Séminaire de Structures Algébriques Ordonnées

1988 – 1989

F. Delon, M. Dickmann, D. Gondard

N° 2

Janvier 1990

LISTE DES EXPOSES

Séminaire de Structures Algébriques Ordonnées.

Delon – Dickmann – Gondard

1988 – 1989

14.10.88 – **D. Pecker** (Univ. de Paris VI).
Sur les surfaces réelles de degré 4.

14.11.88 – **D. Gluschankof** (Univ. de Buenos Aires, Argentine).
Prime ideal and Sikorski extension theorems for some ℓ–groups.

5.12.88 – **H. Sinaceur.**
De Sturm à Tarski, ou de l'analyse des équations à la théorie des modèles.

19.12.88 – **C. Michaux** (Univ. de Mons, Belgique).
Corps valués différentiels.

09.01.89 – **H. Sinaceur.**
Caractéristique de G.W. Leibniz et théorie des modèles selon Abraham Robinson.

06.02.89 – **D. Gondard.**
Sur les théories des corps de Rolle.

17.04.89 – **M.J. de la Puente** (Madrid).
The real Riemann surface of a ring.

18.04.89 – **J.M. Gamboa** (Madrid).
Rings of semialgebraic functions.

24.04.89 – **Z. Chatzidakis** (Paris VII).

Théorie des modèles des groupes profinis.

9.05.89 – **C. Michaux** (Mons).

Machines sur les réels et problèmes NP–complets d'après Smale et al.

22.05.89 – **D. Gondard**

Sur les chaînes d'un corps chaînable.

29.05.89 – **C. Michaux**

Suite de l'exposé du mardi 9 mai.

Machines sur les réels et poblèmes NP–complets, d'après Smale et al.

5.06.89 – **M.A. Dickmann.**

Théorie analytique d'élimination d'après Denef et van den Dries :

Topologie des ensembles semi–algébriques.

12.06.89 – **M.A. Dickmann.**

Théorie analytique d'élimination d'après Denef et van den Dries :

Ensembles sous–analytiques.

26.06.89 – **J. Ruiz** (Université Complutense, Madrid– Espagne).

Sums of 2^{th}–powers of meromorphic functions.

LISTE DES CONTRIBUTIONS

Séminaire de Structures Algébriques Ordonnées.

Delon – Dickmann – Gondard

1988 – 1989

– **D. Pecker** (Univ. de Paris VI).
Construction de surfaces quartiques.

– **D. Gluschankof** (Univ. de Buenos Aires, Argentine).
Prime ideal and Sikorski extension theorems for some ℓ–groups.

– **H. Sinaceur.**
De Sturm à Tarski, ou de l'analyse des équations à la théorie des modèles.

– **C. Michaux** (Univ. de Mons, Belgique).
Corps p–valués différentiels de caractéristique 0.

– **H. Sinaceur.**
Caractéristique de G.W. Leibniz et théorie des modèles selon A. Robinson.

– **D. Gondard.**
Sur les théories des corps de Rolle.

– **M.J. de la Puente** (Madrid).
The real Riemann surface of a ring.

– **J.M. Gamboa** (Madrid).
Rings of continuous semialgebraic functions.

– **C. Michaux** (Mons).

Machines sur les réels et problèmes NP–complets.

– **D. Gondard**

Noyaux de chaînes et corps chaînables.

– **M.A. Dickmann.**

Analytic elimination theory (d'après Denef et van den Dries).

– **J. Ruiz** (Université Complutense, Madrid– Espagne).

Sums of 2^{th}–powers of meromorphic functions.

D.Pecker (Paris 6)

CONSTRUCTION DE SURFACES QUARTIQUES .

§1 INTRODUCTION : Sur le 16ème problème de Hilbert

La géometrie algébrique étudie les figures géométriques définies par des équations polynomiales. Kummer a classifié les surfaces réelles du quatrième degré selon leur nombre de points singuliers coniques (1862,cf [2]). Harnack a montré qu'une courbe projective plane réelle de degré d ne peut avoir plus de $\frac{(d-1)(d-2)}{2}+1$ composantes connexes , et que cette borne était atteinte en tout degré d (1876). Mais ce n'est qu'avec le progrès des idées topologiques que Hilbert a pu formuler la première partie de son 16ème problème: la classification topologique des variétés algébriques réelles, et en particulier des courbes de degré 6 et des surfaces de degré 4 .Dans un article publié en 1909 (cf [6]) il montre le rapport entre ces deux questions et construit une surface quartique de $P_3(\mathbb{R})$ de rang maximal 12 ($r(M) = \frac{1}{2} \dim(H(M,\mathbb{Z}_2))$)(voir aussi [10]) Ce n'est que récemment qu'on a pu répondre aux plus simples de ces questions:

La classification des courbes de degré 6 a été achevée en 1971 grâce aux travaux de Gudkov, Arnol'd et Rohlin (voir [1] ,[4] ,[9] ,[3])

Dans l'étude plus délicate des surfaces réelles de degré 4 les progrès ont été encore plus lents ...

Whitney a montré que tout ensemble algébrique M a un nombre fini de composantes connexes en considérant les extrêmums liés de la fonction d(O,M) qui sont en général en nombre fini. Ensuite , en utilisant la théorie de Morse, R.Thom a pu obtenir des bornes explicites , dont certaines relatives aux rangs maximums des hypersurfaces réelles projectives se sont avérées les meilleures possibles (il obtient en particulier la borne 12 pour les surfaces

quartiques de $P_3(\mathbb{R})$). Simultanément, appliquant la théorie de Morse à l'application normale de Gauss, J.Milnor a obtenu d'autres inégalités, meilleures pour les hypersurfaces affines compactes : $\dim H(M,\mathbb{Z}) \leq d(d-1)^{n-1}$. Mais, dans ce cas les inégalités ne sont pas les meilleures possibles: Kharlamov montre que le rang d'une surface quartique compacte non-singulière de $\mathbb{R}^3$ ne peut dépasser 10 . Sa démonstration utilise la théorie des surfaces K_3 , grâce à laquelle il parvient à classifier les surfaces quartiques de $\mathbb{R}^3$(cf. [7], [8])

Le but de cet exposé est de construire explicitement, et élémentairement,les types topologiques des surfaces quartiques compactes non-singulières de $\mathbb{R}^3$. Nous utiliserons pour cela les constructions de Kummer (cf. [2]), oubliées semble-t-il par les spécialistes. . La méthode de Viro (1979 cf.[12]) semble cependant trés proche de celle de Kummer .

§2 LA METHODE DE KUMMER .

Dans ce qui suit, si E est un sous-ensemble compact de la sphère S^2 le double de E est obtenu en recollant deux copies de E par leurs bords .

PROPOSITION (Kummer)
Si P est un polynôme de degré 4 tel que $P^{-1}(0)$ rencontre transversalement S^2 et si k est assez petit la surface $\mathcal{S}$ d'équation : $(x^2+y^2+z^2-1)^2 + k\,P(x,y,z) = 0$ est homéomorphe au double de $P^{-1}(]-\infty,0])\cap S^2$

Démonstration: Montrons tout d'abord que ,dés que k est assez petit, chaque demi-droite dont l'origine est à l'intérieur de S^2et qui s'éloigne de 0 rencontre $\mathcal{S}$ en au plus deux points :

Une telle demi-droite a pour paramétrisation :

$$\begin{cases} x = x_1 t + x_0 \\ y = y_1 t + y_0 \\ z = z_1 t + z_0 \end{cases} \quad \text{avec:} \quad \begin{cases} x_1^2 + y_1^2 + z_1^2 = 1 \\ x_0^2 + y_0^2 + z_0^2 < 1 \\ x_0x_1 + y_0y_1 + z_0z_1 = 0 \ , \ t \geqslant t_0 \geqslant 0 \end{cases}$$

On voit que la suite des coefficients du polynôme Q(t) :

$Q(t) = (t^2 + x_o^2 + y_o^2 + z_o^2 - 1)^2 + kP(x,y,z)$, présente exactement deux variations de signe , d'où la conclusion par le lemme de Descartes.

Considérons un champ de segments sortants de S^2 tel que $P^{-1}(0) \cap \{x^2+y^2+z^2 \geqslant 1\}$ soit contenu dans la réunion U de ces segments. Chacun de ces segments sortants est porté par une demi-droite sortante dont l'origine est à l'intérieur de la boule: $x^2+y^2+z^2 < 1-\varepsilon$. Choisissons k assez petit pour que $\mathcal{S}$ soit contenu dans la couronne $1-\varepsilon < x^2+y^2+z^2 < 1+\varepsilon$,et pour que toutes nos demi-droites rencontrent $\mathcal{S}$ en deux points au plus. Elles rencontrent donc $\mathcal{S}$ en deux points exactement,l'un intérieur à S^2 l'autre extérieur. La projection le long des segments montre que $\mathcal{S} \cap \{x^2+y^2+z^2 \geqslant 1\}$ est homéomorphe à $P^{-1}(]-\infty\ 0]) \cap S^2$. De même $\mathcal{S} \cap \{x^2+y^2+z^2 \leqslant 1\}$ est homéomorphe à $P^{-1}(]-\infty,0]) \cap S^2$ et $\mathcal{S}$ est donc le double du compact $P^{-1}(]-\infty,0]) \cap S^2$. ■

§3 COURBES SPHÉRIQUES DE DEGRÉ 8 ET SURFACES QUARTIQUES .

Nous allons construire des courbes de degré 8 sur la sphère qui sont l'intersection de la sphère et d'une surface quartique d'équation $P(x,y,z) = 0$; on dira que $P(x,y,z) = 0$ est l'équation d'une telle courbe sphérique. On sait depuis Hilbert qu'une telle courbe a au plus dix ovales . Par projection stéréographique (voir la figure 1) nous identifierons la sphère privée d'un point au plan. Une telle projection "préserve les cercles" (c'est une inversion).

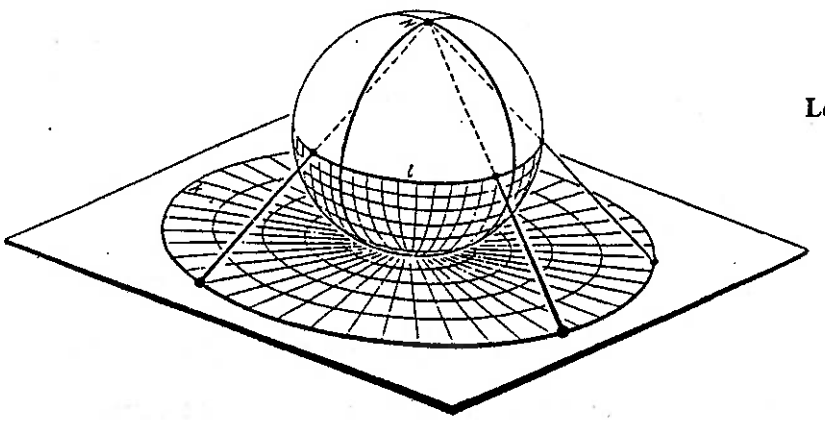


FIGURE 1

Les projections stéréographiques.
Ce sont celles que l'on utilise pour faire des cartes des régions polaires ou des régions du ciel.

Le plan ainsi identifié à la sphère s'appelle plan inversif . Dans le plan inversif cercles et droites ont des équations de degré 1 . Par convention l'équation d'un cercle est négative à l'intérieur de ce cercle .

PROPOSITION 1: Il existe une courbe sphérique ayant une équation de degré 4, possédant les symétries d'un tétraèdre, et ayant dix ovales sans relation d'inclusion .

Démonstration: Prenons quatre cercles du plan inversif disposés comme sur la figure 2 . Leur réunion a une équation de degré 4 : $T(x,y,z) = 0$ .L'ensemble des points de la sphère vérifiant $T(x,y,z,) = \varepsilon$ se compose de dix ovales sans relation d'inclusion . ■

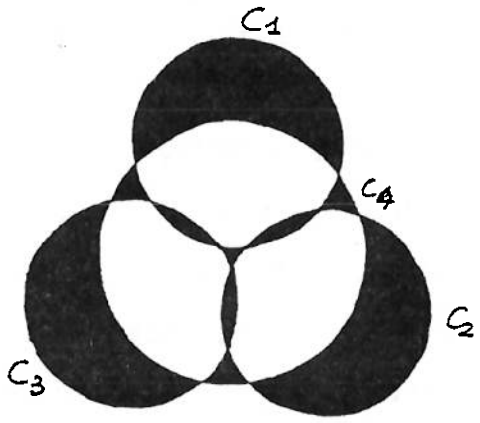


FIGURE 2 : $C_1C_2C_3C_4 \leqslant 0$

Notons selon Utkin et Gudkov $R^o_k + qR^o_o$ une surface ayant une composante connexe de genre k , R^o_k , et q boules sans relation d'inclusion extérieures à R^o_k .Grâce au lemme on obtient immédiatement:

THEOREME 1: Il existe des surfaces quartiques de type R^o_9 et $10R^o_o$. De plus ces surfaces ont les symétries d'un tétraèdre .

REMARQUES: Rohn a construit en 1911 une surface de type $10R^o_o$ (cf. [10]). Utkin en 1967 (cf [5]) et Gudkov en 1971 avaient conjecturé (entre autres) l'existence d'une surface quartique de type R^o_9 trouvée par Kharlamov en 1977 et dont Viro donne en 1979 une construction "élémentaire" utilisant le "catalogue" de Polotovskii (cf. [8],[12])

Nous allons maintenant construire d'autres courbes sphériques par la méthode des petites variations de Harnack-Hilbert-Rohn appliquée à des réunions de cercles sur la sphère .

PROPOSITION 2. Il existe des courbes sphériques ayant des équations de degré 4 des types suivants :

(a) 10 ovales dont un seul est contenu dans un autre .

(b) 10 ovales dont deux sont contenus dans un troisième , les autres étant sans relation d'inclusion .

(c) 8 ovales dont trois seulement sont contenus dans un quatrième, les autres étant sans relation d'inclusion .

De plus les courbes (a) et (b) présentent une symétrie par rapport à un plan .

Démonstration :

(b) Soit C_1, C_2, C_3 trois cercles de la sphère et e_1, e_2, e_3 trois cercles "perturbateurs" en pointillé sur la figure 3 .

Soit $K = C_1C_2C_3 + \varepsilon_1 e_1 e_2 e_3$. On voit que la courbe $K=0$, qui est trés proche de la courbe $C_1C_2C_3=0$, a quatre composantes connexes dont une est "perturbée" . Sur la figure on a noirci la partie du plan inversif où $C_1K < 0$. La courbe $C_1K + \varepsilon = 0$ avec ε assez petit , répond à la question .

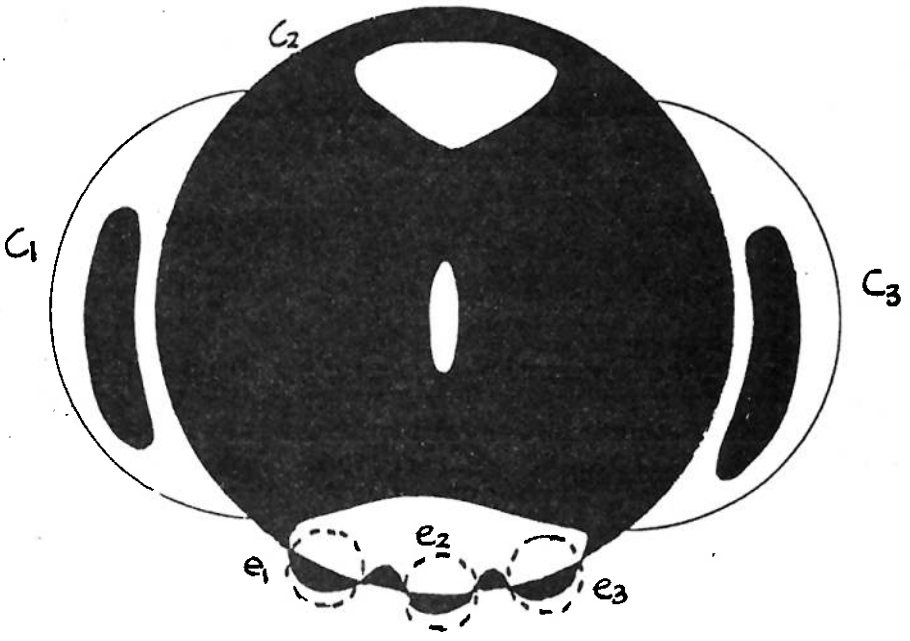


FIGURE 3

(a) Même construction que (b) , mais e_1, e_2, e_3 "perturbant" C_3 (voir figure 4) ,il faut alors prendre ε négatif .

(c) Même démonstration ,mais e_1 et e_2 perturbent C_2, ,tandis que e_3 perturbe C_3 . On prend alors ε négatif dans un petit cercle autour de e_3 et positif ailleurs . ■

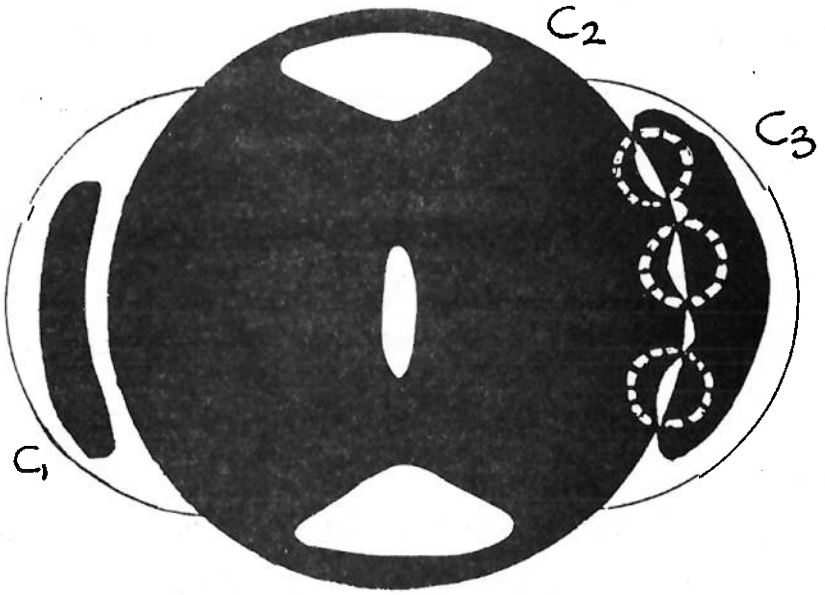


FIGURE 4 .

Dans toutes les configurations obtenues on peut diminuer le nombre d'ovales en modifiant les dispositions des cercles . Grâce au lemme on obtient :

THEOREME :On peut construire par cette méthode 49 types différents de surfaces quartiques:

$R_k^o + qR_o^o$ avec $k+q \leqslant 9$ et k ou $q \leqslant 2$

$R_k^o + qR_o^o$ avec $k \leqslant 4$ et $q \leqslant 3$; $R_3^o + 4R_o^o$

et aussi $R_1^o + R_1^o$ et deux sphères concentriques .

REMARQUE :Si l'on admet l'assertion de Gudkov (cf. [5]) selon laquelle les 31 types possibles de courbes sphériques de degré 8 existent ,et que ces courbes ont des équations de degré 4 transverses à la sphère, alors on peut construire TOUS les types de surfaces quartiques : $R_k^o + qR_o^o$ avec $k+q \leqslant 9$, et les cas triviaux .

REFERENCES BIBLIOGRAPHIQUES .

[1] A'CAMPO Sur la première partie du 16ème problème de Hilbert. Séminaire Bourbaki 1978-1979 n° 537

[2] W.BARTH H.KNÖRRER Algebraic Surfaces. Chapter 2 of Mathematical Models (G.Fisher editor) Vieweg 1986

[3] J·BOCHNAK M.COSTE M.F.ROY Géométrie Algébrique Réelle. Ergebnisse der Mathematik , 12 , Springer Verlag 1987 .

[4] D.A.GUDKOV The Topology Of Real Projective Algebraic Varieties Russ. Math. Surveys 29-4 (1974) pp 1-79

[5] D.A.GUDKOV On The Topology Of Algebraic Curves On A Hyperboloid Russ. Math. Surveys 34-6 (1979) pp 27-35

[6] D.HILBERT Über Die Gestalt Einer Fläche Vierter Ordnung Gesammelte Abhandlungen Vol. 2 (Berlin 1933) pp 449-453

[7] V.M.KHARLAMOV The Topological types Of Non-singular Surfaces In $\mathbb{RP}_3$ Of degree four . Fonctional An.App. n°10 (1976) pp 295-305

[8] V.M.KHARLAMOV Isotopic types of non-singular surfaces of fourth degree in $\mathbb{RP}_3$ Fonctional An. Appl. 12 (1978) pp 68-69

[9] J.J.RISLER Sur le 16ème Problème de Hilbert , un résumé et quelques questions. Publ.Math.Univ.Paris 7 n°9 (1980)

[10] K.ROHN Die maximalzahl von ovalen bei einer fläche vierter ordnung Leipziger Berichte 63 (1911) pp 423-440

[11] G.A.UTKIN Construction of certain types of non-singular fourth order surfaces . Amer.Math.Soc.Transl.(2) Vol 112 (1978)

[12] O.Ja.VIRO Construction of multicomponent real algebraic surfaces Soviet Math.Dokl. Vol 20 (1979) n°5 pp991-995

PRIME IDEAL AND SIKORSKI EXTENSION THEOREMS FOR SOME ℓ-GROUPS [1]

Daniel Gluschankof
Dto. de Matemáticas, Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
1428 Buenos Aires
Argentina

ABSTRACT. In the first part it is proved that the existence of prime ℓ-ideals in any ℓ-group is equivalent to the Prime Ideal Theorem for Boolean algebras (BPI). Moreover, the result implies that Birkhoff's Representation Theorem BRT) for representable ℓ-groups is equivalent to BPI, which extends the analogous result of [FH] and [L] for f-rings. In the second part, whose main theorem is equivalent with Sikorski Extension Theorem (SET), we characterize the injective abelian ℓ-groups with strong unit.

1. EXISTENCE OF PRIME ℓ-IDEALS IN ℓ-GROUPS

For terminology and notations we refer to [BKW]. We shall work in the axiomatic frame of Zermelo-Fränkel set theory (ZF) and explicitly mention when BPI is added to the hypotheses of any theorem.

1.1. THEOREM. (BPI). *Let G be an ℓ-group, H a proper ℓ-ideal, $a \in G\backslash H$. There exists a prime subgroup P such that $a \notin P$. In particular, there exists a value of a.*

1.2. COROLLARY. (BPI). *Let G be an* abelian *ℓ-group, H a proper ℓ-ideal, $a \in G\backslash H$. There exists a prime ℓ-ideal I such that $a \notin I$ and $H \subseteq I$.*

1.3. COROLLARY. (BPI). *Let G be a representable ℓ-group, H a proper ℓ-ideal, $a \in G\backslash H$. There exists a prime ℓ-ideal F_a which is maximal with respect to the condition of not containing a.*

Birkhoff's representation theorem for equational varieties (BRT) (see [B]) states that in a given variety, any algebra can be represented as a subdirect product of subdirectly irreducible algebras of the variety. It was recently proved in [G] that in ZF BRT is equivalent to AC. Since the non-constructive part in BRT involves, for each two given different elements of the algebra a,b, finding a maximal congruence θ such that a and b are not congruent modulo θ we can state the following.

1.4. THEOREM. *BPI implies BRT for the variety of representable ℓ-groups.*

---

[1] To appear in extenso in the Proceedings arising from the workshop on Ordered Algebraic Structures, August 1988, Kluwer Academic Publishers.

Since BRT implies the existence of such congruences we have the

1.5. THEOREM. *In ZF are equivalent BPI and the statement "in any hyper-archimedean ℓ-group any proper ℓ-ideal can be extended to a prime one".*

which implies the following:

1.6. COROLLARY. *BPI is equivalent to BRT for the variety of representable ℓ-groups.*

In [FH] and [L] it was proved that BPI is equivalent to BRT for the variety of f-rings. Since any abelian ℓ-group is representable and can be also thought as an f-ring with the trivial product, we have that the two results intersect for the variety of abelian ℓ-groups.

To complete this first section we shall state two related results.

1.7. COROLLARY. (BPI). i) *Any hyper-archimedean ℓ-group is isomorphic to a subdirect product of subgroups of* $\mathbb{R}$;

ii) *Any archimedean ℓ-group with strong unit is isomorphic to a subdirect product of subgroups of* $\mathbb{R}$.

Observe that both results are well known but relying, for their proofs, on Zorn,s Lemma, equivalent to AC (see [BKW]).

For the last result of the section, let's recall a categorical definition:

For a category $\mathcal{C}$, an object A is *injective* if for any objects B and C such that B is a subobject of C and an arrow $f \in \mathrm{Hom}[B,A]$ there exists an arrow $\bar{f} \in \mathrm{Hom}[C,A]$ which extends f.

1.8. THEOREM. *BPI is equivalent to the statement that $\mathbb{R}$ is injective in the category of hyper-archimedean ℓ-groups and ℓ-homomorphisms.*

2. INJECTIVE ABELIAN ℓ-GROUPS WITH STRONG UNIT

In the sequel we shall work in the category $\mathcal{LGU}$ of abelian ℓ-groups with strong unit. We shall consider the language of ℓ-groups enriched by the constant symbol u which shall represent the strong unit. We shall denote one of those groups by $G(u)$, pointing at the strong unit. The homomorphisms shall be ℓ-homomorphisms which preserve the strong unit.

2.1 THEOREM. *In ZF the following statements are equivalent:*

a) *BPI;*
b) *In any group in $\mathcal{LGU}$ there exist prime ℓ-ideals;*
c) *In any group in $\mathcal{LGU}$ there exist maximal ℓ-ideals;*
d) *$\mathbb{R}(1)$ is injective in $\mathcal{LGU}$.*

Given a family $(G_i(u_i))_{i\in I} \subseteq Ob(\mathcal{LGU})$, and an ℓ-subgroup G of ΠG_i such that $(u_i)_{i\in I} \in G$, we denote by $G^*(u_i)_{i\in I}$ the ℓ-group with strong unit $\{g \in G \;/\; \exists n \in \mathbb{N}$ such that $|g_i| \leq nu_i$ for all $i \in I\}$ and it is easy

to prove that $(\Pi G_i)^*(u_i)_{i\in I}$ is the product of the family $(G_i(u_i))_{i\in I}$ in the category $\mathcal{LGU}$. Making an abuse of notation, if G is an ℓ-subgroup of $\mathbb{R}^I$ for some index set I, we shall denote by $G^*(1)$ the object of $\mathcal{LGU}$ with underlying set $\{g \in G \,/\, \exists n \in \mathbb{N}$ such that $|g_i| \leq n$ for all $i \in I\}$.

2.2. COROLLARY. (BPI). *In $\mathcal{LGU}$ the products of copies of $\mathbb{R}(1)$ (in the sense of the above stated remark) are injective objects.*

For X a compact topological space, let G be an ℓ-subgroup of $D(X)$ such that 1 (the constant map to 1) belongs to G. Consider the interval $[0,1] \subseteq G$, by defining $\neg x = 1-x$, we have a Boolean algebra structure in the set $\mathcal{B}(G) = \{x \,/\, x \in [0,1]$ such that $x \vee \neg x = 1$ and $x \wedge \neg x = 0\}$.

For a given compact space X we shall denote $\mathcal{C}(X,\mathbb{R}_d)$ the ℓ-group of all continuous maps on X with values on the real line with the discrete topology. Observe that $\mathcal{C}(X,\mathbb{R}_d)(1)$ and $\mathcal{C}(X,\mathbb{R}_d)^*(1)$ denote the same object in $\mathcal{LGU}$.

2.3. LEMMA. (BPI). *Let $G(1)$ be a complete and divisible ℓ-group* with strong unit. If $B \subseteq G$ *a Boolean algebra* which is subalgebra of $\mathcal{B}(G(1))$, then G *is isomorphic to* $D(\mathcal{Sp}(\mathcal{B}(G)))^*(1) \simeq \mathcal{C}(\mathcal{Sp}(\mathcal{B}(G)))^*(1)$.

Observe that, for a complete ℓ-group $G \subseteq \mathbb{R}^A$ such that $1 \in G$ are equivalent the properties of being divisible and having all the constant maps. Then we can state the following:

2.54 COROLLARY. (BPI). (Theorem of Stone-Weierstrass for $\mathcal{LGU}$). If $G(1)$ is complete and has all the constant maps then it is isomorphic to $\mathcal{C}(\mathcal{Sp}(\mathcal{B}(G)))^*(1)$.

2.5. COROLLARY. (BPI). *For any ℓ-group with strong unit $G(1)$, it is complete and divisible (has all the constants) if and only if it is isomorphic to $\mathcal{C}(X)^*(1)$ for X extremally disconnected.*

2.6. LEMMA. (BPI). *The injective objects in $\mathcal{LGU}$ are archimedean.*

For the last part we shall recall the statement of SET (see [S]): *Let B be a boolean subalgebra of a boolean algebra B' and A a complete boolean algebra. Any homomorphism $f: B \to A$ can be extended to all of B'.*

Now we can state our main result on injectivity in $\mathcal{LGU}$:

2.7. THEOREM. *In ZF the following statements are equivalent:*
a) SET;
b) Complete and divisible groups are the injective objects in $\mathcal{LGU}$.

REFERENCES

[B] Birkhoff, G., *Subdirect unions in universal algebra*, Bull. Am. Math. Soc., 50 (1944), 764-768.

[BKW] Bigard, A., K. Keimel and S. Wolfenstein, *Groupes et anneaux réticulés*. Springer LNM 608, New York (1977).

[FH] Feldman, D. and M. Henriksen, *f-rings, subdirect products of totally ordered rings, and the prime ideal theorem*, Proc. Koninklijke Nederlandse Akademie van Wetenschappen, Series A 91 (2), (1988), 121-126.

[G] Grätzer, G., *Birkhoff's representation theorem is equivalent to the Axiom of Choice*, Algebra Universalis, 23 1 (1986), 58-60.

[L] Luxemburg, W. A. J., *A remark on a paper by D. Feldman and M. Henriksen concerning the definition of f-rings*, Proc. Kon. Ned. Akad. Wet., Series A 91 (2), (1988), 127-130.

[S] Sikorski, R., *A theorem on extension of homomorphisms*, Ann. Soc. Pol. Math. 21 (1948), 332-335.

DE STURM A TARSKI OU DE L'ANALYSE DES ÉQUATIONS A LA THÉORIE DES MODÈLES.

H. B. Sinaceur

Le théorème d'algèbre de Sturm fut présenté à l'Académie royale des sciences le 25 Mai 1829. Après un résumé [9] paru dans le Bulletin du baron de Férussac dont il était alors rédacteur, Sturm publia un mémoire [10] qui constitue pour nous un document plus complet sur le théorème.

Ce théorème donne une méthode pour déterminer le nombre de racines réelles, comprises entre deux nombres réels a et b, d'une équation polynomiale $V = 0$ où V a la forme :

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0 .$$

Cette méthode consiste à calculer d'abord la dérivée V', puis à appliquer l'algorithme d'Euclide pour trouver le p.g.c.d. (plus grand commun diviseur) de V et V'. On pose $V' = V_1$, en sorte que $V = V_1 Q_1 + R_1$. On dévie alors de l'emploi habituel de l'algorithme d'Euclide en posant $V_2 = -R_1$. On a donc $V = V_1 Q_1 - V_2$.

On réitère l'opération avec V_1 et V_2 pour obtenir :

$$V_1 = V_2\, Q_2 - V_2 .$$

On recommence avec V_2 et V_3 et on poursuit le processus de division jusqu'à parvenir à un reste V_r qui, si V et V_1 n'ont pas de racine commune, cas auquel il est toujours possible de se ramener, est une constante numérique (l'indice r étant majoré par le degré de V). On obtient ainsi le tableau :

$$\begin{aligned}
V &= V_1\, Q_1 - V_2 \\
V_1 &= V_2\, Q_2 - V_3 \\
V_2 &= V_3\, Q_3 - V_4 \\
&\cdots\cdots\cdots\cdots \\
V_{r-3} &= V_{r-2}\, Q_{r-2} - V_{r-1} \\
V_{r-2} &= V_{r-1}\, Q_{r-1} - V_r .
\end{aligned}$$

La suite des fonctions polynomiales $V , V_1 , V_2 , \ldots , V_r$ est communément appelée "suite de Sturm", ou "chaîne de Sturm" selon un usage introduit par Heinrich Weber dans le tome I de son **Lehrbuch der Algebra**, § 91–95.

Etant donné deux nombres réels $a , b , a < b$, on écrit la suite S_a des signes que prennent les fonctions $V , V_1 , V_2 , \ldots, V_r$, pour la valeur a ; et de même la suite analogue S_b. On compte le nombre N_a des variations de signe dans S_a, le nombre N_b des variations dans S_b. On démontre que $N_a - N_b$ est exactement le nombre de racines réelles de $V = 0$ comprises entre a et b.

En son temps, ce théorème fit, à lui tout seul, davantage pour la célébrité de Sturm que tous ses travaux ultérieurs sur les équations différentielles du second ordre, dont l'intérêt ne fut perçu que par la suite (théorie de Sturm–Liouville, à son tour mieux connue aujourd'hui de la grande majorité des mathématiciens). La plupart des mathématiciens en furent très impressionnés et certains l'accueillirent comme un "événement considérable". Il figura aussitôt dans plusieurs traités d'algèbre et engendra dans les recherches de l'époque ce que Sylvester appela un "cycle

d'idées sturmiennes" c'est–à–dire un ensemble de travaux signés des plus grands noms (Sylvester, Cayley, Hermite, et, plus tard, Kronecker).

