THE JOURNAL OF SYMBOLIC LOGIC
Volume 64, Number 2, June 1999

STABILITÉ POLYNÔMIALE DES CORPS DIFFÉRENTIELS

NATACHA PORTIER

Abstract. A notion of complexity for an arbitrary structure was defined in the book of Poizat *Les petits cailloux* (1995): we can define P and NP problems over a differential field K. Using the Witness Theorem of Blum et al., we prove the P-stability of the theory of differential fields: a P problem over a differential field K is still P when restricts to a sub-differential field k of K. As a consequence, if $P = NP$ over some differentially closed field K, then $P = NP$ over any differentially closed field and over any algebraically closed field.

§1. Introduction et définitions. Les classes de complexité P et NP sont définies dans le cas classique pour des ensembles de mots binaires, c'est-à-dire des mots sur l'alphabet $\{0,1\}$. Une autre approche est celle de la complexité algébrique: nous comptons le nombre d'opérations nécessaires à un calcul. Le cas où les mots sont des suites finies d'éléments d'un anneau est traité par Blum, Shub et Smale ([3]), et généralisé pour des suites finies d'éléments d'un modèle d'une théorie quelconque par Poizat dans [5] et [10].

Si le modèle est un corps, les opérations sont les opérations arithmétiques $(+,-,.)$, les tests de la forme $x = 0$?, et éventuellement $x \geq 0$? dans le cas d'un corps ordonné comme $\mathbf{R}$. Les fonctions calculées sont des polynômes conditionnés par des tests: ce sont des fonctions définies par cas, chaque cas étant déterminé par une formule libre, c'est-à-dire par une combinaison booléenne de tests sur des polynômes, et telles que la fonction soit un polynôme dans chaque cas. Une telle fonction y de $\bar{x}$ est définie par une suite finie de formules sans quanteurs $\phi_n(\bar{x})$ et une suite de polynômes $f_n(\bar{x})$ telle que $\bigvee_{1\leq i\leq n}(\phi_i(\bar{x}) \wedge y = f_i(\bar{x}))$. Un ensemble de suites finies d'éléments d'un ensemble M est appelé problème sur M. Dans [10], Poizat utilise les circuits pour définir la complexité des problèmes. Ceux-ci permettent de ne calculer qu'une seule fois une fonction utilisée plusieurs fois: c'est ce que nous faisons en pratique. Si le modèle est un corps différentiel, la dérivation d est une opération supplémentaire, et les fonctions calculées sont des polynômes différentiels conditionnés par des tests.

Un problème P sur un corps différentiel K est défini par une certaine suite de circuit $C_n(\bar{x}, \bar{a})$, à paramètres $\bar{a}$ dans K, alors qu'un problème NP est défini par une suite de circuits dont on quantifie existentiellement certaines entrées. La question

Received July 2, 1997; revised November 26, 1997.
Key words and phrases. Complexity, Differential Field, Definissability of Types, Stability.

0022-4812/99/6402-0028/$2.40

$P = NP$ devient un problème d'élimination algorithmique des quanteurs. Si k est une sous-structure de K, si Π est un problème P sur K, nous pouvons nous demander si sa restriction Π_k aux mots sur k est P sur k. Si cela est vrai pour tous les problèmes et pour tous les modèles k et K d'une théorie T, cette théorie est appelée P-stable par Chapuis et Koiran ([4]). Pour que le problème Π_k soit P, la suite de circuits qui le définit doit utiliser des paramètres uniquement de k. Si nous nous plaçons dans une théorie ω-stable, comme la théorie des corps algébriquement clos ou la théorie des corps différentiellement clos, nous savons qu'une telle suite utilisant uniquement des paramètres de k existe. Il nous faut encore trouver une manière polynômiale d'obtenir cette suite à partir de celle qui définit Π. C'est une version algorithmique et même polynômiale de la définissabilité des types sans quanteurs. Pour les corps de caractéristique 0, la P-stabilité est montrée par Blum, Cucker, Shub et Smale dans [2]. Nous le montrons ici pour les corps différentiels de caractéristique 0. Cela nous conduit à comparer la question $P = NP$ dans les corps algébriquement clos et dans les corps différentiellement clos.

Dans la première partie, nous donnons les propriétés des corps différentiels qui nous sont utiles, puis nous définissons les circuits et les classes de complexité. Dans la deuxième partie, nous donnons une preuve de la P-stabilité de la théorie des corps de caractéristique 0 qui utilise la définition des classes de complexité par les circuits, puis nous montrons la P-stabilité de la théorie des corps différentiels de caractéristique 0 ainsi que certaines conséquences de ce théorème.

1.1. Les corps différentiels. Les définitions et propriétés des corps différentiels peuvent être trouvés dans les livres de Kolchin ([6]) et Poizat ([9]), et dans l'article de Wood ([12]).

Un anneau différentiel est un anneau commutatif $(K, 0, 1, +, -, \times)$ muni d'une dérivation d, c'est-à-dire d'une opération interne de K dans K qui vérifie, pour tout couple (x, y) d'éléments de K: $d(x + y) = dx + dy$ et $d(xy) = xdy + ydx$. Si K est un corps, K est appelé corps différentiel. Dans la suite, nous considérons uniquement des corps et des corps différentiels de **caractéristique nulle**. Les éléments de dérivée nulle de K sont appelées constantes. Ils forment un sous-corps de K. C'est un ensemble définissable au sens de la théorie des corps différentiels. Remarquons que tout corps peut être muni d'une structure de corps différentiel: il suffit de prendre la dérivée nulle partout. Pour noter les dérivées successives, nous écrirons selon les cas $d^n x$ ou $x^{(n)}$.

Définissons l'anneau différentiel des polynômes différentiels en une variable $K[X]_d$. C'est l'anneau $K[X, X^{(1)}, \ldots, X^{(n)}, \ldots]$ des polynômes à coefficients dans K et à une infinité dénombrable de variables $X^{(n)}$. La dérivée prolonge celle de K. Elle est définie de manière unique par les relations: $dX^{(n)} = X^{(n+1)}$. Nous définissons de manière analogue le corps différentiel $K(X)_d$ des fractions rationnelles différentielles et ceux des polynômes différentiels en plusieurs variables. A chaque polynôme différentiel $P(X)$ est associée naturellement une fonction polynôme différentielle. L'image d'un élément a de K par la fonction associée à $X^{(n)}$ est $a^{(n)}$.

