N° 17

Séminaire de Structures Algébriques Ordonnées

1989 – 1990

F. DELON, M.A. DICKMANN, D. GONDARD

Décembre 1990

Seminaire de Structures Algebriques Ordonnees.

Delon – Dickmann – Gondard

1989 – 1990

7.11.89 – **J.L. Duret** (Université d'Angers)
Equivalence élémentaire des corps de fonctions sur un corps algébriquement clos.

20.11.89 – **M. Droste** (Univ. Essen, R.F.A.).

5.12.89 – **A. Louveau** (Univ. Paris 6).
Classification des ordres boreliens.

8.12.89 – **T. Krick** (Univ. de Buenos–Aires, Argentine).
Une borne géométrique pour la programmation entière.

12.12.89 – **E. Becker** (Univ. de Dormund (R.F.A.).
Number of real roots and quadratic forms (a survey).

19.12.89 – **F. Delon.**
L'anneau des entiers algébriques (d'après Prestel et Schmid).

9.01.90 – **F. Delon.**
L'anneau des entiers algébriques (d'après Prestel et Schmid).

16.01.90 – **F. Delon** et **F. Point.**
même titre.

30.01.90 – **J. Gutierez** (Espagne).
Polynomial decomposition on volumes.

6. et 13.02.90 – **M. Dickmann.**

Une structure de géométrie combinatoire sur l'espace d'ordres d'un corps.

20.02.90 – **T. Hyttinen.**

Constructing models by games in infinitary languages.

27.02.90 – **Z. Chatzidakis.**

Un corps indécidable avec une extension finie décidable.

13.03.90 – **E. Becker** (Univ. Dortmund, R.F.A.).

The 17^{th} Hilbert problem for sums of higher powers.

24.04.90 – **D. Gluschankof** (Universités de Buesnos–Aires et d'Angers).

La théorie du premier ordre des produits de groupes abéliens totalement ordonnés.

22.05.90 – **I. Meguerditchian** (Rennes).

Géométrie des polynômes hyperboliques.

19.06.90 – **D. Pecker** (Paris 6).

Projections de variétés algébriques réelles.

Séminaire de Structures Algébriques Ordonnées

Delon – Dickmann – Gondard

1989 – 1990

Liste des contributions

– **Duret, J.–L.** (Université d'Angers).
Corps de courbes sur $\mathbb{C}$ élémentairement équivalents.

– **Droste, M.** (Université d'Essen, Allemagne).
Subgroups of small index in ordered permutation groups.

– **Bank, B., Mandel, R.** (Allemagne) **et Heintz, J., Krick, T. Solerno, P.**
(Buenos Aires, Argentine).
Une borne optimale pour la programmation entière quasi–convexe.

– **Becker, E.** (Université de Dortmund, Allemagne).
Voir :
Sums of squares and quadratic forms in real algebraic geometry.
Cahiers du Séminaire d'Histoire des Mahtématiques, Université Pierre et Marie Curie, Laboratoire de Mathématiques Fondamentales, Printemps 1991, A paraître.

– **Gutiérrez J.** (Université de Cantabria, Santander, Espagne).
The functional decomposition of polynomials.

– **Dickmann, M.** (Université Paris VII).

A combinatorial geometric structure on the space of orders of a field.

– **Hyttinen, T.** (Université d'Helsinki, Finlande).

Constructing models by games for infinitary languages.

– **Chatzidakis, Z.** (Université Paris VII).

Un exemple de corps indécidable dont toutes les extensions finies propres sont décidables.

– **Gluschankof, D.** (Université de Buenos Aires, Argentine et Université d'Angers).

The elementary class of products of totally ordered abelian groups.

– **Meguerditchian, I.** (Université de Rennes).

Géométrie locale des polynômes hyperboliques.

– **Pecker, D.** (Université Paris VI).

Sur la projection de variétés algébriques réelles.

Corps de courbes sur C élémentairement équivalents.

Jean-Louis Duret

Soit $\mathcal{L}$ le langage constitué de deux constantes 0 et 1, et de deux fonctions $+$ et $\cdot$; si A est un sous-ensemble d'une structure de $\mathcal{L}$, nous noterons $\mathcal{L}(A)$ le langage obtenu en ajoutant à $\mathcal{L}$ les éléments de A comme constantes.

A Introduction : le cas du genre différent de 1.

Tous les corps considérés seront commutatifs. Nous appellerons *corps de courbe* sur un corps k une extension de k finiment engendrée de degré de transcendance 1 sur k. Si k est algébriquement clos, d'aprés le théorème de la base séparante, un corps de courbe sur k est de la forme $k(u,v)$ où u n'est pas élément de k et où v est algébrique sur $k(u)$. C'est donc le corps de la courbe sur k d'équation affine $P(x,y)=0$ où $P(u,Y)$ est un polynôme minimal de v sur $k(u)$. C'est aussi le corps d'une courbe non singulière sur k.

Nous appellerons *ensemble de coefficients* d'une courbe sur un corps k un sous-ensemble A de k tel qu'il existe un système de générateurs de l'idéal de cette courbe dont les coefficient sont des éléments de A.

Nous nous proposons de continuer l'étude des corps de courbe sur un corps algébriquement clos commencée dans l'article *Sur la théorie élémentaire des corps de fonctions* [D]. On y avait démontré [D, proposition 21, p. 954] :

1. Proposition. *Pour tout $g \in \mathbf{N}$, il existe un ensemble d'énoncés, $\mathcal{G}_g$, du premier ordre du langage $\mathcal{L}$ tel que, si K est un corps de courbe sur un corps algébriquement clos, alors K est de genre g si et seulement s'il satisfait $\mathcal{G}_g$.*

Il en résulte donc immédiatement que deux corps de courbe sur un corps algébriquement clos élémentairement équivalents dans le langage $\mathcal{L}$, ont même genre. S'ils sont de genre 0, ils sont donc k-isomorphes. D'où la tentation, pour le genre ≥ 2, d'appliquer un corrollaire de la formule de Hurwitz [H, chapitre 4, exemple 2.5.4, p. 303] :

2. Proposition. *Un morphisme dominant de courbes projectives non singulières de même genre ≥ 2, est un isomorphisme.*

Vérifier l'hypothèse de cette proposition se fait en appliquant une fois encore les idées de [D] :

3. Lemme. *Soient K un corps de courbe sur un corps algébriquement clos k, A un ensemble de coefficients d'une courbe dont K est le corps et K' un corps de courbe sur k élémentairement équivalent à K dans le langage $\mathcal{L}(A)$. Alors K et K' ont même genre et il existe un k-homomorphisme de K dans K'. Si C et C' sont des courbes projectives non singulières sur k dont les corps sont respectivement K et K', alors C et C' ont même genre et il existe un morphisme dominant de C' sur C.*

Démonstration. Soit $\mathcal{C}(\mathrm{x})$ une formule : $\exists y(x^d+y^d=1)$, où $\frac{1}{2}(d-1)(d-2)$ est strictement supérieur au genre de K ; $\mathcal{C}(\mathrm{x})$ définit k dans K et dans K' [D, proposition 10]. Soient $P_1(X_1,\ldots,X_m),\ldots,P_n(X_1,\ldots,X_m)$ les générateurs à coefficients dans A d'un idéal (de $k[X_1,\ldots,X_m]$) d'une courbe affine dont K est le corps ; K et donc K' satisfont :

$$\exists x_1,\ldots,x_m\left(\bigwedge_{i=1}^{n}P_i(x_1,\ldots,x_m)=0\ \wedge\ \bigvee_{i=1}^{m}\neg\mathcal{C}(x_i)\right)$$

Soit alors $(a_1,\ldots,a_m)$ un élément de K'^m-k^m tel que pour $i=1,\ldots,n$, on ait : $P_i(a_1,\ldots,a_m)=0$; $k(a_1,\ldots,a_m)$ est un sous-corps de K' k-isomorphe à K.

La deuxième partie du lemme est la réénonciation de la première à l'aide de [H, chapitre I, corollaire 6.12, p.45]. □

Nous venons donc de démontrer :

4. Théorème. *Soient K un corps de courbe de genre différent de 1 sur un corps algébriquement clos k et A un ensemble de coefficients d'une courbe dont K est le corps de fonctions (notamment, dans le cas du genre 0, A peut être l'ensemble vide). Alors tout corps de courbe sur k élémentairement équivalent à K dans le langage $\mathcal{L}(A)$, lui est k-isomorphe.*

On peut aussi sans grande difficulté supplémentaire démontrer :

5. Théorème. *Soit K un corps de courbe de genre différent de 1 sur un corps algébriquement clos k. Alors tout corps de courbe sur k élémentairement équivalent à K dans le langage $\mathcal{L}$ lui est isomorphe.*

Nous aimerions maintenant évidemment montrer la conjecture suivante (ainsi qu'une conjecture analogue au théorème 5) :

6. Conjecture. Si K est un corps de courbe sur un corps algébriquement clos k, il existe un sous-ensemble A de k tel que tout corps de courbe sur k élémentairement équivalent à K dans le langage $\mathcal{L}(A)$, lui est k-isomorphe.