I. DESCRIPTION DU CONTEXTE MATHÉMATIQUE DE LA DÉCOUVERTE DE STURM.

1. Sturm a précisé que son résultat dérive de ses travaux sur les équations différentielles [11,12]. Il y a donc chez lui une solidarité organique de méthode entre la résolution des équations différentielles et celle des équations algébriques. Si la première fut guidée par une "analogie algébrique " comme l'ont relevé certains historiens [2, p. 489], la seconde ne s'interdit, en principe, aucun des concepts ou méthodes de l'analyse. Sturm fait la synthèse entre un esprit géométrico–analytique et un sens aigu de l'abstraction, définissant ainsi une approche qualitative dans l'étude de l'ensemble des solutions d'une équation différentielle [8, Oeuvres, 1, p. XXI–XXII]. C'est peut être la première fois dans l'histoire après Leibniz que l'intuition géométrique s'allie, non pas au calcul comme on le faisait traditionnellment depuis l'institution par Descartes de la géométrie analytique, mais à une analyse formelle et a priori de situations globales.

2. Sturm a reconnu sa dette envers Fourier [4], qui a trouvé, en partant de la règle des signes de Descartes, une méthode pour majorer le nombre des racines réelles d'une équation algébrique. Fourier applique la règle des signes non pas à la suite des coefficients de l'équation, mais à la suite de ses fonctions différentielles. Il fait ainsi basculer l'application de cette règle du cadre algébrique qui était naturellement le sien à un cadre analytique où interviennent les notions de fonction, de fonction continue, de fonction différentielle, de variation infiniment petite, etc.. Et il utilise, comme s'il s'agissait d'une proposition évidente, le théorème de Belzano, selon lequel toute fonction continue et changeant de signe sur un intervalle réel s'annule au moins une fois sur cet intervalle. Fourier apporte d'ailleurs une dimension théorique à sa méthode, en présentant la résolution numérique des équations comme une application du calcul différentiel. Tirant la

conséquence du résultat d'Abel, connu en 1826, sur l'impossibilité d'une résolution algébrique pour les équations de degré ≥ 5 , il fait dépendre le progrès de la résolution numérique des techniques du calcul différentiel.

Sturm, ayant suivi les "principes" de Fourier et "imité" sa démonstration [9, p. 419], participe naturellement de son esprit concordataire qui prône la collaboration des principes de l'algèbre avec ceux de l'analyse et de la géométrie. La démonstration de son théorème est inscrite dans le cadre de ce qu'on appelait, au XIX^{e} siècle, l'"analyse algébrique", discipline qui indique assez par son nom qu'on n'y concevait pas de séparation tranchée entre méthodes algébriques et méthodes analytiques.

II. LA DÉMONSTRATION DU THÉORÈME DE STURM.

Il y a, malgré une parenté certaine de contenu, une grande différence de style entre Fourier [4] et Sturm [10]. Si le premier montre son obstination à mener l'analyse cas par cas et à la poursuivre jusqu'à parvenir au but, qui serait de connaître la valeur numérique des racines réelles des équations, le second pratique une analyse structurale, avec une aisance d'autant plus grande qu'il a pu "étudier à loisir" le travail de Fourier avant sa publication.

1. Dans le théorème de Fourier, l'application de la règle des signes de Descartes ne conduit pas à un résultat univoque. Car la diminution du nombre de variations de signe, entre deux nombres réels $a < b$, de la suite des fonctions différentielles $f^{(m)}(x), f^{(m-1)}(x), \ldots, f''(x), f'(x), f(x)$ ne correspond pas forcément à une racine réelle de l'équation $f(x) = 0$; il arrive, dans certaines conditions, qu'elle corresponde à un couple de racines imaginaires, et c'est pourquoi Fourier obtient seulement un majorant du nombre de racines réelles. En fait, Fourier doit accompagner l'application de la règle des signes de nombreuses règles complémentaires, car il y a un seul cas où la diminution du nombre de variations de signe de la suite $f^{(m)}(x), f^{(m-1)}(x), \ldots, f''(x), f'(x), f(x)$

correspond univoquement à l'existence d'une racine réelle de $f(x) = 0$, c'est le cas où pour une valeur a de x on a :

$$f(a) = f^{(i)}(a) = 0 \text{ et } f^{i-1}(a) = -f^{(i+1)}(a).$$

Fourier constate la particularité de ce cas isolé dans la multiplicité des cas possibles; Sturm y voit l'occasion de "forcer le destin". Il décide a priori que les conditions réunies dans ce cas particulier seront les conditions générales que devra satisfaire toute suite de fonctions dont on observera les variations de signes. Il définit ainsi par la conjonction de quatre propriétés(1) un ensemble de suites (les "suites de Sturm") dont chacune réalise la situation du cas particulier de Fourier : toute diminution de variations de signe dans la suite correspond exactement à l'existence d'une racine réelle de l'équation proposée. Il s'agit d'une définition axiomatique avant la lettre, et, d'une façon générale, il n'est pas nécessaire de spécifier le mode de construction d'une suite particulière ni, *a fortiori*, d'analyser un à un les différents cas éventuellement produits par cette construction. C'est *a priori*, c'est-à-dire dès la définition, qu'on est assuré qu'une suite de Sturm permet de dénombrer exactement le nombre de racines réelles d'une équation.

2. Sturm [10] procède en deux temps : 1° / un exposé "naïf" avec construction explicite d'une suite de Sturm ; 2° / un exposé plus abstrait avec énoncé des quatre conditions nécessaires et suffisantes

---

(1) Ces propriétés sont donc, pour une suite $V, V_1, V_2, \ldots, V_r$ et un intervalle [a,b] :

1. Si une fonction V_i s'annule pour une valeur α de l'intervalle [a,b], $V_{i-1}(\alpha) = -V_{i+1}(\alpha)$;
2. Au voisinage d'une valeur α de l'intervalle [a,b] telle que $V(\alpha) = 0$, $V_1(x)$ a le même signe que $V'(x)$;
3. Deux fonctions consécutives ne s'annulent pas pour une même valeur de l'intervalle [a,b] ;
4. La fonction $V_r(x)$ ne s'annule pour aucune valeur de l'intervalle [a,b] et conserve donc un signe constant sur cet intervalle.

de l'existence, en général, d'une suite de Sturm. Or, pour construire explicitement une suite de Sturm, l'auteur se sert, non plus de la différentiation répétée de la fonction donnée, mais de la division euclidienne modifiée comme vu plus haut. C'est là le procédé algébrique traditionnellement employé dans la recherche des racines multiples. Conjugué à la règle des signes, il rouvre une perspective à laquelle Fourier a volontairement tourné le dos et renoue avec une tradition ancienne, notamment illustrée par Lagrange : chercher, autant que possible, des démonstrations algébriques pour les propositions relatives à la théorie des équations.

Sturm n'a lui–même aucunement souligné cette conséquence épistémologique de son usage de l'algorithme d'Euclide à la place des différentiations successives. D'ailleurs, fidèle non seulement à Fourier mais à toute l'école d'analyse du début du XIX^{e} siècle, il pense naturellement en termes de fonction, de fonction continue, de variation "par degrés insensibles", et utilise constamment, sans en mettre l'évidence en question, le théorème de Bolzano. Mais d'autres mathématiciens s'apercevront que ces notions fondamentales de l'analyse ne sont pas essentielles à la démonstration du théorème de Sturm et que celle–ci peut aussi bien être faite dans le cadre de l'algèbre des polynômes, où l'on dispose d'une version algébrique du théorème de Bolzano[(1)].

3. Historiquement, cette interprétation algébrique de la démonstration du théorème de Sturm a été faite de trois façons différentes. En premier lieu, Ch. Hermite [5] et J.J. Sylvester [13] ont généralisé le théorème de Sturm au cas de plusieurs équations inconnues en en montrant le rapport avec la théorie de l'élimination algébrique et la théorie des formes quadratiques. Ils ont l'un et l'autre insisté sur le fait que leurs démonstrations reposent "entièrement et uniquement" sur des notions purement algébriques. En deuxième lieu, la construction par E. Artin et O. Schreier de l'algèbre réelle [1] fournit enfin un fondement algébrique <u>général</u> à la théorie des équations et des

---

(1) Connue sous le nom de "théorème du changement de signe" ou de "théorème des valeurs intermédiaires", elle énonce que si un polynôme P change de signe entre deux valeurs réelles $a < b$, alors il existe une valeur $c \in [a,b]$ telle que $P(c) = 0$.

inégalités. Le théorème de Sturm, aussi bien que d'autres propositions de l'analyse réelle (théorème de Rolle, théorème des accroissements finis, etc.), sont formulés et démontrés dans le cadre de l'axiomatique algébrique des corps réels clos. A. Tarski, enfin, définit la méthode d'élimination des quantificateurs pour la théorie élémentaire du corps ordonné des nombres réels et des corps réels clos, en généralisant le théorème de Sturm à des systèmes mixtes comprenant à la fois des équations et inégalités [14,15]. Tout en insistant beaucoup sur la possibilité offerte par l'algorithme d'Euclide de construire des fonctions de Sturm par des "moyens purement algébriques", Tarski ne songe guère à rapprocher le théorème de Sturm des procédures classiques de l'élimination algébrique comme, par exemple, le calcul du résultant de deux ou plusieurs polynômes. Aujourd'hui, on connaît mieux, grâce à certains travaux d'Abraham Robinson, le parallélisme entre corps réels clos et corps algébriquement clos et le fait que le théorème de Sturm remplit, dans le premier cas, l'office que le théorème sur le résultant (ou le théorème des zéros de Hilbert) remplit dans le second.

Nous laisserons de côté la transformation du théorème de Sturm par Hermite et Sylvester et l'algèbre réelle d'Artin et Schreier pour nous intéresser à la méthode d'élimination des quantificateurs de Tarski.

III. LA MÉTHODE D'ÉLIMINATION DES QUANTIFICATEURS DE TARSKI.

Elle est définie dans le fameux mémoire sur la complétude et la décidabilité de l'algèbre et de la géométire élémentaires dont il est intéressant, du point de vue historique, d'étudier les deux versions sucessives [14 et 15].

1. Deux sources semblent s'être conjuguées pour donner naissance à la généralisation par Tarski du théorème de Sturm à des systèmes mixtes d'équations et d'inégalités. D'une part, les termes dans lesquels Hilbert et Ackermann [6, p. 72–81] posèrent le problème de la décidabilité et l'atmosphère

générale des recherches logiques dans leur école accordaient une place particulière à l'arithmétique et aux méthodes numériques. Tarski [15] rappelle, en introduction le rôle de Hilbert qui cherchait à traiter les formules logiques d'une "façon numérique qui correspondrait à peu près à la théorie des équations en algèbre". L'analogie de la résolution numérique des équations algébriques était donc bien claire. D'autre part, Tarski s'est intéressé en particulier au résultat de Langford [7] sur la décidabilité de la théorie élémentaire des ordres linéaires denses. Dans son séminaire de l'Université de Varsovie on s'occupe notamment [17, 159–160] d'étendre le résultat de Langford aux ordres discrets. Or Langford considère un langage avec deux symboles de relations primitives, le symbole de l'égalité et celui de l'ordre, les formules atomiques étant du type $x = y$ ou $x > y$. La théorie élémentaire de l'ensemble ordonné des nombres réels peut naturellement être formulée dans ce langage. Et pour formuler la théorie élémentaire du corps ordonné des nombres réels, il suffit de l'enrichir en ajoutant des symboles pour les quatre opérations rationnelles (en fait Tarski se contente de l'addition, de la soustraction et de la multiplication).

2. Il est clair, surtout dans [15] qui définit formellement les notions de polynôme, de degré, de dérivée, de racine multiple, que Tarski voulait construire un "système d'algèbre de réels" où l'on pût formuler ou transposer "des parties importantes" de l'algèbre des polynômes. La notion de fonction continue est trop large pour ses besoins ; en particulier, avant d'adopter l'axiomatique d'Artin et Schreier en 1951, Tarski choisit, dans la première version de son mémoire [14], un système d'axiomes parmi lesquels figure la version algébrique du théorème de Bolzano, c'est–à–dire le théorème des valeurs intermédiaires (axiome XVII'). C'est pourquoi Tarski se sert du théorème de Sturm d'une façon qui en élimine tous les aspects non algébriques. Il donne un relief particulier à la construction de la chaîne de Sturm par division euclidienne et souligne que son lemme d'élimination des quantificateurs se "réduit", sur le plan mathématique, à la possiblité de fournir "un critère (une condition nécessaire et suffisante) purement algébrique permettant de constater que toutes les équations et inégalités (considérées) possèdent au moins une solution réelle commune" [14, Traduction française, p. 218]. Ainsi l'existence d'un critère algébrique pour l'existence d'une solution réelle commune aux équations et inégalités d'un système mixte est

l'indice mathématique de l'existence d'une procédure métamathématique d'élimination des quantificateurs. Le théorème de Sturm est, en fait, une procédure d'élimination des quantificateurs, et sa validité dans la théorie élémentaire des corps réels clos montre que cette théorie admet l'élimination des quantificateurs. Le parallélisme entre élimination des quantificateurs et élimination algébrique est donc mis en évidence sans considération des procédures d'élimination algébrique pour les corps algébriquement clos. Il reviendra à Robinson de combler cette lacune.

Bibliographie.

[1] Artin E., Schreier O., Algebraische Konstruktion reeller Körper, Abhandlungen des mathematischen Seminar der Hamburgischen Universität 5, (1926), 85–99.

[2] Bell E.T., The development of mathematics, New–York–Londres, Mc Graw Hill (1940).

[3] Benis–Sinaceur H., Deux moments dans l'histoire du théorème de Sturm, Revue d'histoire des sciences XLI, 2 (1988), 99–132, Paris P.U.F.

[4] Fourier J., Analyse des équations déterminées, première partie, Paris, F. Didot (1831).

[5] Hermite Ch., Remarques sur le théorème de M. Sturm, Comptes rendus de l'Académie des sciences, 36, (1853), 294–297. Dans Oeuvres de Ch. Hermite, Paris, Gauthier–Villars, t. 1, (1905), 284–287.

[6] Hilbert D., Ackermannn W., Grundzüge der theoretischen Logik, Berlin, Springer (1928), (4° éd., 1959).

[7] Langford C.H., Some theorems on deducibility, Annals of Mathematics, 28 (1927), 16–40 et 459–471.

[8] Poincaré H., Analyse des travaux scientifiques de M. Poincaré par lui–même, Résumé analytique, Acta mathematica 38, (1921), 36–64. Dans Oeuvres de Henri Poincaré, t. 1, I–XXXV Paris, Gautheir–Villars (1928).

[9] Sturm Ch. F., Analyse d'un mémoire sur la résolution des équations numériques, Bulletin des sciences mathématiques, physiques et chimiques publié par le Baron de Férussac, t. 11, n° 271, (1829), 419–422.

[10] Sturm Ch. F., Mémoire sur la résolution des équations numériques, Mémoires présentés par divers savants étrangers à l'Académie royale des sciences, section sciences mathématiques et physiques, t. VI, (1835), 273–318.

[11] Sturm Ch. F., Mémoire sur les équations différentielles linéaires du second ordre, Journal de mathématiques pures et appliquées, t. 1, (1836), 106–186.

[12] Sturm Ch. F., Mémoire sur une classe d'équations à différences partielles, Journal de mathématiques pures et appliquées, t. 1, (1836), 373–444.

[13] Sylvester J.J., On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraic common measure. Philosophical transactions of the Royal Society of London 143, (1853), 407–548. Dans Sylvester, Collected mathematical papers, Cambridge University Press, t. 1, 429–586.

[14] Tarski A., The completeness of elementary algebra and geometry, Paris, Institut Blaise Pascal (1939/67). Dans [16], t. 4, (1986), 289–346. Traduction française dans Tarski, Logique, sémantique, métamathématique, vol. 2 (1974), 203–242, Paris, A. Colin.

[15] Tarski A., A decision method for elementary algebra and geometry (prepared for publication by J.C. Mc Kinsey), (1951), 2° éd., University of California press, Berkeley and Los Angeles. Dans [16], t. 3, (1986), 297–368.

[16] Tarski A., Collected papers, 1,2, 3, 4 (Steven R. Givant et Ralph N. McKenzie éd.), Birkhäuser (1986).

[17] Vaught R., Model theory before 1945, Proc. of the Tarski Symposium, American mathematical society, Proc. symp. pure math. vol. 25, (1974), 153–172, Providence R.I..

Corps p-valués différentiels de caractéristique 0

C. Michaux

Après que l'existence d'une modèle-complétion pour les corps différentiels de caractéristique 0 ait été prouvée d'abord par A. Robinson (voir [Robinson 1959]) puis axiomatisée par L. Blum de façon beaucoup plus simple (voir [Blum 1968]), plusieurs résultats sur la théorie des modèles des corps différentiels parurent: citons entre autres ceux de C. Wood [Wood 1973, 1974, 1976] où l'existence d'une modèle-complétion pour les corps différentiellement parfaits de caractéristique $p \neq 0$ est prouvée et ceux de M. Singer [Singer 1978a, 1978b] qui prouvent l'existence d'une modèle- complétion pour les corps ordonnés différentiels.

Plus récemment les corps valués différentiels ont été étudiés par M. Rosenlicht [Rosenlicht 1979, 80, 81] en liaison avec l'étude des corps de Hardy.

Dans cette note, nous prouvons l'existence d'une modèle-complétion pour les corps p-valués différentiels de caractéristique 0 et en donnons une axiomatisation à la "manière de Blum".

Nous ne donnerons pas ici le détail de la preuve qui sera publiée ultérieurement.

Un corps valué différentiel est un corps valué muni d'une dérivation. Dans un premier temps, nous introduisons la notion de corps hensélien différentiel, c'est-à-dire un corps K valué différentiel, hensélien dans le sens ordinaire du terme et satisfaisant le schéma S d'axiomes suivants (nous notons $\mathrm{val}(a)$, la valuation d'un élément $a \in K$):

pour tout polynôme différentiel $f(X, X', \ldots, X^{(n)})$ à coefficients dans l'anneau O_K de valuation de K

$((\exists \alpha_0, \ldots, \alpha_n \in O_K)(\mathrm{val}(\frac{\partial f}{\partial X^{(n)}}(\alpha_0, \ldots, \alpha_n)) = 0 \text{ et } f(\alpha_0, \ldots, \alpha_n) = 0)) \Rightarrow$

$((\forall \epsilon)(\exists z)(f(z, \ldots, z^{(n)}) = 0 \wedge \bigwedge_{i=0}^{n}((\alpha_i \neq 0 \wedge \mathrm{val}(z^{(i)}) = \mathrm{val}(\alpha_i)) \vee (\alpha_i = 0 \wedge$

$\mathrm{val}(z^{(i)}) > \mathrm{val}(\epsilon)))).$

Approximativement cet axiome dit que s'il existe une solution $\alpha_0, \ldots, \alpha_n$ pour l'équation polynomiale $f(X_0, \ldots, X_n) = 0$, alors il existe une solution différentielle proche de $\alpha_0, \ldots, \alpha_n$

On peut montrer que cette théorie est consistante (voir Michaux 1989).

Un corps p-valué de caractéristique 0 est constitué d'un corps F de caractéristique 0, d'un $\mathbf{Z}$-groupe G (c'est-à-dire un groupe ordonné abélien avec un plus petit élément noté 1, qui vérifie l'axiome suivant $(\forall x)(\exists y)(\exists z)(x = ny + z$ et $0 \leq z < n)$; - la théorie des $\mathbf{Z}$-groupes est une théorie modèle-complète), une valuation val : $F \to G$, un élément $p \in F$, une "cross section" $\chi : G \to F$ telle que $\text{val}(\chi g) = g$ et $\chi 1 = p$. En plus, $\overline{F}$, le corps résiduel de F est $\mathbf{F}_p$, le corps à p-éléments.

On peut montrer que la théorie des corps p-valués henséliens de caractéristique 0 est la modèle-complétion des corps p-valués de caractéristique 0 (voir [Robinson 1968] ou [Ax-Kochen 1966]).

Un corps p-valué différentiel de caractéristique 0 est un corps p-valué de caractéristique 0 muni d'une dérivation. Cette théorie peut être axiomatisée de façon universelle.

On montre alors:

Théorème. La théorie des corps p-valués différentiels de caractéristique 0 qui sont henséliens différentiels est la modèle-complétion de la théorie des corps p-valués différentiels de caractéristique 0.

REFERENCES

- J. Ax - S. Kochen, 1966 : Diophantine problems over local fields III. Ann. of Math., **83**, 437-456.
- L. Blum, 1968 : Generalized algebraic structures. Ph.D. Thesis, M.I.T.
- C. Michaux, 1989 : Model Theory of valued differential fields. En préparation.

- A. Robinson, 1959 : On the concept of a differentially closed field. Bull. Res. Council of Israël, 113,128.
- A, Robinson, 1968 : Problems and Methods of model theory. Centro Internazionale Matematico Estivo, Varenna
- M. Rosenlicht, 1979 : On the value group of a differential valuation II. Amer. J. Math. **101**, 258-266.
- M. Rosenlicht, 1980 : Differential valuations. Pacif. J. Math. **86**, 301-319.
- M. Rosenlicht, 1981 : On the value groups of a differential valuation. Amer. J. Math. **103**, 977-996.
- M. Singer, 1978a : The model theory of ordered differential fields. J. Symb. Logic **43**, 82-91.
- M. Singer, 1978b : A class of differential fields with minimal differential closures, Proc. Amer. Math. Soc. **69**, 319-322.
- C. Wood, 1973 : The model Theory of differential fields of characteristic $p \neq 0$. Proc. Amer Math. Soc. **40**, 577-584.
- C. Wood, 1974 : Prime model extensions for differential fields of characteristic $p \neq 0$. J. Symb. Logic **39**, 469-477.
- C. Wood, 1976 : The model theory of differential fields revisited. Israel J. Math. **25**, 331-352.

Faculté des Sciences
Avenue Maistriau, 15,
B-7000 Mons
Belgique

CARACTÉRISTIQUE DE G. W. LEIBNIZ ET THÉORIE DES MODÈLES SELON A. ROBINSON.

H. B. Sinaceur

Résumé.

Dans un article nécrologique sur Abraham Robinson, Simon Kochen [4] consignait une impression de Gödel que je voudrais mettre à l'épreuve de l'histoire. Gödel, qui s'intéressait beaucoup aux travaux et à la philosophie de Leibniz, voyait dans les résultats d'Abraham Robinson la meilleure réalisation de l'idéal leibnizien d'une logique constituée en ars inveniendi pour les mathématiques. Ce jugement concorde avec la volonté de Robinson, manifeste dans ses premiers articles [10, 11, 12], de faire de la logique "un instrument efficace de recherche mathématique". Le but de l'exposé est d'établir un parallèle entre l'idée d'art d'inventer chez Leibniz et la conception que Robinson a concrétisée dans la théorie des modèles, en invoquant lui–même le patronage de Leibniz [10, 694].

I. QU'EST–CE–QUE L'ART D'INVENTER ?

Leibniz distingue l'art d'inventer de l'art de démontrer. Si celui–ci permet d'établir avec certitude des vérités "connues confusément et imparfaitement", celui–là permet de "dévoiler" des vérités inconnues. Leibniz décrit l'art d'inventer comme une sorte de fil d'Ariane "qui dirige la recherche" et permet non seulement de trouver un résultat mais surtout de le prévoir [7, 161].

Inventer c'est donc moins donner des solutions particulières qu'établir des méthodes générales.

L'idée de "caractéristique", c'est–à–dire de langage symbolique, joue un rôle primordial dans l'art d'inventer. Les "caractères" ou symboles du langage, qui représentent les éléments de nos pensées, fonctionnent simultanément comme des aiguillons pour l'esprit ; ils le poussent à "concevoir des notions universelles" [5, V, 269]. Trouver une méthode c'est trouver "une règle de passage d'une pensée à une autre" et donc une règle de passage d'un caractère à un autre. Il y a là, bien sûr, l'idée de calcul symbolique, qualifié par Leibniz de "calcul universel", susceptible d'interprétations diverses, algébrique, géométrique, logique, musicale, cryptographique, etc. [5, IV, 459–460]. Mai il y a surtout l'idée que l'activité symbolique se développe selon la double polarité du formel et du concret, du général et du spécial, de la méthode et de ses "échantillons", de la théorie et de ses modèles [8]. C'est pourquoi, si le "calcul universel" représente le but de l'art d'inventer ou, comme dit Leibniz, sa "dernière perfection", il n'en épuise cependant pas toutes les ressources [6, VII, 169]. Certaines de celles–ci sont contenues dans une analyse de la caractéristique elle–même qui, de mode d'expression privilégié, devient objet d'étude.

Intéressons–nous, par exemple, aux règles du calcul algébrique plutôt qu'à ses éléments, les quantités finies, et nous serons prêts d'inventer, comme l'a fait Leibniz, l'analyse infinie. Leibniz a insisté sur le fait que l'invention du calcul infinitésimal était une application de son idée de caractéristique universelle. De même sa conception des "nombres fictifs" pour représenter les coefficients des équations d'un système de plusieurs équations l'a conduit à préfigurer notre écriture actuelle des déterminants [3]. De même encore l'analogie symbolique qu'il relève entre le développement d'une puissance d'un binôme et le développement de la différentielle d'un produit de deux facteurs [5, V, 377–381], lui fait voir le parallélisme des langages du calcul algébrique et du calcul différentiel. On a bien là, en germe, la démarche propre à la théorie des modèles : constituer une métathéorie de théories mathématiques différentes par l'analyse de leurs langages.

Comme dans la théorie des modèles à ses débuts l'algèbre tient une place particulière dans l'art d'inventer de Leibniz. C'est qu'elle est l'échantillon par excellence de la caractéristique. Elle nous habitue d'entrée de jeu à l'indétermination des signes, et nous pousse à concevoir par la généralisation des signes ambigus représentant simultanément diverses opérations ou par analogie

des signes représentant autre chose que des nombres : points, relations, quantités ou qualités de propositions logiques, etc.. Elle nous enseigne ainsi l'art de la généralité et de l'analogie, essentiel pour former ce que Leibniz appelle la "méthode de l'universalité". Bien qu'elle ne soit ni le tout des mathématiques ni même la voie royale de l'invention, l'algèbre joue un rôle inducteur remarquable. Ce n'est pas qu'il faille introduire l'algèbre partout ; par exemple, pour la géométirie il vaut mieux raisonner directement sur les positions et les figures que par l'intermédiaire des nombres ; mais on doit établir, autant que faire se peut, des "formules universelles" analogues à celles de la résolution des équations afin de formaliser et généraliser les raisonnements [5,II,229].

II. CARACTÉRISTIQUE ET THÉORIE DES MODÈLES.

A première vue, il y a un certain paradoxe à rapprocher la théorie des modèles de la caractéristique leibnizienne dans la mesure où celle–ci était conçue pour être universelle. Or, on sait bien que la théorie des modèles a tiré la leçon du paradoxe de Richard (1905) et des théorèmes d'incomplétude de Gödel (1931), qui montrent qu'on ne peut concilier les exigences d'une langue exacte avec celles d'une langue universelle. Mais il y a chez Leibniz une ambition de principe et une position de fait. L'institution d'une caractéristique universelle étant une "perfection" irréalisable d'un seul coup, Leibniz ne se prive pas, ici et maintenant, d'analyser les notations existantes, d'en introduire de nouvelles, de mettre en évidence des analogies formelles, car il faut d'abord "avancer nos connaissances".

Les écrits d'A. Robinson ne laissent pas supposer une lecture de l'oeuvre de Leibniz en dehors de quelques textes relatifs à la justification du calcul infinitésimal, cités dans [16] ou [17] et de la lettre à Huyghens citée dans [10]. Cependant ils sont parcourus par une réflexion explicite sur l'art de l'analogie et de la généralité, ancrée, dans un premier temps, dans l'étude des structures algébriques. L'analyse logique de celles–ci doit conduire à en subordonner la mutiplicité à des principes généraux qui révèleront l'identité formelle de structures analogues. C'est ainsi qu'on découvre les "théorèmes métamathématiques de l'algèbre" [9 ; 9], c'est–à–dire des

théorèmes algébriques découverts par des méthodes logiques. Au premier rang de ceux–ci viennent les fameux principes de transfert comme celui de Tarski–Seidenberg. Mais il y a aussi l'invention de concepts nouveaux, comme celui de clôture différentielle [13], analogue pour un corps différentiel de la clôture algébrique d'un corps et de la clôture réelle d'un corps ordonné. Les trois clôtures sont, en fait, des échantillons de la notion logique de modèle–complétion d'une théorie [14 ; 5.5., 128–136]. Bref on voit comment la logique est bien devenue un art d'inventer des mathématiques : en faisant de l'analyse du langage mathématique une méthode systématique de découvertes d'une généralité inaccessible par un autre moyen.

Pour justifier l'invention de calculs nouveaux Leibniz avait recours aux "fictions" ou "notions idéales" dont l'usage est autorisé pour abréger le discours et faciliter la découverte [5 ; IV, 92–93, 98, 110]. Par exemple, les infiniment petits, dont il est difficile de décider s'ils correspondent à des entités existant actuellement ou potentiellement, ont le statut de fictions. Ce statut spécial permet de laisser (provisoirement) de côté les discussions philosophiques sur l'existence de l'infini pour libérer l'imagination mathématique. On reconnaîtra dans une telle attitude une disposition générale du formalisme mathématique. Robinson y a consacré quelques réflexions, peut–être à partir de ce qu'il avait lu de Leibniz, mais aussi et surtout à partir des discussions soulevées par le fameux article de Hilbert [2]. Pour lui, seul un point de vue formaliste permet d'accepter les entités symboliques ou les théories abstraites, c'est–à–dire celles dont l'interprétation, indirecte faute d'un modèle fini, extrapole du fini à l'infini. Ces entités ou théories abstraites sont un élément essentiel de la production mathématique, qui se multiplie dans ce va–et–vient entre fini et infini. Elles ont bien pour ancêtres les "fictions" de Leibniz, mais seulement d'une certaine façon. Car, contrairement à Leibniz, Robinson ne distingue pas, parmi les notions mathématiques, les réelles des imaginaires. Du point de vue ontologique, elles ont toutes le même mode d'existence. Par exemple, un infiniment petit d'un modèle non standard n'est "ni plus ni moins réel", ni plus ni moins fictif qu'un irrationnel standard [16 ; 281–282]. Robinson se sépare de Leibniz et de tous ceux qui associent, de quelque façon que ce soit, formalisme mathématique et réalisme métaphysique [18]. Le formalisme se soutient de lui–même, par ses résultats, il n'a besoin du réalisme ni comme repoussoir ni comme appui. Nous

n'admettons les processus infinitaires ni malgré leur absence de "réalité", comme le voulait Leibniz, ni à cause de leur "réalité" comme le prétendent les adeptes de l'infini actuel. De fait, nous les admettons parce qu'ils sont un prolongement fécond de processus finis, et parce que les refuser c'est couper les ailes à l'invention mathématique. La logique ne saurait pas davantage s'en passer que les mathématiques abstraites. Celles–ci nous ont suffisamment persuadés de leur puissance générative. A son tour, la théorie des modèles nous montre la puissance générative des concepts ou méthodes métamathématiques. L'analyse du langage d'expression des modèles mathématiques est un produit "naturel" [12 ; 51] du formalisme des mathématiques modernes.

Bibliographie

[1] Benis–Sinaceur H., Ars inveniendi aujourd'hui. Les Etudes philosophiques, (1989).

[2] Hilbert D., Über das Unendliche, 1926, Mathematische Annalen 88, 151–165. Traduction française d'André Weil, Acta mathematica 48, 91–122.

[3] Knobloch E., Zur Vorgeschichte der Determinantentheorie, Studia Leibnitiana, Supplementa, XXII, (1982), 96–118.

[4] Kochen S., On Abraham Robinson's work in mathematical logic, The Bulletin of the London Mathematical Society, vol. 8, (1976), 312–315.

[5] Leibniz G.W., Leibnizens mathematische Schriften, éd. C.I. Gerhardt, Berlin et Halle, 1849–1863, 7 volumes. Réimpression à Hildesheim, Georg Olms Verlagsbuchhandlung, 1962.

[6] Leibniz G.W., Die philosophischen Schriften von G.W. Leibniz, éd. C.I. Gerhardt, Berlin, 1875–1890, 7 volumes. Réimpression à Hildesheim, Georg Olms Verlagsbuchhandlung, 1960–1961.

[7] Leibniz G.W., Opuscules et fragments inédits de Leibniz, éd. L. Couturat, Paris, Presses universitaires de France, 1903. Réimpression à Hildesheim, Georg Olms Verlagsbuchhandlung, 1961.

[8] Rescher N., Leibniz's interpretation of his logical calculi, The Journal of Symbolic Logic, 19, (1954), 1–13.

[9] Robinson A., On the metamathematics of algebra, Amsterdam, North–Holland, (1951).

[10] Robinson A., On the application of symbolic logic to algebra. Proceedings of the Intern. Cong. of Math. (Cambridge Mass. 1950), A.M.S., Providence R.I., vol. I, (1952), 686–694. Reproduit dans [19], I, 3–11.

[11] Robinson A., Les rapports entre le calcul déductif et l'interprétation sémantique d'un système axiomatique. Colloques internationaux du C.N.R.S., 36, (1953). Les méthodes formelles en axiomatique, Paris, 35–52.

[12] Robinson A., L'application de la logique formelle aux mathématiques. Actes du 2e colloque intern. de logique math. (1952), Paris, Gauthiers–Villars et Louvain, Nauwelaerts, (1954), 51–64.

