dans $\mathcal{N}_k$ et avec une notion de représentation qui est légèrement plus forte qu'auparavant. La clé en est l'interprétation de l'arithmétique dans les groupes nilpotents, due à Mal'cev [8].

Comme dans Hodges [6], un k-uple de Mal'cev dans le groupe $G \in \mathcal{N}_k$ est un k-uple $g_1, \ldots, g_k$ d'éléments de G, tel que $[g_1, \ldots, g_k]$ est d'ordre infini. Nous disons que le k-uple de Mal'cev $g_1, \ldots, g_k$ représente l'ensemble Y si g_1 le représente.

LEMME 5. Pour les groupes G_α définis dans la section 1, on a pour chaque ensemble P_n de nombres premiers: $n \in S_\alpha$ ssi il existe un k-uple de Mal'cev dans G_α qui représente P_n.

Démonstration. Dans la construction de G_α, le sousgroupe G_X contient un k-uple de Mal'cev, $g_1^X, \ldots, g_k^X$, qui représente X. (C'est ici qu'on utilise g_k^X;

voir Lemma 2(b) de Hodges [6] pour la preuve que c'est un k-uple de Mal'cev.) Le reste est clair. □

LEMME 6. Soit G un groupe e.c. dans $\mathcal{N}_k$, et soit g un élément de G. Sont équivalents:

(a) g est d'ordre infini modulo G'.

(b) $G \models \forall y_1 \ldots y_k \exists z_1 \ldots z_{k-1}\ [y_1,\ldots,y_k] = [z_1,\ldots,z_{k-1},g]$.

Démonstration. Voir Lemma 4 de Hodges [6]. □

LEMME 7. Soit G un groupe e.c. dans $\mathcal{N}_k$, et soient g, h des éléments de G. Sont équivalents:

(a) g est une puissance de h modulo G'.

(b) $G \models \forall y_1 \ldots y_{k-1}([y_1,\ldots,y_{k-1},h] = 1 \to [y_1,\ldots,y_{k-1},g] = 1)$.

Démonstration. Voir Lemma 3 de Hodges [6]. □

LEMME 8. Il y a une formule $\psi(x_1,\ldots,x_k)$ de la forme $\forall\exists$ telle que pour tout groupe G e.c. dans $\mathcal{N}_k$ et tous éléments $g_1, \ldots, g_k$ de G, $g_1, \ldots, g_k$ est un k-uple de Mal'cev ssi $G \models \psi(g_1,\ldots,g_k)$.

Démonstration. $\psi(x_1,\ldots,x_k)$ dit que:

(x_1 est d'ordre infini modulo G') $\wedge$ $\forall y$(y est une puissance de x_1 modulo G' $\wedge$ $[y,x_2,\ldots,x_k] = 1 \to y \in G'$).

C'est de la forme $\forall\exists \wedge \forall y(\forall \to \forall)$, c'est-a-dire $\forall\exists$. □

Etant donné un k-uple de Mal'cev $g_1, \ldots, g_k$ dans un groupe G e.c. dans $\mathcal{N}_k$, nous interprétons l'anneau Z des entiers, en interprétant n comme g_1^n, de la manière suivante:

(6) $\quad \|x \in z\| \equiv$ (x est puissance de g_1 mod G') $\quad (\forall)$

(7) $\quad \|x = n\| \equiv (xg_1^{-n} \in G')$ $\quad (\forall)$

(8) $\quad \|x+y = z\| \equiv (xyz^{-1} \in G')$ $\quad (\forall)$

(9) $\quad \|x.y = z\| \equiv \exists w$(w est puissance de g_k modulo G'
$\wedge\ [x,g_2,\ldots,g_k] = [g_1,g_2,\ldots,g_{k-1},w]$
$\wedge\ [z,g_2,\ldots,g_k] = [y,g_2,\ldots,g_{k-1},w]$) $\quad (\exists\forall)$

D'apres le théorème de Matiyasevič (cf. par ex. Chapter 6 de Bell & Machover [4]), si Y est un ensemble récursivement énumerable d'entiers, alors il y a une formule $\theta_Y(x)$ de la forme

$$(\exists y_1 \in Z)\ldots(\exists y_m \in Z)\ \theta'(x,y_1,\ldots,y_m),$$

ou θ' est une conjonction de formules de la forme $x = n$, $x+y = z$ ou $x.y = z$, et pour tout $n \in Z$, $n \in Y$ ssi $\theta_Y(n)$ est vraie dans Z. Interprétant θ_Y par (6)-(9), nous avons

(10) $\|x \in Y\| \equiv$ une formule $\chi_Y(x)$ de la forme $\exists\forall$.