Pensant au théorème classique de représentation des corps de courbe de genre 1 sur C par des corps de fonctions elliptiques, nous nous limiterons au cas de la caractéristique nulle et même, ici, au cas où k est C. Malheureusement, je ne sais pas traiter la généralité

du cas du genre 1, et nous allons devoir ajouter aux hypothèses que K n'a pas de multiplication complexe (pour la définition, voir plus loin definition 19). De plus pour ne pas dissimuler l'idée principale dans des difficultés supplémentaires, nous accepterons que A dépendent des deux corps de courbe considérés. Nous nous proposons donc de démontrer :

7. Théorème. *Si K est un corps de courbe sur* $\mathbf{C}$ *sans multiplication complexe, tout corps de courbe sur* $\mathbf{C}$ *élémentairement équivalent à K dans le langage $\mathcal{L}(\mathbf{C})$, lui est* $\mathbf{C}$*-isomorphe.*

B Réseaux et fonctions elliptiques.

8. Définition. Nous appellerons *réseau* un sous-groupe additif de $\mathbf{C}$ engendré par deux éléments linéairement indépendants sur $\mathbf{R}$ (i.e. dont le rapport n'est pas réel).

9. Deux réseaux Λ et Λ' sont semblables si et seulement si Λ' est l'image de Λ par une similitude du plan complexe (ce qui est évidemment une relation d'équivalence), i.e. si et seulement s'il exixte un nombre complexe non nul α tel que : $\alpha \cdot \Lambda = \Lambda'$. Nous noterons $< \omega_1, \omega_2 >$ le réseau engendré par $\{\omega_1, \omega_2\}$. Un réseau $< \omega_1, \omega_2 >$ est semblable à un réseau $< 1, \tau >$ où τ n'est pas réel ($\tau = \frac{\omega_2}{\omega_1}$, rapport de similitude : $\frac{1}{\omega_1}$). En remplaçant éventuellement τ par $-\tau$, on peut même supposer que τ est élément de H, demi-plan supérieur ouvert de $\mathbf{C}$.

10. Théorème. *Deux réseaux $< 1, \tau >$ et $< 1, \tau' >$ (où τ et τ' sont élément de H) sont semblables si et seulement si τ et τ' sont élément de la même orbite du groupe (appelé "*groupe modulaire*") d'applications de H sur H engendré par les deux applications : $z \mapsto z + 1$ et $z \mapsto -\frac{1}{z}$* [DV, chapitre 3, § 26, p. 42].

11. Définition. Nous dirons qu'un réseau Λ *a une multiplication complexe* si et seulement s'il est semblable à un réseau $< 1, \tau >$ où τ est un nombre algébrique quadratique (i. e. est un nombre complexe de degré 2 sur $\mathbf{Q}$). D'aprés le théorème 10, c'est équivalent à : pour tout τ tel que $< 1, \tau >$ est semblable à Λ, τ est un nombre algébrique quadratique.

12. Définition. Si Λ est un sur-réseau d'un réseau Λ' (i.e. $\Lambda' \subset \Lambda$) nous noterons :

$$\mathcal{R}(\Lambda, \Lambda') = \{\alpha \in \mathbf{C} \; ; \; \alpha\Lambda \supset \Lambda'\}$$

13. Soit à étudier $\mathcal{R}(\Lambda, \Lambda')$. Si Λ est un sur-réseau de Λ', alors il existe une base de Λ', (ω_1, ω_2) et deux entiers naturels non nuls m et n tels que $(\frac{\omega_1'}{mn}, \frac{\omega_2'}{m})$ soit une base de Λ [DV, § 63, p. 132]. On a :

$$\mathcal{R}\left(< \frac{\omega_1}{mn}, \frac{\omega_2}{m} >, < \omega_1, \omega_2 >\right) = \left\{m\alpha \; ; \; \alpha \in \mathcal{R}\left(< \frac{1}{n}, \frac{\omega_2}{\omega_1} >, < 1, \frac{\omega_2}{\omega_1} >\right)\right\}.$$

On se ramène donc à étudier $\mathcal{R}(< \frac{1}{n}, \tau >, < 1, \tau >)$ que nous noterons $\mathcal{R}(n, \tau)$. On remarque :

$$\frac{1}{\mathbf{Z}} = \left\{ \frac{1}{k} \; ; \; k \in \mathbf{Z} - \{0\} \right\} \subset \mathcal{R}(n, \tau)$$

(quels que soient n et τ) et :

$$\mathcal{R}(1, \tau) \subset \mathcal{R}(n, \tau).$$

Pour justifier la terminologie, signalons que $< 1, \tau >$ a une multiplication complexe si et seulement si : $\mathcal{R}(1, \tau) \neq \frac{1}{\mathbf{Z}}$ (un élément de $\mathcal{R}(1, \tau) - \frac{1}{\mathbf{Z}}$ n'est pas réel, puisque 1 et τ sont linéairement indépendants sur $\mathbf{R}$).

14. Proposition. *Si τ n'est pas un nombre algébrique quadratique (i.e. τ n'est pas solution d'une équation du second degré à coefficients dans $\mathbf{Q}$), alors :*

$$\mathcal{R}(n, \tau) = \frac{1}{\mathbf{Z}}.$$

Démonstration. Soit $\alpha \in \mathcal{R}(n, \tau)$. Il existe des entiers relatifs a, b, c et d tels que :

$$1 = a\frac{\alpha}{n} + b\alpha\tau \quad \text{et} \quad \tau = c\frac{\alpha}{n} + d\alpha\tau$$

c'est à dire :

$$\begin{cases} \dfrac{1}{\alpha} = a\dfrac{1}{n} + b\tau & (1) \\ \dfrac{1}{\alpha}\tau = c\dfrac{1}{n} + d\tau & (2) \end{cases}$$

Remplaçant $\frac{1}{\alpha}$ dans (2), on obtient :

$$b\tau^2 + (\frac{a}{n} - d)\tau - \frac{c}{n} = 0$$

et comme τ n'est pas algébrique quadratique, on a : $b = 0, \frac{a}{n} = d$ et $c = 0$. Donc, de (1) on tire : $\frac{1}{\alpha} = d$. On a donc : $\frac{1}{\mathbf{Z}} \supset \mathcal{R}(n, \tau)$, et donc l'égalité d'après la remarque précédente. □

15. Définition. On appelle *fonction elliptique* sur un réseau Λ une fonction méromorphe dont l'ensemble des périodes contient Λ.

Les fonctions constantes sont donc des fonctions elliptiques. Elles constituent un corps canoniquement isomorphes à $\mathbf{C}$ (que nous noterons $\mathbf{C}$).

16. Théorème. *L'ensemble $\mathcal{E}(\Lambda)$ des fonctions elliptiques sur Λ est un corps (pour l'addition et le produit usuel des fonctions) de courbe sur $\mathbf{C}$ de genre 1. Réciproquement pour tout corps de courbe sur $\mathbf{C}$, K, de genre 1, il existe un réseau Λ tel que K est $\mathbf{C}$-isomorphe à $\mathcal{E}(\Lambda)$* [H, chapitre IV, théorèmes 4.12B et 4.14B, p. 327-328].

17. Théorème. *Tout sous-corps de $\mathcal{E}(\Lambda')$ de degré de transcendance 1 sur* C *est un corps de courbe sur* C *de genre 0 ou 1. Pour tout sous-corps K de $\mathcal{E}(\Lambda')$ de degré de transcendance 1 sur* C *de genre 1, il existe un sur-réseau Λ de Λ' tel que K est égal à $\mathcal{E}(\Lambda)$* [DV, théorème 11.2, p. 196].

18. Théorème. *Deux corps $\mathcal{E}(\Lambda)$ et $\mathcal{E}(\Lambda_0)$ sont* C*-isomorphes si et seulement si Λ et Λ_0 sont semblables. Une application $\Phi : \mathcal{E}(\Lambda) \longrightarrow \mathcal{E}(\Lambda_0)$ est un* C*-isomorphisme si et seulement s'il existe un complexe β et un complexe non nul α satisfaisant à : $\alpha\Lambda = \Lambda_0$, tels qu'on ait :*

$$(\forall f \in \mathcal{E}(\Lambda))(\forall z \in \mathbf{C})(\Phi(f)(z) = f(\frac{z}{\alpha} + \beta))$$

[DV, § 88, p. 191].

19. Définition. Nous dirons qu'un corps de courbe$K$ sur C de genre 1 *a une multiplication complexe* si et seulement s'il est isomorphe à $\mathcal{E}(\Lambda)$ où Λ a une multiplication complexe, si et seulement si (d'aprés le théorème 18), tout réseau Λ tel que K est isomorphe à $\mathcal{E}(\Lambda)$, a une multiplication complexe.

C Démonstration du théorème 7.