Un sous-ensemble I d'un anneau différentiel est appelé idéal différentiel premier si c'est un idéal premier stable par dérivation. Si c est un élément du sur-corps différentiel K du corps différentiel k, le sous-ensemble I_c de $k[X]_d$ constitué des

polynômes différentiels qui annulent c est un idéal différentiel premier de $k[X]_d$. Soit P un polynôme différentiel en une variable X. Nous appelons idéal différentiel engendré par P, noté $(P)_d$, l'idéal de l'anneau des polynômes différentiels $K[X]_d$ engendré par P et ses dérivées successives.

L'**ordre** d'un polynôme différentiel non nul $P(X)$ est le plus grand indice i tel que $X^{(i)}$ apparaisse avec un degré au moins un dans $P(X)$. Si r est l'ordre de $P(X)$, son **degré** est son degré partiel en $X^{(r)}$. Si son ordre est r et son degré est v, son **niveau** est le couple (r, v). Les niveaux sont ordonnés par l'ordre lexicographique sur les couples d'entiers. Par convention, le polynôme nul est de niveau strictement inférieur à tous les autres polynômes différentiels.

Si K est un corps différentiel de caractéristique nulle, si k est un sous corps différentiel de K, un élément c de K sera dit **différentiellement transcendant**, ou d-transcendant sur k s'il n'annule aucun polynôme différentiel non nul à coefficients dans k. Dans le cas contraire, c est appelé **différentiellement algébrique** , ou d-algébrique sur k. Dans ce cas, un polynôme différentiel M de niveau minimal et irréductible qui annule c est appelé **polynôme minimal** de c. Si M est d'ordre r, alors $c, c^{(1)}, \ldots, c^{(r-1)}$ sont algébriquement indépendants sur k.

Si M est un polynôme différentiel non nul d'ordre r et de degré v, la **séparante** S **de** M est le polynôme différentiel $\partial M/\partial X^{(r)}$, de niveau strictement inférieur au niveau de M. Le **coefficient initial** Δ de M est le coefficient dominant de M vu comme un polynôme en $X^{(r)}$. C'est un polynôme différentiel d'ordre strictement inférieur à r. Nous avons la propriété suivante: pour tout polynôme différentiel P, il existe des entiers i et j, des polynômes différentiels Q d'ordre au plus r et R de niveau strictement inférieur à (r, v) tels que $S^i P$ est congru à Q modulo $(M)_d$ et $\Delta^j Q$ est congru à R modulo (M). En particulier, il existe un polynôme différentiel S_i de niveau strictement inférieur à (r, v) et un entier l tels que $\Delta^l S^i$ est congru à S_i modulo (M). Cette propriété nous permet de caractériser I_c. Soit c un élément du corps différentiel K d-algébrique sur le sous-corps différentiel k, M un polynôme minimal de c sur k, de séparante S et de coefficient initial Δ. Alors, l'ensemble I_c des polynômes de $k[X]_d$ qui annulent c est égal à l'ensemble des polynômes P de $k[X]_d$ tels qu'il existe des entiers i et j et $S^i \Delta^j P$ appartient à (M). Si $S^i \Delta^j P$ est congru modulo (M) au polynôme différentiel R de niveau strictement inférieur à M, pour tester si P est nul en c, il suffit de tester si R identiquement nul, i.e. si les v coefficients de R sont identiquement nuls. C'est pourquoi nous utilisons la représentation d'un polynôme différentiel P quelconque modulo I_c par $2(v+1)$ polynômes différentiels d'ordre au plus $(r-1)$: Δ^j, Δ^l, les v coefficients de R et les v coefficients de S_i vus comme des polynômes en $X^{(r)}$ de degré au plus $(v-1)$. Ainsi, si nous connaissons les polynômes différentiels qui représentent $X^{(r)^v} \ldots X^{(r)^{2v-2}}$ modulo $(M)_d$, nous pouvons sommer et multiplier des polynômes différentiels P_1 et P_2 modulo I_c en effectuant un nombre fixe de multiplications et d'additions des polynômes différentiels qui représentent P_1, P_2 et $X^{(r)^v} \ldots X^{(r)^{2v-2}}$. D'autre part, la dérivation de M nous permet de trouver les représentants de $X^{(r+1)}$ modulo $(M)_d$. En dérivant plusieurs fois M, nous calculons par récurrence les dérivées successives de $X^{(r)}$. Le nombre d'opérations que nous devons effectuer sur les représentants dépend polynômialement du nombre de dérivées que nous voulons obtenir.

Il existe un analogue de la clôture algébrique pour les corps: c'est la clôture différentielle pour les corps différentiels. Robinson ([11]) a défini la théorie des corps différentiellement clos de caractéristique 0 comme la modèle-complétion de la théorie des corps différentiels de caractéristique 0. Dans [1], Lenore Blum en donne une axiomatisation. Un corps K est **différentiellement clos** si pour tous polynômes différentiels P et Q tels que Q soit d'ordre strictement inférieur à P, il existe un élément x de K qui annule P mais pas Q. De plus, tout corps K possède une clôture différentielle, i.e. un sur-corps $\bar{K}$ différentiellement clos tel que pour tout sur-corps différentiellement clos L de K, $\bar{K}$ soit isomorphe à un sous-corps de L.

1.2. Les circuits. Les circuits permettent de définir des ensembles. Les ensembles définissables par des circuits sont exactement les ensembles définissables par des formules sans quanteurs. L'intérêt des circuits est de se présenter sous une forme plus concise que les formules. Dans la pratique, quand nous voulons évaluer une formule, nous commençons par calculer tous les termes qui y apparaissent. Quand un terme se trouve à différents endroits, nous ne le calculons qu'une fois. Les circuits formalisent cette technique naturelle de calcul. Dans le circuit qui correspond à la formule, le terme peut n'apparaître qu'une fois, mais être utilisé plusieurs fois.

Un **circuit** est un graphe fini, orienté, et sans cycle orienté. Les sommets sont appelés **portes**, et les arêtes sont appelées **flèches**. Les portes qui ne reçoivent pas de flèches sont les **entrées**, et les portes qui n'en émettent pas sont des **sorties**. Les portes sont étiquetées. Un **circuit arithmétique** sur le corps K est un circuit dont les entrées sont étiquetées par un élément de K, appelé **paramètre**, ou par une variable, et dont les autres portes reçoivent deux flèches et sont étiquetées par une des opérations du corps $\times$, $/$, $+$ ou -. Un **circuit sur la structure** K est un circuit arithmétique sur K qui, en outre, peut avoir des portes qui ne reçoivent qu'une seule flèche et sont étiquetées par le test «$x = 0$?». Un **circuit différentiel** sur un corps différentiel K est un circuit arithmétique sur K dont certaines portes ne reçoivent qu'une flèche et sont étiquetées par d. Un **circuit sur la structure** (K, d) est un circuit différentiel sur K qui peut de plus avoir des portes de test.