[13] Robinson A., On the concept of a differentially closed field, Bull. Res. Council Israel 8 F, (1959), 113–118. Reproduit dans [19], I, 440–455.

[14] Robinson A., Introduction to model theory and to the metamathematics of algebra, Amsterdam, North–Holland, (1963).

[15] Robinson A.,Formalism 64. Proc. Intern. Cong. for Logic, Methodology and Phil. of Sc., Amsterdam, North–Holland, (1965). Reproduit dans [19], II, 505–523.

[16] Robinson A., Non standard analysis. Amsterdam, North–Holland, (1966).

[17] Robinson A., The metaphysics of the calculus. Dans Problems in the philosophy of mathematics, éd. I. Lakatos, Amsterdam, North–Holland, (1967), 28–46.

[18] Robinson A., From a formalist's point of view. Dialectica 23, (1969), 45–49.

[19] Robinson A., Selected Papers I, II, III, éd. H.J. Keisler, S. Körner, W.A.J. Luxemburg, A. D. Young, New Haven and London, Yale University Press, (1979).

SUR LES THEORIES DES CORPS DE ROLLE

DANIELLE GONDARD-COZETTE

Département de mathématiques, U.F.R. 20, Université Paris VI,
4 place Jussieu, 75252 PARIS Cedex 05, FRANCE.

Electronic mail : Gondard@FRMAP711.Bitnet.

INTRODUCTION.

We propose here axiomatizations written in the language of fields, the models of which are Rolle fields (i.e. fields with the Rolle's property for every order) having exactly 2^n orders ($n \geq 0$). In fact, for $n = 0$ we obtain an axiomatization of the theory of real-closed fields ; for $n = 1$, we get exatly the axiomatizations given for the theory of chain-closed fields by the author in [G1].

In fields having a finite number of orders, we characterize Rolle fields as those which are pythagorean at level 4 and do not admit any algebraic extension of odd degree. In the more general setting, we characterize Rolle fields as real fields, pythagorean at level 4 , such that K does not admit any algebraic extension of odd degree and K^2 is a fan.

We also give the lattice of algebraic extensions of a Rolle field having exactly 2^n orders and prove that such a field K is the intersection of $n + 1$ real closures of K .

Finally we make a study of chainable Rolle fields, where chainable is equivalent, as we have shown in a previous paper, to the existence in K of an element α such that α^2 is not a sum of fourth powers in K .

0-RESULTATS PRELIMINAIRES.

Dans tout cet article K désignera un corps commutatif et on notera par $\sum K^{2^n}$ l'ensemble de toutes les sommes d'un nombre fini de puissances 2^n-èmes.

L'axiomatisation, dans le langage des anneaux enrichi d'un symbole de constante α , de la théorie des corps chaîne-clos α-chaînables donnée dans [G1] me paraît devoir trouver sa généralisation en ajoutant $n \geq 0$ symboles de constante α_i au langage des anneaux sous la forme suivante :

1- axiomes de corps commutatif ordonnable (noté ensuite K) ;

2- K est pythagoricien au niveau 4 ($\forall x \forall y \exists z \quad x^4 + y^4 = z^4$) ;

3- aucun des $2^n - 1$ produits de α_i distincts (notés désormais β_j) n'appartient à $\pm \sum K^2$;

4- pour tout $\gamma_j = \pm \beta_j$, l'axiome :

$\forall x \forall y \exists z \quad (x^2 + \gamma_j y^2 = z^2 \vee x^2 + \gamma_j y^2 = \gamma_j z^2)$;

5- K est la réunion de 2^{n+1} classes : K^2, $-K^2$, $\alpha_1 K^2$, $-\alpha_1 K^2$, $\alpha_2 K^2$, $-\alpha_2 K^2$, ..., $\alpha_1\alpha_2 K^2$, $-\alpha_1\alpha_2 K^2$, ..., $(\prod_{i=1}^{n} \alpha_i)\, K^2$, $-(\prod_{i=1}^{n} \alpha_i)\, K^2$;

6- tout polynôme de degré impair a une racine dans K .

Remarquons que ce système d'axiomes peut être écrit dans le langage des corps : il suffit de remplacer les axiomes 3, 4 et 5 par un axiome disant qu'il existe des α_i satisfaisant les axiomes 3, 4, et 5.

Avant de montrer que les modèles de ces théories sont les corps de Rolle ayant un nombre fini (2^n avec $n \geq 0$) d'ordres et d'étudier ceux-ci il convient de rappeler un certain nombre de définitions et résultats connus.

Définition 0.1. ([Del]). *Un corps ordonné K est un corps de Rolle s'il a la propriété de Rolle (i.e. pour tout polynôme $P \in K[X]$ et pour tous $a < b$ dans K vérifiant $P(a) = P(b) = 0$, il existe $c \in K$, $a < c < b$ tel que si P' est la dérivée formelle de P , on ait $P'(c) = 0$).*

Proposition 0.2. ([B-C-P2]). *Si K a la propriété de Rolle pour un ordre alors il a la propriété de Rolle pour tous ses ordres.*

Cette proposition 0-2 résulte en fait de la suivante :

Proposition 0.3. ([B-C-P2]). *Un corps K est de Rolle si et seulement si il existe une valuation hensélienne v sur K telle que le corps résiduel k_v soit réel-clos et le groupe des valeurs vK soit m-divisible pour tout entier m impair (nous dirons désormais impair-divisible).*

Notation. Dans la suite on notera $\mathbf{V(K)}$ l'ensemble des valuations ayant les propriétés de la proposition 0-3.

Proposition 0.4. ([B-C-P1]). *Si K est un corps de Rolle alors :*

(i) K est héréditairement pythagoricien ;

(ii) K est superpythagoricien .

Un corps ordonnable est dit *héréditairement pythagoricien* s'il est pythagoricien, et si toute extension algébrique ordonnable de ce corps est aussi un corps pythagoricien.

Rappelons qu'un corps *superpythagoricien* est un corps où K^2 est un fan. Un fan (voir [Be2] par exemple) est un préordre T ($T + T \subseteq T$, $T \cdot T \subseteq T$, 0 et 1 sont dans T , $-1 \notin T$, T^* est un sous groupe de K^*) tel que pour tout sous-groupe U de $K^* = K - \{0\}$ contenant T et tel que $-1 \notin U$, le sous-groupe U soit additivement fermé.

On dit aussi d'un corps K superpythagoricien qu'il est *strictement pythagoricien* ; cette dernière notion se généralise au niveau 2^n : un corps K est 2^n-*strictement pythagoricien* si K^{2^n} est un fan (c.f. [Be2]).

Enfin un corps K *pythagoricien au niveau* 2^n est tel que $K^{2^n} + K^{2^n} = K^{2^n}$. Un corps 2^n-strictement pythagoricien est bien sûr pythagoricien au niveau 2^n .

Précisons pour terminer que K *superordonné* signifie que $\sum K^2$ est un fan, mais K n'est pas nécessairement pythagoricien.

Proposition 0.5. ([B-C-P 2]). *Si K est un corps de Rolle alors :*

(i) K n'admet pas d'extension algébrique de degré impair ;

(ii) Toute extension algébrique ordonnable de K est un corps de Rolle.

Proposition 0.6. ([B-C-P 1]). *Si K est un corps ayant p ordres, alors K est un corps de Rolle si et seulement si K admet $2p-1$ extensions minimales et K admet une seule place réelle (i. e. une seule $\mathbb{R}$-place).*

Proposition 0.7. ([Las2]). *Soit K un corps de Rolle et v une valuation de $V(K)$, alors K a exactement 2^n ordres si et seulement si la dimension de $vK / 2vK$ comme $\mathbf{F}_2$-espace vectoriel est n .*

Notation. Dans la suite nous désignerons par $\mathbf{M(K)}$ l'ensemble des places réelles (i.e. $\mathbf{R}$-places) du corps K.

Signalons que dans [De1] ou [De2] on trouvera plusieurs résultats de théorie des modèles des corps de Rolle, notamment le fait qu'être un corps de Rolle est une propriété du premier ordre dans le langage des anneaux et que la théorie des corps de Rolle est décidable.

Dans [J] on pourra également trouver comme cas particulier des résultats sur les corps de Rolle.

Exemples. Des exemples simples de corps de Rolle sont donnés par les corps réels-clos et les corps chaîne-clos. Un autre exemple dû à F. Delon est donné par les corps de séries formelles généralisées $K = R((G))$ où R est un corps réel-clos et G est un groupe abélien ordonné impair-divisible ; le nombre des ordres de K est alors égal à 2^d où d désigne la dimension de G comme $\mathbf{F}_2$-espace vectoriel.

I-THEORIE DES CORPS DE ROLLE AYANT UN NOMBRE FINI D'ORDRES.

Théorème 1.1. *Un corps K est un corps de Rolle ayant exactement 2^n (avec $n \geq 0$) ordres si et seulement si c'est un modèle de la théorie suivante (écrite dans le langage des anneaux) et notée T_n :*

(i) axiomes de corps commutatif ordonnable (noté ensuite K) ;

(ii) K est pythagoricien au niveau 4 ($\forall x \, \forall y \, \exists z \quad x^4 + y^4 = z^4$) ;

(iii) il existe dans K n éléments α_1 tels que :

1) aucun des $2^n - 1$ produits de α_1 distincts n'appartient à $\pm \sum K^2$

2) K est la réunion de 2^{n+1} classes : K^2, $-K^2$, $\alpha_1 K^2$, $-\alpha_1 K^2$, $\alpha_2 K^2$, $-\alpha_2 K^2$, ..., $\alpha_1\alpha_2 K^2$, $-\alpha_1\alpha_2 K^2$, ..., $(\prod_{i=1}^{n} \alpha_i)\, K^2$, $-(\prod_{i=1}^{n} \alpha_i)\, K^2$;

(iv) tout polynôme de degré impair a une racine dans K .

Remarquons que pour $n = 0$ on retrouve bien une axiomatisation des corps réels-clos (K corps commutatif ordonnable tel que K est la réunion de K^2 et de $-K^2$, K n'admet pas d'extension algébrique de degré impair et K pythagoricien au niveau 4 (qui équivaut ici à K pythagoricien au niveau 2 car $K = K^2 \cup -K^2$ montre que si $x \in K^2$ alors $x \in K^4$ donc que $K^2 = K^4$). Pour $n = 1$ on trouve une des axiomatisations des corps chaîne-clos que nous avons donnée dans [G1] à la remarque suivant le théorème 3 , ce qui rejoint le résultat de [Di] disant que les corps chaîne-clos sont les corps de Rolle avec exactement deux ordres.

Le théorème résulte immédiatement des deux lemmes a et b démontrés ci-dessous.

Lemme a. les corps de Rolle ayant exactement 2^n ordres sont des modèles de la théorie T_n .

Démonstration du lemme a.

Les corps de Rolle sont évidemment des corps ordonnables par définition même. Ils sont pythagoriciens au niveau 4 (et donc aussi au niveau 2 puisque ordonnables, c.f. [H]) : il suffit d'appliquer le lemme 1 de [D-G] qui caractérise les éléments qui sont une puissance 2^n dans un corps admettant une valuation hensélienne telle que le corps des restes soit réel-clos ; (*démonstration* : soit v une valuation hensélienne à corps des restes réel-clos, considérons $x^4 + y^4$, si $v(x) = v(y)$ alors on a $x^4 + y^4 = x^4 (1 + (y/x)^4)$, les éléments de la parenthèse sont des restes dans un corps réel-clos et leur somme est donc une puissance quatrième ; si $v(x) \neq v(y)$, alors $x^4 + y^4 \propto x^4$ par exemple et $4 \mid v(x^4+y^4)$) .les axiomes (i) et (ii) sont donc satisfaits.

Un corps de Rolle ayant 2^n ordres est tel que si $v \in V(K)$ la dimension de $vK/2vK$, considéré comme $\mathbb{F}_2$-espace vectoriel, est n (d'après la proposition 0-7). Si $(\bar{g}_1 ,..., \bar{g}_n)$ est une base de $vK/2vK$, soient $g_i \in vK$ tels que $g_i/2vK = \bar{g}_i$, et soient $k_i \in K^*$ tels que $v(k_i) = g_i$. Les k_i obtenus satisfont les propriétés imposées aux α_i des axiomes énoncés ci-dessus. En effet les 2^n ordres de K sont déterminés par une condition de signe sur les n éléments k_i donc aucun produit de k_i distincts n'appartient à $\pm K^2$. Enfin un corps de Rolle est superpythagoricien, donc K^2 est un fan et K ayant 2^n ordres $\mid K^* / K^{2*} \mid$ vaut 2^{n+1} ; K satisfait donc bien les axiomes de (iii) 1) et 2) .

Un corps de Rolle n'admettant aucune extension algébrique de degré impair le dernier axiome (iv) est lui aussi satisfait.

Lemme b. Tout modèle de T_n est un corps de Rolle ayant exactement 2^n ordres.

Démonstration du lemme b.

Soit K un modèle de T_n ; le corps K n'admettant pas d'extension algébrique de degré impair, alors toute extension finie non triviale contient une extension quadratique (voir la preuve de la prop. 5 de [D-G]) ; les extensions minimales de K sont donc les extensions quadratiques.

K étant ordonnable et pythagoricien au niveau 4 est aussi pythagoricien à tout niveau 2^n ([H] cor. 2-4) ; montrons que le préordre K^2 est un fan donc que K est superpythagoricien : pour cela on utilise que le nombre de classes modulo K^2 étant fini, K n'admet qu'un nombre fini d'ordres ; K ayant un nombre fini d'ordres alors K admet un nombre fini de places réelles (c.f. la surjection de X_k l'ensemble des ordres de K sur M(K) , voir par exemple [L2] page 73).

K étant pythagoricien au niveau 2^n pour tout n et $|M(K)|$ étant fini on en déduit par le résultat de Harman ([H] cor.2-9) que K est strictement pythagoricien à tout niveau 2^n (donc en particulier que K est superpythagoricien) et que K n'admet qu'une seule place réelle.

Il suffit de compter les extensions minimales dont on sait qu'elles sont ici les extensions quadratiques : il y en a clairement $2^{n+1} - 1$ d'après les axiomes (iii) ; on dénombre ensuite les ordres de K : le nombre de classes modulo les carrés étant 2^{n+1} et K^2 étant un fan , K admet exactement 2^n ordres ([L2] p. 129 par exemple).

On utilise alors la proposition 0-6 caractérisant les corps Rolle pour conclure : le modèle K de T_n ayant 2^n ordres, ayant une seule place réelle et admettant exactement $2^{n+1} - 1$ extensions minimales est un corps de Rolle.

Remarque. Si on supprime l'axiome (iii) 1) du théorème I-1 on obtient une axiomatisation des corps de Rolle ayant au plus 2^n ordres.

Le corollaire suivant donnera lui une axiomatisation des corps de Rolle ayant exactement 2^n ordres avec $n \geq 1$, c'est à dire des corps de Rolle qui sont des corps chaînables ; car les corps de Rolle étant pythagoriciens à tout niveau, dès qu'il existe une constante α n'appartenant pas à $\pm K^2$ alors on a automatiquement que α^2 n'est pas une somme de puissances quatrièmes dans K donc que le corps K est chaînable, et même bien chaînable et α-chaînable au sens de [G2].

Corollaire 1.2. *Un corps K est un corps de Rolle ayant exactement 2^n (où ici $n \geq 1$) ordres si et seulement si c'est un modèle de la théorie suivante (dans le langage des anneaux) notée T'_n :*

(a) axiomes de corps commutatif (noté ensuite K) ;

(b) K est pythagoricien au niveau 2 ($\forall x \, \forall y \, \exists z \quad x^2 + y^2 = z^2$) ;

(c) K est pythagoricien au niveau 4 ($\forall x \, \forall y \, \exists z \quad x^4 + y^4 = z^4$) ;

(d) il existe dans K n éléments α_1 tels que :

1) aucun des $2^n - 1$ produits de α_1 distincts (notés désormais β_j) n'appartient à $\pm \sum K^2$;

2) pour tout $\gamma_j = \pm \beta_j$, l' axiome :

$\forall x \, \forall y \, \exists z \quad x^2 + \gamma_j y^2 = z^2 \vee x^2 + \gamma_j y^2 = \gamma_j z^2$;

3) K est la réunion de 2^{n+1} classes : K^2, $-K^2$, $\alpha_1 K^2$, $-\alpha_1 K^2$, $\alpha_2 K^2$, $-\alpha_2 K^2$, ..., $\alpha_1\alpha_2 K^2$, $-\alpha_1\alpha_2 K^2$, ..., $(\prod_{i=1}^{n} \alpha_i) K^2$, $-(\prod_{i=1}^{n} \alpha_i) K^2$;

(e) tout polynôme de degré impair a une racine dans K .

Démonstration.

Un corps de Rolle ayant 2^n ordres satisfait ces axiomes car le théorème I-1 montre que (a), (c), (d) 1) et 3), et (e) sont vérifiés ; il suffit alors

d'utiliser le fait que K de Rolle est superpythagoricien et que donc K^2 est un fan pour démontrer (d) 2) : dans [Br] on trouve en effet la caractérisation suivante des fans " un préordre T est un fan si est seulement si pour tout a tel que $-a \notin T$ on a : $T + aT = T \cup aT$ " qui donne immédiatement le résultat.

Réciproquement il suffit de montrer qu'un modèle de T'_n satisfait les axiomes du théorème I-1. Pour cela il suffit de vérifier que le corps K est ordonnable ; puisque ici $n \geq 1$, il existe un élément α dans K tel que $\alpha \notin \pm K^2$; si le corps K n'était pas ordonnable, -1 serait une somme de carrés et donc un carré dans K ; alors on peut montrer que l'élément $-1 + \alpha$ n'appartient pas à $K^2 \cup \alpha K^2$ ce qui est impossible d'après (d) 2) ; en effet si $-1 + \alpha = x^2$, alors $\alpha = x^2 + 1$ serait un carré dans K ce qu'il n'est pas ; si $-1 + \alpha = \alpha x^2$ alors $-1 = \alpha (x^2 - 1)$, si -1 est un carré alors $x^2 - 1$ est aussi un carré (qui ne peut être nul en raison de l'égalité ci-dessus) on obtiendrait alors $\alpha = -1 (x^2 - 1)^{-1} = -y^2$ ce qui est aussi impossible.

Théorème 1.3. *Soit K un corps ayant un nombre fini, supérieur ou égal à 1 d'ordres ; alors les propriétés suivantes sont équivalentes :*

(i) K est un corps de Rolle ;

(ii) K est pythagoricien au niveau 4 et n'admet pas d'extension algébrique de degré impair.

De plus on sait qu'alors il existe $n \geq 0$ constantes $\alpha_i \notin \pm K^2$ telles que $K = K^2 \cup -K^2 \bigcup_j (\beta_j K^2 \cup -\beta_j K^2)$ où les β_j représentent les $2^n - 1$ produits de α_i distincts, et que le corps admet exactement 2^n ordres.

On retrouve bien sûr, si K a un seul ordre, les corps réels-clos , et si

K a deux ordres, les corps chaîne-clos.

Démonstration.

(i) ⇒ *(ii)* est bien clair car on a déja montré (c.f. démonstration du lemme a) qu'un corps de Rolle était pythagoricien au niveau 4 et on sait par la proposition 0-5 qu'un corps de Rolle n'admet pas d'extensions algébriques de degré impair.

(ii) ⇒ *(i)* soit K un corps admettant un nombre fini $p \geq 1$ d'ordres, pythagoricien au niveau 4 et n'admettant pas d'extension algébrique de degré impair. K ordonnable et pythagoricien au niveau 4 entraîne que K est pythagoricien à tout niveau 2^n ([H] cor.2-4) ; K ayant un nombre fini d'ordres alors $|M(K)|$ est fini ; K pythagoricien à tout niveau 2^n et $|M(K)|$ fini entraîne ([H] Cor. 2-9) que $|M(K)| = 1$ et que K est 2^n-strictement pythagoricien pour tout n ; K est donc en particulier superpythagoricien et admet une seule place réelle.

K n'admettant pas d'extension algébrique de degré impair alors toute extension minimale est une extension quadratique (déjà utilisé au lemme b) ; K est donc un corps ayant p ordres, superpythagoricien dont les extensions minimales sont les extensions quadratiques ; d'après (b) ⇒ (a) du theorème 6-1 de [B.C.P.2] , K admet exactement 2p-1 extensions minimales.

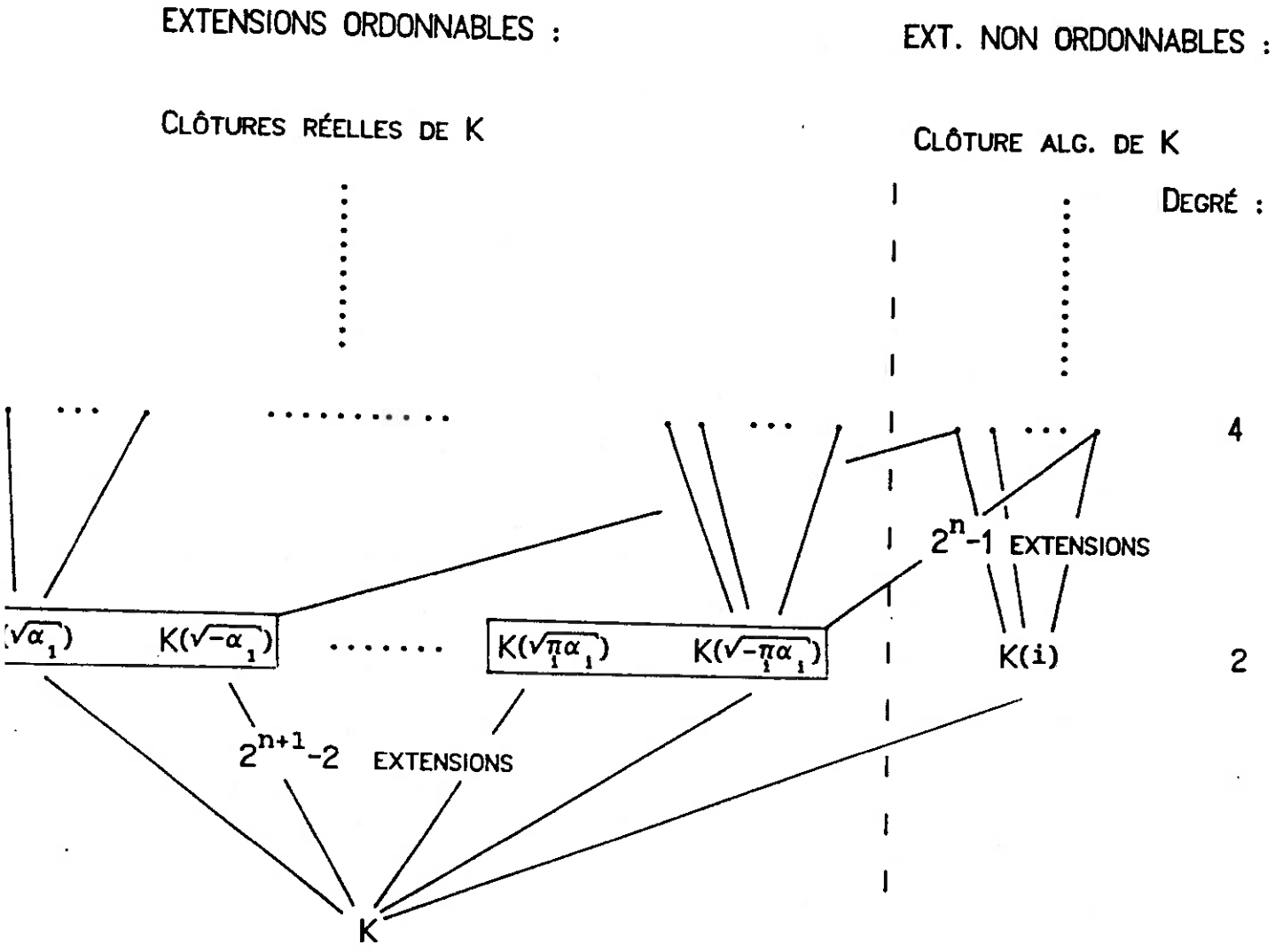
Enfin par la proposition 0-6 le corps K ayant p ordres , 2p-1 extensions minimales et une seule place réelle est donc un corps de Rolle.

L'affirmation finale sur le nombre des ordres résulte du fait que K ayant un nombre fini d'ordres il existe n tel que $| K^* / K^{2*} | = 2^{n+1}$, le corps K étant superpythagoricien K^2 est un fan d'où on déduit que le nombre d'ordres de K est 2^n (voir [L2] p.129 par exemple). L'existence de $n \geq 0$ constantes α_1 et l'allure du corps résulte alors immédiatement du fait que

le corps K étant de Rolle, il satisfait les axiomes du théorème I-1.

Le théorème suivant est une généralisation de celui obtenu dans [D-G] pour les corps chaîne-clos.

Théorème 1.4. *Les extensions algébriques ordonnables d'un corps de Rolle ayant exactement 2^n ordres sont des corps de Rolle ayant 2^n ordres et le treillis des extensions algébriques d'un corps de Rolle avec 2^n ordres est le suivant :*



Démonstration.

Une extension algébrique d'un corps de Rolle ayant 2^n ordres est un corps de Rolle ayant au plus 2^n ordres. Cela résulte du fait qu'une extension algébrique d'un corps de Rolle est un corps de Rolle (proposition 0-5) ; de celui qu'un corps de Rolle avec 2^n ordres admet $2^{n+1} - 1$ extensions minimales qui sont toutes quadratiques et sont explicitables par les axiomes du theorème 1 ; et enfin du fait qu'une extension quadratique d'un corps de Rolle ayant exactement 2^n ordres est un corps ayant au plus 2^n ordres : en effet un ordre de K s'étend à $K(\sqrt{\beta_1})$ si et seulement si β_1 appartient à l'ordre, or β_1 appartient à 2^{n-1} ordres de K mais pour chacun de ces ordres il y a exactement deux extensions possibles.

Il reste à montrer qu'une extension quadratique de K a exactement 2^n ordres ; on reprend pour cela la preuve faite dans [D-G] pour montrer qu'il existe sur K une valuation hensélienne avec corps des restes réel-clos, vK impair-divisible et $| vK / 2vK | = 2n$; en utilisant la proposition 0-7 on concluera que le nombre d'ordres est bien exactement 2^n .

Soit $v \in V(K)$; si M est une extension algébrique de K , v se prolonge de façon unique à M et reste hensélienne, l'extension $k_v \subseteq m_v$ est algébrique et $vK \subseteq vM$ rationnelle (c'est à dire que vM se plonge dans la clôture divisible de vK). Le théorème d'Ostrowski ([R1] p. 237) nous dit, pour $[M : K]$ fini que $[M : K] = [m_v : k_v] (vM ; vK)$. Si $[M : K] = 2$, ou bien $[m_v : k_v] = 2$ et m_v est algébriquement clos, donc M non ordonnable (et donc égal à $K(i)$ en utilisant le théorème I-1), et $vM = vK$; ou bien $m_v = k_v$ et $(vM ; vK) = 2$; dans ce cas là, M reste un corps de Rolle ayant exactement 2^n ordres car v est hensélienne sur M , $m_v = k_v$ est réel-clos, vM reste impair divisible car M n'a pas d'extension algébrique de degré impair et satisfait $| vM / 2vM | = 2n$ à cause de la relation $(vM ; vK) = 2$. Compte tenu du théorème I-1 il y a

$2^{n+1} - 2$ telles extensions .

Théorème 1.5. *Soit K un corps commutatif, sont équivalents :*

(i) K est un corps de Rolle ayant 2^n ordres ;

(ii) K admet $n+1$ ordres $P_0, P_1, ..., P_n$, tels que $P_0 \cap P_1 \cap ... \cap P_n = K^2$ et pour tout j de 0 à n , $\bigcap_{i \neq j} P_i$ est distincte de K^2 ;

K est Pythagoricien au niveau 4 ;

K n'admet pas d'extension algébrique de degré impair.

Démonstration.

(i) ⇒ (ii) est clair :

en appliquant le théorème I-1 : on définit P_i , pour i de 0 à n-1 , comme étant l'ordre qui rend une des n constantes , α_i , négative et toutes les autres positives, et P_n comme l'ordre tel que les n constantes α_i , pour i de 0 à n-1 , soient positives.

(ii) ⇒ (i) :

Montrons que les conditions (ii) entrainent que K a un nombre fini d'ordres. Puisque $P_1 \cap ... \cap P_n$ n'est pas égal à K^2 il existe α_0 non dans K^2 mais appartenant à $P_1 \cap ... \cap P_n$; donc $\alpha_0 \notin P_0$ et $\alpha_0 \in -P_0$ et aussi $\alpha_0 \in P_1 \cap ... \cap P_n$. On peut ainsi trouver n constantes α_i , i de 0 à n-1 , qui sont distinctes, appartiennent à P_n et telles que pour tout i $\alpha_i \in -P_i$ et pour tout j différent de i $\alpha_i \in P_j$. Alors tous les produits de α_i distincts sont dans des classes modulo K^2 qui sont distinctes car ils n'ont, deux à deux, jamais le même signe pour tous les ordres de K .

Considérons alors $F = \pm K^2 \cup \pm \beta_k K^2$ où les β_k représentent tous les

produits possibles de α_i (i de 0 à n-1) distincts. Supposons que F ne soit pas égal à K ; il existerait alors dans K un élément $\gamma \notin F$; si $\gamma \in P_n$, alors on regarde pour chaque i de 0 à n-1 si γ appartient à P_i ou à $-P_i$; on note ε_i l'élément 1 si $\gamma \in P_i$ et l'élément α_i si $\gamma \in -P_i$; alors il est clair que $\varepsilon_0 \varepsilon_1 \dots \varepsilon_{n-1} \gamma$ est un élément de $P_0 \cap \dots \cap P_{n-1}$; d'après l'hypothèse c'est aussi un élément de P_n , c'est donc un élément de K^2 ce qui entraîne, le produit des ε étant un produit de α , que l'élément γ appartient à F ce qui est impossible. Si $\gamma \in -P_n$ on définit de même des η_i par $\eta_i = 1$ si $\gamma \in -P_i$ et $\eta_i = \alpha_i$ si $\gamma \in P_i$ alors l'élément $\eta_0 \eta_1 \dots \eta_{n-1} \gamma$ est dans $-P_1 \cap \dots \cap -P_{n-1}$; c'est aussi un élément de $-P_n$, c'est donc un élément de $-K^2$ ce qui entraîne aussi $\gamma \in F$ et qui est donc impossible. Donc $F = K$ et K n'a qu'un nombre fini d'ordres ; enfin puisque $| K^* / K^{2*} | = 2^{n+1}$, K a au plus 2^n ordres.

Le corps K n'ayant qu'un nombre fini d'ordres, alors en utilisant la caractérisation donnée par le théorème I-3, on obtient bien que K est un corps de Rolle. Compte tenu de la décomposition de K en réunion de classes modulo les carrés obtenue ci-dessus et du théorème 1-1 K a exactement 2^n ordres.

Remarque. Ce théorème contient en corollaire la caractérisation 4-3 des corps chaîne-clos donnée dans [H] : "soit R un corps ayant une chaîne $(P_i)_{i \in \mathbb{N}}$; alors R est chaîne-clos si et seulement si $P_0 \cap P_1 = R^2$ et R n'admet pas d'extension algébrique de degré impair".

En effet si R est chaîne-clos R est un corps de Rolle ayant exactement 2 ordres qui satisfont donc d'après le théorème 1-5 $P_0 \cap P_1 = R^2$ et le même théorème montre que R n'admet pas d'extension algébrique de degré impair.

Réciproquement, si un corps R chaînable par une chaîne $(P_i)_{i \in \mathbb{N}}$ n'admet

pas d'extension algébrique de degré impair et est tel que $P_0 \cap P_1 = R^2$, alors le raisonnement fait au début de la preuve de (ii) $\Rightarrow$ (i) du théorème 1-5 montre que R admet au plus deux ordres, et puisqu'il est chaînable exactement deux ordres. La condition $P_0 \cap P_1 = R^2$ montre que R est pythagoricien, et il suffit alors d'utiliser la dernière partie du résultat de [Bel] (cor.2 p.43) qui donne la chaîne d'un corps n'ayant que deux ordres pour déduire que R est pythagoricien au niveau 4 ; le théorème 1-5 donne alors que R est un corps de Rolle ayant exactement deux ordres et R est donc un corps chaîne-clos.

Notons aussi que bien sûr pour $n = 0$ le théorème 1-5 redonne une caractérisation connue d'un corps réel-clos.

Corollaire 1.6. *Soit K un corps de Rolle ayant 2^n ordres, alors il existe sur K $n+1$ ordres P_i tels que $K = R_0 \cap \ldots \cap R_n$, où R_i désigne la clôture réelle de K pour l'ordre P_i.*

Remarque. Ce corollaire généralise le résultat de [Bel] qui montre que les corps réel-clos généralisés (i.e. corps de Rolle ayant exactement deux ordres) sont l'intersection des deux clôtures réelles.

Démontration.

Par le théorème I-5 on sait qu'il existe sur K $n+1$ ordres P_i ayant les propriétés : $P_0 \cap P_1 \cap \ldots \cap P_n = K^2$ et pour tout j de 0 à n, $\bigcap_{i \neq j} P_i$ est distincte de K^2.

Soit $L = R_0 \cap \ldots \cap R_n \supseteq K$, notons P'_i l'ordre induit sur L par celui de R_i qui prolonge donc l'ordre P_i de K. On a $\bigcap_{i=0}^{n} P'_i \supseteq L^2$ d'où aussi $\bigcap_{i=0}^{n} P'_i \cap K \supseteq L^2 \cap K$ et donc d'après l'hypothèse $K^2 \supseteq L^2 \cap K$. L ne contient donc aucune extension quadratique de K ce qui prouve, K étant un corps de Rolle, que $L = K$.