20. Soient K' un corps de courbe sur C élémentairement équivalent à K dans le langage $\mathcal{L}(\mathbf{C})$. D'après le lemme 3, K' est de genre 1 et il existe un C-homomorphisme de K dans K' ; sans perte de généralité, nous pouvons supposer que K est un sous-corps de K' : $K \subset K'$. Pour démontrer le théorème 7, il suffit donc de démontrer que, si de plus K et K' ne sont pas C-isomorphes, alors ils ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(\mathbf{C})$, c'est-à-dire qu'il existe un énoncé de ce langage vrai dans K et faux dans K'.

D'aprés les théorèmes 16 et 17, il existe un réseau Λ' et un sur-réseau Λ de Λ' tel que K' et K soient respectivement C-isomorphes à $\mathcal{E}(\Lambda')$ et $\mathcal{E}(\Lambda)$; d'aprés 13, il existe une base (ω_1, ω_2) de Λ' et deux entiers naturels m et n tels que : $\Lambda' =< \omega_1, \omega_2 >$ et $\Lambda =< \frac{\omega_1}{mn}, \frac{\omega_2}{m} >$; d'aprés le théorème 18, K est C-isomorphe à $\mathcal{E}(< \frac{\omega_1}{n}, \omega_2 >)$; enfin d'aprés le théorème 18, K' est C-isomorphe à $\mathcal{E}(< 1, \tau >)$ et K au sous-corps $\mathcal{E}(< \frac{1}{n}, \tau >)$. Désormais, nous noterons $K' = \mathcal{E}(< 1, \tau >)$ et $K = \mathcal{E}(< \frac{1}{n}, \tau >)$.

Soient w un élément primitif de K' sur K : $K' = K[w]$, u et v tels que : $K = \mathbf{C}(u, v)$, $P(X, Y) \in \mathbf{C}[X, Y]$ tel que $P(u, Y)$ soit polynôme minimal de v sur $\mathbf{C}(u)$, $Q(X, Y, Z) \in \mathbf{C}[X, Y, Z]$ tel que $Q(u, v, Z) \in K[Z]$ soit polynôme minimal de w sur K ($\mathrm{d}^\circ Q > 1$). Soit $\mathcal{C}(x)$ une formule définissant C dans K et K' [D, proposition 10]. On a :

$$K \models \exists x, y(\neg\mathcal{C}(x) \ \wedge \ P(x, y) = 0 \ \wedge \ \forall z(Q(x, y, z) \neq 0))$$

Il suffit donc de démontrer :

$$K' \models \forall x, y(\neg\mathcal{C}(x) \ \wedge \ P(x, y) = 0 \ \rightarrow \ \exists z(Q(x, y, z) = 0))$$

Soient donc u_0 et v_0 des éléments de K' tels que : $u_0 \notin \mathbf{C}$ et $P(u_0, v_0) = 0$, et $\varphi_0 : K \to \mathbf{C}(u_0, v_0)$ le C-isomorphisme défini par : $\varphi_0(u) = u_0$ et $\varphi_0(v) = v_0$. Il s'agit de démontrer qu'il existe un C-homomorphisme de K' dans K' prolongeant φ_0. D'aprés 18, il existe $\alpha, \beta \in \mathbf{C}$ tels que φ_0 est défini par :

$$(\forall f \in K)(\forall z \in \mathbf{C})(\Phi(f)(z) = f(\frac{z}{\alpha} + \beta))$$

$(\mathbf{C}(u_0, v_0) = \mathcal{E}(\alpha < \frac{1}{n}, \tau >))$. Puisque par hypothèse, τ n'est pas un nombre algébrique quadratique, d'aprés la proposition 14, α est un élément de $\frac{1}{\mathbf{Z}}$, et $\alpha < 1, \tau >$ est un sur-réseau $< 1, \tau >$. Le C-isomorphisme $\varphi : K' = \mathcal{E}(< 1, \tau >) \to \mathcal{E}(\alpha < 1, \tau >)$ défini par :

$$(\forall f \in K')(\forall z \in \mathbf{C})(\Phi(f)(z) = f(\frac{z}{\alpha} + \beta))$$

est le prolongement cherché de φ_0. □

D Le cas avec multiplication complexe.

21. On voit que la démonstration précédente reste valide si l'on peut affirmer que le complexe α qui est élément de $\mathcal{R}(n, \tau)$ est aussi élément de $\mathcal{R}(1, \tau)$. S'inspirant de [H, chapitre IV, théorème 4.19, p.330], on peut calculer $\mathcal{R}(n, \tau)$:

22. Proposition. *Si τ est un nombre algébrique quadratique : $\tau = r + is\sqrt{d}$ (où : $r \in \mathbf{Q}, s \in \mathbf{Q}^*, d \in N$ et où d est libre de carré (i. e. 1 est le seul carré diviseur de d)), alors :*

$$\mathcal{R}(n, \tau) = \left\{ (\frac{a}{n} + b\tau)^{-1} \; ; \; a, b \in \mathbf{Z} \text{ et } a \text{ ou } b \neq 0 \text{ et } n(r^2 + ds^2)b, \; \frac{a}{n} + 2rb \in \mathbf{Z} \right\}$$

23. Corollaire. *Si : $\tau = \frac{1}{m}(k + il\sqrt{d})$ (où : $k \in \mathbf{Z}$, l, $m \in \mathbf{N} - 0$ et où d est libre de carré), alors si m et n sont premiers entre eux et notamment si : $m = 1$), on a : $\mathcal{R}(n, \tau) = \mathcal{R}(1, \tau)$.*

En modifiant l'énoncé avec les mêmes idées, on peut obtenir aussi le résultat lorsqu'il existe un nombre premier divisant n et ne divisant pas m. On obtient donc :

24. Proposition. *Soient $\tau = \frac{1}{m}(k + il\sqrt{d})$ (où : $k \in \mathbf{Z}$, l, $m \in \mathbf{N} - 0$ et où d est libre de carré) et $n \in \mathbf{N}$. S'il existe un nombre premier diviseur de n et non de m, alors :*

$$\mathcal{E}(< 1, \tau >) \underset{\mathbf{C}}{\not\equiv} \mathcal{E}(< \frac{1}{n}, \tau >)$$

RÉFÉRENCES

[D] JEAN-LOUIS DURET, *Sur la théorie élémentaire des corps de fonctions*, **The Journal of Symbolic Logic**, vol. 51, N° 4, Dec. 1986, pp. 948-956.

[DV] PATRICK DU VAL, **Ellictic Functions and Elliptic Curves**, London Mathematical Society Lecture Note Series, 9, Cambridge University Press.

[H] ROBIN HARTSHORNE, **Algebraic Geometry**, Graduate Texts in Mathematics 52, Springer-Verlag.

Subgroups of Small Index in Ordered Permutation Groups

To appear in: Quart. J. Math. Oxford

M. Droste (Essen) and J.K. Truss (Leeds)

§1 Introduction and results

This paper presents results supplementary to those of [11,12] in the specific context of ordered permutation groups. The first type of result concerns the least number of conjugates which are needed to express an element f of the normal closure $\langle g\rangle^G$ of some $g \in G$ as a product of the form $\prod_{i=1}^{n} (g^{\pm 1})^{h_i}$. In [11] it was shown that for the groups $A(\mathbb{Q})$ and $A(\mathbb{R})$ of all order-automorphisms of the rationals $(\mathbb{Q},\leq)$ and the reals $(\mathbb{R},\leq)$, respectively, this least number is 4. Let us call an infinite chain $(C,\leq)$ *doubly homogeneous*, if its order-automorphism group $A(C) = \mathrm{Aut}(C,\leq)$ acts transitively on the 2-element subsets of C. Notice that such chains include, for example, all linearly ordered fields; their automorphism groups $A(C)$ are important in the theory of ordered permutation groups, see [7]. In [1] it was proved that if C is any doubly homogeneous chain, then the 'least number of conjugates' for $A(C)$ is at most 8; in [4] this result was extended to any 'large' subgroup G of $A(C)$ (precise definitions are given below). It is our first aim to show by a combination of the methods of [1,4,11] that for any such group G the 'least number of conjugates' is actually 4.

The second kind of result, which concerns the "small index property", was initially proved in [2] for the symmetric group on a countably infinite set, and was then extended to various other cases in [4,6,12].