Dans le cas général défini par Poizat ([5, 9]), si nous ne nous restreignons pas comme ici à des structures de corps ou de corps différentiels, nous avons besoin de portes de sélection. Ce sont des portes qui reçoivent trois flèches et qui permettent un calcul par cas: si x est nul le calcul donne y, si x vaut 1 le calcul donne z, et sinon peut importe. Si nous avons à notre disposition les opérations arithmétiques, une telle porte peut être simulée par le polynôme $(1 - x)y + xz$. C'est pour cela qu'ici, nous n'utilisons pas de porte de sélection.

Si un circuit a n entrées étiquetées par les variables $\bar{x} = (x_1, \ldots, x_n)$, le circuit est noté $C(\bar{x})$. Le **calcul sur un n-uple** d'éléments de K s'effectue alors de manière naturelle, de proche en proche. Aux variables d'entrée sont affectés les éléments de K. Une porte étiquetée par une opération effectue cette opération. Une porte étiquetée par une test émet 1 si la valeur qu'elle reçoit est nulle, et 0 sinon. Un **circuit de décision** est un circuit qui n'a qu'une sortie, laquelle est étiquetée par un test. S'il a n entrées, il décide un ensemble E de n-uples s'il calcule 1 pour un n-uple de cet ensemble et 0 sinon. La **taille** d'un circuit est son nombre de portes, et sa **profondeur** est la longueur du plus long chemin qui relie une entrée à une sortie. Deux circuits sont par définition **équivalents** si, pour toute entrée, les deux calculs sont égaux.

Remarquons ensuite que tout circuit sur la structure K est équivalent à un circuit de taille comparable qui n'utilise pas la division. En effet, toutes les portes d'un circuit arithmétique calculent des fractions rationnelles des entrées. Nous pouvons dédoubler chaque porte p en un couple de portes (p_1, p_2) qui calculera respectivement le numérateur et le dénominateur, et simuler les opérations arithmétiques sans plus utiliser la division. Par exemple, si la porte r est étiquetée par une division et reçoit des flèches des portes p et q alors, dans le nouveau circuit, la porte r_1 est étiquetée par une multiplication et reçoit des flèches des portes p_1 et q_2, et la porte r_2 est étiquetée par une multiplication et reçoit des flèches des portes p_2 et q_1. Pour les portes de test, il suffit de tester si le numérateur est nul. Cette technique reste valable dans le cas des circuits sur sur la structure (K, d). Le circuit obtenu a au plus six fois plus de portes que le circuit de départ. Par la suite, il n'y aura plus de porte de division dans les circuits.

Les sorties d'un circuit arithmétique sur un corps calculent des polynômes dont les variables sont les variables d'entrée du circuit, et dont les coefficients sont des polynômes à coefficients entiers des paramètres d'entrée. Soit C un circuit arithmétique, à une seule variable d'entrée x, sur un corps K infini. Soit $P(x)$ le polynôme calculé par une de ses sorties. Ce polynôme est-il identiquement nul? Nous pouvons le savoir facilement si nous connaissons son développement: le polynôme est identiquement nul si et seulement si tous les coefficients de son développement sont nuls. Or nous ne connaissons du polynôme qu'un circuit qui le calcule. Nous pouvons certes en déduire la forme développée. Mais alors que le circuit est de taille τ, la forme développée peut faire apparaître un nombre exponentiel en τ de monômes. C'est le cas par exemple pour $(1 + x)^{2^n}$, qui peut se calculer par un circuit de taille $(n + 4)$, mais qui compte $(2^n + 1)$ monômes dans sa forme développée. Or, en général, nous voulons garder des objets de taille minimale, et donc si possible polynômiale. Développer les polynômes n'est donc pas une bonne méthode. Une façon rapide de faire nous sera donnée par le théorème des témoins de [2].

1.3. Les classes de complexité. Si K est un corps différentiel, un problème Π est $P_K/poly$ (resp. $P_K^d/poly$) s'il existe une suite de circuits de décision sur la structure $\{0, 1\}$ (resp. sur la structure $(\{0, 1\},d)$), c'est-à-dire sans paramètre, $(C_n(x_1, \ldots, x_n, y_1, \ldots, y_m))_{n\geq 0}$, dont la taille est bornée polynômialement en n, et des éléments $\bar{c} = (c_1, \ldots, c_m)$ de K tels que pour toute suite $\bar{a} = (a_1, \ldots, a_n)$ d'éléments de K, $\bar{a}$ appartienne à Π si et seulement si $C_n(\bar{a}, \bar{c})$ calcule 1. Le problème Π est P_K (resp. P_K^d) si, de plus, la suite de circuits sans paramètres est calculable par un algorithme standard en temps polynômial en n.

Un problème Π est $NP_K/poly$ (resp. $NP_K^d/poly$, NP_K, NP_K^d) s'il existe un problème Σ qui est $P_K/poly$ (resp. $P_K^d/poly$, P_K, P_K^d), et un polynôme q, tels qu'une suite $\bar{x} = (x_1, \ldots, x_n)$ d'éléments de K soit dans Π si et seulement s'il existe une suite $\bar{y} = (y_1, \ldots, y_{q(n)})$ d'éléments de K telle que la suite $(\bar{x}, \bar{y})$ appartienne à Σ.

Si C est une classe de complexité, $C/poly$ est sa version non-uniforme.

Nous voyons ici que le problème $P = NP$? est un problème d'élimination rapide des quanteurs. En particulier, le problème n'a aucun sens dans une structure qui n'élimine pas les quanteurs.

§2. L'élimination des paramètres.

2.1. L'élimination des paramètres dans les corps. Commençons par énoncer le théorème des témoins de Blum, Cucker, Shub et Smale ([2]), généralisé pour un corps K quelconque de caractéristique nulle.