II-THEORIE GENERALE DES CORPS DE ROLLE.

Théorème 2.1. *Soit K un corps commutatif, les propriétés suivantes sont équivalentes :*

(i) K est un corps de Rolle ;

(ii) K est ordonnable, pythagoricien au niveau 4 , tel que K^2 soit un fan et que K n'admette pas d'extension algébrique de degré impair.

Remarque. Nous avions initialement démontré que (ii) ⇒ (i) à l'aide de divers résultats dont en particulier une partie de la preuve de (b) ⇒ (c) du théorème 6-1 de [B-C-P2] qui n'utilise pas réellement que le nombre d'ordres du corps est fini.

F. Delon nous a fait remarquer que les corps de Rolle avaient déjà été étudiés dans le cadre plus général des corps héréditairement S-pythagoriciens dans [J]. L'hypothése faite dans [J] lorsque l'on considère le cas particulier de $S = \{2\}$ est celle d'un corps K ordonnable, où K^4 est un fan et où K n'admet pas d'extension algébrique de degré impair. Il est clair que cette hypothèse entraîne (ii) de II-1 car si K^4 est un fan alors K^2 en est aussi un (voir [Bel] p. 64) ; par contre K^2 est un fan n'entraîne pas en général que K^4 en soit un.

A la suite de cette remarque, nous avons préféré changer la preuve et utiliser le résultat de [J] pour montrer que (ii) ⇒ (i) .

Démonstration.

(i) ⇒ (ii) est clair :

on sait par définition que K est ordonnable ; par les propositions 0-4 et

0-5 on sait aussi que K est superpythagoricien et n'admet pas d'extension algébrique de degré impair ; enfin la démonstration du fait que le corps K est pythagoricien au niveau 4 faite dans [D-G] et déjà utilisée au lemme a reste valable ici.

(ii) $\Rightarrow$ (i) :

K corps ordonnable pythagoricien au niveau 4 est pythagoricien à tout niveau 2^n pour $n \geq 1$ (d'après [H] cor. 2-4).

K^2 étant un fan par hypothèse le corps K est superpythagoricien.

Le corps K étant superpythagoricien, on en déduit que, si on note $F(K) = \{ n \in \mathbb{N} \mid K^{2^n}$ est un fan de $K \}$, alors $1 \in F(K)$ qui n'est donc pas vide. On peut alors utiliser le résultat 3-17 de [Be2] et en déduire que l'on a $| M(K) | \leq 2$.

On utilise à nouveau un résultat de Harman (cor.2-9 de [H]) pour montrer que puisque K est pythagoricien au niveau n pour tout $n \geq 1$ et que $| M(K) |$ est fini, alors K est 2^n-strictement pythagoricien pour tout n , donc qu'en particulier K^4 est un fan .

Le corps K est donc ordonnable tel que K^4 est un fan et que K n'admet pas d'extension algébrique de degré impair ; il est donc héréditairement $\{2\}$-pythagoricien au sens de Jacob. Dans [J] il est montré que les corps héréditairement S-pythagoriciens admettent une valuation hensélienne à corps des restes réels-clos, et les corps héréditairement $\{2\}$-pythagoriciens n'admettant pas d'extension de degré impair ces derniers satisfont donc la caractérisation des corps de Rolle donnée à la proposition 0-3, ce qui termine la preuve.

Corollaire 2.2. *Une axiomatisation des corps de Rolle dans le langage des anneaux est donnée par la théorie T suivante :*

1- Axiomes de corps commutatif ;

2- Pour chaque $n \geq 1$ l'axiome : $\forall x_1 \ldots \forall x_n \ \neg (-1 = x_1^2 + \ldots + x_n^2)$;

3- $\forall x \ \forall y \ \exists z \quad x^4 + y^4 = z^4$;

4- $\forall x \ \forall y \ \forall z \ \exists t \ (x = -t^2 \ \vee \ y^2 + x z^2 = t^2 \ \vee \ y^2 + x z^2 = x t^2)$;

5- Pour chaque $p \geq 1$ l'axiome :

$$\forall x_0 \ldots \forall x_{2p+1} \ \exists y \ (x_{2p+1} = 0 \ \vee \ x_0 + x_1 y + \ldots + x_{2p+1} y^{2p+1} = 0).$$

Preuve.

Cette axiomatisation se déduit immédiatement du théorème II-1.

Remarque. On peut aussi y remplacer le schéma d'axiome 2 par l'axiome 2' :

2'- $\forall x \ \forall y \ \exists z \ (\neg (-1 = x^2) \ \wedge \ x^2 + y^2 = z^2)$.

III-CORPS DE ROLLE ET CHAINABILITE.

[B1] et [H] sont les références de base sur les ordres de niveau supérieur et sur les chaînes d'ordres de niveau supérieur, cependant sur le sujet des corps chaînables on pourra aussi consulter l'exposé en français [G4].

Un corps qui n'admet qu'un seul ordre n'est jamais chaînable, les corps de Rolle ayant exactement un ordre qui sont les corps réels-clos sont donc non chaînables. Dès qu'un corps de Rolle admet au moins deux ordres alors il est chaînable car il existe au moins un élément α de K qui n'est ni un carré ni un opposé de carré : le corps étant pythagoricien au niveau 4, si, pour tout α dans K, α^2 était une somme de puissances quatrièmes alors il serait une puissance quatrième et α serait un carré ou un opposé de carré ce qui est faux comme on l'a vu. Un corps de Rolle ayant au moins deux ordres est donc toujours chaînable et même bien chaînable au sens de [G2].

Théorème 3.1. *Si K est un corps de Rolle ayant au moins deux ordres, alors pour toute extension algébrique L de K il existe une chaîne d'ordres de niveau supérieur de K qui ne s'étend pas fidèlement à L.*

Démonstration.

D'après ce qui précède on sait que toute extension algébrique ordonnable d'un tel corps contient une extension quadratique $K(\sqrt{\alpha})$ avec $\alpha \notin \pm K^2$. Le corps K étant pythagoricien au niveau 4, $\alpha^2 \notin K^4$ entraîne que $\alpha^2 \notin \sum K^4$ et le corps K est donc α-chaînable (voir [G2]) ; il admet donc au moins une

α-chaîne (i.e. une chaîne $(P_i)_{i\in\mathbb{N}}$ telle que $\alpha^2 \notin P_2$) qui ne saurait s'étendre fidèlement à $K(\sqrt{\alpha})$ car $\alpha^2 \in \sum (K(\sqrt{\alpha}))^4 \subseteq P_2'$ pour tout ordre P_2' de niveau exact 2 de $K(\sqrt{\alpha})$, ce qui termine la preuve.

Théorème 3.2. *Un corps de Rolle chaînable (i.e. ayant au moins deux ordres) est totalement chaînable (i.e. tout ordre peut être inclus dans une chaîne d'ordres de niveau supérieur, voir [D-G] et [G2]) et de plus toute paire d'ordres est le début d'une chaîne d'ordres de niveau supérieur.*

Démonstration.

Cela résulte du fait que si K est un corps de Rolle il existe une valuation hensélienne à corps des restes réel-clos k_v (c.f. prop.0-3). Une telle valuation est compatible avec tous les ordres du corps K et tous les ordres résiduels coincident avec l'unique ordre de k_v .

Il suffit alors d'appliquer le corollaire 1-5 de [H] (deux ordres P_0 et P_1 sont le début d'une chaîne d'ordres de niveau supérieur si et seulement si il existe une valuation compatible avec ces ordres telle que les ordres induits sur le corps résiduel coincident) pour obtenir que non seulement tous les ordres sont chaînables mais que toutes les paires d'ordres sont le début d'une chaîne d'ordres de niveau supérieur.

Une question naturelle est de chercher si un corps de Rolle est simplement chaînable (i.e. par chaque ordre de niveau supérieur il ne passe qu'une chaîne voir [G2]). On peut répondre par le théorème suivant.

Théorème 3.3. *Seuls les corps de Rolle ayant exactement deux ordres, c'est à dire les corps chaîne-clos, sont simplement chaînables.*

Démonstration.

Cela résulte de la caractérisation des corps simplement chaînables donnée dans [G2] : un corps chaînable K est simplement chaînable si et seulement si pour toute valuation réelle de groupe des valeurs vK on a $| vK / 2vK | \leq 2$, et du fait que si un corps de Rolle K a 2^n ordres pour $v \in V(K)$ on sait (voir [Las2]) que $vK / 2vK$ a pour dimension n comme $\mathbb{F}_2$-espace vectoriel.

Remerciements. Je tiens à remercier ici F. Delon qui a bien voulu me consacrer du temps pour de très utiles discussions notamment à propos du corollaire I-6.

BIBLIOGRAPHIE

[B-C-P1] R. Brown, T. Craven, M.J. Pelling :*"Ordered fields satisfying Rolle's theorem"*, The Rocky Mountain Journal of Math. , vol. 14, # 4, 819-820, Fall 1984.

[B-C-P2] R. Brown, T. Craven, M.J. Pelling : *"Ordered fields satisfying Rolle's theorem"*, Illinois Journal of Mathematics, vol.30, # 1, 66-78, Spring 1986.

[Be1] E. Becker :*"Hereditarily pythagorean fields and orderings of higher types"*, Lectures Notes # 29, Rio de Janeiro, I.M.P.A., 1978..

[B2] E. Becker : *"The real holomorphy ring and sums of 2n-th powers"*, Proceedings, Rennes 1981, Geométrie Algébrique Réelle et Formes Quadratiques. (Lecture notes Math., vol. 959, pp. 139-181) Berlin Heidelberg New York : Springer 1982.

[Br] L. Bröcker :*"Characterization of fans and hereditarily Pythagorean fields"*, Mathematische Zeitschrift 151, 149-163, Springer 1976

[De1] F. Delon :*"Rolle's fields and rings"*, Proc. first int. symposium. on ordered algebraic structures, pp. 155-160, Luminy-Marseille 1984.

[De2] F. Delon :*"Corps et anneaux de Rolle"*, Proceedings de l'A.M.S., vol. 97, pp. 315-319, 1986.

[D-G] F. Delon et D. Gondard :*"17ème problème de Hilbert au niveau n dans les corps chaîne-clos"*, preprint in Séminaire D.D.G. 1986-87 Univ. Paris 7 ; Soumis J. of Symb. Logic.

[Di] M. Dickmann :*"The model theory of chain-closed fields"*, Journal of Symbolic Logic vol. 53 , pp. 73-82, 1988.

[G1] D. Gondard :*"Théorie du premier ordre des corps chaînables et des corps chaîne-clos"*, C. R. Acad. Sc. Paris, tome 304, # 16, 463-465, Paris 1987.

[G2] D. Gondard :*"Etude des chaînes d'un corps chaînable"*, en préparation.

[G3] D. Gondard :*"On Rolle's fields theories"*, Abstract soumis A.M.S..

[G4] D. Gondard :*"Ordres de niveau supérieur, extensions et corps chaîne-clos"* in "Structures Algébriques Ordonnées 1984-87" (Sém D.D.G.), publications Math. de l'Université Paris VII (à paraître).

[H] J. Harman :*"Chains of higher level orderings"*, Proceedings San Francisco 1981, Ordered fields and real algebraic geometry. (Contemporary Mathematics, vol. 8, pp. 141-174) A.M.S. 1982.

[J] B. Jacob :" *The model theory of pythagorean fields* " Thèse (ch. 1 et 2) Princeton University, Princeton, N. J. 1979.

[L1] T. Y. Lam :*"The theory of ordered fields"*, Proceedings of Alg. Conference pp. 1-152, M. Dekker 1980.

[L2] T. Y. Lam :*"Orderings, valuations and quadratic forms"*, C.B.M.S. regional conference vol. 52, A.M.S. 1983.

[Las1] B. Laslandes :*"Théorie des modèles des corps n-ordonnés"*, Thèse de 3ème cycle, Université Paris VII, 1984.

[Las2] B. Laslandes :*"Corps de Rolle portant un nombre fini d'ordres"*, Cr. Acad. Sc. Paris, t. 102, Série I, # 11, 401-404, 1986.

[R1] P. Ribenboim :*"Théorie des valuations"*, Les Presses de l'Université de Montréal, Quebec, 1964.

[R2] P. Ribenboim :*"Arithmétique des corps"*, Hermann Paris 1972.

THE REAL RIEMANN SURFACE OF A RING

by M. J. de la Puente

Let A be a real commutative ring with unit. The aim of this note is to present the definition and main properties of the real Riemann surface of A, as a topological space S. Two concepts, those of real spectrum of A and of Riemann surface of a field (in the algebraic sense of [Z–S]) are combined together to give rise to S. Essentially, the points of S are pairs $(\leq, \mathcal{B})$, where $\leq$ is a total order in the quotient field $\kappa(p)$ of the domain A/p, and $\mathcal{B}$ is a valuation ring of $\kappa(p)$, convex with respect to $\leq$, as p runs through Spec$A$. In practice, the points of S are defined in a slightly different way, but soon we will see the advantages of such a choice. For example, we get an easy proof of the compactness of S.

The chief results are construction 12 and theorem 14. Proposition 13 is interesting too, and also serves us as an useful piece of language. In 12 and 14 we show how the topology of S accurately expresses some algebraic facts about convex valuation rings, such as composite valuations. More precisely, a point $(\leq', \mathcal{C})$ in S lies in the closure of another one $(\leq, \mathcal{B})$ if and only if

(i) $\leq'$ is a generalization of $\leq$, (roughly speaking, inequalities involving $\leq$ are also true for $\leq'$) and

(ii) there exists a decomposition $\mathcal{B}'$ and $\overline{\mathcal{B}}$ of $\mathcal{B}$, (in the sense of proposition 11) such that either (a) $\mathcal{C} = \mathcal{B}'$ or (b) $\mathcal{C}$ is the restriction of $\overline{\mathcal{B}}$ to an adecuate residue field of A.

Not only the *topology* of S is well suited to the study of questions about convex valuation rings of residue fields of A, but also the very *definition* of the points of S helps in this task. For example, the property (ii) (b) above is expressed by an extraordinary simple intersection formula, (see claim, construction 12).

To come to an end, we show in theorem 15 that S has some of the topological properties of the real spectrum of A, the space over which S is constructed.

We start with an easy

Example 1. $A = \mathbf{R}[x]$, x is transcendental over $\mathbf{R}$. For each $\beta \in \mathrm{Spec}_R A$, let p be its support, $\mathrm{supp}(\beta) = \beta \cap -\beta$, and consider all the valuation rings $\mathcal{B}$ over $\mathbf{R}$, of the quotient field $\kappa(p)$ of A/p, which are convex with respect to $\leq_\beta$ i.e.,

$$\text{if } a \in \kappa(p), b \in \mathcal{B}, 0 \leq_\beta a \leq_\beta b \Rightarrow a \in \mathcal{B}.$$

It is well known that $\mathrm{Spec}_R A = \{a, a^+, a^- : a \in \mathbf{R}\} \cup \{\infty^+, \infty^-\}$.

Now, let $a \in \mathbf{R}$. The ordering represented by a has residue field $\mathbf{R}$ and this is the only valuation ring over $\mathbf{R}$, convex with respect to $\leq_a$.

The residue field of a^+ is $\mathbf{R}(x)$ and the only valuation rings over $\mathbf{R}$, convex with respect to $\leq_{a^+}$ are $A_{(x-a)}$ and $\mathbf{R}(x)$. Similarly, for a^-, we have convex valuation rings $A_{(x-a)}$ and $\mathbf{R}(x)$.

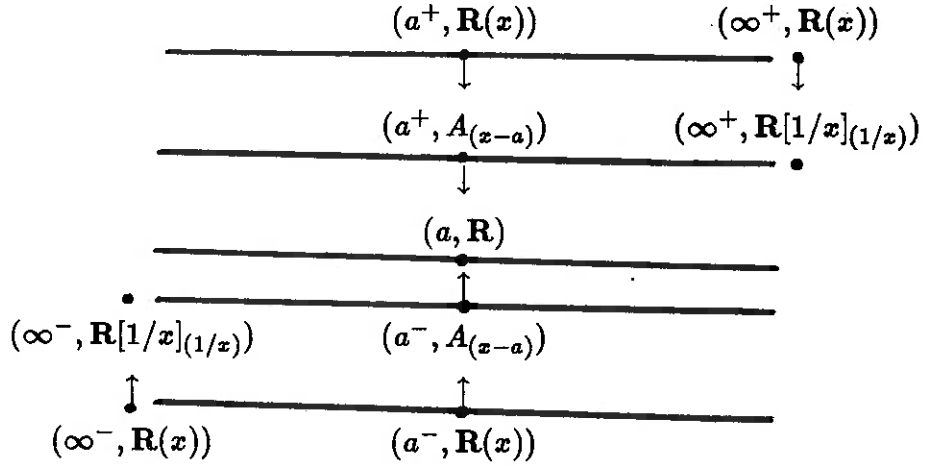
Finally, the valuation rings of the residue field $\mathbf{R}(x)$ of ∞^+ convex with respect to this ordering are $\mathbf{R}[1/x]_{(1/x)}$ and $\mathbf{R}(x)$. The same holds true for ∞^-.

If we gather this information in a space S, whose points are pairs $(\beta, \mathcal{B})$, with β in $\mathrm{Spec}_R A$ and $\mathcal{B}$ a valuation ring as above, we get the set–theoretical real Riemann surface of A:

$$S = \{(a, \mathbf{R}), (a^+, A_{(x-a)}), (a^+, \mathbf{R}(x)), (a^-, A_{(x-a)}), (a^-, \mathbf{R}(x)) : a \in \mathbf{R}\} \cup$$

$$\{(\infty^+, \mathbf{R}[1/x]_{(1/x)}), (\infty^+, \mathbf{R}(x)), (\infty^-, \mathbf{R}[1/x]_{(1/x)}), (\infty^-, \mathbf{R}(x))\}.$$

Below we have a picture of S, containing 5 copies of $\mathbf{R}$ and 4 points "at infinity". An arrow from a point (β, B) to a point (γ, C) means that the latter belongs to the closure of the former. This will be clear after we study the closure of a point in theorem 14.



One of the two main ingredients of the *real* Riemann surface is:

Definition 2. *The Riemann surface of A is the collection T of valuation rings $\mathcal{B}$ of the fields $\kappa(p)$ as p runs through* Spec$A$. *In this situation, p is called the support of $\mathcal{B}$.*

We establish a bijection between points of T and subsets of $A \times A$:

$$T \xrightarrow{\phi} 2^{A \times A} \; ; \; \kappa(p) \supseteq \mathcal{B} \mapsto B = \{(x, y) \in A \times A : y \notin p, \bar{x}/\bar{y} \in \mathcal{B}\},$$

where $\bar{x}$ denotes the class of x modulo p.

We identify T with its image $\phi(T)$. The advantage of the B's over the $\mathcal{B}$'s is that the former avoid the difficulty of working with subsets of different sets $\kappa(p)$, p running through Spec$A$.

T is endowed with a topology, called the W *topology*, which has the following family as a sub–basis:

$$\{W(x, y) : (x, y) \in A \times A\},$$

where $W(x, y) = \{B \in T : (x, y) \in B\}$. This topology in T is a natural generalization of the Zariski topology, considered in [Z–S], in the following sense: if $p \subset A$ is a prime ideal and T_p is the Riemann surface of $\kappa(p)$ then, in the embedding $T_p \subseteq T$, the restriction of the W topology to T_p coincides with the Zariski topology on T_p.

The W topology is weaker than the Tychonoff topology, induced on T as a subset of $2^{A \times A}$.

Definition 3. *The real Riemann surface of A is the collection S of pairs (β, B), where β is in $\mathrm{Spec}_R A$ and $\mathcal{B} = \phi^{-1}(B)$ is a valuation ring of $\kappa(p)$, convex with respect to $\leq_\beta$, where p is the support of β. In this situation we say that β and B are compatible.*

We give to S the initial topology for the projections:

$$\begin{array}{ccc} S & \xrightarrow{\pi_2} & T \\ {\scriptstyle \pi_1}\downarrow & & \\ \mathrm{Spec}_R A & & \end{array} \qquad \begin{array}{ccc} (\beta, B) & \longrightarrow & B \\ \downarrow & & \\ \beta & & \end{array}$$

This is the weakest topology in S making both π_1 and π_2 continuous, and the following family is a sub–basis for it:

$$\{\dot{W}(t; x, y) : t \in A, (x, y) \in A \times A\},$$

where $\dot{W}(t; x, y) = \{(\beta, B) \in S : t \notin \beta, (x, y) \in B\}$. We call it the $\dot{W}$ *topology.*

Theorem 4. *T and S are compact.*

Sketch of the proof. It is enough to show that T and S are Tychonoff closed in $2^{A \times A}$ and in $2^A \times 2^{A \times A}$ respectively, because the topologies of T and S are weaker than the Tychonoff topologies in those spaces. A proof similar to the one done for the real spectrum in [L, p. 783] shows that T is Tychonoff closed. Indeed, we axiomatize the properties of the sets B of type $B = \phi(\mathcal{B})$, and observe that those properties are expressed in terms of $\in$ and $\notin$ conditions. A similar argument works also for S, (see [P] for more details). ■

We turn to the study of the properties of S. Let β be an ordering of A with support p. As the collection of valuation rings of $\kappa(p)$ which are convex with respect to $\leq_\beta$ is totally ordered by inclusion, we view S as a union of totally ordered fibers over $\mathrm{Spec}_R A$. Thus, we have studied the map $\pi_1 : S \to \mathrm{Spec}_R A$ and have pointed out several sections of π_1 whose images are homeomorphic to $\mathrm{Spec}_R A$. We proceed with their description.

The trivial valuation ring of a field is the field itself. Accordingly, the trivial points of the real Riemann surface of A are $(\beta, \kappa(\mathrm{supp}\,\beta))$, where β runs through $\mathrm{Spec}_R A$.

Proposition 5. *The map*

$$\rho : \mathrm{Spec}_R A \to S \ ; \ \beta \mapsto (\beta, \kappa(\mathrm{supp}\,\beta))$$

is a continuous section of π_1 and it is a homeomorphism onto the image.

Proof. To check that ρ is continuous, it is enough to show that the composites $\pi_1\rho$ and $\pi_2\rho$ are continuous, since S has the initial topology for π_1 and π_2. Clearly, $\pi_1\rho$ is the identity. So, all we need to check is that, for any $x, y \in A$, the set $(\pi_2\rho)^{-1}W(x, y)$ is open. But this is so since, if $\bar{x}$ denotes the class of x modulo $\mathrm{supp}(\beta)$, then

$$(\pi_2\rho)^{-1}W(x, y) = \{\beta \in \mathrm{Spec}_R A : y \notin \mathrm{supp}(\beta), \bar{x}/\bar{y} \in \kappa(\mathrm{supp}\,\beta)\} =$$

$$= \{\beta \in \mathrm{Spec}_R A : y \notin \mathrm{supp}(\beta)\} = \{\beta \in \mathrm{Spec}_R A : y <_\beta 0\} \cup \{\beta \in \mathrm{Spec}_R A : y >_\beta 0\}$$

is an open set in $\mathrm{Spec}_R A$. ■

Fixing a subring A_1 of A, we obtain some other sections of π_1. In the applications, we are interested in the cases $A_1 = \mathbf{Z}$, $A_1 = A$ and, if k is a field and A is a finitely generated k–algebra, $A_1 = k$.

Let β be an ordering of A with support p and let $p_1 = p \cap A_1$. Consider the *convex hull* $\mathcal{O}_\beta A_1$ of A_1/p_1 in $\kappa(p)$, with respect to the order $\leq_\beta$. The ring $\mathcal{O}_\beta A_1$ is the smallest convex valuation ring of $\kappa(p)$ containing A_1/p_1:

$$\mathcal{O}_\beta A_1 = \{\bar{x}/\bar{y} \in \kappa(p) \colon |\bar{x}/\bar{y}| <_\beta \bar{a}, \text{for some } a \in A_1\}.$$

Proposition 6. *The map*

$$\theta \colon \mathrm{Spec}_R A \to S \ ; \ \beta \mapsto (\beta, \mathcal{O}_\beta A_1)$$

is a continuous section of π_1 and it is a homeomorphism onto the image.

Proof. As in the proof of proposition 5, it is sufficient to show that, for any x, $y \in A$, the set $(\pi_2\theta)^{-1}W(x,y)$ is open. But this is clear from the expression

$$(\pi_2\theta)^{-1}W(x,y) = \{\beta \in \mathrm{Spec}_R A \colon y \notin \mathrm{supp}(\beta), |\bar{x}/\bar{y}| <_\beta \bar{a}, \text{for some } a \in A_1\} =$$

$$\bigcup_{a \in A_1} \{\beta \in \mathrm{Spec}_R A \colon y \notin \mathrm{supp}(\beta), \overline{-ay^2} <_\beta \overline{xy} <_\beta \overline{ay^2}\}. \blacksquare$$

Definition 7. *A point (β, B) in the real Riemann surface of A is finite (relative to A) if $\mathcal{O}_\beta A \subseteq B$.*

It is rutinely checked that this condition is equivalent to $A \times \{1\} \subseteq B$.

Now we devote ourselves to the study of the relation between $\pi_1^{-1}(\beta)$ and $\pi_1^{-1}(\gamma)$, for orderings β, γ of A with $\beta \subseteq \gamma$. This is done in theorems 12 and 13. These results are achieved by "weaving" some well–known facts, (here numbered 8, 9 and 11) about the real spectrum and about convex valuation rings. With the help of 12 and 13, we "discover" in 14 what it means for a point (γ, C) to be in the closure of another one (β, B), in terms of the "classical" valuation rings $\mathcal{B}$ and $\mathcal{C}$ rather than in terms of the "formal" valuation rings B and C.

In addition, 12 and 14 show how simple it is to express, *in* S, certain concepts about valuation rings.

Finally, 13 and 14 are a first sample of why it is useful to have constructed S.

As to notation, $m_\mathcal{B}$ denotes the maximal ideal of a valuation ring $\mathcal{B}$ of a field K and $\Delta_\mathcal{B}$ denotes the residue field $\mathcal{B}/m_\mathcal{B}$. An order $\leq$ in K making $\mathcal{B}$ convex induces an order in $\Delta_\mathcal{B}$, and throughout these notes, $\Delta_\mathcal{B}$ will be tacitly endowed with this order.

Proposition 8 [Br p.149]. *Given an ordered field $(K, \leq)$, a subring $\mathcal{A} \subseteq K$ and a convex prime ideal $Q \subset \mathcal{A}$ then, the convex hull $\mathcal{H}$ in K of the localization $\mathcal{A}_Q$ is a valuation ring of K with*

$$Q = m_\mathcal{H} \cap \mathcal{A}.$$

Moreover, $\Delta_{\mathcal{H}}$ is an archimedean extension of the quotient field of $\mathcal{A}_Q$.

Proposition 9 [B–C–R p.82]. *Let β be an ordering of A with support p. There is a bijection ψ between the orderings γ of A containing β and the prime ideals $q \subset A$ containing p which are convex with respect to $\leq_\beta$. More precisely, $\psi(\gamma) = \text{supp}(\gamma)$ and $\psi^{-1}(q) = q \cup \beta$.*

Definition 10. (a) *Given a field K, a subring $\mathcal{A} \subseteq K$ and a valuation ring $\mathcal{D} \subseteq K$ containing $\mathcal{A}$, the ideal*

$$Q = m_{\mathcal{D}} \cap \mathcal{A}$$

is called the center of $\mathcal{D}$ at $\mathcal{A}$.

(b) *Let (β, B) be a finite point of S, $p = \text{supp}(\beta)$ and let*

$$q/p = m_{\mathcal{B}} \cap A/p$$

be the center of $\mathcal{B}$ at A/p. Then, the preimage q of q/p under the canonical homomorphism $A \to A/p$ is called the center of B (at A).

Proposition 11. *Given an ordered field $(K, \leq)$, a convex valuation ring $\mathcal{B} \subseteq K$ and a convex valuation ring $\overline{\mathcal{B}}$ of $\Delta_{\mathcal{B}}$, then $\mathcal{B}' = \{x \in \mathcal{B} : x + m_{\mathcal{B}} \in \overline{\mathcal{B}}\}$ is a convex valuation ring of K contained in $\mathcal{B}$. Moreover, if m' is the maximal ideal of $\mathcal{B}'$, then $\mathcal{B}'_{m'} = \mathcal{B}$ and $\mathcal{B}'/m_{\mathcal{B}} = \overline{\mathcal{B}}$.*

In other words, given $(K, \leq)$ and $\mathcal{B}$ as above, there is a bijection between the family of convex valuation rings of $\Delta_{\mathcal{B}}$ and that of convex valuation rings of K contained in $\mathcal{B}$.

This fact follows from realizing that convexity is preserved throughout the proof of the analogous result in [N p.35].

Construction 12. Let $\beta \subseteq \gamma$ be orderings of A with $p = \text{supp}(\beta)$, $q = \text{supp}(\gamma)$. In 8, take $K = \kappa(p)$, $\mathcal{A} = A/p$, $Q = q/p$ and let $\mathcal{H}$ be the convex hull of $(A/p)_{q/p}$ in $\kappa(p)$. It follows that $\kappa(q) \subseteq \Delta_{\mathcal{H}}$ is an archimedean extension of fields.

For each valuation ring B of A compatible with β, we define a valuation ring C of $\kappa(q)$, convex with respect to $\leq_\gamma$. The ring C depends on (β, B) and γ. Afterwards, we claim that the valuation ring $C = \phi(C)$ is expressed by an easy intersection formula.

Given B compatible with β, consider $\mathcal{B} = \phi^{-1}(B)$. If $\mathcal{B} \subseteq \mathcal{H}$, then $\mathcal{B}/m_{\mathcal{H}}$ is a convex valuation ring of $\Delta_{\mathcal{H}}$, by proposition 11. Therefore, $\mathcal{B}/m_{\mathcal{H}} \cap \kappa(q)$ is a valuation ring of $\kappa(q)$, convex with respect to the order $\leq_\gamma$, induced on $\kappa(q)$ by $\leq_\beta$. Let

$$C = \begin{cases} \mathcal{B}/m_{\mathcal{H}} \cap \kappa(q), & \text{if } \mathcal{B} \subseteq \mathcal{H}, \\ \kappa(q), & \text{otherwise.} \end{cases}$$

Clearly, if $C = \phi(C)$ then, (γ, C) belongs to S.

Claim. $C = B \cap A \times (A \setminus q)$.

Proof of the claim. The center of $\mathcal{H}$ in A/p is q/p, by proposition 8, i.e.,

$$q/p = m_{\mathcal{H}} \cap A/p.$$

This equality means that, if $y \in A$ and $y \notin p$ then,

$$y \in q \iff \bar{y} \in m_{\mathcal{H}},$$

where $\bar{y}$ denotes the class of y modulo p. Then, in the inclusion $\kappa(q) \subseteq \Delta_{\mathcal{H}}$, the element $\tilde{x}/\tilde{y}$ is identified with $(\bar{x}/\bar{y}) + m_{\mathcal{H}}$, where $\tilde{y}$ denotes the class of y modulo q. As a consequence, the definition of C means that, for every $y \notin q$ (hence $y \notin p$, $\bar{y} \notin m_{\mathcal{H}}$ and $\tilde{x}/\tilde{y} \in \kappa(q)$), it holds:

$$\tilde{x}/\tilde{y} \in C \iff \tilde{x}/\tilde{y} \in \mathcal{B}/m_{\mathcal{H}} \iff \bar{x}/\bar{y} \in \mathcal{B}.$$

Thus,

$$(x,y) \in C \iff y \notin q, \tilde{x}/\tilde{y} \in C \iff y \notin q, \bar{x}/\bar{y} \in \mathcal{B} \iff (x,y) \in B \cap A \times (A \setminus q),$$

as was to be shown. ■

Theorem 13. *Let $\beta \subseteq \gamma$ be orderings of A. The map*

$$\pi_1^{-1}(\beta) \to \pi_1^{-1}(\gamma)\ ;\ (\beta, B) \mapsto (\gamma, C),$$

given by construction 12, is surjective. Moreover, this map preserves the trivial section and the section determined by any subring A_1 of A.

Proof. Let p, q, C and $\mathcal{H}$ be as in 12. Consider the convex hull $\overline{\mathcal{H}}$ of C in $\Delta_{\mathcal{H}}$ and let $\mathcal{H}' \subseteq \mathcal{H}$ be as in proposition 11. Then, $H' \cap A \times (A \setminus q)$ is the valuation ring of A associated to

$$\mathcal{H}'/m_{\mathcal{H}} \cap \kappa(q) = \overline{\mathcal{H}} \cap \kappa(q) = C.$$

Thus, $C = H' \cap A \times (A \setminus q)$, and this concludes the proof of the surjectivity.