To say that the permutation group $G \leq \mathrm{Sym}\ \Omega$ has the *small index property* means that any subgroup of G of index $< 2^{\aleph_0}$ contains the pointwise stabilizer $G_{(F)}$ of a finite subset F of Ω. In [12] the only group of order-automorphisms considered was $A(\mathbb{Q})$; indeed that was the only possibility since the goal was to look at permutation groups of countable degree. The same argument used in that proof shows however that $A(\mathbb{R})$ has the small index property in a strong sense; namely that the only subgroup of $A(\mathbb{R})$ having index $< 2^{\aleph_0}$ is in fact $A(\mathbb{R})$ itself. It is this that we generalize here, considering subgroups G of $A(C)$ where C is dense in $\mathbb{R}$ having the small index property. The conditions we need to impose on C and G are just that C is doubly homogeneous and that, as before, G is large in $A(C)$. The idea behind the notion of largeness is that it allows us to perform many of the typical constructions possible in $A(C)$ also in G. However, to illustrate the scope of this extension we cite various instances, such as the groups preserving certain colourings, or the locally linear or locally differentiable homeomorphisms. Some care is required here to keep in mind which set the group acts on; the finite set F whose stabilizer is contained in the given subgroup of small index may need to be taken in the order-completion $\overline{C} = \mathbb{R}$ of C, rather than in C itself (so strictly speaking we need to modify slightly the definition of the "small index property"). This is immediately clear for instance in taking for C the set of irrational numbers (where $A(C)$ is "the same as" $A(\mathbb{Q})$). A sufficient condition for $F \subseteq C$ when considering $A(C)$ is that $|\mathbb{R} \setminus C| = 2^{\aleph_0}$.

Finally we use the methods of [11; §5] to distinguish large subgroups of $A(C)$ in some cases, and examine the numbers of conjugacy classes of stabilizers of singletons.

Before stating precisely our two main results, let us introduce some notation. Throughout C will be a chain (a linearly ordered set with ordering $\leq$ understood). In this paper (contrary to the convention in [11]) permutations will act on the right, so that xg, or sometimes x^g, is the image of x under g. The *support* supp g of $g \in A(C)$ is $\{x \in C: xg \neq x\}$. We let $\overline{C}$ denote the Dedekind-completion of C and $\hat{C} = \overline{C} \cup \{-\infty,\infty\}$ where $-\infty < x < \infty$ for each $x \in \overline{C}$. We regard $A(C)$ as a subgroup of $A(\overline{C})$ in the natural way.

Let $G \leq A(C)$. We say that G is *closed under disjoint patching*, if whenever $\{g_i: i \in I\}$ are members of G whose supports are pairwise disjoint, then $g \in A(C)$ given by

$$xg = \begin{cases} xg_i & \text{if } x \in \text{supp } g_i \text{ for some } i \in I \\ x & \text{otherwise} \end{cases} \qquad (x \in C)$$

lies in G. We say that G is *closed under piecewise patching*, if whenever $a_i, b_i \in C$ for $i \in \mathbb{Z}$ are such that $a_i < a_{i+1}$, $b_i < b_{i+1}$ for each $i \in \mathbb{Z}$ and $\lim_{i\to\infty} a_i = \lim_{i\to\infty} b_i$ and $\lim_{i\to\infty} a_{-i} = \lim_{i\to\infty} b_{-i}$ in $\hat{C}$ and $g_i \in G$ are such that $[a_i,a_{i+1}]g_i = [b_i,b_{i+1}]$, then $g \in A(C)$ given by

$$xg = \begin{cases} xg_i & \text{if } x \in [a_i,a_{i+1}] \ (i \in I) \\ x & \text{otherwise} \end{cases} \qquad (x \in C)$$

lies in G. Finally we say that G is *large* in $A(C)$, if G acts doubly homogeneously on C and is closed under disjoint patching and piecewise patching. If $g \in G$, we let $\langle g \rangle^G$ denote the normal subgroup of G generated by g. Now we can state our main results.

Theorem 1.1. *Let C be any doubly homogeneous chain and G a large subgroup of $A(C)$.*

(a) Let $f,g \in G$ *such that* $f \in \langle g \rangle^G$. *Then* $f = g_1 \cdot g_2^{-1} \cdot g_3 \cdot g_4^{-1}$ *for some conjugates* g_i *of* g *in* G.

(b) There are $f,g \in G$ *with* $\langle f \rangle^G = \langle g \rangle^G = G$, *but* f *is not the product of three conjugates of* g *or* g^{-1}.

Moreover, we show that Theorem 1.1(b) even remains true for the cosets of f and g in $G/(G \cap B(C))$, where $B(C)$ is the normal subgroup of $A(C)$ comprising all those $h \in A(C)$ whose support is bounded above and below in C.

If $G \leq A(C)$ and $F \subseteq \overline{C}$, let F^G denote the set of images of elements of F under members of G.

Theorem 1.2. *Let* C *be any dense doubly homogeneous subset of* $\mathbb{R}$ *and* G *a large subgroup of* $A(C)$. *Then for any subgroup* H *of* G, $|G : H| < 2^{\aleph_0}$ *if and only if* $H = G_{(F)}$ *and* $|F^G| < 2^{\aleph_0}$ *for some finite subset* $F \subseteq \mathbb{R}$.

References

1. R.N. Ball, M. Droste: Normal subgroups of doubly transitive automorphism groups of chains, *Trans. Amer. Math. Soc.* 290 (1985), 647-664.

2. J.D.Dixon, P.M. Neumann, S. Thomas: Subgroups of small index in infinite symmetric groups, *Bull. London Math. Soc.* 18 (1986), 580-586.

3. M. Droste: The normal subgroup lattice of 2-transitive automorphism groups of linearly ordered sets, *Order* 2 (1985), 291-319.

4. M. Droste, W.C. Holland, H.D. Macpherson: Automorphism groups of infinite semilinear orders (I) and (II), *Proc. London Math. Soc. (3)* 58 (1989), 454-478 and 58 (1989), 479-494.

5. M. Droste, S. Shelah: A construction of all normal subgroup lattices of 2-transitive automorphism groups of linearly ordered sets, *Israel J. Math.* 51 (1985), 223-261.

6. D. Evans: Subgroups of small index in infinite general linear groups, *Bull. London Math. Soc.* 18 (1986), 587-590.

7. A.M.W. Glass: *Ordered Permutation Groups*, London Math. Soc. Lecture Note Series, vol. 55, Cambridge, 1981.

8. Y. Gurevich, W.C. Holland: Recognizing the real line, *Trans. Amer. Math. Soc.* 265 (1981), 527-534.

9. G. Higman: On infinite simple permutation groups, *Publ. Math. Debrecen* 3 (1954), 221-226.

10. S. McCleary: The lattice-ordered group of automorphisms of an α-set, *Pacific J. Math.* 49 (1973), 419-424.

11. J.K. Truss: Infinite permutation groups. Products of conjugacy classes, *J. Algebra* 120 (1989), 454-493.

12. J.K. Truss: Infinite permutation groups. Subgroups of small index, *J. Algebra* 120 (1989), 494-515.

Authors' addresses:

Fachbereich 6 - Mathematik, Universität GHS Essen, D - 4300 Essen 1, Germany,

and

Department of Pure Mathematics, University of Leeds, Leeds LS2 9JT, England.

UNE BORNE OPTIMALE POUR LA PROGRAMMATION ENTIÈRE QUASICONVEXE

Bernd BANK , Joos HEINTZ , Teresa KRICK , Reinhard MANDEL
& Pablo SOLERNÓ

Résumé - Soient $F_1,\dots,F_s \in \mathbb{Z}[X_1,\dots,X_n]$ des polynômes quasiconvexes de degré majoré par $d \geq 2$, et ℓ une borne pour la longueur binaire de leurs coefficients. On montre que si le systeme $F_1 \leq 0,\dots,F_s \leq 0$ admet une solution entière, alors il existe une telle solution à longueur binaire majorée par $(sd)^{cn}.\ell$ (où c est une constante, indépendante de s,d,n et ℓ). Le caractère simplement exponentiel de cette borne est intrinsèque au problème. On obtient aussi une borne similaire pour le problème de minimisation correspondant.

INTRODUCTION ET NOTATIONS.-

En 1983, L.G.Khachiyan et S.P.Tarasov ([13],[6]) ont annoncé que si $F_1,\dots,F_s$ sont des polynômes convexes en n indéterminées, de degré $d \geq 2$ et à coefficients entiers, tous de longueur binaire majorée par ℓ, alors le système d'inégalités polynomiales $F_1 \leq 0,\dots,F_s \leq 0$ admet une solution entière si et seulement si il admet une solution entière contenue dans une boule centrée à l'origine et de rayon entier R, de longueur binaire majorée par $d^{c(\tilde{n}+d)}.n^{cd}.\ell$ (où $\tilde{n} := \min\{s,n\}$ et c est une constante indépendante des paramètres considérés). L'intérêt de cette question est qu'elle représente une solution effective pour le problème de stabilité correspondant au problème d'optimisation (de minimisation) pour la programmation entière à contraintes polynomiales convexes, généralisation naturel-

le du problème de la programmation linéaire entière.

Dans ce travail, nous nous intéressons en premier lieu à ce même problème de calcul d'une borne géométrique pour le cas des polynômes quasiconvexes.

Pour préciser les résultats, fixons tout d'abord les notations:

Dans ce qui suit, $\mathbb{R}$ représentera le corps des nombres réels et $\mathbb{Z}$ l'anneau des entiers. Soient $X_1,\ldots,X_n$ des indéterminées sur $\mathbb{R}$. On dit qu'un polynôme $F\in\mathbb{R}[X_1,\ldots,X_n]$ est quasiconvexe si pour tout $t\in\mathbb{R}$, l'ensemble de niveau $\{x\in\mathbb{R}^n: F(x)\leq t\}$ est un sous-ensemble convexe de $\mathbb{R}^n$.