THÉORÈME 1 (théorème des témoins). *Soit $F(\bar{x}, \bar{t}) = F(x_1, \dots, x_r, t_1, \dots, t_s)$ un polynôme produit par un circuit arithmétique d'entrées $1, x_1, \dots, x_r, t_1, \dots, t_s$ et de taille τ. Soit $N \geq 2^{4(r+s)\tau^2+4}$. Pour tout uple $\bar{a} = (a_1, \dots, a_r)$ d'éléments du corps K de caractéristique nulle, nous définissons $F_{\bar{a}}(\bar{t}) = F(\bar{a}, \bar{t})$. Alors $F_{\bar{a}}$ est le polynôme nul si et seulement si pour tout w appartenant à $\{2, a_1, \dots, a_r\}$, $F_{\bar{a}}(w^N, w^{N^2}, \dots, w^{N^s}) = 0$.*

DÉMONSTRATION DU THÉORÈME 1. Ce théorème est un ensemble d'énoncés universels du premier ordre de la théorie des corps. Le cas où K est la clôture algébrique de $\mathbf{Q}$ est traité dans [2]. Puisque la théorie des corps algébriquement clos de caractéristique nulle est complète, ce théorème est vrai pour tout corps algébriquement clos. De plus, tout corps possède une extension algébriquement close. Donc le théorème est vrai pour tout corps de caractéristique nulle. ⊣

Nous pouvons maintenant énoncer le théorème d'élimination dans les corps de Blum, Cucker, Shub et Smale ([2]):

THÉORÈME 2 (P-stabilité de la théorie des corps de caractéristique nulle). *Soit K un corps de caractéristique nulle, et k un sous-corps de K. Soit Π un problème P_K. Alors la restriction de Π à k est P_k. Le théorème est également vrai pour le cas non-uniforme.*

Dans [2], les classes de complexité sont définies à l'aide d'une généralisation des machines de Turing, alors qu'ici elles le sont à l'aide de circuits. Nous adaptons donc la démonstration aux circuits.

LEMME 1 (élimination des paramètres dans un circuit). *Soit K un corps de caractéristique nulle, k un sous-corps de K et $\bar{a} = (a_1, \dots, a_m)$ un uple de paramètres de K. Alors il existe des paramètres $(b_1, \dots, b_r)$ de k tels que si $A(x_1, \dots, x_n, y_1, \dots, y_m)$ est un circuit de décision sur la structure $\{0, 1\}$, il existe un circuit $B(x_1, \dots, x_n, z_1, \dots, z_r)$ sur la structure $\{0, 1\}$ tel que $A(\bar{x}, \bar{a})$ et $B(\bar{x}, \bar{b})$ sont équivalents pour des entrées de k. De plus, B peut-être obtenu par un algorithme en temps polynômialement borné par la taille de A.*

DÉMONSTRATION. Il suffit de considérer $K = k(\bar{a}) = k(a_1) \dots (a_m)$. De plus, si pour $m = 1$ et $K = k(a)$, et indépendemment de A, nous pouvons éliminer en temps polynômial les paramètres de $k(a)$ en ajoutant des paramètres de k, alors, par récurrence, nous aurons prouvé le théorème pour tout m.

En effet, supposons que a n'appartient pas à k. Si e est un paramètre de $k(a)$, alors e est une fraction rationnelle de a à coefficients dans k. Nous remplaçons donc l'entrée e par la sortie d'un circuit qui calcule cette fraction, et qui a pour entrées a ainsi que des paramètres de k. Nous obtenons une suite de circuits qui n'a plus e comme paramètre, et qui utilise la division. D'après la remarque faite lors de la définition des circuits, nous avons aussi une suite de circuits équivalents qui n'utilise pas la division. Nous pouvons donc éliminer tous les paramètres de

$k(a)$ en multipliant la taille du circuit par six. Il ne nous reste maintenant plus qu'à éliminer a.

Lorsque nous voulons connaître la valeur de la sortie de $A(\bar{x}, a)$ sur une entrée donnée, nous devons tester si certains polynômes calculés au fur et à mesure par le circuit sont nuls en $(\bar{x}, a)$. Ces polynômes peuvent être considérés comme des polynômes en a dont les coefficients sont des polynômes à coefficients entiers de $\bar{x}$.

Si a est transcendant sur k, un polynôme P à coefficients dans k est nul en a si et seulement s'il est identiquement nul. Le théorème des témoins nous donne alors une méthode pour tester la nullité de ce polynôme sans utiliser a. Nous l'appliquons avec $s = 1$, τ est la taille de A, $x_1 \dots x_r$ sont les entrées de A autres que y et $N = 2^{4(r+1)\tau^2+4}$. Nous commençons par former le circuit qui calcule 2^N: c'est un circuit arithmétique, qui a une entrée étiquetée par le paramètre 2, et $(4(r+1)\tau^2+4)$ portes étiquetées par des multiplications. La première reçoit ses deux flèches de l'entrée, dont elle calcule le carré. La deuxième reçoit ses deux flèches de la première, et ainsi de suite jusqu'à la dernière, qui calcule donc 2^N. Nous formons de la même manière les circuits qui calculent $\{x_1^N, \dots, x_r^N\}$. Nous obtenons un circuit total de taille $(r+1)(4(r+1)\tau^2+5)$, donc polynômiale en τ. Or P est identiquement nul si et seulement s'il s'annule sur $\{2^N, x_1^N, \dots, x_r^N\}$. Nous remplaçons dans le circuit A l'entrée y par la sortie du circuit qui calcule 2^N. Nous obtenons un circuit qui teste si P s'annule en 2^N. Avec r copies de A, nous testons de même si P s'annule en $\{x_1^N, \dots, x_r^N\}$. Avec r portes supplémentaires, nous multiplions ces $(r+1)$ tests, et nous obtenons un test équivalent au test $P(a) = 0$ sans utiliser le paramètre a dans le circuit. Nous remplaçons ensuite les flèches issues des portes qui testent la nullité de P en a dans les $(r+1)$ copies de A par des flèches issues de la porte qui calcule le produit. Nous faisons cela pour toutes les portes de test du circuit A. Nous obtenons finalement de manière algorithmique et en temps polynômial un circuit équivalent et qui n'utilise que des paramètres de k. Sa taille est bornée par un polynôme en τ^4.