Now, the trivial point of $\pi_1^{-1}(\beta)$ is mapped to the trivial point of $\pi_1^{-1}(\gamma)$ since

$$A \times (A \setminus p) \cap A \times (A \setminus q) = A \times (A \setminus q).$$

Finally, let A_1 be an arbitrary subring of A. Then, $(\beta, \mathcal{O}_\beta A_1)$ is mapped to $(\gamma, \mathcal{O}_\gamma A_1)$ since

$$\mathcal{O}_\beta A_1 \cap A \times (A \setminus q) = \mathcal{O}_\gamma A_1.$$

Indeed, let $(x,y) \in \mathcal{O}_\gamma A_1$. Then $y \notin q$ and there exists $a \in A_1$ such that $|\tilde{x}/\tilde{y}| <_\gamma \tilde{a}$ and so $\pm xy - ay^2 \notin \gamma$. As $\beta \subseteq \gamma$, then $\pm xy - ay^2 \notin \beta$. Thus, $(x,y) \in \mathcal{O}_\beta A_1 \cap A \times (A \setminus q)$. Conversely, if $y \notin q$ and there is $a \in A_1$ such that $|\bar{x}/\bar{y}| <_\beta \bar{a}$, then $\pm xy + ay^2 \in \beta \subseteq \gamma$. Hence $|\tilde{x}/\tilde{y}| <_\gamma \widetilde{a+1}$ and $(x,y) \in \mathcal{O}_\gamma A_1$, concluding the proof. ■

Now we turn to the study of the closure of a point (β, B) in S. From the definition of the $\dot{W}$ topology, it consists of those points (γ, C) with $\beta \subseteq \gamma$ and $C \subseteq B$.

Theorem 14. *Let (β, B) be a point of the real Riemann surface of A. The points (γ, C) in the closure of (β, B) are of two types:*

(a) *$\beta = \gamma$ and $C \subseteq B$ or*

(b) $\beta \subset \gamma$ *and there exists a valuation ring* $\mathcal{D}$ *of* $\kappa(\operatorname{supp}\beta)$, *convex with respect to* $\leq_\beta$, *such that* $\mathcal{D} \subseteq \mathcal{B}$ *and* $C = \mathcal{D}/m_{\mathcal{B}} \cap \kappa(\operatorname{supp}\gamma)$.

Proof. Let $p = \operatorname{supp}(\beta)$ and $q = \operatorname{supp}(\gamma)$. First, if (γ, C) is of type (a), then $C \subseteq B$. Conversely, if (γ, C) is in the closure of (β, B) and $\beta = \gamma$, then necessarily $C \subseteq \mathcal{B}$.

Suppose now that $\beta \neq \gamma$. If (γ, C) is of type (b), then $C = D \cap A \times (A \setminus q) \subseteq B$, hence (γ, C) is in the closure of (β, B). Conversely, we will be done if we find a valuation ring D of A, compatible with β, contained in B and such that $C = D \cap A \times (A \setminus q)$. But in the proof of 13, we have seen that

$$C = H' \cap A \times (A \setminus q),$$

for a certain valuation ring H' of A, compatible with β. As the valuation rings of A compatible with β form a set totally ordered by inclusion, we have either $H' \subseteq B$ or $B \subseteq H'$. If the former holds, we are finished, taking $D = H'$. Otherwise,

$$C \subseteq B \cap A \times (A \setminus q) \subseteq H' \cap A \times (A \setminus q) = C,$$

and letting $D = B$, we are done too. ∎

To close this note, we present a list of properties common to the real spectrum and the real Riemann surface.

Theorem 15. (a) *The closure of a point* (β, B) *contains a unique closed point.*

(b) *The set of closed points of* S *is homeomorphic to the set of closed points of* $\operatorname{Spec}_R A$ *; in particular it is compact and Hausdorff.*

(c) *The retraction of* S *to the set of closed points is a continuous closed map.*

Proof. (a) Let $\gamma \in \operatorname{Spec}_R A$ be the maximal ordering of A containing β. Then $(\gamma, \mathcal{O}_\gamma A_1)$ is the only closed point in the closure of (β, B).

(b) Take $A_1 = \mathbf{Z}$ and consider the continuous map λ that sends each ordering β of A to the maximal ordering containing β. Then, the restriction of π_1 to the set of closed points of S coincides with the composite continuous map $\pi_1\theta\lambda\pi_1$ and has θ as an inverse.

(c) This retraction is the continuous map $\theta\lambda\pi_1$, and it is closed since the domain is compact and the target is Hausdorff. ∎

REFERENCES

[Br] G. BRUMFIEL, *Partially ordered rings and semi-algebraic geometry*, LMS Lecture Note Series **37**, Cambridge University Press, 1979.

[B–C–R] J. BOCHNAK, M. COSTE, M.–F. ROY, *Gèomètrie algèbrique rèelle*, Ergebnisse der Math. 3 Folge Band 12, Springer–Verlag, Berlin–Heidelberg–New York, 1987.

[L] T. Y. LAM, An introduction to real algebra, Rocky Mountain jour. of math., vol. 14, no. 4, Fall 1984, 767–814.

[N] M. NAGATA, *Local rings*, Intersc. tracts in pure and appl. math. vol. 13, John Willey and sons, New York, 1962.

[P] M. J. de la PUENTE, The Riemann surface of a ring, preprint, 1989.

[Z–S] O. ZARISKI and P. SAMUEL, *Commutative algebra, vol. II*, GTM **29**, Springer–Verlag, Berlin–Heidelberg–New York, 1960.

María Jesús de la Puente
Depto. Algebra
Facultad CC. Matemáticas
Universidad Complutense
28040–MADRID, SPAIN.

RINGS OF CONTINUOUS SEMIALGEBRAIC FUNCTIONS

J.M. Gamboa

Let R be a real closed field and let $M \subset R^n$ be a semialgebraic subset. We have studied some elementary properties of the ring $S(M)$ of continuous functions from M to R with semialgebraic graph. First of all

Theorem 1. $\dim S(M) = \dim M$.

Of course $\dim S(M)$ is the Krull dimension, and $\dim M$ is the semialgebraic topological dimension. The equality was proven by Carral and Coste, [C–C] in case M is locally closed. The inequality $\dim M \leq \dim S(M)$ is clear: if $\tilde{M}$ is the constructible subset of the real spectrum of $R[x_1, \ldots, x_n]$ associated to M, there exists an embedding of spectral spaces

$$\tilde{M} \hookrightarrow \mathrm{Spec} S(M) \colon x \mapsto \{f \in S(M) \colon f(x) = 0\}$$

because given distinct points x, $y \in \tilde{M}$ and a polynomial P with $P(x) \geq 0$, $P(y) < 0$, the semialgebraic function $f = P - |P|$ verifies $f(x) = 0$, $f(y) \neq 0$. Hence $\dim M = \dim \tilde{M} \leq \dim S(M)$, the first equality by [B–C–R], Ch. VII. The argument for the converse inequality was inspired by M. Coste. Let $p_0 \subsetneq \cdots \subsetneq p_d$ be a chain of primes in $S(M)$. We can choose $f_i \in p_i \setminus p_{i-1}$, $1 \leq i \leq d$. Let $X \subset R^{n+d}$ be the graph of the semialgebraic map $f = (f_1, \ldots, f_d) \colon M \to R^d$, and let $g_1, \ldots, g_d$ be the restrictions to the closure $\overline{X}$ of X of the canonical projections $R^{n+d} \to R$ onto the last d coordinates. We get ring homomorphisms $S(\overline{X}) \xrightarrow{j} S(X) \xrightarrow{u} S(M)$, where j is the restriction map and u is the isomorphism which sends $F \in S(M)$ to $G \in S(M)$ defined by $G(x) = F(x, f(x))$. Thus if $q_i = (u \circ j)^{-1}(p_i)$, then $g_i \in q_i \setminus q_{i-1}$ and so $q_0 \subsetneq \cdots \subsetneq q_d$. Whence $\dim S(M) \leq \dim S(\overline{X})$. Also, since $\overline{X}$ is locally closed, $\dim S(\overline{X}) = \dim \overline{X} = \dim X = \dim M$, and the proof is finished.

This result indicates some finiteness character of $S(M)$. On the other hand we get

Theorem 2. (1) *A prime ideal in $S(M)$ is finitely generated if and only if it is the maximal ideal of an isolated point in M.*

(2) *$S(M)$ is noetherian if and only if M is finite.*

Evidently the second part is the immediate consequence of the first one. Also, if $a \in M$ is an isolated point, its maximal ideal m_a is generated by the function $f \in S(M)$ that vanishes at a and takes the constant value 1 outside. So we are concerned with the "only if" part in (1). Let $p = (f_1, \ldots, f_k)$ be a finitely generated prime ideal in $S(M)$. It is rather obvious that $f = (f_1^2 + \cdots f_k^2)^{\frac{1}{3}}$ generates p since the functions

$$g_j \colon M \to R \colon x \mapsto \begin{cases} f_j^3(x) \left(\sum_{i=1}^k f_i^2(x) \right)^{-1} & \text{if } \sum_{i=1}^k f_i^2(x) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

are in $S(M)$, because $0 \leq f_j^2(x) \leq \sum_{i=1}^k f_i^2(x)$ if $x \in M$.

In particular, the zero–set Z of f is non–empty, and we claim that it contains exactly one point. For, if f vanishes at two distinct points $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, we consider $g = \sum_{i=1}^{n}(x_i - a_i)^2$, $h = \sum_{i=1}^{n}(x_i - b_i)^2$, $F = |g-h| - (g-h)$, $G = |g-h| + (g-h)$. Clearly, $FG = 0 \in p$ but F, $G \notin p$ because $F(a) = 2h(a) \neq 0$, $G(b) = 2g(b) \neq 0$.

From now on, a denotes the unique zero of g. It is an isolated point in M. Otherwise, by the curve selection lemma [D–K], there exists a continuous semialgebraic map $\gamma\colon [0,1] \to M$ verifying $\gamma(1) = a$, $\gamma([0,1)) \subset M \setminus \{a\}$. Moreover, since $p = fS(M)$ is a prime ideal, there exists a continuous semialgebraic function $H \in S(M)$ such that $f(1 - fH^2)$ is identically zero on M, and in particular, $1 = f(\gamma(t))H^2(\gamma(t))$ for each $t \in [0,1)$. But, by [B–C–R] Ch. II, $H^2 \circ \gamma([0,1])$ is contained in some interval $(-r, r) \subset R$ and since $f(\gamma(1)) = 0$, $f \circ ([\delta, 1]) \subset (-r^{-2}, r^{-2})$ for some $0 < \delta < 1$. Hence, if $\epsilon = (1+\delta)/2$, $1 = |f(\gamma(\epsilon))H^2(\gamma(\epsilon))| < r^{-2}r^2 = 1$, a contradiction.

Finally, all reduces to check that f generates m_a. But, a being isolated, if a function $l \in S(M)$ vanishes at a, then $l = fu$ where $u\colon M \to R$, maps a onto zero and coincides with l/f on $M \setminus \{a\}$.

In a forthcoming joint paper with J.M. Ruiz, we shall extend these results to a more general setting: abstract semialgebraic functions on constructible subsets of the real spectrum of excellent rings.

REFERENCES

[B–C–R] Bochnak, J.; Coste, M.; Roy, M.F. *Gèomètrie Algèbrique Rèelle*, Ergebnisse der Math. Vol. 12, Springer (1987).

[C–C] Carral, M.; Coste, M.; Normal Spectral Spaces and their Dimensions. J. Pure Appl. Algebra, **301** (1983), 227–235.

[D–K] Delfs, H.; Knebusch, M.; Semialgebraic Topology over a Real Closed Field II: Basic Theory of Semialgebraic Spaces, Math. Zeit. **178** (1981), 175–213.

Machines sur les réels et problèmes NP-complets

(d'après L. Blum, M. Shub, S. Smale et al.)

par C. Michaux

Le but de ces deux exposés est de donner un survol de l'article [BSS] de L. Blum, M. Shub et S. Smale intitulé *"On a Theory of Computation and Complexity over the Real Numbers: NP-Completeness, Recursive Functions and Universal Machines"*, en privilégiant certaines parties de l'article, qui ont déjà des prolongements chez d'autres auteurs.

Avant-Propos

Classiquement la théorie de la récursion concerne les entiers positifs ou des structures essentiellement dénombrables (par exemple les structures récursives au sens de Rabin). C'est toujours via une sous-structure dénombrable de $\mathbb{R}$ que, par exemple, M.B. Pour-El et I. Richards ou H. Friedman et K. Ko traitent de "fonctions calculables sur $\mathbb{R}$".

L'émergence depuis la fin des années septante des arbres de décision algébriques, des R.A.M. ("random access machine") en tant que modèle de calculabilité sur les réels, précédés par les U.R.M. ("unlimited register machine") sur les réels de Herman et Isard, n'a pas été suivi du développement d'une théorie analogue à la théorie classique des fonctions récursives sur $\mathbb{N}$, quoique de nombreux articles sur la complexité dans ces modèles de calculabilité aient été écrits (par exemple, Dobkin-Lipton, Steele-Yao, Ben-Or, Preparata-Shamos, ...).

Le but des auteurs de [BSS] (et peut-être particulièrement de S. Smale) est justement de développer une théorie de la calculabilité sur les réels en vue d'analyser des algorithmes courants en analyse numérique sans s'embarrasser de la représentation décimale des réels (ni de leur approximation par des rationnels), dans le sens où les U.R.M. sont un modèle de calculabilité sur $\mathbb{N}$ qui ne s'embarrasse pas de la représentation d'un entier sous forme de suites de 0,1 (voir Cutland). On peut trouver certaines de ces considérations dans S. Smale (1985).

Tous les résultats présentés ici sont extraits de [BSS] sauf mention contraire.

1. Exemples de machines sur R

Avant de donner une définition relativement précise des machines sur les réels, nous allons décrire quelques exemples informels.

Exemple 1

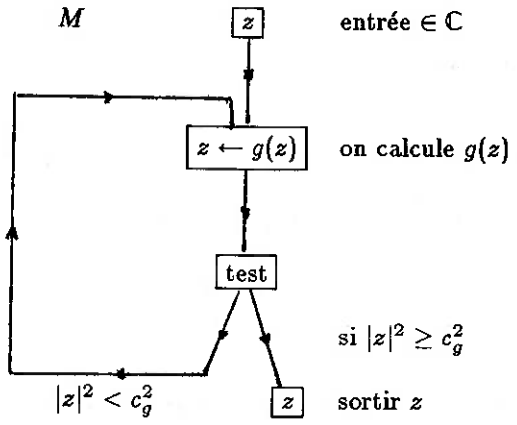
Soit $g : z \to g(z)$ de $\mathbb{C} \to \mathbb{C}$, une application polynomiale de degré ≥ 2.

Lemme 3.1. - Il existe $c_g \in \mathbf{R}$ tel que $|z| \geq c_g$ implique

$$\lim_{k \to \infty} |g^k(z)| = \infty \qquad (g^k \text{ désigne } \underbrace{g \circ \cdots \circ g}_{k \text{ fois}})$$

La preuve est classique $|g^k(z)|$ se comporte presque comme $|z^{d^k}|$ (où d est le degré de g) quand $|z|$ est suffisamment grand.

Dans ce qui suit $\mathbb{C}$ est identifié à $\mathbb{R}^2$. Considérons la machine M décrite par le diagramme suivant:



Remarquons que $|z|^2$ est une fonction polynomiale de $\mathbb{R}^2 \to \mathbb{R}^2$ (si on identifie $\mathbb{C}$ avec $\mathbb{R}^2$).

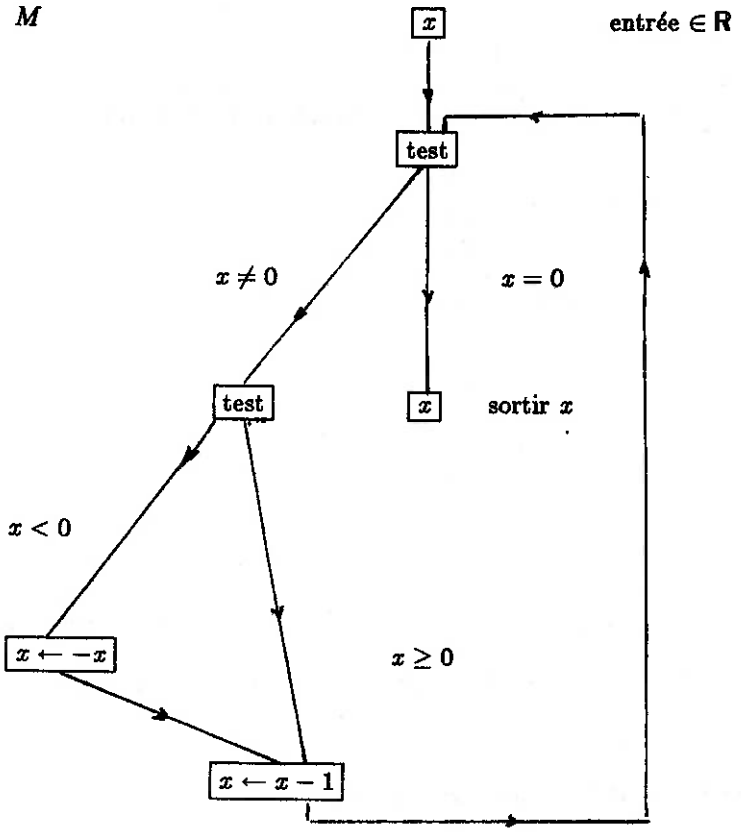
L'ensemble Ω_M des points où M s'arrête (c'est-à-dire où le calcul se termine) est exactement l'ensemble des z tels que $|g^k(z)| \to \infty$ quand $k \to \infty$.

On dira que Ω_M est récursivement énumérable sur $\mathbb{R}$.

Remarque : Ω_M est évidemment dans le cas présent non dénombrable.

Dans [BSS] section 1, on trouvera une preuve du fait que Ω_M^c (le complémentaire de Ω_M) n'est pas récursivement énumérable sur $\mathbb{R}$ lorsque $g(z) = z^2+c$ avec $|c| > 4$. Cet exemple est lié aux ensembles de Julia des endomorphismes rationnels de $\mathbb{C} \to \mathbb{C}$. Dans le cas $g(z) = z^2 + c, \Omega_M^c$ est justement l'ensemble de Julia de $z^2 + c$, $|c| > 4$.

Exemple 2



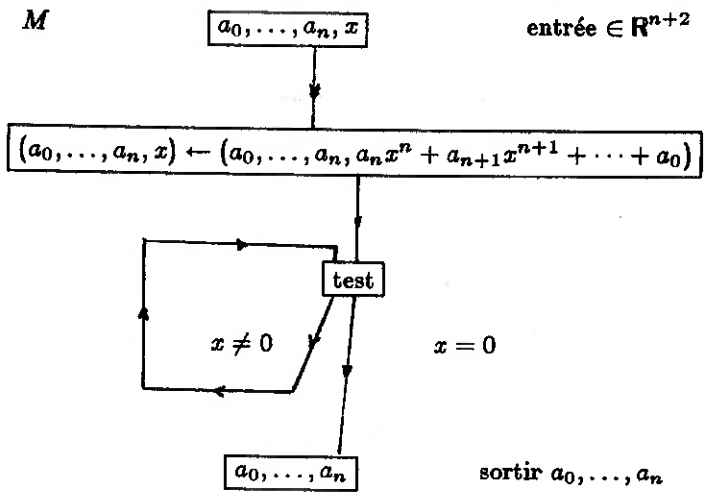
Il est clair ici que le domaine Ω_M de M est Z.

Z est donc récursivement enumérable sur R; nous laissons au lecteur le soin de montrer que R \ Z est également récursivement énumérable sur R.

On dira que Z est décidable sur R ou pour rejoindre la terminologie usuelle en calculabilité, que Z est récursif sur R.

Terminons cette introduction par un exemple qui sera repris plus tard.

Exemple 3



Clairement $\Omega_M = \{(a_0, \ldots a_n, x) | a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0\}$; l'ensemble de sortie de $M = \{(a_0, \ldots, a_n) | \exists x \in \mathbf{R} : a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0\}$

2. Machines sur un anneau ordonné R

Dans cette section, nous allons décrire brièvement les machines sur un anneau ordonné; le lecteur trouvera une définition complète dans [BSS] section 2, certaines précisions seront apportées au cours de l'exposé.

Dans le reste de l'exposé R désigne un anneau ordonné commutatif intègre avec unité; les principaux exemples sont $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$.

Approximativement, on peut dire qu'une machine sur R est semblable à une "unlimited register machine" (dénotée U.R.M., voir Cutland, ch. 1) excepté

que le contenu de chaque registre est un élément de R (au lieu d'un entier positif).

Une machine M sur R possède un nombre fini ou infini de registres (formant l'espace des états, dont la dimension est égale au nombre de registres; l'espace des états est identifié avec R^n ou $R^\infty = \oplus_{n\in\omega} R^n$ suivant les cas); chaque registre contient à tout instant un élément de R. Les instructions - appelées noeuds dans la terminologie de [BSS] - effectuées par M sont outre l'entrée de la donnée (un uple d'éléments de R, l'espace des entrées possibles sera noté $\overline{I}$ et sera du type $\overline{I} = R^n, n \leq \infty$) et la sortie du résultat (également un uple d'éléments de R, l'espace de sortie sera noté $\overline{O}$ et sera du type $\overline{O} = R^n, n \leq \infty$), les instructions de calculs (modification du contenu des registres par une application polynomiale [1] à coefficients dans R), les instructions de branchement (comparaison du contenu du premier registre avec 0) et les instructions de transfert entre registres (noeuds de "cinquième type" dans [BSS]), ces dernières étants régies par le contenu de deux registres spéciaux de M qui lors de l'instruction d'entrée sont mis à 1 et lors des instructions de calculs sont soit mis à 1, soit incrémenté de 1.

Par applications polynomiales, on entend ici une application polynomiale de R^m dans $R^n, m, n \in \mathbf{N}$ $(g = (g_1, \ldots, g_n))$ telle que le contenu x_i du registre n°i est remplacé par $g_i(x_1, \ldots, x_m)$. Ce type de noeud sera souvent représenté par

$$\boxed{x_1, \ldots, x_m \leftarrow g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m)}$$

[1] dans le cas où R est un corps, les fonctions associées aux noeuds de calcul sont les applications rationnelles à coefficients dans R

On appelera dimension d'un tel noeud de calculs, le nombre de variables qui interviennent ou sont modifiées effectivement dans g, c'est-à-dire $\max(n, m)$.
Le nombre de noeuds de M est fini, par conséquent le nombre d'applications polynomiales associées à M (et donc le nombre de leurs coefficients, appelés coefficients de M) est fini.
Une relation successeur β sur les noeuds de M détermine l'ordre de leur exécution, chaque noeud de M a un unique successeur excepté le noeud de sortie qui n'a pas de successeur et les noeuds de branchement qui ont deux successeurs, l'un exécuté quand le contenu du premier registre est inférieur à zéro, l'autre quand ce contenu est supérieur ou égal à zéro.

Remarquons que, à tout instant T d'une exécution, le contenu des registres (appelé état à l'instant T) est un uple ou une suite presque nulle c'est-à-dire seul un nombre fini de registres ont un contenu non nul.
La structrure de la machine M est souvent représentée par un graphe dirigé et étiquetté par des naturels dont les sommets sont les noeuds ou instructions, le noeud d'entrée étant étiquetté par 1 et ainsi de suite, et où les arêtes représentent la relation successeur (voir [BSS]).
Une machine fini-dimensionnelle sera une machine dont les espaces d'entrée, de sortie et des états sont fini-dimensionnels. C'était un problème ouvert dans une première version de [BSS] d'établir si toute machine M sur R dont les espaces d'entrée et de sortie sont fini-dimensionnels (c'est-à-dire $\overline{I} = R^m$ et $\overline{O} = R^n$ avec $n, m < \infty$) est équivalente à une machine M' fini-dimensionnelle sur R

(c'est-à-dire M et M' calculent la même fonction). L. Harrington et les auteurs de [BSS] donnent une réponse positive à ce problème (voir page 28 de [BSS]), on trouvera une autre preuve dans [Mi1].

La définition de machine présentée ici est en fait ce qui est appelé la forme normale dans [BSS], section 3.

De la même façon que le comportement d'un automate est décrit par sa fonction de transition, le comportement d'une machine sur R peut être décrit par une fonction de transition appelée dans [BSS], l'endomorphisme de calcul.

L'endomorphisme de calcul H_M d'une machine M est une application de $\overline{N} \times \overline{S}$ dans $\overline{N} \times \overline{S}$ où $\overline{N} = \{1, \ldots, N\}$ est l'ensemble des noeuds de M et $\overline{S}$ est l'espace d'états de M, c'est-à-dire R^n ou R^∞ suivant que le nombre de registres est n ou infini.

Le lecteur trouvera la construction explicite de H_M dans [BSS], section 3. Par conséquent, la suite des instructions exécutées par une machine M sur R avec l'entrée $\overline{x}$ ($\overline{x}$ est un n-uple ou une suite presque nulle, x_i dénotera la $i$ième composante de $\overline{x}$). est représentée par une suite $z_0, z_1, \ldots, z_k, \ldots$, où $z_k \in \overline{N} \times \overline{S}$ vérifiant

(1) [2] $z_0 = (1, \overline{x})$

(2) $H_M(z_{k-1}) = z_k$

[2]Dans le cas où l'espace d'états est infini-dimensionnel, il y a lieu d'entrer $\overline{x}$ dans les registres de façon à se ménager un espace de travail (voir [BSS]).

Ces conditions (1) et (2) nécessaires et suffisantes pour qu'une suite $z_0, \ldots, z_k, \ldots$, où $z_k \in \overline{N} \times \overline{S}$ soit une exécution sur la machine M (pour une entrée $\overline{x}$), sont appelées les équations des registres de la machine M.
Les conditions peuvent être transformées de façon à s'exprimer presqu'uniquement par des équations polynomiales à coefficients dans R (en fait les coefficients de la machine M) et dans le cas où $R = \mathbf{Z}, \mathbf{Q}$ ou $\mathbf{R}$ (1) et (2) sera équivalent à un système d'équations polynomiales (éventuellement infini).

Plus explicitement, on étend d'abord H_M à $R \times \overline{S}$ par interpolation polynomiale de façon que H_M soit une composition d'applications polynomiales et de la fonction caractéristique de l'ordre ($\chi(\overline{x}) = 1$ si $x_1 > 0, \chi(\overline{x}) = 0$ si $x_1 = 0, \chi(\overline{x}) = 1$ si $x_1 < 0$), ceci est possible sans difficulté dans le cas d'une machine n'utilisant pas d'instructions de transfert.
Dans le cas où M utilise ces dernières instructions, le résultat précédent n'est vrai que si on restreint H_M à $R \times \overline{S_k}$ où $\overline{S_k}$ est l'espace des états pour lesquels les contenus des deux registres spéciaux (pour les instructions de transfert) n'excèdent pas k.

Ce résultat permet dans le cas où tout élément positif de R est une somme bornée de carrés (par exemple dans $\mathbf{R}, \mathbf{Z}, \mathbf{Q}$) de transformer (1) et (2) en des conditions polynomiales équivalentes (moyennant l'introduction de nouvelles variables).

On trouvera des démonstrations de ces résultats dans la section 3 de [BSS].

3. Mesure de la complexité dans le modèle de calculabilité BSS

Parmi les exécutions effectuées par une machine M (toujours sur un anneau R), on va s'intéresser à celles qui après un nombre fini d'étapes atteignent le noeud de sortie de M. Plus précisément on considère les suites finies $(n_k, \overline{x_k})$ d'éléments de $\overline{N} \times \overline{S}$ qui outre les conditions (1) et (2) vérifient $n_T = N$ pour $T < \infty$ où N est l'étiquette du noeud de sortie. Si on note $\varphi_M(\overline{x})$ la fonction calculée par M, le temps nécessaire à M pour calculer $\varphi_M(\overline{x})$ sera noté $T_M(\overline{x})$ et sera égal à l'indice T tel que $n_T = N$ pour une exécution effectuée par M avec la donnée $\overline{x}$. On dit encore que la machine M s'arrête au temps T pour la donnée $\overline{x}$. L'ensemble des entrées $\overline{x}$ pour lesquelles la machine s'arrête au temps T est noté $\overline{I_T}$.

Par définition les équations de registres jusqu'à l'instant T seront les équations (1) et (2) limitées au temps T avec la condition supplémentaire $n_T = N$, c'est-à-dire

(1) $z_0 = (1, \overline{x})$

(2) $H_M(z_{k-1}) = z_k \quad k = 1, \ldots, T$

(3) $z_T = (N, \overline{x_T})$

Remarquons que les $\overline{x_k}$, $k = 1, \ldots, T$ appartiennent à $\overline{S_T}$ défini comme dans la section précédente (p. 10).

Dans le cas où M est fini-dimensionnelle, ces conditions sont équivalentes à un système (d'un nombre) fini d'équation polynomiales si ($\star$) tout élément positif de R est une somme bornée de carrés (exemple dans $\mathbb{Q}$, tout élément positif est somme de quatre carrés).

Dans le cas où M est infini-dimensionnelle, ce système n'est pas fini (notamment $\overline{x}$ est une suite infinie), il y a alors lieu de scinder en deux parties le système (1) (2) et (3), une partie (qui est finie-dimensionnelle) réellement modifiée lors des instructions effectuées par M endéans le temps T, l'autre partie inchangée par ces mêmes instructions (les applications polynomiales ne modifient qu'un nombre fixe de coordonnées de $\overline{x}$, les noeuds de cinquième type jusqu'au temps T ne modifient que les T premières composantes de $x_1, \ldots, x_T$).

La première partie du système sous l'hypothèse ($\star$) est équivalente à un système fini d'équations polynomiales (voir section 4 de [BSS]).

Etudions pendant quelques instants le cas particulier de $\mathbb{R}$.

Bien entendu dans ce cas ($\star$) est vérifiée. De plus tout système d'équations polynomiales est équivalent à un système quadratique (la façon la plus brutale de le voir est de remplacer chaque monôme x^α du système initial par une nouvelle variable t_α, d'introduire en plus une nouvelle variable t_α pour chaque variable x_i - même si x_i n'apparaît pas comme monôme dans le système initial - et d'écrire outre les équations du système initial dans ces nouvelles variables, les équations quadratiques $t_\alpha t_\beta = t_{\alpha+\beta}$ où t_β représente un x_i, qui mènent à la constitution de chaque monôme du système initial à partir des x_i, exemple: pour le monôme

X^3Y^2 on ajoutera les équations $t_{01}t_{01} = t_{02}, t_{02}t_{10} = t_{12}, t_{12}t_{10} = t_{22}, t_{22}t_{10} = t_{32}$ avec $t_{10} = X, t_{01} = Y$).

Puisque tout système quadratique est équivalent à une équation de degré au plus 4 ($f = 0$ et $g = 0 \leftrightarrow f^2 + g^2 = 0$ dans un anneau ordonné), le système (1), (2) et (3) est équivalent à une seule équation de degré au plus 4.

On obtient alors le

Théorème 3.1 [BSS] - Soit M une machine sur $\mathbf{R}$, pour tout $T \in \mathbf{N}$, il existe un polynôme $f_T : \mathbf{R}^{K_T} \times \mathbf{R}^s \to \mathbf{R}$ de degré ≥ 4 tel que la machine M s'arrête au temps T pour la donnée $\overline{y}$ si et seulement s'il existe un uple $\overline{z} \in \mathbf{R}^s$ tel que $f_T(y_1, \ldots, y_{K_T}, \overline{z}) = 0$, où K_T est le maximum de T et des dimensions des noeuds de calculs de M (voir section 2) et s peut être choisi borné par un polynôme en T (et donc le nombre de monômes de f_T est aussi borné par un polynôme en T).

De la preuve, nous dirons seulement qu'il s'agit d'un comptage attentif du nombre de monômes et de variables nécessaires dans les transformations qui mènent à f_T à partir des équations de registres (1) et (2).

■

Nous pouvons maintenant introduire les notions nécessaires pour mesurer la complexité dans le modèle BSS.

La longueur d'un élément $\overline{x} \in R^n (n \leq \infty)$ est définie comme le plus grand entier k tel que $x_k \neq 0$ où $\overline{x} = (x_1, x_2, \ldots, x_k, 0, 0, \ldots$. Nous ne définirons la hauteur (notée $h_R(x)$) de $x \in R$ que dans les cas $R = \mathbf{Z}, R = \mathbf{Q}$ ou $R = \mathbf{R}$. Si

$x \in R, R = \mathbf{Z}, h_{\mathbf{Z}}(x) = |log(x+1)|$, si $R = \mathbf{Q}$ et $x = \frac{p}{q}$ avec p et q premiers entre eux $\in \mathbf{Z}$, $h_{\mathbf{Q}}(x) = \max(h_{\mathbf{Z}}(p), h_{\mathbf{Z}}(q))$, si $x \in \mathbf{R}, h_{\mathbf{R}}(x) = 1$; la hauteur de $\overline{x} \in \mathbf{R}^n$ sera le maximum des $h_R(x_i)$ où $\overline{x} = (x_i)$.

La taille de $\overline{x} \in R^n$ est maintenant définie comme le produit de la longueur de $\overline{x}$ par la hauteur de $\overline{x}$.

La proposition suivante est évidente :

Proposition 3.1 [BSS] - Soit M une machine sur R, soit $\overline{x} \in \overline{I}$, soit $a(\overline{x})$ le nombre d'opérations arithmétiques élémentaires $(+, ., -,$ si R est un corps également $\div)$ et de 5ième noeuds utilisé pour calculer $\varphi_M(\overline{x})$ alors $a(\overline{x}) \leq kT_M(\overline{x})$, où k est une constante dépendant de M.

■

On définit la fonction de coût standard $C_M(\overline{x})$ d'une machine M pour la donnée $\overline{x}$ comme le produit de $T_M(\overline{x})$ et du maximum parmi les hauteurs des états de M pendant le calcul de $\varphi_M(\overline{x})$, explicitement:

$$C_M(\overline{x}) = T_M(\overline{x}) * \max_{0 \leq k \leq T_M(\overline{x})} h(\overline{x'_k})$$

où $H^k(1, \overline{x}) = (n_k, x_k), n_k \in \overline{N}, \overline{x_k} \in \overline{S}, x'_k$ identique à x_k sur les $K_{T_M(\overline{x})}$ premières coordonnées, 0 sur les autres.