Pour un ensemble fini $V\subseteq\mathbb{Z}^n$ de vecteurs à coordonnées entières, nous noterons par $\ell(V)$ la longueur binaire maximale des coordonnées de tout vecteur de V. De même, si $\mathcal{F}\subseteq\mathbb{Z}[X_1,\ldots,X_n]$ est un ensemble fini de polynômes à coefficients entiers, $\ell(\mathcal{F})$ notera la longueur binaire maximale des coefficients des polynomes de $\mathcal{F}$.

La boule fermée de rayon $R\in\mathbb{R}_{\geq 0}$ et centrée à l'origine sera indiquée par $B(0,R)$. Nous adopterons aussi la notation standard $O(n)$, $n\in\mathbb{N}$, pour désigner une fonction linéaire en n, c'est-à-dire, il existe une constante c, indépendante de n, telle que $O(n)\leq cn$.

Passons maintenant à l'énoncé des résultats:

THEOREME 1.- Soient $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ des polynômes quasiconvexes à coefficients entiers, de degré majoré par $d \geqslant 2$ et tels que $\ell := \ell(\{F_1, \ldots, F_s\})$.
Il existe un rayon $R \in \mathbb{N}$, de longueur binaire $\ell(R) = (sd)^{O(n)} \cdot \ell$ tel que si l'ensemble $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ est non vide, alors il contient un point (entier) dans la boule $B(0,R)$.
Ce rayon R ne dépend pas du caractère particulier des polynômes $F_1, \ldots, F_s$ mais seulement des paramètres s, d, n, ℓ considérés.

Etant donné que les polynômes convexes constituent un cas particulier des polynômes quasiconvexes, ce résultat généralise et améliore la borne annoncée par Khachiyan et Tarasov.

D'autre part, le caractère exponentiel de la borne obtenue est intrinsèque au problème, comme le prouve l'exemple suivant étudié dans [13] : les auteurs considèrent les polynômes quadratiques et convexes $F_1 = -X_1 + 2^{\ell}$, $F_2 = X_1^2 - X_2$, ..., $F_n = X_{n-1}^2 - X_n$ et montrent que toutes les solutions du systeme $F_1(x) \leq 0, \ldots, F_n(x) \leq 0$ se trouvent en dehors de la boule $B(0,R)$, où $\ell(R) = 2^{n-1} \cdot \ell$. Ceci signifie que la borne du Théorème 1 est optimale en fonction des paramètres considérés, en tant que mesure générale de complexité.

Ce théorème géométrique entraîne aussi le résultat algorithmique suivant:

COROLLAIRE.- On peut décider à l'aide d'une machine de Turing non déterministe si l'ensemble $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ est non vide en temps $(sd)^{O(n)} \cdot \ell$. En d'autres mots, le problème de la programmation entière à contrain-

tes polynomiales quasiconvexes appartient à la classe de complexité NEXPTIME ("non deterministically simply exponential time"). Ceci signifie qu'on peut vérifier si un candidat à solution du système considéré est effectivement une solution en temps simplement exponentiel.

Finalement, les méthodes appliquées pour montrer le Théorème 1 entraînent aussi le résultat d'optimisation entière à contraintes polynomiales quasiconvexes correspondant:

THEOREME 2.- Soient $F, F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ des polynômes quasiconvexes à coefficients entiers, de degré majoré par $d \geq 2$ et tels que $\ell := \ell(\{F, F_1, \ldots, F_s\})$ et posons $M := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$.
Si l'ensemble $M \cap \mathbb{Z}^n$ est non vide et

$$\inf\{F(x) : x \in M \cap \mathbb{Z}^n\} = m > -\infty$$

(où inf note l'infimum),
alors il existe un rayon $R \in \mathbb{N}$, de longueur binaire $\ell(R) = (sd)^{O(n)} \cdot \ell$ tel que

$$m = \inf\{F(x) : x \in M \cap \mathbb{Z}^n \cap B(0,R)\}.$$

PREUVES DES RESULTATS.-

Preuve du Théorème 1 - Le Théorème 1 est une conséquence des nouveaux résultats en géométrie semi-algébrique algorithmique (élimination "rapide" des quantificateurs dans la théorie élémentaire des corps réels clos) qu'on trouve dans [12], [3], [4], [5] et [9], appliqués au problème grâce à des techniques de réduction pour la programmation quasiconvexe développées dans [1], chapitres 4 et 5, et simplifiées dans [2]. Nous considérerons ici plus en détail les méthodes nouvelles particulières à notre problème, nous remettant aux travaux cités ci-dessus pour les démonstrations des résultats préliminaires qui y figurent. Une borne légèrement moins précise, avec les preuves complètes,

est aussi présentée dans [7].

Dans le but de fournir la démonstration la plus claire possible, nous la diviserons en différentes sections.

1. Propriétés fondamentales des polynômes quasiconvexes.

Nous décrivons ici quelques propriétés théoriques qui sont indispensables pour l'obtention de la borne annoncée.

Propriété d'"uniformité": Soit $F \in \mathbb{R}[X_1, \ldots, X_n]$ un polynôme quasiconvexe. Soient $x, u \in \mathbb{R}^n$, $u \neq 0$, fixés. Si le polynôme $F(x + Tu)$, en l'indéterminée T, est strictement décroissant (respectivement constant) alors, pour tout $y \in \mathbb{R}$, le polynôme $F(y + Tu)$ est strictement décroissant (respectivement constant).

Preuve: Nous utiliserons la définition équivalente de polynôme quasiconvexe suivante, qui est plus opérative: $F \in \mathbb{R}[X_1, \ldots, X_n]$ est quasiconvexe ssi pour tout $x, y \in \mathbb{R}^n$ et pour tout $\alpha \in \mathbb{R}$, $0 \leq \alpha \leq 1$, on a:

$$F(\alpha x + (1-\alpha)y) \leq \max\{F(x), F(y)\}$$

Il est facile de vérifier qu'un polynôme quasiconvexe non constant $F \in \mathbb{R}[X]$ (en une seule variable) n'admet pas de maximum local, et que donc, s'il est de degré pair, son coefficient conducteur est positif et s'il est de degré impair, la fonction qu'il définit est strictement croissante ou décroissante suivant le signe de son coefficient conducteur.

La preuve de la propriété d'"uniformité" suit maintemant de la définition de polynôme quasiconvexe qui implique que si $x, y, u \in \mathbb{R}^n$, $u \neq 0$, alors $F(x + Tu)$ et $F(y + Tu)$ sont ou bien tous deux constants ou bien de même degré $d \neq 0, -1$ et ont même coefficient conducteur. Voir [1], Chapitre 4, ou [2] pour les détails. ■

Propriété de "linéarité" d'une forme homogène quasiconvexe:
Soit $P \in \mathbb{R}[X_1, \ldots, X_n]$ une forme homogène quasiconvexe de degré $d \geq 1$, et soient $L := \{x \in \mathbb{R}^n : P(x) = 0\}$

$K := \{x \in \mathbb{R}^n : P(x) \leq 0\}$

Alors: - L est un sous-espace linéaire de $\mathbb{R}^n$.

- Si d est pair, K = L
- Si d est impair, L est un hyperplan et K est un des demi-espaces limités par L.

Preuve: C'est une conséquence immédiate de la propriété antérieure (Voir [1], Chapitre 4, ou [2]). ■

Nous montrerons maintenant une version effective de cette propriété, qui exhibe une base $\mathcal{B}$ de L (et un système de générateurs $\mathcal{G}$ de K) construite à partir des coefficients de la forme homogène quasiconvexe P.

Lemme 1: Soit $P \in \mathbb{Z}[X_1, \ldots, X_n]$ une forme homogène quasiconvexe (à coefficients entiers) de degré d, et soit $\tilde{d} := \max\{2, d\}$.
Alors le sous-espace linéaire $L = \{x \in \mathbb{R}^n : P(x) = 0\}$ admet une base entière $\mathcal{B}$ telle que $l(\mathcal{B}) = \tilde{d}^{O(r)}(l(P) + n)$ ou $r := n - \dim_{\mathbb{R}} L$, et, si d est impair, le demi-espace K admet un système de générateurs entier $\mathcal{G}$ (i.e. $K = \{\sum_{v \in \mathcal{G}} \lambda_v . v, \lambda_v \geq 0\}$) tel que $l(\mathcal{G}) = l(\mathcal{B})$.

Preuve: On observe tout d'abord que si P est quasiconvexe, il existe une variable X_j telle que $\deg_{X_j} P = d$ (voir [1] et [2] pour les détails). Sans perte de généralité, supposons que X_1 est cette variable.
On procède par induction en n:
Soit $n \geq 2$. Si $L \neq \{0\}$, soit $u \in L - \{0\}$. Le fait que pour tout $t \in \mathbb{R}$, $P(tu) = t^d P(u) = 0$ implique par la propriété d'"uniformité" que pour tout $x \in \mathbb{R}^n$, le polynôme $P(x + Tu)$ est constant comme polynôme en T; c'est-à-dire

que pour tout $x \in \mathbb{R}^n$, $P(x) = P(x+u)$.