Si a est algébrique sur k, un polynôme P est nul en a si et seulement s'il est multiple du polynôme minimal M de a, ou encore si et seulement si le reste de la division euclidienne de P par M est le polynôme identiquement nul. Si ce reste est donné comme la suite de ses coefficients, qui sont des polynômes à coefficients entiers dont les variables sont les entrées autres que y, tester la nullité de P en a revient à tester si tous ces coefficients sont nuls. De plus, le nombre de ces coefficients est borné par le degré t de M. Dans le circuit A, nous allons remplacer chaque porte qui n'est pas un test, et qui donc calcule un polynôme Q, par un t-uple de portes, qui calcule les coefficients du reste de la division euclidienne de Q par M. Les additions deviennent des additions terme à terme des t-uples, et pour la multiplication, nous n'avons besoin que de connaître les t-uples qui représentent $y^t \dots y^{2t-2}$, et donc de nouveaux paramètres de k. Les tests sont remplacés par t tests suivis de la multiplication des résultats. La taille du nouveau circuit est bornée linéairement par τ, et il est clair que nous avons bien décrit ici un algorithme polynômial. ⊣

DÉMONSTRATION DU THÉORÈME 2. Si Π est un problème $P_K/poly$ (resp. P_K), il existe une suite de circuits de décision $(A_n(x_1, \dots, x_n, y_1, \dots, y_m))_{n\geq 1}$ sur la structure $\{0, 1\}$, de tailles polynômiales en n (resp. produits par un algorithme travaillant en temps polynômial en n) et des éléments $\bar{a} = (a_1, \dots, a_m)$ de K tels

que pour toute suite $\bar{x} = (x_1, \ldots, x_n)$ d'éléments de K, $\bar{x}$ appartient à Π si et seulement si $A_n(\bar{x}, \bar{a})$ calcule 1.

En appliquant le lemme précédent à chaque circuit A_n, nous obtenons de manière polynômiale une suite de circuits équivalents sur k et n'utilisant que des paramètres de k, et nous avons donc montré le résultat. ⊣

2.2. L'élimination des paramètres dans les corps différentiels. A partir de maintenant, K est un corps différentiel de caractéristique nulle, et k est un sous-corps différentiel de K.

THÉORÈME 3 (P-stabilité de la théorie des corps différentiels de caractéristique nulle). La restriction à k d'un problème P_K^d est P_k^d. Le résultat vaut également pour la classe non-uniforme $P/poly$.

Si Π est un problème P_K^d, il existe une suite de circuits de décision sur la structure (K, d) qui résout le problème Π. Cette suite de circuits utilise des paramètres de K. Ce sont ces paramètres que nous voulons éliminer, de manière à obtenir une suite de circuits sur la structure (k, d) qui décide de la restriction de Π à k.

Un circuit sur la structure (K, d) effectue, outre les opérations possibles dans les corps, des dérivations. Dans un premier temps, nous allons transformer le circuit de manière à ce que les dérivations soient les toutes premières opérations effectuées sur les entrées, les opérations suivantes étant celles autorisées dans les corps. Un circuit mis sous cette forme est appelé un circuit réduit. Nous pourrons alors dans un deuxième temps éliminer les paramètres de K, en nous ramenant au cas des corps.

Pour dériver plusieurs fois, nous utiliserons les puissances symboliques. Pour cela, nous avons besoin des coefficients binômiaux.

LEMME 2 (calcul du triangle de Pascal). *Il existe un circuit T_m arithmétique de taille au plus $[2 + m(m-1)/2]$, ayant pour seule entrée le paramètre 1, calculable par un algorithme standard en temps polynômial, dont les portes calculent les C_j^i pour j compris entre 1 et m, et i compris entre 0 et j.*

DÉMONSTRATION DU LEMME 2. Le circuit cherché reproduit les calculs du triangle de Pascal, grâce à l'égalité: $C_{i+1}^{j+1} = C_i^j + C_i^{j+1}$. Le circuit T_1 est constitué uniquement de deux entrées, étiquetées 1, qui sont aussi des sorties. A partir du circuit T_m de taille $(2+m(m-1)/2)$, nous construisons le circuit $T_{(m+1)}$ en ajoutant m portes: la première somme 1 et la première sortie de T_m, la deuxième somme la première et la deuxième sortie de T_m, et ainsi de suite jusqu'à la dernière qui somme la dernière sortie de T_m et 1. Le circuit $T_{(m+1)}$ est de taille $[2 + m(m-1)/2 + m]$, i.e. $[2 + m(m+1)/2]$. ⊣

REMARQUE. Comme le triangle de Pascal est symétrique, il suffit de calculer les C_{2n}^i pour i compris entre 1 et n, et les C_{2n+1}^i pour i compris entre 1 et n. Nous aurions donc pu trouver un circuit un peu plus petit.

LEMME 3 (réduction d'un circuit). *Tout circuit sur la structure (K, d), $A(\bar{x})$ de taille τ et de profondeur h, est équivalent à un circuit $B(\bar{x})$ sur la structure (K, d), réduit, de taille au plus $4\tau^3$ et de profondeur au plus $2h \log_2 h$ (pour τ et h assez grands). De plus, $B(\bar{x})$ peut être obtenu à partir de $A(\bar{x})$ par un algorithme standard en temps polynômial en τ.*

DÉMONSTRATION DU LEMME 3. Définissons la **d-hauteur** $\delta(p)$ d'une porte p d'un circuit C par le nombre maximal de portes de dérivations sur un chemin allant de p exclue à une sortie s du circuit incluse. Si p est une porte d'un circuit C, **le circuit au dessus de** p est le sous circuit de C qui permet de faire le calcul en p, i.e. c'est le sous-circuit de C qui contient p et tel que si la porte q en fait partie, alors toutes les portes qui émettent une flèche vers q en font partie également.

Soit δ le nombre de portes de dérivation de $A(\bar{x})$. Nous ajoutons sous chaque porte p du circuit qui n'est pas une dérivation δ portes de dérivations successives. Ce faisant, nous ajoutons de nouvelles sorties. La taille du circuit est au plus multipliée par $(\delta+1)$, et le nouveau nombre de dérivées est au plus $\delta\tau$. Nous allons transformer ce circuit pas à pas, par le bas, en supprimant les portes de dérivation de d-hauteur nulle qui ne sont pas situées directement sous les entrées, et en ajoutant des portes d'addition et de multiplication, mais en laissant inchangés les circuits au dessus des autres portes de dérivations, ce qui nous permettra de garder un nombre de portes polynômial. Nous commençons par adjoindre le circuit T_δ du Lemme 2, qui a $[2+\delta(\delta-1)/2]$ portes et est de hauteur $(\delta-1)$.

Considérons une porte de dérivation p de d-hauteur nulle qui n'est pas une sortie. Elle est la dernière d'une suite de portes $p_0, \ldots, p_m = p$ reliées par des flèches, où p_0 n'est pas une porte de dérivation, $p_1, \ldots, p_m$ sont des portes de dérivations successives de p_0 et m est au plus égal à δ. Si p_0 est une porte d'entrée, il n'y a rien à faire. Si p_0 est un test, alors le résultat est soit 0 soit 1, donc des constantes, et nous remplaçons toutes ses dérivées par le paramètre 0. Si p_0 est une addition, une soustraction ou une multiplication, alors elle reçoit des flèches de deux portes q et r. Sous chacune de ces portes, il y a δ portes de dérivations successives: $q_1, \ldots, q_\delta$ et $r_1, \ldots, r_\delta$. Si p_0 est une addition (resp. une soustraction), alors pour i compris entre 1 et m, nous remplaçons p_i par une porte d'addition (resp. de soustraction) qui somme q_i et r_i. La profondeur du circuit n'augmente pas.