On dit qu'une machine M sur R est dans la classe P (temps polynomial) sur R ou que φ_M la fonction calculée par M est dans la classe P sur R s'il existe des constantes $c, q \in \mathbf{N}$ telles que

$$\forall \overline{x} \in \overline{I} : C_M(\overline{x}) \leq c(\text{taille}(\overline{x}))^q$$

Dans le cas $R = \mathbf{Z}$, on retrouve la notion classique de calculable en temps polynomial.

On appelle problème de décision sur R, une paire (Y, X) où $X \subset Y \subset \overline{I} = R^n$ $(n \leq \infty)$. Un algorithme (ou machine) qui résoud le problème (Y, X) sur R est une paire (M, Y) où M est une machine dont l'espace des entrées admissibles est Y telle que $\forall \overline{y} \in Y$ $\varphi_M(\overline{y}) = 1$ ou 0 et $\varphi_M(\overline{y}) = 1$ si et seulement si $\overline{y} \in X$. (Y, X), où $Y \subset R^\infty$, est dans la classe P si et seulement si il existe un algorithme dans la classe P qui le résoud. (Y, X) , où $Y \subset R^\infty$, est dans la classe NP (temps polynomial non déterministe s'il existe $c, q \in \mathbf{N}$ et une machine M sur R dont l'espace des entrées admissibles est $Y \times R^\infty$, telle que

(i) $\varphi_M(\overline{y}, \overline{y'}) \in \{0, 1\}$;

(ii) $\varphi_M(\overline{y}, \overline{y'}) = 1$ si et seulement si $\overline{y} \in X$ et

(iii) pour tout $\overline{y} \in X$, il existe $\overline{y'} \in \overline{I'}$ tel que $\varphi_M(\overline{y}, \overline{y'}) = 1$ et $C_M(\overline{y}, \overline{y'}) \leq c(\text{taille}(\overline{y}))^q$

De nouveau si $R = \mathbf{Z}, NP$ est la notion classique sur $\mathbf{Z}$.

On notera $P_R(NP_R)$ la classe de problème de décision de classe P (de classe NP) sur l'anneau R.

On trouvera dans [BSS], un exemple de problème de classe NP, autre que celui présenté dans la section suivante de cet exposé.

Remarque : Dans le modèle de calculabilité BSS présenté ici, on peut montrer que tout problème de décision sur R est dans la classe "Linear Space", c'est un

corollaire de la preuve du résultat présenté dans [Mi1].

4. Un problème NP-complet sur $\mathbf{R}$

Adoptons la représentation suivante dans $\mathbf{R}^\infty$ pour les polynômes de degré 4 de $\mathbf{R}^n$ dans $\mathbf{R}$: f sera représenté par $(4, n)$ suivi par une suite de (α, a_α) où $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4), \alpha_i \in \{0, \ldots, n\}, \alpha_i \leq \alpha_{i+1}$ et $a_\alpha \in \mathbf{R}$, la paire (α, a_α) code le monôme $a_\alpha x_{\alpha_1} x_{\alpha_2} x_{\alpha_3} x_{\alpha_4}$, on pose $x_0 = 1$ pour permettre les monômes de degré < 4. Les (α, a_α) sont rangés selon l'ordre lexicographique sur les α.

Considérons le problème $(F_4, F_{4\,\text{zéro}})$ où F_4 est l'ensemble des polynômes de degré ≤ 4 de $\mathbf{R}^n$ dans $\mathbf{R}$ représentés comme ci-dessus et $f \in F_{4\,\text{zéro}}$ si et seulement s'il existe $\overline{x} \in \mathbf{R}^n$ tel que $f(\overline{x}) = 0$.

Proposition 4.1 [BSS] - $(F_4, F_{4\,\text{zéro}})$ est de classe NP sur $\mathbf{R}$.

Preuve - Soit $f \in F_4$, la machine M (qui prouve que $(F_4, F_{4\,\text{zéro}})$ est de classe NP) prend comme entrée admissible $(f, \overline{y'})$ et teste si $f(\overline{y'}) = 0$, ce test nécessite l'évaluation de f. Cette évaluation est réalisée en temps polynomial (par rapport à la représentation décrite ci-dessus de f).

■

Problèmes :

- Les classes $P_{\mathbf{R}}$ et $NP_{\mathbf{R}}$ sont-elles distinctes ?
- Quel est le rapport entre la question $P_{\mathbf{Z}} \neq NP_{\mathbf{Z}}$ et $P_{\mathbf{R}} \neq NP_{\mathbf{R}}$?

On dira que le problème de décision (Y, X) sur l'anneau R est NP-complet sur R s'il est de classe NP et si pour tout problème de décision (Y', X') de classe NP sur R, il existe une application $\psi : Y' \to Y$ satisfaisant les propriétés suivantes.

(i) $\psi(\overline{y}) \in X$ si et seulement si $\overline{y} \in X'$

(ii) $\psi = \varphi_M / Y'$ pour une machine M de classe P, c'est-à-dire ψ est calculable en temps polynomial.

Pour le cas $R = \mathbf{Z}$, on retrouve la définition classique du problème NP-complet.

Théorème 4.1 [BSS] - $(F_4, F_{4\,\text{zéro}})$ est NP-complet sur $\mathbf{R}$.

Preuve - Il nous reste à prouver que $(F_4, F_{4\,\text{zéro}})$ est NP-complet.

Soit M, la machine non déterministe de la définition NP pour un problème (Y, X) de classe NP sur $\mathbf{R}$. Soit $f_{\overline{y}}$ le polynôme de degré ≤ 4 obtenu par le processus suivant:

Considérons les équations de registres (1), (2) et (3) jusqu'à l'instant $T_M(\overline{y}, \overline{y'})$ pour $\overline{y} \in Y, \overline{y'} \in \mathbf{R}^\infty$ plus l'équation $x_{T_M}(\overline{y}, \overline{y'}) = 1$; ce système par une légère modification du théorème de la section 3 est équivalent à un polynôme $f_{\overline{y}}$ de degré ≤ 4.

L'application ψ requise par la définition de problème NP-complet est ici: $\psi : Y \to F_4 : \overline{y} \to f_{\overline{y}}$, le fait que ψ est calculable au temps polynomial est une conséquence du fait que la taille de $f_{\overline{y}}$ est polynomiale en temps $T_M(\overline{y}, \overline{y'})$ et que $T_M(\overline{y}, \overline{y'})$ est lui-même borné par un polynôme dépendant de la taille de $\overline{y}$

(cela découle de la définition de la classe NP).

Il est facile (en utilisant les définitions) de montrer que $y \in X$ ssi $f_{\overline{y}} \in F_{4\,\text{zéro}}$.

■

Corollaire 4.1 [BSS] - S'il existe un algorithme d'élimination des quantificateurs de classe P sur $\mathbf{R}$ pour $\exists \overline{x} f(\overline{x}) = 0, f$ de degré ≤ 4, alors $P = NP$ sur $\mathbf{R}$.

■

Contrairement au cas $R = \mathbf{Z}$ (voir [Garey-Johnson] pour le cas $R = \mathbf{Z}$), on connaît très peu de problème NP-complet sur $\mathbf{R}$.

Soit $d \geq 4$, clairement $(F_d, F_{d\,\text{zéro}})$ défini de façon analogue à $(F_4, F_{4\,\text{zéro}})$ est NP-complet puisque $F_4 \subset F_d$.

Corollaire 4.2 [BSS] - Soit F l'ensemble des représentations (définies de façon semblable au cas F_4) des systèmes polynomiaux constitué d'équations du type $X_i X_j = X_k$ et d'une équation $\sum_{i \in J} X_i = c$. Soit $F_{\text{zéro}}$, les systèmes de ce type qui ont un zéro dans $\mathbf{R}$, alors $(F, F_{\text{zéro}})$ est NP-complet.

Preuve - C'est une conséquence du théorème ci-dessus et des techniques de réduction utilisées pour obtenir $f_{\overline{y}}$.

■

Très récemment, Eberhard Triesch a montré que les problèmes $(F_2, F_{2\,\text{zéro}})$ et $(F_3, F_{3\,\text{zéro}})$ sont de classe P sur $\mathbf{R}$.

En fait, on peut facilement montrer que tout polynôme à coefficients réels de

degré impair en n variables, a toujours un zéro dans $\mathbf{R}$, donc il reste à montrer que $(F_2, F_{2\,\text{zéro}})$ est de classe P.

La preuve utilise essentiellement une réduction à un problème linéaire.

Klaus Meer a montré que le problème $(F_4, F_{4\,\text{zéro}+})$ où $F_{4\,\text{zéro}+}$ est l'ensemble des polynômes de degré ≤ 4 qui ont un zéro positif dans $\mathbf{R}$, est NP-complet sur $\mathbf{R}$.

C'est une conjecture que $(F_2, F_{2\,\text{zéro}+})$ est NP-complet ou du moins que $(F_2, F_{2\,\text{zéro}+})$ est dans $NP_{\mathbf{R}} \setminus P_{\mathbf{R}}$ sous l'hypothèse $P_{\mathbf{R}} \neq NP_{\mathbf{R}}$.

5. Un peu plus loin sur les ensembles récursivement énumérables sur un anneau ordonné

Soit M une machine sur R, rappelons que le domaine Ω_M de M est le sous-ensemble de $\overline{I}$ (l'espace d'entrée de M) sur lequel M s'arrête (c'est-à-dire $\overline{x} \in \Omega_M$ s'il existe une exécution avec la donnée $\overline{x}$ qui atteint le noeud de sortie de M après un laps de temps fini).

Comme dans le cas classique, un ensemble $X \subset R^n (n \leq \infty)$ est dit récursivement énumérable sur R (r.e. sur R) si et seulement si X est le domaine d'une machine M sur R, c'est-à-dire $X = \Omega_M$. $X \subset R^n (n \leq \infty)$ sera dit décidable (ou récursif) sur R si X et son complémentaire X^c sont r.e. sur R.

Il est clair, au vu des définitions précédentes, que Ω_M est la réunion des $\overline{I}_T$ ($\overline{I}_T$ = ensemble des éléments de Ω_M pour lesquels M s'arrête au temps T, c'est-à-dire atteint le noeud de sortie à la $T^{\text{ième}}$ étape).

Soit $\overline{x} \in \overline{I}_T$, soit la suite de calculs associée à $\overline{x}$: $z_0 = (1, \overline{x}), z_1 = (n_1, \overline{x_1}), \ldots, z_T = (N, \overline{x_T})$, la suite des noeuds $1, n_1, \ldots n_{T-1}, N$ est appelée le chemin de calcul de $\overline{x}$ dans M, il sera noté $\gamma(\overline{x})$.

Notons V_γ l'ensemble des éléments $\overline{y}$ de $\overline{I}_T$ tels que $\gamma(\overline{y}) = \gamma(\overline{x})$. On a donc $\overline{I}_T = \cup_\gamma V_\gamma$ où γ est un chemin quelconque de longueur T dans M (il y en a au plus $|N|^T$).

Théorème 5.1 [BSS] - Soit γ un chemin de longueur T

(i) V_γ est un ensemble semi-algébrique de base

(ii) $\overline{I}_T$ est un ensemble semi-algébrique

(iii) Ω_M est une réunion dénombrable d'ensembles semi-algébriques.

Preuve - (ii) et (iii) sont évidents dès que (i) est prouvé. Clairement en suivant le chemin γ à travers la machine M et notant les branches choisies à chaque noeud de branchement de γ, on voit que V_γ est défini par des inégalités du type.

$$g_{k_\ell}(\ldots(g_{k_2}(g_{k_1}(\overline{x}))]_1 < 0$$

et

$$g_{k_m}(\ldots(g_{k_2}(g_{k_1}(\overline{x}))]_1 \leq 0$$

où $]_1$ désigne la projection sur la première composante et où les g_i sont les applications polynomiales de M (ou rationnelles si R est un corps, dans ce cas on obtient ce résultat en remarquant que $\frac{p}{q} < 0$ si et seulement si $(p < 0 \wedge q > 0) \vee (p > 0 \wedge q < 0)$)

Remarquons que dans le cas où M est infini-dimensionnelle, le nombre de coordonnées intervenant dans les équations est K_T.

■

Remarquons que φ_M restreinte à V_γ (et aux K_T premières coordonnées) est une application polynomiale (rationnelle si R est un corps).

Corollaire 5.1 [BSS] - Tout sous-ensemble récursivement énumérable sur les réels a un nombre dénombrable de composantes connexes.

Preuve - C'est une conséquence triviale du théorème et du résultat bien connu qui dit que tout semi-algébrique a un nombre fini de composantes connexes [Milnor].

■

Le corollaire fournit un critère facile pour donner des exemples d'ensembles r.e. non décidables, par exemple le complémentaire de l'ensemble tryadique de Cantor est un ensemble r.e. sur $\mathbb{R}$ mais non décidable, voir [BSS].

On peut remarquer dans le théorème 5.1 que l'ensemble S des coefficients des polynômes (ou fonctions rationnelles) qui apparaissent dans la description de Ω_M comme une union dénombrable d'ensembles semi-algébriques de R, est finiment engendré, c'est-à-dire $\mathbb{Z}[S]$ est un anneau finiment engendré sur $\mathbb{Z}$ (si R est un corps, $\mathbb{Q}(S)$ est finiment engendré sur $\mathbb{Q}$). Cela découle trivialement du fait que le nombre d'applications polynomiales associées à une machine M sur R est fini, on a donc

Corollaire 5.2 - Tout ensemble r.e. sur R est une union dénombrable *finiment engendrée* d'ensembles semi-algébriques de R (où finiment engendrée est employé dans le sens décrit ci-dessus).

■

Corollaire 5.3 - Soit $X \subset R^n$ un ensemble r.e. sur un anneau ordonné R. Supposons que $t_1, \ldots, t_n$ sont algébriquement indépendants sur $\mathbf{Q}(c_1, \ldots, c_\ell)$ où $c_1, \ldots, c_\ell$ sont les coefficients d'une machine dont le domaine Ω_M est X. Si $(t_0, \ldots, t_n) \in X$, alors il existe un ouvert O (pour la topologie induite par l'ordre de R) contenant $t_1, \ldots, t_n$ tel que $O \subset X$.

La preuve est triviale et découle du corollaire 5.2.

■

Ce résultat donne un nouveau critère pour construire des ensembles r.e. non décidables.

Intéressons-nous momentanément au cas des ensembles r.e. sur $\mathbf{R}$.
Il est facile de montrer que $\mathbf{N}, \mathbf{Z}$ sont décidables sur $\mathbf{R}$, en utilisant un compteur, nous en laissant le soin au lecteur (voir l'exemple 2, section 1 et aussi [BSS]).

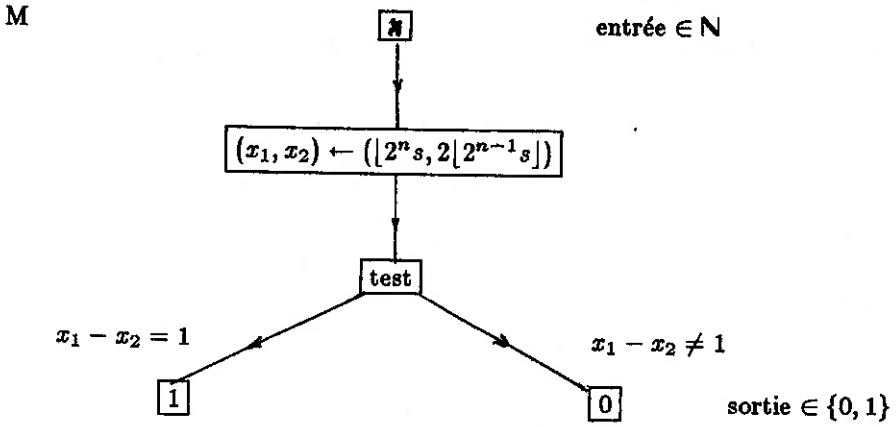
En fait, tout sous-ensemble $S \subset \mathbf{N}$ est décidable sur $\mathbf{R}$. Soit r le réel dont l'écriture binaire est

$$0.r_1.r_2 \ldots r_n \ldots$$

où

$$r_n = \begin{cases} 1 & \text{si } n \in S \\ 0 & \text{autrement} \end{cases}$$

Soit $x \in \mathbf{R}$, tout d'abord on décide si $x \in \mathbf{N}$ ou non, si $x \in \mathbf{N}$, on utilise la machine suivante.



$\lfloor u \rfloor$ denote la partie entière de u.

$x \in S$ si et seulement si la sortie est 1; s est le seul coefficient éventuellement irrationnel de la machine M.

Proposition 5.1 - ([Mi2]) Toute union dénombrable finiment engendrée d'ensembles semi-algébriques de $\mathbf{R}$ est un ensemble récursivement énumérable sur $\mathbf{R}$.

De la preuve, nous dirons simplement qu'elle est assez facile (c'est un argument de codage) dès qu'on remarque que le fait que tout sous-ensemble $S \subset \mathbf{N}$ est décidable sur $\mathbf{R}$, implique que tout sous-ensemble de $\mathbf{Z}[X_1, \ldots, X_n, \ldots]$ est

décidable sur $\mathbf{R}$ (en utilisant une représentation semblable à celle de la section 4 pour les polynômes et le fait bien connu que $\mathbf{Z}[X_1, \ldots, X_n, \ldots]$ est un anneau récursif au sens de Rabin ([Ra])).

Lors de ces exposés M. Ziegler a remarqué que tout ouvert de $\mathbf{R}$ est r.e. sur $\mathbf{R}$. Il suffit de remarquer que tout ouvert de $\mathbf{R}$ est une union dénombrable d'intervalles ouverts et que tout réel est limite d'une suite de rationnels.

Les ensembles r.e. sur un anneau R ont été défini comme les domaines des fonctions φ_M calculées par les machines M sur R. Les ensembles de sortie sont les ensembles images de ces mêmes fonctions. Dans le cas classique (sur $\mathbf{N}$ ou sur $\mathbf{Z}$), la classe des ensembles r.e. est égale à la classe des ensembles de sortie. Ce n'est pas le cas pour un anneau ordonné quelconque (voir [Mi2]), mais on a cependant le résultat suivant:

Proposition 5.2 [BSS] - Pour un corps réel clos, la classe des ensembles de sortie est égale à la classe des ensembles r.e.

Preuve - Pour tout anneau ordonné, on a clairement que la classe des ensembles r.e. est incluse à la classe des ensembles de sortie. La preuve de l'inclusion réciproque dans le cas réel clos est basée sur le fait que les corps réels clos admettent une procédure effective d'élimination des quantificateurs dans le langage $< +, ., -, <, 0, 1 >$. Plus explicitement, soit $E \subset \mathbf{R}^n (n \leq \infty)$, l'ensemble de sortie d'une machine M. Une machine M^* dont le domaine est E, exécutera la procédure suivante: soit $\overline{x}$ l'entrée, M^* dispose d'un compteur qui au départ est égal à 1, pour chaque valeur T du compteur M^* exécute la routine suivante

(excepté si M^* s'est arrêtée à l'étape $T-1$): construire les équations de registres de la machine M limitée au temps t (mise sous la forme d'un système S d'équations polynomiales - voir section 3), ces équations expriment l'existence d'une exécution de longueur T par la machine M. Via une machine (qui réalise l'algorithme de Tarski-Seidenberg par exemple voir [vdD]), M^* élimine les quantificateurs et teste s'il existe une exécution de M (c'est-à-dire une solution au système S) qui sort $\overline{x}$, si la réponse est affirmative M^* s'arrête, sinon M^* incrémente le compteur d'une unité. Il est clair que $\Omega_{M^*} = E$. Pour plus de détails, on lira [BSS].

■

Dans l'article [BSS], apparaît la question de caractériser les anneaux ordonnés commutatifs qui satisfont la propriété de la proposition 5.2 (cette propriété sera désormais notée $E = S$). On remarque aisément (par le théorème 3.1) que R satisfait la propriété $E = S$ si et seulement si R satisfait la propriété "la projection d'un ensemble r.e. est encore un ensemble r.e.". Ceci éclaire le fait que cette propriété $E = S$ est liée à l'élimination des quantificateurs.
En fait, on a le lemme suivant:

Lemme 5.1 [Mi2] - Si R satisfait $E = S$, alors l'ensemble $A_n = \{(a_0, \ldots, a_{n-1}, a_n) \in R | \exists x \in R : a_n x^n + \cdots + a_0 = 0\}$ est un ensemble r.e. sur R. De même, l'ensemble $B_n = \{(c_0, \ldots, c_{n-1}, c_n) \in R(i) | \exists x \in R(i) : c_n x^n + \cdots + c_0 = 0\}$ est un ensemble r.e. sur R (où $i^2 = -1$ et $R(i)$ est identifié avec R^2, donc $B_n \subset R^{2n+2}$).

Preuve - A_n est l'ensemble de sortie de la machine décrite par l'exemple 3 de la section 1. Il est aussi facile de montrer que B_n est l'ensemble de sortie d'une machine sur R.

■

Au vu du théorème 5.1, cela montre que la formule $\exists X(a_n X^n + \cdots + a_0 = 0)$ est équivalente dans R a une disjonction dénombrable de formules *sans quantificateurs* du langage $< +, -, ., <, 0, 1, c_{r(r \in R)} >$ mais où seulement un nombre fini de constantes additionnelles c_r apparaissent dans la disjonction dénombrable; donc si R satisfait $E = S, R$ a une élimination "faible" des quantificateurs pour les formules existentielles.

Dans le théorème qui suit, nous résumons les résultats de [Mi2].

Théorème 5.2 - Soit R un anneau ordonné commutatif intègre,

(i) si R est finiment engendré sur $\mathbf{Z}$, alors R satisfait $E = S$;

(ii) si R est un corps finiment engendré sur $\mathbb{Q}$, alors R satisfait $E = S$ (on permet d'utiliser les fonctions rationnelles dans la définition des machines sur R c'est-à-dire $^{-1}$ dans le langage, sinon ce résultat n'est plus valable, voir (i));

(iii) si R est archimédien et $tr_{\mathbb{Q}} R$ (le degré de transcendance de R sur $\mathbb{Q}$) est infini et si les ensembles B_n $n \geq 1$ (défini dans le lemme 1) sont r.e. sur R, alors R est un corps réel clos:

(iv) si R est dense dans sa clôture réelle et $tr_{\mathbb{Q}} R$ est infini, alors R satisfait $E = S$ ssi R est un corps réel clos.

De la preuve, nous dirons simplement que (i) et (ii) sont obtenus en adaptant la preuve du cas classique $R = \mathbb{Z}$, (iii) est obtenu par une preuve à la "McKenna, Macintyre, van den Dries" (voir [MMV]), (iv) est obtenu par une généralisation de (iii).

■

On peut montrer (voir [Mi2]) que si $\{r_i, i \in \omega\}$ est un ensemble dénombrable de réels algébriquement indépendants, alors $\mathbb{Z}[r_i, i \in \omega]$ ne satisfait pas $E = S$, quoiqu'il soit récursif au sens de Rabin.

Jusqu'à présent, il n'y a pas à notre connaissance de classification générale des anneaux ordonnés intègre dénombrable par rapport à la propriété $E = S$.

Macintyre a remarqué que si le prédicat de divisibilité dans un anneau R réel clos (voir [CD]) est récursif sur R, alors R satisfait $E = S$.

Dans un article [BS] très récent (non publié), L. Blum et S. Smale tentent de classer les anneaux ordonnés dont tous les ensembles définissables (dans le langage $< +, ., -, <, 0, 1 >$) sont décidables; cette hypothèse sur R est a priori plus forte que l'hypothèse $B_n, n \geq 1$ est un ensemble r.e. sur R.

Signalons enfin que dans la section 9 de [BSS], on trouvera une tentative de caractérisation des ensembles r.e. sur R en terme d'ensembles diophantiens, et dans la section 10, une démonstration du fait que les ensembles de Julia sur $\mathbb{R}$ sont presque tous indécidables sur $\mathbb{R}$.

6. Terminons ce survol de [BSS] en mentionnant l'équivalence entre fonctions calculables sur R et fonctions récursives sur R (voir section 7 de [BSS]) et l'existence d'une machine universelle sur R (section 8 de [BSS]).

References

[B] Ben-Or, M., Lower bounds for algebraic computation trees in "Proceedings 15th ACM STOC", pp. 80-86, 1983.

[BSS] Blum, L., Shub, M., Smale, S., On a theory of computation and complexity over the real numbers : NP-completeness, recursive functions and universal machines, Bull. A.M.S., 21, 1, pp. 1-46, 1989.

[BS] Blum, L., Smale, S., The Gödel incompleteness theorem and decidability over a ring, preprint, 1989.

[CD] Cherlin, G., Dickmann, M.A., Real closed rings II, Model Theory, Ann. of pure and applied Logic, 25, pp. 213-232, 1983.

[C] Cutland, N., "Computability", Cambridge Univ. Press, Cambridge, 1980.

[DL] Dobkin, D., Lipton, R., On the complexity of computations under varying set of primitives, Journal of Computer and Systems Science, 18, pp. 86-91, 1979.

[FK] Friedman, H., Ko, K., Computational complexity of real functions, Journal of Theoretical Computer Science, 20, pp. 323-352, 1982.

[GJ] Garey, M., Johnson, D., "Computers and intractability", Freeman, N.Y., 1979.

[HI] Herman, G.T., Isard, S.D., Computability over arbitrary fields, J. London Math. Soc. (2), 2, pp. 73-79, 1970.

[MMV] Mc Kenna, K., van den Dries, L., Macintyre, A., Elimination of quantifiers in algebraic structures, Adv. in Math., 47, pp. 74-87, 1983.

[M] Meer, K., Computation over $\mathbf{Z}$ and $\mathbf{R}$: a comparison, preprint n°7, Lehrstuhl C für Mathematik, RWTH Aachen, mai 1989.

[Mi1] Michaux, C., Une remarque à propos des machines sur $\mathbf{R}$ introduites par Blum, Shub et Smale, Comptes Rendus Acad. Sc., série 1, 309, 7, pp. 435-437, 1989.

[Mi2] Michaux, C., Manuscript, Communication écrite aux auteurs de [BSS], juillet 1989, à paraître.

[Mil] Milnor, J., On the Betti-numbers of real varieties, Proceedings of the A.M.S., 15, pp. 275-280, 1964.

[PR] Pour-El, M.B., Richards, I., Computability and noncomputability in classical analysis, Trans. Amer. Math. Soc., 275, pp. 539-560, 1983.

[PS] Preparata, F.P., Shamos, M.I., "Computational geometry", Springer Verlag, 1985.

[Ra] Rabin, M.O., Computable algebra, general theory and theory of computable fields, Trans. Amer. Math. Soc., 95, pp. 341-360, 1960.

[S] Smale, S., On the efficiency of algorithms of analysis, Bull. A.M.S., 13, 2, pp. 87-121, 1985.

[SY] Steele, J.M., Yao, A.C., Lower bounds of algebraic decision trees, Jour. of Algorithms, 3, pp. 1-8, 1982.

[T] Triesch, E., A note on a theorem of Blum, Shub and Smale, preprint n ° 6, Lehrstuhl C für Mathematik, RWTH Aachen, avril 1989.

[vdD] van den Dries, L., Alfred Tarski's elimination theory for real closed fields, Jour. of Symb. Logic, 53, 1, pp. 7-19, 1988.

NOYAUX DE CHAINES ET CORPS CHAINABLES.

DANIELLE GONDARD-COZETTE

Université Paris VI

INTRODUCTION

Les corps ordonnables sont de deux sortes : les corps non chaînables où toute somme de carrés est une somme de puissances quatrièmes (par exemple $\mathbb{R}$, $\mathbb{Q}$ et ses extensions algébriques ordonnables), et les corps chaînables où il existe un élément α tel que α^2 ne soit pas somme de puissances quatrièmes ; dans ce cas nous dirons que K est un *corps α-chaînable* (par exemple $\mathbb{Q}(X)$ et $\mathbb{R}((X))$ sont des corps X-chaînables) .

La nécessité de faire intervenir une constante α a été mise en évidence par les axiomatisations des théories des corps chaînables et des corps chaîne-clos que nous avons données dans [G1] . Ce point de vue a ensuite permis d'obtenir des résultats du type 17ème problème de Hilbert dans [D-G] et de créer un analogue à l'algèbre réelle dans [B-G] ou [B-G2], et nous le conservons ici pour poursuivre l'étude des corps chaînables.

Le plan de cette étude est le suivant :

I-Noyaux de chaînes ;

II-Corps uniquement α-chaînables ;

III-Une autre extension du 17ème problème de Hilbert au niveau n ;

IV-Corps bien chaînables ;

V-Corps simplement chaînables ;

VI-Corps totalement chaînables ;

VII-Extensions de chaînes .

I-NOYAUX DES CHAINES D'UN CORPS CHAINABLE *(Kernels of chains).*

Définition I-1 : Un corps K sera dit α-chaînable s'il existe dans K un élément α tel que α^2 ne soit pas somme de puissances quatrièmes d'éléments de K .

Définition I-2 : Un préordre T de niveau 2^n (i.e. $T + T \subseteq T$, $T \cdot T \subseteq T$, $K^{2^n} \subseteq T$) sera dit un α-péordre si $\alpha^{2^{n-1}} \notin T$ (il est alors de niveau exact 2^n car $\sum K^{2^{n-1}}$ n'est pas contenu dans T). De même un ordre P de niveau exact 2^n sera dit un α-ordre si $\alpha^{2^{n-1}} \notin P$.

Definition I-3 : Nous appelerons α-chaîne une chaîne d'ordres de niveau supérieur $(P_i)_{i\in\mathbb{N}}$ telle que $\alpha^2 \notin P_2$.

Proposition I-4 : Un corps K est α-chaînable si et seulement s'il existe au moins une α-chaîne.

Ceci résulte des définitions I-1 et I-3 et du résultat de Becker-Harman qui donne l'expression suivantes des sommes de puissances :
$\sum K^4 = (\bigcap_i P_{i2}) \cap \sum K^2$ où P_{i2} désigne un ordre de niveau exact 4 quelconque de K . Donc si α^2 n'est pas une somme de puissances quatrièmes dans K , il existe au moins un j tel que $\alpha^2 \notin P_{j2}$. D'après le corollaire I-4 de [H] il existe au moins une chaîne d'ordres de niveau supérieur passant par ce P_{j2} .

Proposition I-5 : Dans un corps K α-chaînable tout ordre P_n de niveau exact 2^n d'une α-chaîne $(P_i)_{i\in\mathbb{N}}$ est un α-ordre.

En effet si $\alpha^{2^{n-1}} \notin P_n$, alors P_n est bien un α-ordre. Si $\alpha^{2^{n-1}} \in P_n$ P_n étant de α-chaîne $\alpha^2 \notin P_2$, on en déduit qu'il existe $i \geq 2$ tel que $\alpha^{2^{i-1}} \notin P_i$ et $\alpha^{2^i} \in P_{i+1}$, puisque d'après la relation de chaîne dès que α^{2^p} est dans un P_i on a $\alpha^{2^{p+q}}$ qui est dans P_{i+q} pour tout $q \geq 1$; reprenons le début de la preuve du théorème 2 p.5 de [Bel] pour montrer que si $a \in K^*$ alors a^2 appartient à un ordre P de niveau exact 2^n entraîne que $a \in P \cup -P$: en effet si $a \notin P$ alors $P + Pa$ est un préordre propre contenant strictement P et donc $P + Pa = K$, d'où $-1 = u + va$ avec u et v dans P et enfin $a \in -P$. On déduit de ce résultat que $\alpha^{2^i} \in P_{i+1}$ entraine que $\alpha^{2^{i-1}} \in P_{i+1} \cup -P_{i+1}$, puis par la relation de chaîne $P_{i+1} \cup -P_{i+1} = (P_0 \cap P_i) \cup -(P_0 \cap P_i)$ que $\alpha^{2^{i-1}} \in P_i$ ce qui est contraire à l'hypothèse.

Lemme I-6 : Soit K un corps α-chaînable.

Pour tout $n \in \mathbb{N}^*$, $T_n = \sum K^{2^n} - \alpha^{2^{n-1}} \sum K^{2^n}$ est un α-préordre propre (i.e. $-1 \notin T_n$) de niveau exact 2^n.

C'est tout à fait clair pour $n = 1$ et $n = 2$; pour $n \geq 3$ K étant α-chaînable $\alpha^2 \notin \sum K^4$ et par la proposition I-4 il existe une α-chaîne $(P_i)_{i \in \mathbb{N}}$; par I-5 tout P_n de α-chaîne est un α-ordre donc $\alpha^{2^{n-1}} \notin P_n$ et la relation de chaîne jointe au fait que P_{n-1} contient toutes les puissances 2^{n-1}-èmes montre que $-\alpha^{2^{n-1}} \in P_n$; P_n contenant toutes les puissances 2^n-èmes d'éléments de K contient donc T_n. T_n est clairement un préordre de niveau 2^n, et le niveau est exactement 2^n car $\alpha^{2^{n-1}}$ n'appartenant pas à P_n ne peut donc pas appartenir à T_n ; de même -1 ne peut appartenir à T_n qui est donc propre.

corollaire I-7 : Dans un corps α-chaînable pour toute α-chaîne $(P_i)_{i\in\mathbb{N}}$ on a $T_k = \sum K^{2^k} - \alpha^{2^{k-1}} \sum K^{2^k} \subseteq P_k$, pour tout $k \geq 2$.

C'est clair d'après la preuve du lemme I-6.