Ainsi:

(*) $P(X) = P(X+u)$: pour tout $u \in L$

Posons:

$$P(X_1,\ldots,X_n) = a_d(X_2,\ldots,X_n)X_1^d + a_{d-1}(X_2,\ldots,X_n)X_1^{d-1} + \ldots + a_1(X_2,\ldots,X_n)X_1 + a_0(X_2,\ldots,X_n)$$

où $a_d(X_2,\ldots,X_n) \neq 0$, et, pour tout $0 \leq i \leq d$, $a_i(X_2,\ldots,X_n) \in \mathbb{Z}[X_2,\ldots,X_n]$ est une forme homogène de degré d-i (i.e. $a_d(X_2,\ldots,X_n) = a_d \in \mathbb{Z} - \{0\}$ et $a_{d-1}(X_2,\ldots,X_n) := \sum_{2\leq k\leq n} b_k X_k$ est une forme linéaire entière).

Evaluons le polynôme P en $X+u := (X_1+u_1,\ldots,X_n+u_n)$:

$$P(X+u) = a_d.(X_1+u_1)^d + (\sum_{2\leq k\leq n} b_k.(X_k+u_k)).(X_1+u_1)^{d-1} + \ldots + a_0(X_2+u_2,\ldots,X_n+u_n)$$

$$= P(X) + X_1^{d-1}(da_d u_1 + \sum_{2\leq k\leq n} b_k u_k) + \ldots + P(u)$$

(où les termes compris dans les points de suspension sont de degré en X_1 inférieur à (d-1)).

Par (*), on conclut que $L \subseteq L^1 := \{u \in \mathbb{R}^n : da_d u_1 + \sum_{2\leq k\leq n} b_k u_k = 0\}$

L'hyperplan L^1 admet la base entiere

$$\{(-b_2, da_d, 0,\ldots,0),\ldots,(-b_n,0,\ldots,0,da_d)\}$$

(qui se complète à une base $\mathcal{B}^1$ de $\mathbb{R}^n$ en ajoutant le vecteur $(1,0,\ldots,0)$), de manière que $\ell(\mathcal{B}^1) = \ell + \log_2 d)$.

Si la forme homogène P restreinte à L^1 n'est pas la forme nulle (c'est-à-dire si $L \neq L^1$), on pose:

$$P^1(Y_1,\ldots,Y_{n-1}) := P(-b_2Y_1-\ldots-b_nY_{n-1}, da_dY_1,\ldots,da_dY_{n-1})$$

et on obtient la forme homogène quasiconvexe P^1 en (n-1) variables, qui représente (dans la base $\mathcal{B}^1$) la forme P restreinte à L^1.

P^1 vérifie l'estimation suivante:

$$\ell(P^1) \leq \ell(P) + d(\log_2 d + \ell(\mathcal{B}^1)) + n\log_2(d+1)$$

$$= (d+1)\ell(P) + 2d.\log_2 d + n\log_2(d+1)$$

$$= \tilde{d}^c(\ell(P) + n)$$ (où c est une constante universelle).

Etant donné que $L \neq L^1$, la forme quasiconvexe P^1 n'est pas la forme nulle et on répète la procédure avec elle. Supposons que $L = L^r$, pour un certain $0 \leq r \leq n$), c'est-à-dire que la forme P^{r-1} restreinte à L^r est la forme nulle, alors $\dim_{\mathbb{R}} L = n - r$ et $\ell(P^{r-1}) \leq \tilde{d}^{c(r-1)}(\ell(P) + (r-1)n)$
De plus, on a: $\ell(\mathcal{B}^r) \leq \ell(P^{r-1}) + \log_2 d =$

$$\tilde{d}^{c(r-1)}(\ell(P) + (r-1)n)$$

(où $\mathcal{B}^r$ est la base correspondante de L, écrite en termes de la base $\mathcal{B}^{r-1}$ de L^{r-1}).
On récupère finalement l'écriture canonique $\mathcal{B}$ de la base $\mathcal{B}^r$ de L en multipliant r matrices de passage, à coefficients de longueurs binaires contrôlées par $\tilde{d}^{c(r-1)}(\ell(P) + (r-1)n)$, obtenant ainsi:

$$\ell(\mathcal{B}) \leq (r-1)\log_2 n + r(\tilde{d}^{c(r-1)}(\ell(P) + (r-1)n))$$
$$= \tilde{d}^{O(r)}(\ell(P) + n).$$

La borne pour $\ell(\mathcal{G})$,si d est impair, est claire. ∎

Ce lemme a la conséquence suivante:

<u>Corollaire:</u> Soit $F = \sum_{0 \leq i \leq d} P_i \in \mathbb{Z}[X_1, \ldots, X_n]$ un polynôme quasiconvexe écrit comme somme de formes homogènes de degré i , et soit $\tilde{d} := \max\{2, d\}$.
Alors, pour tout $0 \leq i \leq d$, l'ensemble:

$$L_i(F) := \{x \in \mathbb{R}^n : P_d(x) = 0, \ldots, P_i(x) = 0\}$$

est un sous-espace linéaire de $\mathbb{R}^n$, qui admet une base entière $\mathcal{B}_i$ avec $\ell(\mathcal{B}_i) = \tilde{d}^{O(n)}\ell(F)$
et l'ensemble:

$$K_i(F) := \{x \in \mathbb{R}^n : P_d(x) = 0, \ldots, P_{i+1}(x) = 0, P_i(x) \leq 0\}$$

est ou bien un demi-sous-espace de $\mathbb{R}^n$, qui admet un système de générateurs entier $\mathcal{G}_i$ avec $\ell(\mathcal{G}_i) = \tilde{d}^{O(n)}\ell(F)$ ou bien coincide avec $L_i(F)$.

<u>Preuve:</u> C'est une application immédiate du fait que si F est un polynôme quasiconvexe, sa forme homogène P_d de plus

haut degré est aussi quasiconvexe, et du lemme précédent.■

Après des considérations d'ordre général sur les polynômes quasiconvexes, passons au caractère particulier de notre problème.

2. Elimination des contraintes superflues et réduction à un ensemble borné.

Soient $F_1,\dots,F_s \in \mathbb{Z}[X_1,\dots,X_n]$ des polynômes quasiconvexes de degré majoré par $d \geq 2$, et soit $l := l(\{F_1,\dots,F_s\})$ Soit M l'ensemble convexe défini par:

$$M := \{ x \in \mathbb{R}^n : F_1(x) \leq 0,\dots,F_s(x) \leq 0 \}$$

Le but de cette section est d'étudier lesquelles des contraintes $F_1,\dots,F_s$ sont de trop, c'est-à-dire de déterminer à partir des contraintes F_i $(1 \leq i \leq s)$ qui définissent M un ensemble convexe M' d'aspect plus uniforme que M et vérifiant principalement la condition:

$$M \cap \mathbb{Z}^n \neq \emptyset \iff M' \cap \mathbb{Z}^n \neq \emptyset$$

Pour cela, faisons le raisonnement suivant:
Supposons qu'il existe une direction $u \in \mathbb{R}^n - \{0\}$ telle que $F_1(Tu)$ soit strictement décroissant et $F_2(Tu),\dots,F_s(Tu)$ soient décroissants ou constants (dans ce cas on dit que u est une direction de récession de $F_1,\dots,F_s$, non constante pour F_1), et supposons de plus que $u \in \mathbb{Z}^n$. Soit alors $x_1 \in \mathbb{Z}^n$ tel que $F_2(x_1) \leq 0,\dots,F_s(x_1) \leq 0$; l'hypothèse et la propriété d'"uniformité" de F_1 impliquent que $F_1(x_1 + Tu)$ est strictement décroissant et on peut choisir $t \in \mathbb{N}$ de manière que $F_1(x_1 + tu) \leq 0$.
Posons $x := x_1 + tu$. Le même argument que ci-dessus montre que pour $2 \leq i \leq s$, $F_i(x) = F_i(x_1 + tu) \leq F_i(x_1) \leq 0$.
Donc, $x \in \mathbb{Z}^n$ est tel que $F_1(x) \leq 0,\dots,F_s(x) \leq 0$, et dans ce cas nous dirons que F_1 est une contrainte superflue.
Il est clair que le rôle de F_1 peut être joué par n'importe quelle contrainte F_j $(1 \leq j \leq s)$, et pour la consi-

dération de l'ensemble M, nous supprimerons la contrainte superflue. Une fois éliminée une contrainte superflue, on peut répéter le procédé jusqu'à la suppression (dans un certain ordre) de toutes les contraintes superflues.
Les questions qui se posent sont alors les suivantes: Comment choisir les directions de récession entières u ? Que se passe-t-il quand il n'y a plus de contraintes superflues ?
La réponse est dans la proposition suivante:

Proposition: Il existe $\{i_1,\dots,i_t\} \subseteq \{1,\dots,s\}$ tel que si $M' := \{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \dots, F_{i_t}(x) \leq 0\}$, alors

(i) $M \cap \mathbb{Z}^n \neq \emptyset \iff M' \cap \mathbb{Z}^n \neq \emptyset$

(ii) A partir de chaque point entier $x' \in M'$, on récupère un point entier $x \in M$ de manière que $\ell(x) = d^n \ell(x') + d^{O(n)} \ell$
(Dans le cas ou $t = s$, on peut choisir $x' = 0$)

(iii) $M' = V + (M' \cap V^{\perp})$, où V est un sous-espace linéaire de $\mathbb{R}^n$, qui admet une base entiere $\mathcal{B}$ telle que $\ell(\mathcal{B}) = d^{O(n)} \ell$ et $M' \cap V^{\perp}$ est un sous-ensemble compact de $\mathbb{R}^n$.