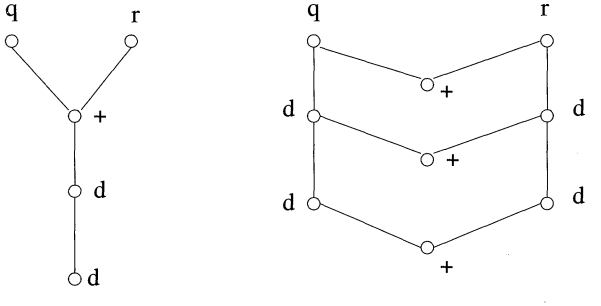

Figure. *Calcul de* $d^2(q+r) = d^2q + d^2r$

Si p_0 est une multiplication, alors pour i compris entre 1 et m, nous devons former le circuit qui calcule

$$d^i(p_0) = d^i(qr) = \sum_{j=0}^{i} C_i^j \, d^j(q) \, d^{i-j}(r) = \sum_{j=0}^{i} C_i^j \, q_i \, r_{i-j}.$$

Ce circuit a pour entrées les q_i, les r_j et des portes du circuit qui calcule le triangle de Pascal. *Il a en outre $2i$ portes de multiplication et i portes d'addition. La* profondeur du circuit augmente d'au plus $(\ln(i+1)+1)$.

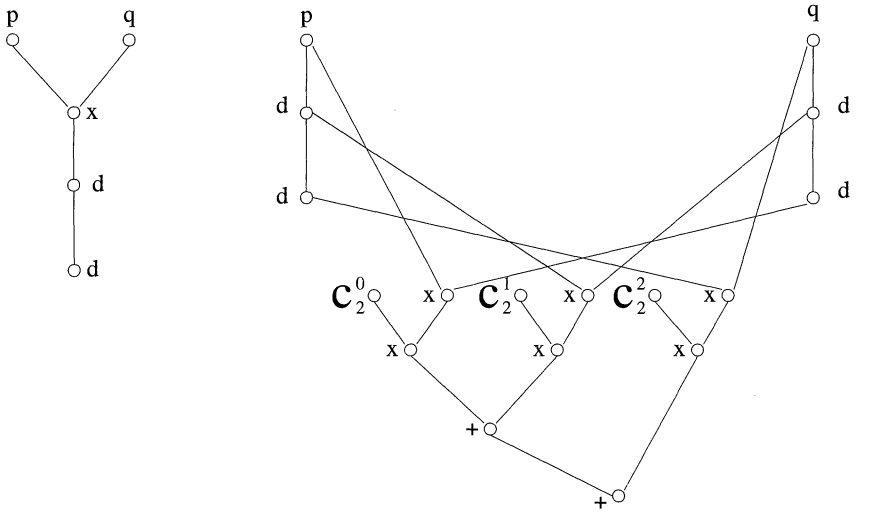

Figure. *Calcul de* $d^2(qr) = rd^2q + 2dqdr + qd^2r$

Dans tous les cas, nous pouvons supprimer les portes $p_1, \ldots, p_m$, et donc diminuer le nombre total de portes de dérivation du circuit. Pour chaque porte de dérivation du circuit d'origine, et pour chaque porte de calcul que nous devons «remonter», nous créons au plus 3δ portes et la profondeur augmente d'au plus $(1+\ln(\delta+1))$. Or δ est majoré à la fois par τ et par h. Donc le circuit obtenu est de taille au plus $[2+\tau(\tau-1)/2+\tau(\tau+1)+3\tau^3]$ et de profondeur au plus $2h\log_2 h$.

Lorsque toutes les portes de d-hauteur nulle sont des entrées, nous pouvons les supprimer, de manière à ce qu'il ne reste plus qu'une sortie: celle du circuit initial. De cette manière, nous obtenons le circuit $B(\bar{x},\bar{y})$ par un algorithme standard en temps polynômial en τ. ⊣

Maintenant que nous savons mettre un circuit sous forme réduite, nous éliminons les paramètres.

LEMME 4 (élimination des paramètres d'un circuit sur la structure (K,d)).

Si $(a_1,\ldots,a_m)$ sont des paramètres de K, il existe des paramètres $(b_1,\ldots,b_r)$ de k tels que tout circuit de décision $A(\bar{x},\bar{a})$ sur la structure (K,d) est équivalent pour les entrées de k à un circuit de décision $B(\bar{x},\bar{b})$ sur la structure (k,d). De plus, B peut-être obtenu par un algorithme en temps polynômialement borné par la taille de A.

DÉMONSTRATION. Nous pouvons considérer le cas où K est le corps différentiel engendré par k et $\bar{a}$, i.e. $K = k(\bar{a})_d$. De même que dans le cas des corps, nous allons montrer que si $K = k(a)_d$, nous pouvons éliminer les paramètres de $k(a)_d$

en ajoutant des paramètres de k, indépendemment du circuit considéré. Nous supposons donc que $\bar{a} = (a, a_1, \ldots, a_m)$, où $a_1, \ldots, a_m$ sont des éléments de $k(a)_d$.

Appliquons le Lemme 3 de réduction au circuit A: nous obtenons un circuit réduit $C(x_1, \ldots, x_n, y, y_1, \ldots, y_m)$, calculable par un algorithme standard en temps polynômial et équivalent à A. Nous supposons que sous chaque entrée de B, il y a au plus δ dérivations successives.

Si a_m n'appartient pas à k mais appartient à $k(a)_d$, alors a_m est égal à une fraction rationnelle différentielle de a à coefficients dans k. Nous remplaçons l'entrée y_m par un circuit à paramètres dans k qui calcule a_m et qui utilise la division. Nous faisons de même pour $a_{m-1}, \ldots, a_1$. Puis nous dédoublons les portes pour ne plus utiliser la division. Nous obtenons le nouveau circuit par un algorithme standard linéaire, mais le circuit obtenu n'est plus réduit: il faut lui appliquer le lemme de réduction à nouveau avant d'éliminer a.