Proposition I-8 : Dans un corps K α-chaînable, tout P_n, ordre de niveau exact 2^n qui contient $T_n = \sum K^{2^n} - \alpha^{2^{n-1}} \sum K^{2^n}$ est un P_n de α-chaîne.

En effet seulement l'un des deux éléments $\alpha^{2^{n-1}}$ ou $-\alpha^{2^{n-1}}$ appartient à P_n. Donc $\alpha^{2^{n-1}} \notin P_n$ et on en déduit que toute chaîne passant par P_n est une α-chaîne puisque si $\alpha^2 \in P_2$, en utilisant la condition de chaîne (qui s'exprime au niveau 3 par : $P_3 \cup -P_3 = (P_2 \cap P_0) \cup -(P_2 \cap P_0)$) on obtiendrait $\alpha^2 \in P_3 \cup -P_3$ d'où $\alpha^4 \in P_3$; on déduirait en itérant que $\alpha^{2^{n-1}} \in P_{n-1}$ ce qui est impossible.

Toute chaîne $(P_i)_{i\in\mathbb{N}}$ passant par P_n est donc une α-chaîne.

Proposition I-9 : Dans un corps α-chaînable T_n est égal à l'intersection de tous les α-ordres de niveau exact 2^n (qui appartiennent à au moins une α-chaîne).

D'après le théorème 1 de Becker [Be1], un préordre propre de niveau 2^n est égal à l'intersection de tous les ordres de même niveau, exact ou non, qui le contiennent ; un ordre qui contient T_n est un α-ordre car $-\alpha^{2^{n-1}} \in T_n \subseteq P_n$ ce qui entraîne que $\alpha^{2^{n-1}} \notin P_n$; enfin P_n est bien de niveau exact 2^n puisque $\sum K^{2^{n-1}}$ n'est pas contenu dans P_n.

Corollaire I-10 : Dans un corps K α-chaînable , T_n est égal à l'intersection des P_n , ordres de niveau exact 2^n des α-chaînes.

Cela résulte immédiatement de I-7, I-8 et I-9.

Remarque I-11 : Dans un corps K α-chaînable $T'_n = \sum K^{2^n} + \alpha^{2^{n-1}} \sum K^{2^n}$ est toujours un préordre propre de niveau 2^n mais il n'est pas forcément de niveau exact 2^n .

Définition I-12 : Appelons , pour $n \geq 2$, T_n noyau au niveau n des α-chaînes.

II-CORPS UNIQUEMENT α-CHAINABLES *(uniquely α-chainable fields).*

Definition II-1 : Un corps α-chainable qui n'admet qu'une seule α-chaîne $(P_i)_{i\in\mathbb{N}}$, à échange de P_0 et P_1 près, sera dit uniquement α-chaînable.

Proposition II-2 : si un corps K α-chaînable n'admet qu'une seule α-chaîne $(P_i)_{i\in\mathbb{N}}$, à échange de P_0 et P_1 près, alors l'ordre de niveau exact 2^n de celle-ci est pour tout $n \geq 2$, $P_n = T_n = \sum K^{2^n} - \alpha^{2^{n-1}} \sum K^{2^n}$.

En effet par le corollaire I-7 toute α-chaîne $(Q_i)_{i\in\mathbb{N}}$ est telle que $Q_n \supseteq T_n$ pour tout $n \geq 2$, d'après l'hypothèse faite que K n'admet qu'une seule α-chaîne le corollaire I-10 donne alors $P_n = T_n$.

Definition II-3 : nous appelerons coeur au niveau n de α-chaînes *(heart of level n of α-chains)* relativement au fan trivial $P_0 \cap P_1$: $C_n = \sum (P_0 \cap P_1)^{2^{n-1}} - \alpha^{2^{n-1}} \sum (P_0 \cap P_1)^{2^{n-1}}$ où $n \geq 2$.

Proposition II-4 : Soit K α-chaînable et P_0 , P_1 des ordres qui soient le début d'une α-chaîne $(P_i)_{i\in\mathbb{N}}$;
pour $n \geq 2$, C_n est égal à l'intersection de tous les α-ordres P_n le contenant ; de tels P_n sont alors de niveau exact 2^n et sont de α-chaîne .

La démonstration est analogue à celle de I-10 dès que l'on a montré que C_n est un préordre propre de niveau exact 2^n . Si $(P_i)_{i\in\mathbb{N}}$ est une

α-chaîne commençant par $P_0 \cap P_1$ alors $(P_0 \cap P_1)^{2^{n-1}} \subseteq P_n$: c'est vrai pour $n = 2$ d'après la relation $P_2 \cup -P_2 = (P_0 \cap P_1) \cup -(P_0 \cap P_1)$, et par récurrence si $(P_0 \cap P_1)^{2^{n-1}} \subseteq P_n$ alors par la relation de chaîne, au niveau $n+1$, $P_{n+1} \cup -P_{n+1} = (P_0 \cap P_n) \cup -(P_0 \cap P_n)$ on déduit que $(P_0 \cap P_1)^{2^n}$ est contenu dans P_{n+1}. P_n étant de α-chaîne $\alpha^{2^{n-1}} \notin P_n$ et $-\alpha^{2^{n-1}} \in P_n$ donc on a $C_n \subseteq P_n$. On en déduit que C_n, qui est clairement un préordre de niveau au plus 2^n, est un préordre propre de niveau exact 2^n. Il est donc égal à l'intersection de tous les ordres P qui le contiennent, ceux-ci sont de niveau au plus 2^n car si le niveau était supérieur on aurait $\sum K^{2^n}$ non contenu dans P ce qui est impossible puisque $\sum (P_0 \cap P_1)^{2^{n-1}} \supseteq \sum K^{2^n}$. Le niveau est évidemment au moins 2^n puisque $\sum K^{2^{n-1}}$ n'est pas contenu dans P qui contenant C_n ne peut contenir $\alpha^{2^{n-1}}$. Etant de niveau exact 2^n et tels que $-\alpha^{2^{n-1}} \in P_n$, ces ordres P contenant C_n sont des ordres de niveau exact 2^n de α-chaînes.

Proposition II-5 : Si K a une seule α-chaîne $(P_i)_{i \in \mathbb{N}}$, à échange de P_0 et P_1 près, alors pour tout $n \geq 2$ $P_n = C_n = T_n$.

Preuve analogue à celle de II-1 .

Remarque II-6 : Dans K α-chaînable si $\sum K^{2^n}$ est un fan alors $T_n = \sum K^{2^n} \cup \alpha^{2^{n-1}} \sum K^{2^n}$; de même si $\sum (P_0 \cap P_1)^{2^{n-1}}$ est un fan, $C_n = \sum (P_0 \cap P_1)^{2^{n-1}} \cup \alpha^{2^{n-1}} \sum (P_0 \cap P_1)^{2^{n-1}}$.

Corollaire II-7 : Pour qu'un corps α-chaînable admette une seule α-chaîne, à échange des deux premiers ordres près, il faut qu'il existe deux ordres P_0 et P_1 tels que pour tout $n \geq 2$ $C_n = T_n$.

Le corollaire II-7 résulte de II-5.

Corollaire II-8 : Dans K α-chaînable sont équivalentes :

(i) K est uniquement α-chaînable .

(ii) K admet deux ordres vrais P_0 et P_1 , et deux seulement, tels que pour tout $n \geq 2$ $C_n = \sum (P_0 \cap P_1)^{2^{n-1}} - \alpha^{2^{n-1}} \sum (P_0 \cap P_1)^{2^{n-1}}$ soit un ordre de niveau exact 2^n .

(iii) pour tout $n \geq 2$ $T_n = \sum K^{2^{n-1}} - \alpha^{2^{n-1}} \sum K^{2^{n-1}}$ est un ordre de niveau exact 2^n .

Preuve immédiate en utilisant ce qui précède.

On peut remarquer qu'on obtient une partie du résultat du corollaire 2 p. 43 de [Bel] si K est chaînable et a exactement deux ordres car alors $\sum K^2 = (P_0 \cap P_1)$ est un fan.

Dans certains cas, dont évidemment K simplement chaînable (c.f. la partie V) , les conditions de II-8 pour $n = 2$ suffisent.

III-UNE AUTRE GENERALISATION DU 17ème PROBLEME DE HILBERT AU NIVEAU n.

Théorème III-1 : Soit K un corps chaîne-clos α-chaînable n'admettant qu'une seule valuation hensélienne à corps des restes réel-clos, et soit $f \in K(X_1, \ldots, X_p) = K(\overline{X})$; alors les propriétés suivantes sont équivalentes pour $n \geq 2$:

(i) $f \in \sum K(\overline{X})^{2^n} - \alpha^{2^{n-1}} \sum K(\overline{X})^{2^n}$;

(ii) $\forall \overline{x} \in K^n$ où f est définie $f(\overline{x}) \in P_n$, où P_n désigne l'unique ordre de niveau exact 2^n de K .

La preuve utilise le corollaire I-10 du présent article et le lemme obtenu avec Delon dans [D-G] suivant :

Lemme III-2 [D-G] : Soient K et L deux corps chaîne-clos tels que $K \subseteq L$ et K n'admet qu'une seule valuation hensélienne à corps des restes réel-clos ; alors sont équivalents :

(i) $K \cap L^2 = K^2$;

(ii) K est relativement algébriquement clos dans L .

(iii) $K \prec L$ (où "$\prec$" est une inclusion élémentaire).

De l'expression d'un corps chaîne clos α-chaînable sous la forme $K = K^2 \cup -K^2 \cup \alpha K^2 \cup -\alpha K^2$ et du lemme précédent il résulte si K n'a qu'une seule valuation hensélienne à corps des restes réel-clos et est contenu dans un autre corps chaîne-clos α-chaînable L , alors on a $K \prec L$.

Preuve de III-1.

Il suffit de montrer le théorème pour $f \in K[\overline{X}]$ car si $f = g / h$ alors $f = gh^{2^n-1} / h^{2^n}$ et l'on sait que d'une part $\sum K^{2^n} \subseteq P_n$ et que d'autre part

$T_n(K(\overline{X})) = \sum K(\overline{X})^{2^n} - \alpha^{2^{n-1}} \sum K(\overline{X})^{2^n}$ est un préordre (voir & 1) .

Pour prouver (i) ⇒ (ii) il suffit de vérifier que si f , appartenant à $\sum K(\overline{X})^{2^n} - \alpha^{2^{n-1}} \sum K(\overline{X})^{2^n}$, est définie en x , alors $f(x)$ appartient à $\sum K^{2^n} - \alpha^{2^{n-1}} \sum K^{2^n}$. En effet dans un corps chaîne-clos α-chaînable K l'unique ordre de niveau exact 2^n est donné par les expressions suivantes : $P_n = \sum K^{2^n} - \alpha^{2^{n-1}} \sum K^{2^n} = K^{2^n} \cup - \alpha^{2^{n-1}} K^{2^n}$; la première forme résulte du fait qu'un corps chaîne-clos α-chaînable est uniquement α-chaînable et du théorème II-2 , et la seconde vient de l'expression des ordres de niveau supérieur d'un corps n'admettant que deux ordres usuels donnée par Becker dans [B1].

La preuve du fait que si f , appartenant à $\sum K(\overline{X})^{2^n} - \alpha^{2^{n-1}} \sum K(\overline{X})^{2^n}$, est définie en x , alors $f(x)$ appartient à $\sum K^{2^n} - \alpha^{2^{n-1}} \sum K^{2^n}$ est due à Becker et nous le remercions de nous autoriser à la reproduire ici :

Notons $f \in \sum K(\overline{X})^{2^n} - \alpha^{2^{n-1}} \sum K(\overline{X})^{2^n}$ sous la forme $f = \sum r_i^{2^n} - \alpha^{2^{n-1}} \sum s_j^{2^n}$ où les r_i , $s_j \in K(\overline{X})$; soient $x = (x_1, \ldots, x_p) \in K^p$, $\mathcal{O}_x$ le localisé en x $K[\overline{X}]_{(X_1 - x_1, \ldots, X_p - x_p)}$ et soient $\lambda : K(\overline{X}) \longrightarrow K$ la place définie par $X \longmapsto x_i$ et V_λ l'anneau correspondant ; alors si f est définie en x , $f \in \mathcal{O}_x \subseteq V_\lambda$. Il suffit de montrer que r_i , $s_j \in V_\lambda$ d'où l'on déduit $\lambda(f) = f(x_1, \ldots, x_p) = \sum \lambda(r_i)^{2^n} - \alpha^{2^{n-1}} \sum \lambda(s_j)^{2^n} \in P_n$.

Soit par exemple r_1 tel que $v(r_1) = \min \{ v(r_i) , v(s_j) \}$, si $r_1 \notin V_\lambda$, alors on a $f = r_1^{2^n} [1 + \sum (r_i/r_1)^{2^n} - \alpha^{2^{n-1}} \sum (s_j/r_1)^{2^n}]$; on sait que $f \in V_\lambda$ et le crochet , noté z dans la suite , dans l'expression ci-dessus est une unité ce qui donne une contradiction ; en effet si z n'était pas une unité alors dans le corps résiduel $V_\lambda / m_\lambda = K$ on aurait, puisque les r_i / r_1 et s_j / r_1 appartiennent à V_λ :

$\lambda(z) = 1 + \sum y_i^{2^n} - \alpha^{2^{n-1}} \sum y_j'^{2^n} = 0$ ce qui est impossible puisque $-1 \notin P_n$.

L'autre cas où l'on a par exemple s_1 défini par :

$v(s_1) = \min \{ v(r_1) , v(s_j) \}$ se traite bien sûr de manière analogue.

(ii) $\Rightarrow$ (i) . On considère la théorie des corps chaîne-clos α-chaînables et on utilise le langage des anneaux augmenté d'un symbole de constante α . Dans le corps K chaîne-clos α-chaînable l'hypothèse (ii) se traduit, en notant f par P / Q avec $P , Q \in K[\overline{X}]$, par la formule suivante :
" $\forall \overline{x} \; \exists y \; \exists z \; (Q(\overline{x}) = 0 \; \vee \; f(\overline{x}) = y^{2^n} \; \vee \; f(\overline{x}) = - \alpha^{2^{n-1}} z^{2^n})$ " ; dans $K(\overline{X})$ qui est α-chaînable on fixe une α-chaîne $(P_i)_{i \in \mathbb{N}}$ et on considère L la clôture chaîne de $K(\overline{X})$ pour cette chaîne . D'après le lemme III-2 et l'hypothèse faite sur K on a $K \{ L$, donc dans L la même formule
" $\forall \overline{x} \; \exists y \; \exists z \; (Q(\overline{x}) = 0 \; \vee \; f(\overline{x}) = y^{2^n} \; \vee \; f(\overline{x}) = - \alpha^{2^{n-1}} z^{2^n})$ " est satisfaite ; on choisit alors $\overline{x} = \overline{X}$ dans L et on obtient que f appartient à l'unique ordre de niveau exact 2^n de L ; cet ordre prolongeant l'ordre P_n de niveau 2^n de l' α-chaîne choisie sur $K(\overline{X})$, nous avons aussi que f appartient à P_n . Ce raisonnement est faisable pour toutes les α-chaîne de $K(\overline{X})$, par conséquent f appartient à l'intersection de tous les ordres de niveau exact 2^n des α-chaînes de $K(\overline{X})$ dont on sait par le corollaire I-10 qu'elle est égale à $\sum K(\overline{X})^{2^n} - \alpha^{2^{n-1}} \sum K(\overline{X})^{2^n}$.

IV-CORPS BIEN CHAINABLES *(fair chainable fields).*

Revenant maintenant à l'étude des corps chaînables et plus précisément à celle des corps α-chaînables, il nous apparait indispensable de distinguer deux cas et de poser quelques définitions.

Il est clair, le carré d'une somme de carrés étant une somme de puissances quatrièmes d'après [Bel], que si α^2 n'est pas une somme de puissances quatrièmes alors α n'appartient pas à $\pm \sum K^2$. Par contre la réciproque n'est pas vraie dans tout corps chaînable.

Définition IV-1 : Un corps tel que pour tout α dans K le fait que α n'appartient pas à $\pm \sum K^2$ entraîne que α^2 n'est pas une somme de puissances quatrièmes sera dit *bien chaînable.*

Harman dans [H] a étudié le problème de la réciproque de la propriété " $a \in \pm \sum K^2 \Rightarrow a^2 \in \sum K^4$ ". Si on désigne par (*) cette propriété réciproque, Harman a montré que (*) était équivalent à la connexité de l'espace $M(K)$ des $\mathbb{R}$-places de K (muni de la topologie définie comme étant la plus grossière rendant continues les applications de $M(K)$ dans $\mathbb{R} \cup \{\infty\}$, le compactifié de $\mathbb{R}$, qui pour chaque $a \in K$ sont définies par $\lambda \longmapsto \lambda(a)$).

Il a également montré que pour un corps ordonnable K, K pythagoricien et a la propriété (*) était équivalent à K pythagoricien au niveau 4 ou encore à K pythagoricien à tout niveau 2^n. Becker a lui démontré que $(\sum K^2)^2 = \sum K^4$ entrainait $M(K)$ connexe et que la réciproque était vraie dans le cas où K était pythagoricien.

Dans un tel corps Harman a pu montrer dans [H] le lemme suivant :

Lemme IV-2 [H] : Soit K un corps bien chaînable ; si une puissance 2^m d'un élément a est une somme de puissances 2^n-èmes dans le corps (avec $n > m$) alors a est égal ou opposé à une somme de puissances 2^{n-m}-èmes.

Cela entraîne le corollaire suivant :.

corollaire IV-3 : Dans un corps bien chaînable si $\alpha \notin \pm \sum K^2$ alors pour tout $n > 1$ on a $\alpha^{2^{n-1}} \notin \sum K^{2^n}$.

Du travail de Harman on peut déduire des exemples de corps bien chaînables : $\mathbb{Q}(X)$, $\mathbb{Q}(X,Y)$, $\mathbb{Q}((t))$, $\mathbb{Q}((t_1))((t_2))$, $\mathbb{R}(X_1,\ldots,X_n)$, $\mathbb{R}((t))$, ..., et bien sûr les corps chaîne-clos ou plus généralement d'après [G3] les corps de Rolle admettant au moins deux ordres usuels ; Harman a en fait montré que K bien chaînable entraîne $K(X)$ et $K((t))$ bien chaînables .

Une partie de l'intérêt de la notion de bien chaînable apparaitra dans certains des paragraphes qui suivent.

V-CORPS SIMPLEMENT CHAINABLES *(clearly chainable fields).*

Définition V-1 : un corps K tel que par tout ordre de niveau exact supérieur ou égal à 4 il ne passe qu'une seule chaine $(P_i)_{i\in\mathbb{N}}$, à échange de P_0 et P_1 près , sera dit simplement chaînable.

Un corps chaînable qui n'admet qu'une seule chaîne, comme les corps chaîne clos ou $\mathbb{R}((X))$ par exemple, est évidemment simplement chaînable.

Proposition V-2 : Un corps chaînable K est simplement chaînable si et seulement si pour toute valuation réelle sur K de groupe des valeurs β , β satisfait $| \beta / \beta^2 | \leq 2$.

La démonstration est un corollaire immédiat des deux lemmes suivants :

Lemme V-3 : ([Bl] ou [L] page 135)

Pour tout ordre de niveau supérieur P , (K,P) a une seule clôture réelle géneralisée, à K-isomorphisme près, si et seulement si pour toute valuation réelle de groupe des valeurs Γ on a : $| \Gamma / \Gamma^2 | \leq 2$.

Lemme V-4 : ([H] corollary 4-9)

Soit K un corps et P un ordre de niveau supérieur de K . Deux clôtures réelles généralisées de (K,P) sont K-isomorphes si et seulement si elles déterminent la même chaîne $(P_i)_{i\in\mathbb{N}}$, à échange de P_0 et P_1 près , de K .

Preuve de V-2 :

$\Rightarrow$ clairement par V-3 un ordre P a une seule clôture réelle généralisée et donc, en utilisant V-4 , P n'appartient qu'à une seule chaîne.

$\Leftarrow$ si on suppose qu'il existe une valuation réelle de groupe des valeurs β qui ne satisfasse pas la condition $| \beta / \beta^2 | \leq 2$, alors par V-3 il existe un ordre de niveau supérieur P de K tel que (K , P) n'a pas une clôture réelle généralisée unique ; par V-4 on conclut que par ce P il passe au moins deux chaînes distinctes.

Corollaire V-5 : Les corps de Pasch sont des corps simplement chaînables.

On rappelle qu'un corps ordonnable est de Pasch si et seulement si on a :

(1) pour toute valuation réelle de groupe des valeurs β , β satisfait $| \beta / \beta^2 | \leq 2$;

(2) si pour une valuation réelle de groupe des valeurs β on a $| \beta / \beta^2 | = 2$, alors le corps résiduel correspondant n'admet qu'un seul ordre .

Un exemple est donné par $\mathbb{R}(X)$ qui est un corps de Pasch, $\mathbb{Q}(x)$ lui n'est pas de Pasch, mais ces deux corps sont simplement chaînables.

Le corollaire V-5 résulte alors immédiatement de V-2.

Dans [G3] on trouvera un exemple de corps non simplement chaînable : tout corps de Rolle admettant au moins quatre ordres n'est pas simplement chaînable On en déduit que bien chaînable n'entraîne pas simplement chaînable.

Remarque V-6 : D'après [Bel] ou [L] , si (K , P) a plus d'une clôture réelle généralisée alors il en a une infinité. On en déduit que si dans K non simplement chaînable, en tout ordre de niveau supérieur P où il y a croisement de chaînes il se croise en fait une infinité de chaînes.

Conjecture V-7 : Un corps simplement chaînable est bien chaînable.

VI-CORPS TOTALEMENT CHAINABLES *(totally chainable fields).*

Dans [D-G], écrit avec F. Delon, nous avons donné un corollaire du théorème principal valable dans certains des corps dont tous les ordres vrais sont chaînables, c'est à dire sont le début d'une chaîne ; il conviendrait donc d'essayer de caractériser ces corps.

Définition VI-1 : nous appelerons corps totalement chaînables un corps tel que tout ordre est le début d'une chaîne, et corps complètement totalement chainable un corps tel que toute paire d'ordres est le début d'une chaîne.

Des exemples de corps complètement totalement chaînables sont donnés par $\mathbb{R}((X))$ et les corps chaîne-clos ; de [Di2] on déduit que $\mathbb{R}(X)$ est totalement chaînable, alors que $\mathbb{Q}(X)$ ne l'est pas .

Dans [G3] nous avons démontré que les corps de Rolle chaînables, c'est à dire ayant au moins deux ordres, étaient des corps complètement totalement chaînables.

Théorème VI-2 : Un corps K complètement totalement chaînable est bien chaînable.

Preuve de VI-2.

Supposons que K ne soit pas bien chaînable ; alors il existe $\beta \notin \pm \sum K^2$ tel que $\beta^2 \in \sum K^4$; il existe donc deux ordres P_0 et P_1 tels que l'on ait $\beta \in P_0 \cap -P_1$ et K n'admet pas de β-chaîne. S'il existait une α-chaîne de début (P_0,P_1) on aurait $\alpha \in P_0 \cap -P_1$ d'où on déduirait $\alpha\beta \in P_0 \cap P_1$;

on obtiendrait alors ([H] 3-11) que l' α-chaîne considérée s'étend à l'extension algébrique non triviale de K suivante : $L = K(\sqrt{\alpha\beta})$; dans L on aurait alors $\alpha^2 = (\sqrt{\alpha\beta})^4 \ / \ \beta^2 \in \sum L^4$ et donc α^2 appartiendrait à l'extension de l'ordre de niveau exact 4 de l' α-chaîne, ce qui est impossible.

Remarque : $\mathbb{Q}(X)$ est bien chaînable et pourtant d'après [Di2] ce corps n'est pas totalement chaînable.

VII-EXTENSIONS DE CHAINES *(extensions of chains).*

Nous avons montré dans [G3] que les corps de Rolle étaient tels que pour toute extension algébrique L de K il existait une chaîne de K qui ne s'étendait pas fidèlement à L. En fait la preuve n'utilise pas toutes les conditions pour qu'un corps soit de Rolle et on a donc le résultat suivant :

Théorème VII-1 : Un corps chaînable K tel que K est pythagoricien au niveau 4 et K n'admet pas d'extension algébrique de degré impair vérifie que pour toute extension algébrique L de K il existe une chaîne de K qui ne s'étend pas fidèlement à L.

Preuve de VII-1.

K n'admet pas d'extension algébrique de degré impair entraîne que toute extension algébrique ordonnable de K contient une extension quadratique $K(\sqrt{\alpha})$ avec $\alpha \notin \pm \sum K^2$.

K pythagoricien au niveau 4 entraîne K bien chaînable donc $\alpha^2 \notin K^4$.

K est donc α-chaînable.

Si une α-chaîne s'étendait à $K(\sqrt{\alpha})$ fidèlement on aurait :

$\alpha^2 \in \sum (K(\sqrt{\alpha}))^4 \subseteq \overline{P}_2$ d'où $\alpha^2 \in P_2$ ce qui est impossible.

On peut alors se poser le problème de la réciproque et essayer d'obtenir pour les chaînes un résultat analogue à la caractérisation des corps réels K tels que pour toute extension algébrique L de K il existe un ordre de K qui ne s'étend pas à L : " K est pythagoricien et K n'admet pas d'extension algébrique de degré impair " (c.f. [R]).

Théorème VII-2 : Soit K un corps totalement chaînable. Alors K pythagoricien et K n'admet pas d'extension algébrique de degré impair entraîne que pour toute extension algébrique L de K il existe une chaîne de K qui ne s'étend pas à L .

C'est clair en utilisant le résultat de [R] cité ci-dessus, car dès qu'il existe un ordre qui ne s'étend pas il existe une chaîne qui ne s'étend pas fidèlement.

Conjecture VII-3 : un corps chaînable K est tel que pour toute extension algébrique L de K il existe une chaîne de K qui ne s'étend pas fidèlement à K si et seulement si K est pythagoricien au niveau 4 et n'admet pas d'extension algébrique de degré impair.

Lemme VI-4 : [Bel] Pour toute extension L de K contenue dans la clôture pythagoricienne de K un ordre de niveau supérieur s'étend fidèlement à L .

Lemme VI-5 : [Bel] Pour toute extension algébrique de degré impair L de K un ordre de niveau supérieur s'étend fidèlement à L .

Un sens résulte de VI-1.
Pour l'autre, le lemme VI-4 de Becker entraîne que le corps est pythagoricien (au niveau 2) ; d'après le lemme VI-5 un ordre admet toujours une extension fidèle à une extension algébrique de degré impair, donc K n'a pas d'extension algébrique de degré impair.
Pour montrer que K est pythagoricien au niveau 4 il suffirait de montrer que K doit être bien chaînable et d'utiliser le résultat de Harman suivant :

K pythagoricien et bien chaînable équivaut à K pythagoricien au niveau 4.

Pour que la conjecture soit vraie il faut qu'un corps totalement chaînable qui est pythagoricien et n'admet pas d'extension de degré impair soit un corps bien chaînable. Becker a pu donner un exemple de corps pythagoricien totalement chaînable qui ne soit pas pythagoricien au niveau 4, en prenant la clôture pythagoricienne de $\mathbb{R}((t))$, mais ce corps peut avoir des extensions de degré impair.

BIBLIOGRAPHIE

[Be1] E. Becker :*"Hereditarily pythagorean fields and orderings of higher types"*, I.M.P.A., Lectures Notes # 29 (1978), Rio de Janeiro.

[Be2] E. Becker :*"The real holomorphy ring and sums of 2n-th powers"*, in Géométrie Algébrique Réelle et Formes Quadratiques, Lectures Notes # 959, Springer-verlag (1982).

[B-G] E. Becker et D. Gondard : *"Anneaux semi-chaînables"*, Preprint en français de [B-G2], in Séminaire D.D.G. Université Paris VI , 1987-88.

[B-G2] E. Becker et D. Gondard : *"On rings admitting orderings and 2-primary chains of orderings of higher level"*, à paraître dans Manuscripta Mathematica.

[Br1] L. Bröcker :*"Characterization of fans and hereditarily pythagorean fields"*, Math. Zeit., 151 (1976), pp. 149-163.

[De1] F. Delon :*"17ème problème de Hilbert sur les corps chaîne-clos : suite"* à paraître Séminaire D.D.G. , 1987-88, Université Paris VII.

[De2] F. Delon :*"Corps et anneaux de Rolle"*, Proceedings de l' A.M.S., # 97, 1986, pp. 315-319.

[D-G] F. Delon et D. Gondard :*"17ème problème de Hilbert au niveau n dans les corps chaîne-clos"*, Séminaire (D.D.G.) 1986-87, Université Paris VII ; Soumis J.S.L..

[Di1] M. Dickmann :*"The model theory of chain closed fields"*, J.S.L., # 53 (1988), pp. 73-82.

[Di2] M. Dickmann :*"Couples d'ordres chaînables"*, Exposé au Séminaire "Structures algébriques ordonnées" (D.D.G.), 1987-88.

[G1] D. Gondard :*"Théorie du premier ordre des corps chaînables et des corps chaîne-clos"*, C. R. Acad. Sc. Paris, Tome 304, # 16, 1987,

[G2] D. Gondard : *"Chainable fields and real algabraic geometry"*, à paraître in Proceedings "Real Algebraic and Analytic Geometry" (Trento Oct. 88) , Lectures Notes, Springer Verlag.

[G3] D. Gondard :*"Sur les théories des corps de Rolle"*, preprint in Séminaire D.D.G. 1988-89, Univ.Paris VII , à paraître.

[G4] D. Gondard :*"Kernels of chains and chainable fields"*, à paraître in Abstracts A.M.S..

[G5] D. Gondard :*"On Rolle fields theories"*, Abstracts A.M.S. , Mars 1989.

[H] J. Harman :*"Chains of higher level orderings"*, Contemporary Mathematics, vol. 8, 1982, pp. 141-174, A.M.S..

[J] B. Jacob :*"The model theory of generalized real closed fields"*, J. für die reine und ang. Mathematik, 323 (1981), pp.213-220.

[L1] T. Y. Lam :*"The theory of ordered fields"*, Proceedings of Alg. Conference, pp 1-152, M. Dekker (1980).

[L2] T. Y. Lam :*"orderings, valuations and quadratic forms"*, C.B.M.S. regional conference, # 52, 1983, A.M.S..

[P] A. Prestel :*"Lectures on formally real fields"*, I.M.P.A., Monografias de Matematica, # 22, 1975, Rio de Janeiro.

[R] P. Ribenboim :*"Arithmétique des corps"*, Herman, Paris 1972.

ANALYTIC ELIMINATION THEORY
(d'après Denef et van den Dries)

M. A. DICKMANN
CNRS – Université Paris VII

§1. INTRODUCTION. In the first three sections of their paper [2], J. Denef and L. van den Dries present a p–adic analogue of the real variable theory of semi–analytic and subanalytic sets. In the fourth section the ideas arising in the p–adic context are fed back into the real case to give new, shorter, more explicit and unified proofs of many of the foundational results of the theory.

The presentation proceeds along a path parallel to one by now well established in the study of *semi–algebraic* sets, both in the real and the p–adic cases. In the first of these two lectures we gave a summary of the geometric theory of real semi–algebraic sets, aimed at illustrating the line of argument. We omit this part of the exposé, as the theory just mentioned is presented with wealth of detail in Chapter IV of [3]. The fragment of the (cousin) theory of semi–algebraic subsets of $\mathbb{Q}_p^n$ dealing with Milnor's curve selection lemma and dimension theory is developed at length in [9].

The gist of the method consists in finding a language L in which the basic mathematical objects under study —subanalytic sets and functions in Denef–van den Dries' paper — coincide with those (parametrically) definable in the first–order calculus associated to L. Usually, the identity between these classes of objects is established by means of a quantifier elimination theorem in the language L for the first–order theory of the structures under study.

For the case of real semi–algebraic sets the language L is the language for unitary ordered rings consisting of the symbols $+, -, ., 0, 1, <$, and the elimination theorem is Tarski's celebrated result.

For semi–algebraic subsets of $\mathbb{Q}_p^n$, the appropriate language L has been introduced by Macintyre and consists of the symbols $+, -, ., 0, 1$ plus countably

many unary predicates P_2, P_3,...; P_n is interpreted as the multiplicative group of non–zero n–th powers. The elimination theorem required in this case was proved by Macintyre in 1976; see [7] and [8].

In the case of real and p–adic subanalytic sets, Denef and van den Dries succeeded in isolating suitable languages $L = L^D_{an}$ (same name in both cases, although they are not identical), and proving elimination theorems which make possible carrying out the program summarized above.

Owing to the audience's (and the lecturer's) preferences, we have inverted the priorities of Denef–van den Dries' paper giving, in the second lecture, a summary of their analytic elimination theory in the real case. In the next two sections we present this summary, and in the last we describe the modifications to be made in order to obtain a similar theory for the p–adic case; we also state an important result with no meaningful real analog.

§2. THE REAL ANALYTIC ELIMINATION THEOREM; SUBANALYTIC SETS.

We shall be concerned with the interval $I = [-1, 1]$ construed as a structure in the language L^D_{an} consisting of:

—A binary relation symbol (interpreted as the order of I).

—A binary function symbol D (interpreted in I by the function

$$D(x, y) = \begin{cases} x/y & \text{if } |x| \leq |y| \text{ and } y \neq 0 \\ 0 & \text{otherwise.)} \end{cases}$$

—An m–ary operation symbol for each power series in $\mathbb{R}[[X_1,...,X_m]]$ converging at every point of some neighborhood of I^m and sending I^m into I.