Preuve: Selon le raisonnement fait auparavant, le procédé consiste à trouver des directions entières de récession u, non constantes pour une contrainte donnée.
Pour tout $F \in \mathbb{Z}[X_1,\dots,X_m]$ quasiconvexe, posons:

$$L(F) := \{u \in \mathbb{R}^n : \sup \{F(tu),\ t \in \mathbb{R}\} < +\infty\}$$

et $$K(F) := \{u \in \mathbb{R}^n : \sup \{F(tu),\ t \geq 0\} < +\infty\}$$

Il est alors clair que $u \in \mathbb{Z}^n - \{0\}$ est une direction de récession de $F_1,\dots,F_S$, non constante pour F_j si et seulement si $u \in K(F_1) \cap \dots \cap K(F_S)$ et $u \notin L(F_j)$
Dans [1], Chapitre 4, ou [2], il est montré que pour tout $F = \sum_{0 \leq i \leq d} P_i$ quasiconvexe, écrit comme somme de formes homogènes de degré i , il existe i_0, $1 \leq i_0 \leq d$, tel que

$$L(F) = \{u \in \mathbb{R}^n : P_d(u)=0, \ldots, P_{i_0}(u)=0\}$$
et $$K(F) = \{u \in \mathbb{R}^n : P_d(u)=0, \ldots, P_{i_0+1}(u)=0, P_{i_0}(u) \leq 0\}$$
C'est-à-dire, suivant la notation du Corollaire, $L(F) = L_{i_0}(F)$ et $K(F) = K_{i_0}(F)$; ainsi, une direction $u \in \mathbb{Z}^n - \{0\}$ est de récession de $F_1, \ldots, F_s$ non constante pour F_j si et seulement si $u \neq 0$ appartient au cône polyhedral (i.e. à l'intersection d'un nombre fini de demi-espaces de $\mathbb{R}^n$) $K(F_1) \cap \ldots \cap K(F_s)$ mais non au sous-espace linéaire $L(F_j)$. La preuve de la Proposition s'obtient maintenant à l'aide des résultats suivants:

Lemme 2: Dans les conditions de la Proposition, supposons que $K(F_1) \cap \ldots \cap K(F_s) \not\subseteq L(F_j)$, et soit $x_1 \in \mathbb{Z}^n$ tel que $F_i(x_1) \leq 0$, pour tout $i \neq j$, alors il existe $x \in M \cap \mathbb{Z}^n$ tel que $\ell(x) = d(\ell(x_1) + d^{O(n)}\ell)$.

Preuve: Si le cône polyhedral $K(F_1) \cap \ldots \cap K(F_s)$ n'est pas contenu dans $L(F_j)$, il existe un générateur u du cône qui n'appartient pas à $L(F_j)$. D'après la démonstration du Théorème de Farkas-Minkowski-Weyl (qui affirme qu'un cône convexe est polyhedral si et seulement si il admet un nombre fini de générateurs; voir par exemple [11], Corollary 7.1.a, ou [10]) et les bornes énoncées dans le Lemme 1, il existe un système de générateurs entier g du cône polyhedral $K(F_1) \cap \ldots \cap K(F_s)$ tel que $\ell(g) = d^{O(n)}.\ell$. Ceci montre qu'on peut choisir $u \in \mathbb{Z}^n - \{0\}$, tel que $\ell(u) = d^{O(n)}.\ell$. Le raisonnement présenté auparavant montre aussi qu'il existe $t \in \mathbb{N}$ tel que $F_j(x_1 + tu) \leq 0$. Un tel t dépend de la taille des coefficients du polynome $F_j(x_1 + Tu)$, c'est-à-dire des coefficients de F_j, de x_1 et de u (voir par exemple [8] pour cette relation). On pose alors: $x := x_1 + tu$, et on obtient $\ell(x) = d(\ell(x_1) + d^{O(n)}\ell)$. ■

Pour compléter la preuve de (i) et (ii) de la Proposi-

tion, on procède par récurrence en travaillant maintenant avec les contraintes F_i, $1 \le i \le s$, $i \neq j$, et en supprimant une à une, dans un certain ordre, toutes les contraintes superflues. On obtient ainsi un ensemble:

$$M' := \left\{ x \in \mathbb{R}^n : F_{i_1}(x) \le 0, \ldots, F_{i_t}(x) \le 0 \right\}$$

de manière que pour tout j, $1 \le j \le t$, $K(F_{i_1}) \cap \ldots \cap K(F_{i_t}) \subseteq L(F_{i_j})$. Cet ensemble vérifie la condition (i) de la Proposition: $M \cap \mathbb{Z}^n \neq \emptyset \iff M' \cap \mathbb{Z}^n \neq \emptyset$

Pour (ii), on a le lemme suivant:

Lemme 3: Soit M' défini comme précédemment, et soit $x' \in M' \cap \mathbb{Z}^n$. Alors, il existe $x \in M \cap \mathbb{Z}^n$ tel que

$$\ell(x) = d^n \cdot \ell(x') + d^{O(n)} \ell$$

(Dans le cas où M' n'est défini par aucune contrainte, on pose $x' := 0$).

Preuve: Supposons sans perte de généralité que pour définir M', on ait supprimé, dans cet ordre, $F_s, F_{s-1}, \ldots, F_{r+1}$ et qu'ainsi. $M' := \left\{ x \in \mathbb{R}^n : F_1(x) \le 0, \ldots, F_r(x) \le 0 \right\}$

Si on appliquait récursivement le résultat du lemme précédent, on obtiendrait l'estimation suivante:

$$\ell(x) \le d^s (\ell(x') + s d^{\alpha(n)} \ell)$$

puisqu'à priori la seule borne sur le nombre de contraintes qu'on supprime est le nombre total s de contraintes. Ceci n'est pas l'estimation désirée étant donné que s apparaît dans l'exposant. Le raisonnement suivant permet de borner le nombre de répétitions de la procédure du Lemme par la dimension n de l'espace ambiant.

Rappelons que si $K \subseteq \mathbb{R}^n$ est un ensemble convexe,

$\dim_{\mathbb{R}} K := \min \left\{ \dim_{\mathbb{R}} L,\ L \text{ sous-espace linéaire de } \mathbb{R}^n \text{ qui contient } K \right\}$

Et par simplicité, définissons:

$$K_{r+1} := K(F_1) \cap \ldots \cap K(F_r) \cap K(F_{r+1})$$

et $K_{r+i} := K_{r+i-1} \cap K(F_{r+i})$, pour tout $i > 1$.

Clairement $K_s \subseteq K_{s-1} \subseteq \ldots \subseteq K_{r+1}$

On considérera en une seule étape tous les ensembles convexes K_{r+i} de même dimension, par exemple, soit:

$$\dim_{\mathbb{R}} K_{r+1} = \ldots = \dim_{\mathbb{R}} K_{r+j} > \dim_{\mathbb{R}} K_{r+j+1} = \ldots$$

Alors, pour tout $1 \leq i \leq j$, le fait qu'on ait supprimé la contrainte F_{r+i} de l'ensemble $\{F_1, \ldots, F_{r+i}\}$ implique que

$$\dim_{\mathbb{R}}(K_{r+1} \cap L(F_{r+i})) < \dim_{\mathbb{R}} K_{r+1} = \ldots = \dim_{\mathbb{R}} K_{r+j} \quad (1 \leq i \leq j)$$

On affirme que dans ce cas on peut choisir $u \neq 0$, $u \in K_{r+j}$ tel que $u \notin L(F_{r+i})$ $(1 \leq i \leq j)$ (c'est-à-dire que la direction u va servir pour supprimer en une fois toutes les contraintes $F_{r+j}, \ldots, F_{r+1}$ de l'ensemble $\{F_1, \ldots, F_{r+j}\}$). Pour cela, on considère un système de générateurs $\mathcal{G}$ du cône polyhédral K_{r+j}, tel que $\ell(\mathcal{G}) = d^{O(n)} \cdot \ell$, et on pose $u := v_1 + \ldots + v_e$, où $\{v_1, \ldots, v_e\} \subseteq \mathcal{G}$ est un système linéairement indépendant maximal de $\mathcal{G}$. La propriété d'"uniformité" des polynômes quasiconvexes permet de montrer l'affirmation, et d'autre part il est clair que $\ell(u) = d^{O(n)} \ell$.