Si a est d-transcendant sur k, nous pouvons l'éliminer sans ajouter de paramètre de k, en utilisant l'élimination d'un paramètre transcendant pour un corps. En supprimant les flèches entre les entrées et leurs dérivées successives, nous créons de nouvelles entrées. Nous obtenons un circuit au sens des corps, $C(x_1, \ldots, x_{n(\delta_n+1)}, y_0, \ldots, y_{\delta_n})$, calculable par un algorithme standard en temps polynômial, et tel que tout uple $\bar{x}$ de K appartient à Π si et seulement si $C(\bar{x}, \bar{x}^{(1)}, \ldots, \bar{x}^{(\delta)}, a, a^{(1)}, \ldots, a^{(\delta)})$ calcule 1. Les paramètres $a, a^{(1)}, \ldots, a^{(\delta)}$ sont algébriquement indépendants sur k. Nous pouvons donc appliquer l'élimination des paramètres transcendants dans le cas des corps et les éliminer un à un. Ensuite, il suffit de restaurer les flèches de dérivations successives entre les entrées.

Si a est d-algébrique sur k, soit $M(X)$ son polynôme différentiel minimal sur k. Il est de niveau (r, v). Ses coefficients sont des paramètres de k. A priori, il y a δ portes de dérivations successives sous l'entrée y. Nous ne laissons que les $(r-1)$ premières, et nous supprimons les autres. Nous allons calculer modulo I_a dans le circuit.

Pour cela, nous remplaçons toutes les portes p de C par un $2(v+1)$-uple de portes qui calculent les $2(v+1)$ polynômes différentiels de niveau strictement inférieur à (r, v) qui représentent le polynôme différentiel calculé en p modulo I_a. Nous ajoutons les circuits qui calculent $y^{(r)^v} \ldots y^{(r)^{2v-2}}$ ainsi que $y^{(r+1)}$ modulo I_a. Puis nous effectuons les calculs comme ceci est expliqué dans le paragraphe sur les corps différentiels. Nous commençons par calculer les dérivées de y jusqu'à l'ordre δ, puis nous simulons la suite des calculs. Comment faire lorsque nous avons une porte de test? Imaginons que nous voulons tester si le polynôme $P(a)$ calculé par la porte p de l'ancien circuit est nul. Nous savons que la réponse est oui si et seulement si R est le polynôme nul. Or parmi les $2(v+1)$ portes qui remplacent p, v portes calculent les coefficients de R, vu comme un polynôme en $y^{(r)}$, qui sont des polynômes différentiels d'ordre au plus $(r-1)$. Il suffit donc, pour tester si R est nul, de tester si les v coefficients sont nuls, et de multiplier les résultats.

D'autre part, comme M est d'ordre r, les éléments $(a, a^{(1)}, \ldots, a^{(r-1)})$ sont algébriquement indépendants sur k. Pour éliminer a, il suffit de procéder comme dans le cas où a est d-transcendant sur k. ⊣

DÉMONSTRATION DU THÉORÈME 3. Soit Π un problème $P_K^d/poly$ (resp. P_K^d). Alors il existe une suite de circuits sur la structure $(\{0,1\},d),(A_n(x_1,\ldots,x_n,y_1,\ldots,y_m))_{n\geq 1}$, de tailles polynômiales (resp. que nous pouvons obtenir par un algorithme standard polynômial), et un uple $\bar{a}=(a_1,\ldots,a_m)$ d'éléments de K, tels que $\bar{x}=(x_1,\ldots,x_n)$ appartient à Π si et seulement si $A_n(\bar{x},\bar{a})$ calcule 1. Nous appliquons le lemme précédent à la suite de circuits, et nous obtenons par un algorithme polynômial une suite de circuits de décision sur la structure (k,d) équivalents. ⊣

2.3. Le problème $P = NP$? pour les corps différentiels. D'après [2], la question $P = NP$? a la même réponse dans tous les corps algébriquement clos de caractéristique nulle. Le théorème est également vrai pour les corps différentiellement clos de caractéristique nulle.

PROPOSITION 4. *La question $P = NP$? a la même réponse dans tous les corps différentiellement clos de caractéristique nulle. Il en est de même pour la question $P/poly = NP/poly$?.*

DÉMONSTRATION DE LA PROPOSITION 4. Comme deux corps différentiels quelconques ont une extension commune, il suffit de montrer que la réponse est la même pour deux corps différentiellement tels que: $k \subset K$.

Montrons tout d'abord que si $P_K^d = NP_K^d$, alors $P_k^d = NP_k^d$. Soit Π un problème NP_k^d. il existe un polynôme p, un entier q, des éléments $\bar{c}=(c_1,\ldots,c_q)$ de k, une suite de circuits $(C_n(y_1,\ldots,y_{p(n)},x_1,\ldots,x_n,z_1\ldots z_q))_{n\geq 1}$ sur la structure $(\{0,1\},d)$, obtenue en temps polynômial par un algorithme standard, tels que, pour tout uple $\bar{t}=(t_1,\ldots,t_n)$ d'éléments de k, $\bar{t}$ appartienne à Π si et seulement s'il existe un uple $\bar{b}=(b_1,\ldots,b_{p(n)})$ d'éléments de k, tels que k satisfasse $C_n(\bar{b},\bar{t},\bar{d})$. Soit Π_K l'ensemble des uples $\bar{t}=(t_1,\ldots,t_n)$ d'éléments de K tels qu'il existe un uple $\bar{b}=(b_1,\ldots,b_{p(n)})$ d'éléments de K, et K satisfait $C_n(\bar{b},\bar{t},\bar{c})$. Par définition, Π_K est NP_K^d, donc P_K^d. Or Π est la restriction de Π_K à k. Donc, d'après le théorème 3, nous pouvons éliminer les paramètres de K. Nous avons montré que $P_k^d = NP_k^d$.

La réciproque découle directement d'un résultat de Michaux ([8]). Soit SAT_K le problème de la satisfaisabilité des formules à paramètres dans K. C'est l'ensemble des mots $\bar{m}\bar{a}$ sur K tels que $\bar{m}$ est un mot booléen codant une formule du langage des corps différentiel $\phi(\bar{x},\bar{y})$ et K satisfait $\exists\bar{x}\phi(\bar{x},\bar{a})$. Or $P = NP$ dans un modèle donné si et seulement si SAT est P (cf. [10]). Supposons que $P_k^d = NP_k^d$ et que SAT_k est P_k^d.