Finalement nous avons besoin de formules $\psi(g_1,x)$ qui expriment que "$(g_1)^{1/p}$ existe modulo G', où x est l'interprétation du nombre premier p", de la forme $\exists\forall$ et aussi de la forme $\forall\exists$. La forme $\exists\forall$ n'offre aucune difficulté:

(11) $\exists y(g_1$ est puissance de y mod G' $\wedge\ \exists w(w$ est puissance de g_k mod G'
$\wedge\ [x,g_2,\ldots,g_k] = [g_1,\ldots,g_{k-1},w]$
$\wedge\ [g_1,\ldots,g_k] = [y,g_2,\ldots,g_{k-1},w])).$

Pour la forme $\forall\exists$ nous utilisons le lemme qui suit:

LEMME 9. Soit G un groupe e.c. dans $\mathcal{N}_k$ et soient a, b_1, ..., b_k, c des éléments de G, tels que a est d'ordre infini modulo G'. Alors sont équivalents:

(a) Pour tout entier n, si $[b_1,\ldots,b_k]^n = 1$ alors $c.a^{-n} \notin G'$.

(b) $G \models \exists w_2\ldots w_k([a,w_2,\ldots,w_k] = [b_1,\ldots,b_k] \wedge [c,w_2,\ldots,w_k] \neq 1)$.

Démonstration. (b) implique (a) par multilinearité des commutateurs $[x_1,\ldots,x_k]$ dans $\mathcal{N}_k$. Pour la réciproque, supposons (a); puisque G est e.c. dans $\mathcal{N}_k$, il suffit de trouver un groupe $H \supseteq G$, $H \in \mathcal{N}_k$, avec des éléments w_2, ..., w_k comme dans (b). Soit F le groupe $\in \mathcal{N}_k$ libre de générateurs x_2, ..., x_k. Dans G*F, soit N le sousgroupe normal engendré par $[a,x_2,\ldots,x_k][b_1,\ldots,b_k]^{-1}$. Il faut montrer que $G \cap N = \{1\}$, et que $[c,x_2,\ldots,x_k] \notin N$.

Tous les éléments de N ont la forme

(12) $([a,x_2,\ldots,x_k][b_1,\ldots,b_k]^{-1})^m \qquad (m \in Z)$

puisque les commutateurs de poids k sont centraux. Supposons que (12) soit égal

à un élément h de G. Alors $[a,x_2,\ldots,x_k]^m \in G$, ça qui implique que $[a,x_2,\ldots,x_k]^m = 1$ (envoyez x_2, ..., x_k sur 1). Puisque a est d'ordre infini modulo G', m = 0 (voir Lemma 2(b) de Hodges [6]), et alors h = 1 comme demandé.

Maintenant supposons que $[c,x_2,\ldots,x_k] = ([a,x_2,\ldots,x_k][b_1,\ldots,b_k]^{-1})^m$. Alors $[b_1,\ldots,b_k]^m = [a^m c^{-1},x_2,\ldots,x_k]$, et comme ci-dessus on déduit que $[a^m c^{-1},x_2,\ldots,x_k] = 1$, d'où $a^m c^{-1} \in G'$ (voir Lemma 2 de Hodges [6]). Par (a), cela implique que $[b_1,\ldots,b_k]^m \neq 1$; contradiction. □

En conséquence nous avons une formule de la forme $\forall\exists$ qui équivaut a (11) dans le groupe G e.c. $\in \mathfrak{N}_k$ avec le k-uple de Mal'cev g_1, ..., g_k. D'après le lemme 2 et les lois de $\mathfrak{N}_k$, nous pouvons exprimer (11) comme

$$(13) \qquad \bigwedge_{m\in Z}(xg_1^{-m} \in G' \to \forall y_2\ldots y_k(y_k^m \in G' \to [g_1,y_2,\ldots,y_k] = 1)).$$

Arrangée de nouveau, ce devient:

$$(14) \qquad \forall y_2\ldots y_k(\bigwedge_{m\in Z}(y_k^m \in G' \to xg_1^{-m} \notin G') \vee [g_1,y_2,\ldots,y_k] = 1),$$

ou en utilisant le lemme 7 et les lois de $\mathfrak{N}_k$,

$$(15) \qquad \forall y_2\ldots y_k(\exists z_1\ldots z_{k-1}\bigwedge_{m\in Z}([z_1,\ldots,z_{k-1},y_k]^m = 1 \to xg_1^{-m} \notin G') \vee [g_1,y_2,\ldots,y_k] = 1).$$

D'apres le lemme 9, la conjonction infinie dans (15) peut être remplacée par une formule existentielle, ce qui donne une forme $\forall\exists$ pour (11).