Note that product appears in L^D_{an}, corresponding to the series $X_1.X_2$. Sum and difference do not occur in L^D_{an} for + and − do not map I^2 into I. However, L^D_{an} does have a "poor man's" substitute for these operations, namely $\frac{1}{2}(X_1 + X_2)$ and $\frac{1}{2}(X_1 - X_2)$. A similar device makes possible, for instance, to represent a statement of form "$f(X_1,...,X_n) > 0$", where f is any power series converging in a neighborhood of I^m (but not necessarily sending I^m into I), as an L^D_{an}–formula, by replacing the function f by the term c.f, where $0 < c < 1/\sup\{f(\bar{x}) \mid \bar{x} \in I^m\}$.

The paper's key result is:

Theorem 1. (Analytic elimination theorem; real case).
The first–order theory of the interval I construed as an L^D_{an}–structure (as above) admits quantifier elimination. □

The (rather technical) proof uses the Weierstrass preparation theorem to reduce an occurence of a fixed (quantified) variable, say Z, in an L^D_{an}–term (e.g., a power series) of a given formula, to a polynomial occurrence. This can be achieved, while simultaneously keeping at bay unwanted appearances of the term D. After this reduction is performed, Tarski's quantifier elimination theorem is used to get rid of the quantifier binding the variable Z. Quantifiers are eliminated, one by one, in this way. The argument uses compactness of I.

The language L^D_{an} has been taylored to make quantifier–free definable sets coincide with subanalytic sets (in I^m). Before dwelling on this point we define the concepts involved.

Definition 2. (Semi– and subanalytic sets).
(a) A set $S \subseteq \mathbb{R}^n$ is called *semi–analytic at a point* $\overline{x} \in \mathbb{R}^n$ iff there is an open neighborhood U of $\overline{x}$ in $\mathbb{R}^n$ such that $U \cap S$ is a finite union of sets of form

$$\{\overline{y} \in U \mid f(\overline{y}) = 0 \wedge g_1(\overline{y}) > 0 \wedge \ldots \wedge g_k(\overline{y}) > 0\}$$

where $f, g_1, \ldots, g_k$ are real analytic functions defined on U.

(b) A subset of $\mathbb{R}^n$ is *semi–analytic* if it is semi–analytic at each point of $\mathbb{R}^n$.
(c) A set $S \subseteq \mathbb{R}^n$ is *subanalytic at* $\overline{x} \in \mathbb{R}^n$ iff there is an open neighborhood U of $\overline{x}$ in $\mathbb{R}^n$, an integer $m \geq 0$ and a bounded semi–analytic set $S' \subseteq \mathbb{R}^{n+m}$ such that $U \cap S = U \cap \pi[S']$, where $\pi : \mathbb{R}^{n+m} \longrightarrow \mathbb{R}^n$ is the projection which forgets the last m coordinates.
(d) A subset of $\mathbb{R}^n$ is *subanalytic* if it is subanalytic at each point of $\mathbb{R}^n$. □

Thus, a semi–analytic set is a set which <u>locally</u> admits a description similar to that of a semi–algebraic set, with polynomials replaced by analytic functions. Of course, semi–algebraic sets are semi–analytic, but many other sets are semi–analytic as well. For example, so are certain sets with countably many connected components, e.g., $\{x \in \mathbb{R} \mid x.\sin(x)\ ?\ 0\}$, where ? is any one of the signs $>$, $<$, or $=$. The projection condition defining subanalytic sets enlarges the class of

semi–analytic sets; however, the first examples of subanalytic sets which are not semi–analytic, occur in dimension 3:

3. Examples. (a) The set $\{<x, x.y, x.\exp(y)> \mid x, y \in \mathbb{R}\}$ is subanalytic but not semi–analytic at the origin.
(b) Another way to get subanalytic sets which are not semi–analytic is by means of the following remark: let $S \subseteq \mathbb{R}^n$ be a subanalytic set; let $C(S) \subseteq \mathbb{R}^{n+1}$ denote the cone with vertex at the origin over base S:

$$C(S) = \{<tx_1,...,tx_n,t> \mid t \in \mathbb{R} \text{ and } <x_1,...,x_n> \in S\}.$$

Then C(S) is subanalytic (this follows easily from Theorem 4 below), but by looking at the behaviour at the origin it is easily seen that C(S) is semi–analytic if and only if S is semi–algebraic. See Hironaka [5; Remark 3.7]. □

The supporting pillar of semi–algebraic geometry is the fact that *semi–algebraic sets possess a finite <u>global</u> description* by polynomial equalities and inequalities. Since the definition of subanalytic sets is of a local nature, it is not at all clear that they admit a similar finite global description in terms of analytic or related functions. The analytic elimination theorem shows that such a description does exist indeed (at least within the class of <u>bounded</u> subanalytic sets).

Theorem 4. ([2; Cor. 4.15]). *The following are equivalent for a set $S \subseteq [-1, 1]^n$:*
(1) S is defined in I by an L^D_{an}–formula (quantifiers and parameters allowed).
(2) S is a finite union of D–basic subsets (see definition below).
(3) S is subanalytic in $\mathbb{R}^n$. □

<u>D–basic sets</u> are sets of the form

$$\{\bar{x} \in I \mid f(\bar{x}) = 0 \wedge g_1(\bar{x}) > 0 \wedge ... \wedge g_k(\bar{x}) > 0\}$$

where the functions $f, g_1,...,g_k : I^n \longrightarrow I$ —called <u>D–functions</u>— are (arbitrary) finite compositions of the functions defining the language L^D_{an}; in other words, D–functions are those corresponding to <u>terms</u> of the language L^D_{an} (under the interpretation given at the beginning of this section).

§3. GEOMETRIC THEORY OF SUBANALYTIC SETS.

All the basic results concerning the geometric structure of subanalytic sets now

follow in cascade from the two theorems of the preceding section. Here are the main headlines.

Theorem 5. (Basic properties of bounded real subanalytic sets).
The family of subsets of I^n (some $n \geq 1$) subanalytic in $\mathbb{R}^n$ is:
(1) A boolean algebra. (The crucial result that the complement of a subanalytic set is subanalytic is due to Gabrielov [4].)
(2) Closed under first–order definable operations such as closure, interior, projections.
(3) Closed under images and inverse images by subanalytic functions. □

Note. A function $f : S \longrightarrow I^n$, where $S \subseteq I^m$, is called *subanalytic* if its graph $Gr(f) = \{\langle \bar{x}, f(\bar{x})\rangle \mid \bar{x} \in S\}$ is subanalytic in $\mathbb{R}^{m+n}$.

Theorem 6. (Existence of uniform bounds; [2; 3.2]).
For every subanalytic set $S \subseteq I^{m+n}$ there is an integer N so that for every $\bar{x} \in I^m$, if the fiber $S_{\bar{x}} = \{\bar{y} \in I^n \mid \langle \bar{x}, \bar{y}\rangle \in S\}$ is finite, then $card(S_{\bar{x}}) \leq N$. Furthermore, the set $\{\bar{x} \in I^m \mid S_{\bar{x}}$ is finite$\}$ is subanalytic. □

Theorem 7. (Selection theorem; [2; 3.6]).
Let $S \subseteq I^{m+n}$ be a subanalytic set and $\pi : \mathbb{R}^{m+n} \longrightarrow \mathbb{R}^m$ the projection which forgets the last n coordinates. There is a subanalytic map $f : \pi[S] \longrightarrow I^n$ whose graph is contained in S. □

Theorem 8. (Partition theorem; [2; 3.14]).
Each subanalytic subset of I^m is a disjoint union of finitely many subanalytic manifolds. □

Note. By a *manifold* we mean a real analytic manifold which is Hausdorff and of the same dimension at each of its points. A *subanalytic manifold* is a subanalytic set which is a manifold in this sense.

A well–behaved dimension theory stems from Theorem 8 upon defining dim(S) as the maximum of the dimensions of subanalytic manifolds contained in S. This theory produces results similar in many respects to those known for semi–algebraic sets.

Theorem 9. (Dimension formula; [2; 3.16]).
Let $S_1,\ldots,S_n$ be subanalytic subsets of I^m; then $dim(\cup_i S_i) = max\{dim(S_i) \mid i = 1,\ldots,n\}$; the same holds for countably many sets S_i, provided $\cup_i S_i$ is subanalytic. □

Theorem 10. (Product formula; [2; p. 111]).
If $S_1 \subseteq I^n$, $S_2 \subseteq I^m$ are subanalytic sets, then $dim(S_1 \times S_2) = dim(S_1) + dim(S_2)$. □

Theorem 11. (Invariance of dimension; [2; 3.21]).
The image of a subanalytic set under a subanalytic map does not increase dimension. If the map is injective, dimension is preserved. □

Theorem 12. (Characterization of dimension; [2; 3.23])
Let $S \subseteq I^m$ be a non–empty subanalytic set. Dim(S) is the largest integer d, $0 \leq d \leq m$, so that the image of S under some projection $I^m \longrightarrow I^d$ has non–empty interior in I^d. □

Theorem 13. (Dimension of closure; [2; 3.26]).
Let $S \subseteq I^m$ be subanalytic and cl(s) denote the closure of S in I^m. Then

$$dim(cl(S) - S) < dim(S).$$

In particular, $dim(cl(S)) = dim(S)$. □

This result is crucial in obtaining subanalytic stratifications (cf. Hironaka [5; Prop. III, p. 179]). The following theorem establishes a connection between subanalytic and analytic, functions:

Theorem 14. ([2; 3.29]). *Given $S \subseteq I^m$ and a subanalytic map $f: S \longrightarrow I^n$, there is a partition of S into finitely many subanalytic manifolds $M_1,\ldots,M_k$ so that each restriction $f|_{M_i}$ is an analytic function.* □

The analytic elimination theorem may be combined with the embedded resolution of singularities in order to yield a new proof of Hironaka's rectilinearization theorem. This result establishes a <u>global</u> relationship, by means of well–behaved analytic maps, between (arbitrary) m–dimensional subanalytic sets of $\mathbb{R}^n$ and semi–analytic subsets of $\mathbb{R}^m$ of a particularly simple form; for details, see [2; pp. 132–134]. Among the consequences of this theorem we have the following

results, originally proved by Lojasiewicz [6; Thms. 1 and 2, p. 127]:

Theorem 15. (a) *One–dimensional subanalytic subsets of* I^m *(any* $m \geq 1$*) are semi–analytic.*
(b) *Every subanalytic subset of* I^2 *is semi–analytic.* □

§4. THE p–ADIC CASE.

The theory summarized in §3 can be reproduced, with suitable modifications, for the field of p–adic numbers (p a fixed prime number). All results obtained in [2; §§ 2, 3] for this case are new.

The ring $\mathbb{Z}_p$ of p–adic integers plays the role of the interval I (recall that $\mathbb{Z}_p$ is compact in the p–adic topology). p–adic analytic functions are, of course, functions which admit a development in power series convergent in the p–adic topology. The elimination language L^D_{an} should be modified as follows:

—The binary relation symbol $<$ is replaced by countably many unary relation symbols P_n, as in Macintyre's language for p–adic semi–algebraic sets (cf. Introduction).

—The function symbol D is interpreted as follows:

$$D(x, y) = \begin{cases} x/y & \text{if } v(y) \leq v(x) \text{ and } y \neq 0 \\ 0 & \text{otherwise,} \end{cases}$$

where v denotes $\mathbb{Q}_p$'s valuation.

The analytic elimination theorem takes, in the p–adic context, a form very similar to that of Theorem 1:

Theorem 16. (Analytic elimination theorem; p–adic case).
The first–order theory of the ring $\mathbb{Z}_p$ *of p–adic integers construed as an* L^D_{an}*–structure (as indicated) admits quantifier elimination.* □

Exact analogs of Theorem 4, and of all the results mentioned in §3, hold in the present case as well. In addition, Denef and van den Dries prove versions of the following results —well–known in the real case—, for arbitrary subanalytic subsets of $\mathbb{Z}_p^n$:

(17) Milnor's curve selection theorem ([2; 3.34]).

(18) The Lojasiewicz inequalities ([2; 3.37]).
(19) The rationality of the Lojasiewicz exponents ([2; 3.37]).

Proofs of these results for real semi–algebraic sets can be found in Dickmann [3; Chs. IV and VII]; a proof of (17) for p–adic semi–algebraic sets is given in Scowcroft–van den Dries [9].

Most important among results for the p–adic case without a meaningful real analog is an extension of Denef's theorem on the rationality of the Poincaré series from semi–algebraic sets to subanalytic sets.

Definition 20. Let S be a subset of $\mathbb{Z}_p^m$. For each integer $n \geq 1$ we denote by S_n $(\subseteq (\mathbb{Z}/p^n\mathbb{Z})^m$ the image of S under the (m–fold product of the) residue map $\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$. Let $N_n(S)$ denote the cardinality of S_n. The series $P_S(T) = \sum_{n=0}^{\infty} N_n(S)T^n$ is called the *Poincaré series* associated to the set S. □

Theorem 21. (Rationality theorem; [2; 2.8]).
If $S \subseteq \mathbb{Z}_p^m$ is a subanalytic set, then the Poincaré series $P_S(T)$ is a rational function of T. □

For semi–algebraic S this was proved by Denef [1], solving a long–standing conjecture. For subanalytic S this gives a complete answer to a question raised by Serre and Oesterlé.

REFERENCES.

[1] Denef, J., The rationality of the Poincaré series associated to the p–adic points on a variety, Invent. Math. 77 (1984), 1–23.
[2] Denef, J. and van den Dries, L., p–adic and real subanalytic sets, Ann. of Math. 128 (1988), 79–138.
[3] Dickmann, M. A., **Model–theoretic methods in real algebraic geometry**, Math. Library, North–Holland Publ. Co., Amsterdam (to appear).
[4] Gabrielov, A. M., Projections of semi–analytic sets, Funktsionalnyi Analiz'eigo prilozheniya 2 (1968), 18–30 (in Russian; English translation: Funct. Anal. and its Appl. 2 (1968), 282–291.
[5] Hironaka, H., Triangulation of algebraic sets, *Algebraic Geometry Arcata 1974*,

Proc. Symp. Pure Math. 29 (1974), 165–185.
[6] Lojasiewicz, S., *Ensembles semi–analytiques* (mimeographed notes), I.H.E.S., Bures–sur–Yvette, 1965.
[7] Macintyre, A., On definable subsets of p–adic fields, J. Symb. Logic 41 (1976), 605–610.
[8] Prestel, A. and Roquette, P., **Formally p–adic fields**, Lect. Notes in Math. 1050, Springer–Verlag, Berlin, 1984.
[9] Scowcroft, P. and van den Dries, L., On the structure of semialgebraic sets over p–adic fields, J. Symb. Logic 53 (1988), 1138–1164.

Equipe de Logique Mathématique
Université Paris VII
2, Place Jussieu
75251 Paris Cédex 05 – FRANCE

SUMS OF 2n-TH POWERS OF MEROMORPHIC FUNCTIONS

Jesús M. Ruiz
Depto. Geometría & Topología, Univ. Complutense
28040 Madrid, Spain

In this paper we shall be concerned with real meromorphic functions. Thus, we fix from now on a compact connected real analytic manifold M of dimension m. By the identity principle, the ring $\mathcal{O}(M)$ of (global) analytic functions on M is a domain, and its field of quotients $\mathcal{M}(M)$ is the field of meromorphic functions on M. In other words, a *meromorphic function* on M is a quotient $h=f/g$ where f,g are analytic functions, $g\neq 0$. The *set of poles* Z of h is the zero-set of all g's appearing as denominators of h. Since M is compact, $\mathcal{O}(M)$ is noetherian, and so Z is the zero-set of finitely many g_i's. Then if $h=f_i/g_i$, The usual s.o.s. trick gives $h=\sum f_i g_i/\sum g_i^2$. Hence, any meromorphic function can be written $h=f/g$ with set of poles Z=zero-set of g. We are interested in the sums of 2n-th powers of meromorphic functions on M, i.e. sums of 2n-th powers of the field $\mathcal{M}(M)$. The key result to analyze these sums is, always, Becker's valuative criterion:

Theorem 1 [B].- Let F be a formally real field, and $h\in F$ a sum of squares. Then h is a sum of 2n-th powers if and only if $v(h)$ is a multiple of 2n for every real valuation v of F.

A natural simplification of this criterion is to substitute the very large family of all real valuations by a smaller one. This has been done when F is the field of rational functions of a real algebraic variety: [Br-Sc],[K-P]. Here we shall do it when F is the field of real meromorphic functions $\mathcal{M}(M)$. Also, we shall obtain some topological properties of sums of 2n-th powers of $\mathcal{M}(M)$. Of course, the first result is

Theorem 2 [J],[Rz1].- A function $h \in \mathscr{K}(M)$ is a sum of squares if and only if it is positive semidefinite.

Consequently, we concentrate our attention on the valuative criterion. We have:

Theorem 3.- Let Γ be a finitely generated ordered abelian group and $d \geq 0$ such that the rational rank of Γ is $\leq m-d$. Then a positive semidefinite meromorphic function $h \in \mathscr{K}(M)$ is a sum of 2n-th powers if and only if $v(h)$ is a multiple of 2n for every (real) valuation v of $\mathscr{K}(M)$ whose value group is Γ and whose residue field is a pure transcendental extension of $\mathbf{R}$ of degree d.

The proof of this theorem is based on the same approach that led to the geometric criterion of [Rz2] (cf. [K] for a different proof if $\dim(M)=2$). In the end, that criterion becomes an easy corollary of Th.3:

Proposition 1.- A meromorphic function $h \in \mathscr{K}(M)$ is a sum of 2n-th powers if and only if for every analytic curve $\sigma:(-\varepsilon,\varepsilon) \to M$, we have $h \circ \sigma = at^v + \ldots$, with $a > 0$ and v a multiple of 2n.

Proof.- The only if part. Every $\sigma:(-\varepsilon,\varepsilon) \to M$ gives a homomorphism

$$\mathscr{O}(M) \longrightarrow \mathbf{R}\{t\}: f \to \text{Taylor expansion of } f \circ \sigma \text{ at } 0,$$

whose kernel we denote by $\mathfrak{p}$. Then $\mathscr{O}(M)_{\mathfrak{p}}$ is a regular local ring, and the real valuation $\bar{v}$ induced by the embedding $\mathscr{O}(M)/\mathfrak{p} \to \mathbf{R}\{t\}$ lifts to another one v of $\mathscr{K}(M) = qf(\mathscr{O}(M)_{\mathfrak{p}})$. Now, if h is a sum of 2n-th powers, $v(h)$ is a multiple of 2n, which using the construction implies $\bar{v}(h)$ is a multiple of 2n too. But if $h \circ \sigma = at^v + \ldots$, then $v = \bar{v}(h)$ and 2n divides v. On the other hand, $h \circ \sigma$ is positive semidefinite by Th.2, and so $a > 0$.

The if part. Suppose $h \in \mathscr{K}(M)$ is not a sum of 2n-th powers. If $h(x) < 0$ for some $x \in M$, the conclusion is inmediate. Otherwise, by Th.2, h is a sum of squares and by Th.3 with $\Gamma = \mathbf{Z}$, $d=0$, we find a homomorphism $\varphi: \mathscr{O}(M) \to \mathbf{R}[[t]]$ with

$\varphi(h)=at^{\upsilon}+\ldots$, and 2n not dividing υ. Let $\mathfrak{m}$ be the inverse image of the maximal ideal (t) of R[[t]] and $x\in M$ the point corresponding to $\mathfrak{m}$ (which exists because M is compact). Then φ can be extended to a local momomorphism $\varphi:\mathcal{O}_x\to R[[t]]$, where $\mathcal{O}_x$ is the local ring of germs of analytic functions at x. As is well known $\mathcal{O}_x\equiv R\{x_1,\ldots,x_m\}$, so that φ can be approximated by local homomorphisms $\phi:\mathcal{O}_x\to R\{t\}$. If the approximation is good enough, $\phi(h)\equiv\varphi(h)$ mod $t^{\upsilon+1}$, and so $\phi(h)=at^{\upsilon}+\ldots$ Finally, ϕ gives an analytic curve $\sigma:(-\varepsilon,\varepsilon)\to M$ with $\sigma(0)=x$, and $h\circ\sigma=\phi(h)=at^{\upsilon}+\ldots$ We are done.

Now we shall use the precedent criteria to analyze some topological properties of the h's which are sums of 2n-th powers for all n. These h's are called *positive units.*

Proposition 2.- Let $h\in\mathcal{A}(M)$ be a positive unit and denote by Z its set of poles. Then:

(1) h is positive definite off Z.

(2) $\operatorname{cod}(Z)\geq 2$.

Proof.- (1) By Th.2, h is positive semidefinite on $M\setminus Z$. Then suppose $h(x)=0$ for some $x\notin Z$, and pick an analytic curve $\sigma:(-\varepsilon,\varepsilon)\to M\setminus Z$ with $\sigma(0)=x$. We get $h\circ\sigma=at^{\upsilon}+\ldots$, with $\upsilon\geq 1$, since $h\circ\sigma(0)=h(x)=0$. By Prop. 1, h is not a sum of 2υ-th powers, which is a contradiction.

(2) Suppose Z has an irreducible component Y of codimension 1. Then the ideal $\mathfrak{p}$ of Y is a heigth 1 real prime ideal of $\mathcal{O}(M)$. Since $\mathcal{O}(M)_{\mathfrak{p}}$ is a regular local ring, we conclude it is a real discrete valuation ring, whose valuation we denote by υ. By Th.1, 2n divides $\upsilon(h)$ for all n, and this implies $\upsilon(h)=0$. Hence, h belongs to $\mathcal{O}(M)_{\mathfrak{p}}$, i.e. $h=f/g$ with $g\notin\mathfrak{p}$. This means $\{g=0\}\supset Z\supset Y$, but also $g\notin\mathfrak{p}$=ideal of Y, a contradiction.

Finally we shall show with two examples the limits of the topological conditions (1) and (2) above.

Example 1.- For any (global) analytic subset Z of M, there is a sum of squares $h \in \mathscr{P}(M)$, whose set of poles is Z, and is positive definite off Z, but which is not a positive unit.

Indeed, take any equation g of Z and set $h=1/g^2$. Clearly Z is the critical locus of h and $h|M\setminus Z>0$. Furthermore, pick any $x\in Z$ and $\sigma:(-\varepsilon,\varepsilon)\to M$ such that $\sigma(0)=x$, $\sigma(t)\notin Z$ for $t\neq 0$ (this is the curve selection lemma). Then $h\circ\sigma=at^{-\upsilon}+\ldots$, with $a>0$ $\upsilon\geq 1$, because $h\circ\sigma(t)\to h\circ\sigma(0)=h(x)=1/g(x)^2=+\infty$. Consequently, h is not a sum of 2υ-th powers.

Anyhow, we can construct many positive units.

Example 2.- For any (global) analytic subset Z of M of codimension ≥ 2, there is a positive unit $h\in\mathscr{P}(M)$ with set of poles Z.

The construction requires some previous work with Z. Firstly, consider the irreducible components $Z_1,\ldots,Z_r$ of Z, and pick in each Z_i a regular point x_i which does not lie in any other Z_j. Here regular means there are global analytic equations of maximum rank, which vanish on Z and describe Z locally at x_i. Taking the first one of them, say f_i, we have

$$\operatorname{rank}(J_{x_i}(f_i))=1,\ \{f_i=0\}\supset Z.$$

Now choose a global analytic function g_i which vanish at x_j for $j\neq i$ but not at x_i, and consider $f=g_1f_1+\ldots+g_rf_r$. Clearly $J_{x_i}(f)=g_i(x_i).J_{x_i}(f_i)$ and

$$\operatorname{rank}(J_{x_i}(f))=1,\ \{f_i=0\}\supset Z.$$

Finally, denote by U the open set of regular points x of Z such that $\operatorname{rank}(J_x(f))=1$. Clearly, $x_1,\ldots,x_r\in U$, so that each intersection $U\cap Z_i$ is a non-empty open set of regular points of Z_i. This implies that any analytic function vanishing on U, vanishes on the whole Z.

On the other hand, let g be any equation of Z and put

$$h=\frac{2h_1^2+h_2^2}{h_1^2+h_2^2}, \quad \text{where } h_i=f+ig^2.$$

We claim h is the function we sougth. Clearly, $v(h)=0$ for any real valuation of $\mathscr{H}(M)$ and so, by Th.1, h is a holomorphy unit. Furthermore, the set of poles Y of h is contained in

$$\begin{cases} 0=h_1=f+g^2 \\ 0=h_2=f+2g^2 \end{cases}, \quad \text{i.e. in} \quad \begin{cases} f=0 \\ g=0 \end{cases},$$

which are equations of Z. Conversely, we have $Z\subset Y$. For this, it is enough to show $U\subset Y$. Hence fix $x\in U$. Then

$$J_x(h_i)=J_x(f), \text{ as } x\in Z=\{g=0\},$$

and so x is a regular point of dimension m-1 of $H_i=\{h_i=0\}$. Moreover, x is adherent to $H_i\setminus H_j$, because otherwise $H_1\cap H_2=Z$ would have dimension m-1 at x. Thus, there is an analytic curve $\sigma_i:(-\varepsilon,\varepsilon)\to M$, $\sigma_i(0)=x$, $\sigma_i(t)\in H_i\setminus H_j$ for $t\neq 0$, and:

$$h\circ\sigma_i(t)=\frac{2h_1(\sigma_i(t))^2+h_2(\sigma_i(t))^2}{h_1(\sigma_i(t))^2+h_2(\sigma_i(t))^2} \equiv i$$

when $t\to 0$, i.e. when $\sigma_i(t)\to x$. Whence, h cannot be extended to x.

Finally, we shall sketch the

Proof of Theorem 3.- Consider a sum of squares $h\in\mathscr{H}(M)$ which is not a sum of 2n-th powers. We look for a valuation v of $\mathscr{H}(M)$ with value group Γ and residue field $R(z_1,\ldots,z_d)$, such that $v(h)$ is not a multiple of 2n. If $h=f/g$ we replace h by $g^{2n}h=g^{2n-1}f$ and can assume from now on that $h\in\mathscr{O}(M)$.

First, Th.1 gives a real valuation v_0 of $\mathscr{H}(M)$ such that $v_0(h)$ is not a multiple of 2n. Fix an ordering α of $\mathscr{H}(M)$ compatible with v_0, and let V be the convex hull of R in $\mathscr{H}(M)$ with respect to α. One easily sees that the value of h for V is not a multiple of 2n, and can so suppose V is the ring of v_0. Also, V dominates a local ring $\mathscr{O}(M)_{\mathfrak{m}_x}$ where $\mathfrak{m}_x$ is the maximal ideal

of a point $x \in M$ (here we use M in compact). Then by Hironaka's resolution of singularities, V dominates a regular local ring of dimension m, $B = \mathcal{O}(M)[g_1,\dots,g_k]_{\mathfrak{n}} \subset \mathcal{R}(M)$, with residue field R. Furthermore, there are regular parameters $y_1,\dots,y_m \in \mathfrak{n}$ and a unit u of B with $h = u y_1^{p_1} \dots y_m^{p_m}$.

Then, since $v_0(h) = p_1 v_0(y_1) + \dots + p_m v_0(y_m)$ is not a multiple of 2n, some p_i, say p_1, cannot be either. Once we have this, the valuation v_0 will be substituted by another one. First, making 2n quadratic transforms of B, always dividing by y_1, we obtain:

$$h = u y_1^{q_1} y_2^{q_2} \dots y_m^{q_m} \quad \text{(with new } y_2,\dots,y_m\text{)}$$

and $q_1 = p_1 + 2n \sum_{j \neq 1} p_j$ is not a multiple of 2n. Let A be the 2n-th quadratic transform. Then

(i) $A = \mathcal{O}(M)[h_1,\dots,h_s]_{\mathfrak{m}} \subset \mathcal{R}(M)$ is regular of dimension m, with residue field R.

(ii) There are regular parameters $y_1,\dots,y_m \in \mathfrak{m}$ and a unit u of A such that $h = u y_1^{q_1} \dots y_m^{q_m}$, where q_1 is not a multiple of 2n.

(iii) The localizations $A_{(y_1,\dots,y_j)}$ dominate $\mathcal{O}(M)_{\mathfrak{m}_x}$ and have residue field $R(z_{j+1},\dots,z_m)$, the residue classes z_i of y_i algebraically independent over R.

Some further work with the extension $\mathcal{O}(M)_{\mathfrak{m}_x} \to \mathcal{O}_x \cong R\{x_1,\dots,x_m\}$ shows that

(iv) There is a local embedding $A \to R\{y_1,\dots,y_m\}$.

After this preparation, which follows closely [Rz2], we can construct a new valuation v with the required value group and residue field.

First case: rank $\Gamma = 1$.

Since Γ is finitely generated, we may find $1 = \xi_1,\dots,\xi_r \in R$ rationally independent with $\Gamma \cong \xi_1 Z + \dots + \xi_r Z \subset R$. Thus the hypothesis on the rational rank of Γ is $r \leq m\text{-}d = j$, and we have a diagram

$$\begin{array}{ccccc} R\{y\}_{(y')} & \xrightarrow{\hat{}} & R(\{z\})[[y']] & \xrightarrow{\phi} & R(\{z\})[[t^{\Gamma}]] \\ \uparrow & & \uparrow & & \uparrow \\ A_{(y')} & \xrightarrow{\hat{}} & R(z)[[y']] & \xrightarrow{\phi} & R(z)[[t^{\Gamma}]], \end{array}$$

where $y=(y_1,\dots,y_m)$, $y'=(y_1,\dots,y_j)$, $z=(z_{j+1},\dots,z_m)$, $[[t^{\Gamma}]]$ means formal power series with exponents in Γ (cf. [F]), and ϕ is defined by the substitutions

$$\begin{cases} \phi(y_i)=t^{\xi_i} & \text{for } i=1,\dots,r, \\ \phi(y_i)=t^{2n}(1+\Phi_i(t^{\xi_r})) & \text{for } i=r+1,\dots,j, \end{cases}$$

with $t,\Phi_{r+1},\dots,\Phi_j\in R[[t]]$ series analytically independent of order ≥ 1. This latter condition guarantees that the resulting local homomorphism $A_{(y')}\to R(z)[[t^{\Gamma}]]$ is inyective. Consequently, it induces a valuation v in $qf(A_{(y')})=\mathcal{K}(M)$: this is the needed valuation.

For, its residue field is in between the one of $A_{(y')}$ and the one of $R(z)[[t^{\Gamma}]]$, but these are both $R(z)=R(z_{j+1},\dots,z_m)$. Hence v is a real valuation and its residue field is a pure transcendental extension of R of degree m-j=d. On the other hand, the value group of v is obviously contained in Γ, but in turn contains $v(y_i)=\xi_i$, $1\leq i\leq r$, which generate Γ. Finally, $\phi(h)=\phi(uy_1^{q_1}\dots y_m^{q_m})=\text{unit}.\phi(y_1^{q_1}\dots y_j^{q_j})$, and we find

$$v(h)=q_1\xi_1+\dots+q_r\xi_r+2nq_{r+1}+\dots+2nq_j=(q_1+2nq)\xi_1+q_2\xi_2+\dots+q_r\xi_r$$

(remember $\xi_1=1$). Now since $\xi_1,\dots,\xi_r$ are rationally independent, and 2n does not divide q_1, it cannot divide $v(h)$.

Thus, the proof in the case rank $\Gamma=1$ is finished.

Second case: rank $\Gamma>1$.

Let Γ_1 be a maximal proper isolated subgroup of Γ, so that $\Gamma'=\Gamma/\Gamma_1$ has rank 1. Denote by r the rational rank of Γ'. Then, the procedure of the case already solved gives a real valuation v' of $\mathcal{K}(M)=qf(A_{(y',)})$, $y'=(y_1,\dots,y_r)$

with residue field $\mathbf{R}(z_{r+1},\ldots,z_m)$ and such that $v'(h)$ is not a multiple of 2n. Now we have:

$$\text{rational rank of } \Gamma_1 = \text{rational rank of } \Gamma - r \leq (m-d)-r = (m-r)-d,$$

and this condition allows us to find a valuation $\bar{v}$ of $\mathbf{R}(z_{r+1},\ldots,z_m)$ with value group Γ_1 and residue field a pure transcendental extension of $\mathbf{R}$ of degree d. We end by taking the valuation v of $\mathcal{A}(M)$ composite of v' and $\bar{v}$.

References.

[B] E. Becker: The real holomorphy ring and sums of 2n-th powers, in Lecture Notes in Math. 959, Berlin-Heildelberg-New York, Springer 1982.

[Br-Sc] L. Bröcker, H.-W. Schülting: Valuations of function fields from the geometrical point of view, J. reine angew. Mathematik 365 (1986) 12-32.

[F] L. Fuchs: Partially ordered algebraic systems, Pergamon Press 1963.

[J] P. Jaworski: Extensions of orderings on fields of quotients of rings of real analytic functions, Math. Nachr. 125 (1986) 329-339.

[K] W. Kucharz: Sums of 2n-th powers of real meromorphic functions, to appear.

[K-P] F.V. Kuhlmann, A. Prestel: On places of real algebraic function fields, J. reine angew. Mathematik 358 (1984) 181-195.

[Rz1] J.M. Ruiz: On Hilbert's 17 problem and real Nullstellensatz for global analytic functions, Math. Z. 190 (1985) 447-454.

[Rz2] J.M. Ruiz: A characterization of sums of 2n-th powers of global meromorphic functions, to appear.

Prépublications de l'Equipe de Logique

N° 1. **D. Lascar.**
Les beaux automorphismes, janvier 1990.

N° 2. **F. Delon, M. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées 1988–89, janvier 1990.

N° 3. **J.L. Krivine.**
Opérateurs de mise en mémoire et traduction de Gödel, janvier 1990.