Le résultat d'un calcul d'un circuit de décision ne dépend que des valeurs des tests du circuit. Pour un calcul du circuit $C(\bar{x},\bar{c})$ sur l'entrée $\bar{x}$, il existe une formule $\psi(\bar{x},\bar{c})$ de la théorie des corps différentiels telle que k satisfait $\psi(\bar{y},\bar{c})$ si et seulement si les résultats des tests du circuit sont les mêmes sur l'entrée $\bar{y}$ et sur l'entrée $\bar{x}$. En considérant tous les calculs qui acceptent l'entrée, c'est-à-dire dont le test final vaut 1, nous obtenons une formule $\Psi(\bar{x},\bar{c})$ telle que $C(\bar{x},\bar{c})$ calcule 1 si et seulement si $\Psi(\bar{x},\bar{c})$ est vraie. Si C est le circuit qui décide de SAT_k pour les entrées de taille n avec les paramètres $\bar{c}$, alors pour tout $\bar{m}$ code booléen d'une formule $\phi(\bar{x},\bar{y})$, k satisfait $\forall\bar{a}(\exists\bar{y}\phi(\bar{y},\bar{a}) \leftrightarrow \Psi(\bar{m}\bar{a},\bar{b}))$. Donc K satisfait aussi cette formule, et le circuit C décide des entrées de taille n de SAT_K avec les paramètres $\bar{b}$. Ceci nous

montre que le problème SAT_K est P_K^d et que $NP_K^d = P_K^d$. La démonstration est la même dans le cas non-uniforme. ⊣

PROPOSITION 5. *Si $P = NP$ pour les corps différentiellement clos de caractéristique nulle K, alors $P = NP$ pour les corps algébriquement clos de caractéristique nulle. Ceci est encore vrai pour la relation entre classes non-uniformes $P/poly = NP/poly$.*

DÉMONSTRATION DE LA PROPOSITION 5. Soit k un corps algébriquement clos de caractéristique nulle, et soit Π un problème NP_k. Il existe un polynôme p, un entier q, des éléments $\bar{c} = (c_1, \ldots, c_q)$ de k, une suite de circuits $(C_n(y_1, \ldots, y_{p(n)}, x_1, \ldots, x_n, z_1, \ldots, z_q))_{n \geq 1}$ sur la structure $\{0, 1\}$, obtenue en temps polynômial par un algorithme standard, tels que, pour tout uple $\bar{t} = (t_1, \ldots, t_n)$ d'éléments de k, $\bar{t}$ appartienne à Π si et seulement s'il existe un uple $\bar{b} = (b_1, \ldots, b_{p(n)})$ d'éléments de k, tels que k satisfasse $C_n(\bar{b}, \bar{t}, \bar{d})$.

Nous munissons k de la structure de corps différentiel en prenant une dérivée nulle sur k. Soit K la clôture différentielle de k. Cette clôture existe, et est différentiellement algébrique sur k ([7]). Soit Π_K l'ensemble des uples $\bar{t} = (t_1, \ldots, t_n)$ d'éléments de K tels qu'il existe un uple $\bar{b} = (b_1, \ldots, b_{p(n)})$ d'éléments de K, et K satisfait $C_n(\bar{b}, \bar{t}, \bar{c})$. Par définition, Π_K est NP_K, donc NP_K^d. Nous en déduisons, d'après l'hypothèse, que Π_K est P_K^d. Or Π est la restriction de Π_K à k. Donc, d'après le théorème 3, nous pouvons éliminer les paramètres de K. De plus, comme tous les éléments de k sont de dérivée nulle, nous pouvons remplacer toutes les portes de dérivation du circuit par 0. Donc Π est P_k. Nous avons montré que $P_k = NP_k$, et donc que $P = NP$ pour tous les corps algébriquement clos de caractéristique nulle. La démonstration du cas non-uniforme est exactement la même. ⊣

REMARQUE. Si Π est un problème P_K^d sur le corps différentiel K, mais si Π est également défini par une suite de circuits de décision sur la structure k, où k est le corps des constantes de K, utilisant un nombre fini de paramètres pour toute la suite, alors Π est P_K. Cela signifie que la dérivée ne nous aide pas à résoudre plus rapidement le problème. Nous ne savons pas si cela est encore valable en utilisant des paramètres non constants.

REFERENCES

[1] LENORE BLUM, *Generalized algebraic structures: A model theoretic approach*, ***Ph.D. thesis***, Massachussets Institute of Technology, 1968.

[2] LENORE BLUM, FELIPE CUCKER, MIKE SHUB, et STEVE SMALE, *Algebraic settings for the problem "$P \neq NP$?"*, ***Mathematics of numerical analysis*** (Renegar et al., editor), Lectures in Applied Mathematics, vol. 32, 1996, pp. 125–144.

[3] LENORE BLUM, MIKE SHUB, et STEVE SMALE, *On a theorey of computation and complexity over real numbers: NP-completeness, recursive functions and universal machines*, ***Bulletin of the Americal Mathematical Society***, vol. 21 (1989), no. 1, pp. 1–46.

[4] OLIVIER CHAPUIS et PASCAL KOIRAN, ***Saturation and stability in the theory of computation over the reals***, Prepublications de l' Institut Girard Desargues, 1997.

[5] JOHN B. GOODE, *Accessible telephone directories*, this JOURNAL, vol. 59 (1993), no. 1, pp. 92–105.

[6] E. KOLCHIN, ***Differentially Algebra and Algebraic Groups***, Academic Press, 1973.

[7] D. MARKER, M. MESSMER, et A. PILLAY, ***Model Theory of Fields***, Lecture Notes in Logic, Springer, 1996.

[8] CHRISTIAN MICHAUX, *$P \neq NP$ over the non-standard reals implies $P \neq NP$ over R*, ***Theoretical Computer Science*** (1994), no. 133, pp. 95–104.

[9] B. POIZAT, ***Cours de théorie des modèles***, Nur Al-Mantiq Walma'rifah, 1985.

[10] ———, ***Les petits cailloux***, ALEAS éditeur, 1995.

[11] ABRAHAM ROBINSON, *On the concept of a differentially closed field*, ***Bulletin of Research of the Israel Council***, vol. F8 (1959), pp. 113–128.

[12] CAROL WOOD, *The model theory of differential fields revisited*, ***Israel Journal of Mathematics***, vol. 25 (1976), pp. 331–352.

INSTITUT GIRARD DESARGUES– UPRES-A 5028 DU CNRS
UNIVERSITÉ CLAUDE BERNARD LYON-I
BÂTIMENT DU DOYEN JEAN BRACONNIER (101)
43, BOULEVARD DU 11 NOVEMBRE 1918
69 622 VILLEURBANNE CEDEX, FRANCE
E-mail: portier@desargues.univ-lyon1.fr