Finalement nous exprimons, pour chaque ensemble récursif Y de nombres premiers, que g_1, ..., g_k est un k-uple de Mal'cev dans lequel g_1 représente Y:

$$(16) \qquad (g_1,\ldots,g_k \text{ est un k-uple de Mal'cev}) \wedge \forall x(\|x \text{ est premier}\| \to ((11) \to \|x \in Y\|) \wedge (\neg\|x \in \omega\setminus Y\| \to (15))).$$

Par (10) et le lemme 8, c'est une formule $\phi'_Y(g_1,\ldots,g_k)$ de la forme $\forall\exists$. Alors la proposition $\exists y_1\ldots y_k\phi'_Y(y_1,\ldots,y_k)$ exprime qu'il y a un k-uple de Mal'cev qui représente Y, et cette proposition ϕ_Y est de la forme $\exists\forall\exists$.

Par la construction de la section 1, il y a une famille $\{G_\alpha : \alpha < 2^\omega\}$

de groupes e.c. dans $\mathcal{N}_k$, telle que si $\alpha \neq \beta$ alors il existe Y tel que $G_\alpha \models \phi_Y$ et $G_\beta \models \neg\phi_Y$. Le théorème est démontré.

Il y a des questions naturelles.

(1) Quels sont les ensembles E d'ensembles de nombres premiers, tels qu'il existe un groupe G e.c. dans $\mathcal{N}_k$, pour quel E est l'ensemble des ensembles de nombres premiers qui sont représentés (par des k-uples de Mal'cev) dans G?

(2) Peut-on caractériser un groupe G denombrable e.c. dans $\mathcal{N}_k$ par les ensembles de nombres premiers qui sont représentés (a) par des éléments et (b) par des k-uples de Mal'cev dans G? Si non, alors quelle information complémentaire est nécessaire pour caractériser G?

J'exprime mes remerciements à Gabriel Sabbagh et aux autres organisateurs de la table ronde de logique à Paris (Octobre 1983); au British Council qui a soutenu une visite à Paris; et à Bruno Poizat pour ses corrections linguistiques (ce qui était très nécessaire).

REFERENCES

[1] A. B. Apps, On $\aleph_0$-categorical class two groups, J. Algebra 82 (1983) 516-538.

[2] Jon Barwise & Abraham Robinson, Completing theories by forcing, Ann. Math. Logic 2 (1970) 119-142.

[3] О. В. Белеградек (O. V. Belegradek), Элементарные свойства алгебраически замкнутых групп, Fundamenta Math. 98 (1978) 83-101.

[4] J. L. Bell & M. Machover, A course in mathematical logic, North-Holland, Amsterdam 1977.

[5] Joram Hirschfeld & William H. Wheeler, Forcing, Arithmetic, Division rings, Lecture Notes in Mathematics 454, Springer, Berlin 1975.

[6] Wilfrid Hodges, Interpreting number theory in nilpotent groups, Arch. Math. Logik Grundlag. 20 (1980) 103-111.

[7] Wilfrid Hodges, Building models by games, Cambridge U.P. (à apparaître).

[8] A. I. Mal'cev, A correspondence between rings and groups, dans The metamathematics of algebraic systems, collected papers, North-Holland, Amsterdam 1971, pp. 124-137.

[9] Berthold Maier, On existentially closed and generic nilpotent groups (à apparaître).

[10] D. Saracino, Existentially complete nilpotent groups, Israel J. Math. 25 (1976) 241-248.

[11] Dan Saracino & Carol Wood, Periodic existentially closed nilpotent groups, J. Algebra 58 (1979) 189-207.

[12] Martin Ziegler, Algebraisch abgeschlossene Gruppen, dans Word Problems II, The Oxford Book, ed. S. I. Adian et al., North-Holland, Amsterdam 1980, pp. 449-576.

Wilfrid Hodges
Bedford College
Regent's Park
LONDON NW1 4NS