Ce procédé permet de contrôler le nombre de répétitions du lemme par la dimension n de l'espace ambiant, ce qui fournit la borne:

$$\ell(x) = d^n(\ell(x') + n d^{O(n)} \ell) = d^n \ell(x') + d^{O(n)} \ell \qquad \blacksquare$$

Finalement, étant donné que le fait que l'ensemble $M' = \{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \ldots, F_{i_t}(x) \leq 0\}$ ne contienne plus aucune contrainte superflue est équivalent à la condition $K(F_{i_1}) \cap \ldots \cap K(F_{i_t}) = L(F_{i_1}) \cap \ldots \cap L(F_{i_t})$, on achève la preuve de la Proposition à l'aide du lemme suivant:

<u>Lemme 4:</u> Soient $F_{i_1}, \ldots, F_{i_t} \in \mathbb{Z}[X_1, \ldots, X_n]$ quasiconvexes tels que $K(F_{i_1}) \cap \ldots \cap K(F_{i_t}) = L(F_{i_1}) \cap \ldots \cap L(F_{i_t})$, soit $M' = \{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \ldots, F_{i_t}(x) \leq 0\}$ et soit $\ell := \ell(\{F_{i_1}, \ldots, F_{i_t}\})$, alors:

$$M' = V + (M' \cap V^{\perp})$$

où V est un sous-espace linéaire de $\mathbb{R}^n$ qui admet une base $\mathcal{B}$ telle que $\ell(\mathcal{B}) = d^{O(n)}\ell$ et $M' \cap V^{\perp}$ est un sous-ensemble compact de $\mathbb{R}^n$.

Preuve: On définit $V := L(F_{i_1}) \cap \ldots \cap L(F_{i_t})$
Il est clair que V est un sous-espace linéaire de $\mathbb{R}^n$ et on peut facilement en construire une base $\mathcal{B}$ telle que $\ell(\mathcal{B}) = d^{O(n)}\ell$ (en utilisant le fait que chaque $L(F_{i_j})$ admet une base de longueur binaire majorée par $d^{O(n)}\ell$).
Soit maintenant $x \in M'$, il existe une représentation de x de la forme $x = y + u$, où $y \in V^{\perp}$ et $u \in V$.
Alors, $y = x - u \in M'$ (puisque $-u \in V$ et que par la définition de V, $F_{i_k}(x + (-u)) \leq F_{i_k}(x) \leq 0$ $(1 \leq k \leq t)$), c'est-à-dire $x \in (M' \cap V^{\perp}) + V$.
L'inclusion réciproque se montre similairement.
Il suffit de montrer maintenant que l'ensemble $(M' \cap V^{\perp})$ est compact : si l'ensemble fermé et convexe $M' \cap V^{\perp}$ ne l'était pas, il contiendrait une demi-droite $\{x + tu; t \geq 0\}$, où $x \in M' \cap V^{\perp}$ et $u \in \mathbb{R}^n - \{0\}$ (voir par exemple [10]). Ceci entraînerait que la direction u est une direction de récession de $F_{i_1}, \ldots, F_{i_t}$, et ainsi, $u \in V$. D'un autre coté, on obtient que $u \in V^{\perp}$; par conséquent, $u=0$, contradiction. ■ ■

3. La borne semi-algébrique.

En vertu de la Proposition de la section précédente, il suffit, pour conclure la démonstration du Théorème 1, de montrer que si l'ensemble $M' \cap V^{\perp}$ est non vide, alors il contient un point entier x' de longueur binaire $\ell(x') = (sd)^{O(n)}\ell$.

Etant donné que M' se décompose comme somme d'un sous-espace linéaire de $\mathbb{R}^n$ et d'un ensemble compact, nous nous réduirons à la considération d'un ensemble borné, de rayon dépendant de celui du compact, et nous appliquerons ensui-

te les résultats précis de géométrie semi-algébrique de par exemple [12] ou [5] pour borner le rayon du compact.

Sans perte de généralité, on peut supposer dans cette section que $M = \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ ne contient aucune contrainte superflue (dans le sens donné dans la section précédente), ce qui entraîne que $M = V + (M \cap V^\perp)$, où $M \cap V^\perp$ est compact et V linéaire admet une base entiere $\mathcal{B}$ telle que $l(\mathcal{B}) = d^{O(n)} l$.

Observation: Si $M \cap \mathbb{Z}^n$ est non vide, alors M contient un point entier dans l'ensemble $M \cap V^\perp + B$, ou $B := \{\sum_{v \in \mathcal{B}} \beta_v v, 0 \leq \beta_v < 1\}$.

Preuve: Soit $x \in M \cap \mathbb{Z}^n$. On a la décomposition $x = y + u$, $y \in M \cap V^\perp$ et $u \in V$. Soit $\mathcal{B} := \{v_1, \ldots, v_m\}$ la base entière de V et soit $u = \alpha_1 v_1 + \ldots + \alpha_m v_m$ ($\alpha_1, \ldots, \alpha_m \in \mathbb{R}$) la représentation de u dans la base $\mathcal{B}$.
Pour tout $1 \leq i \leq m$, posons:

$$\alpha_i = \lfloor \alpha_i \rfloor + \beta_i \quad \text{où} \quad \lfloor \alpha_i \rfloor \in \mathbb{Z} \quad \text{et} \quad 0 \leq \beta_i < 1$$

et soit $\bar{x} := y + \beta_1 v_1 + \ldots + \beta_m v_m$. Alors $\bar{x} = x - (\lfloor \alpha_1 \rfloor v_1 + \ldots + \lfloor \alpha_m \rfloor v_m) \in \mathbb{Z}^n$. De plus, $\bar{x} \in M + V \subseteq M$; par conséquent, $\bar{x} \in M \cap \mathbb{Z}^n$ et $\bar{x} \in M \cap V^\perp + B$. ∎

Ceci signifie que si l'ensemble $M \cap \mathbb{Z}^n$ est non vide, il contient un point "près" de l'ensemble borné $M \cap V^\perp$. Etant donné que la base $\mathcal{B}$ de V est telle que $l(\mathcal{B}) = d^{O(n)} \cdot l$, pour conclure la démonstration du théorème, il suffit de montrer l'existence d'un rayon $R \in \mathbb{N}$ tel que $M \cap V^\perp \subseteq B(0,R)$ et $l(R) = (sd)^{O(n)} l$.

Lemme 5: $M \cap V^\perp \subseteq B(0,R)$, où $R \in \mathbb{N}$ est tel que $l(R) = (sd)^{O(n)} \cdot l$.

Preuve: L'ensemble semi-algébrique $M \cap V^\perp$ peut être défini à l'aide d'une formule sans quantificateurs du langage de premier ordre de $\mathbb{R}$ à constantes dans $\mathbb{Z}$, dans

laquelle apparaissent les coefficients des polynômes $F_1, \ldots, F_s$ et les équations de $V^{\perp}$. On peut alors décrire l'ensemble semi-algébrique $S := \{\rho \in \mathbb{R} : M \cap V^{\perp} \subseteq B(0,\rho)\}$ par la formule Φ suivante (qui a un seul bloc de quantificateurs):

$$\Phi : \quad (\forall X) \quad (X \in M \cap V^{\perp} \Rightarrow \|X\|^2 \leq \rho^2)$$

où $X := (X_1, \ldots, X_n)$ sont les variables liées de Φ et ρ est la seule variable libre.

Si on applique à Φ l'algorithme rapide d'élimination des quantificateurs pour le cas particulier d'une formule à une variable libre et un bloc de quantificateurs (voir par exemple [12]), on obtient une formule Ψ sans quantificateurs, en la variable ρ, qui décrit exactement l'ensemble S.

Ψ est une disjonction de conjonctions de conditions de signes sur certains polynômes $G_1, \ldots, G_m \in \mathbb{Z}[\rho]$. Etant donné que dans la formule originale Φ tous les paramètres sont de longueur binaire majorée par $d^{O(n)}\ell$ et le nombre et les degrés des polynômes peuvent l'être par s et d respectivement, l'algorithme d'élimination des quantificateurs garantit que ces polynômes $G_1, \ldots, G_m$ vérifient:

$$\deg(G_i) = (sd)^{O(n)} \quad (1 \leq i \leq m) \quad \text{et} \quad \ell(\{G_1, \ldots, G_m\}) = (sd)^{O(n)}\ell$$

De plus, si $\alpha \in \mathbb{R}$ est la plus grande racine réelle qui apparaît dans les polynômes $G_1, \ldots, G_m$, on observe que la formule Ψ est toujours vraie ou toujours fausse dans l'intervalle $]\alpha, +\infty[$ (puisqu'à la droite de α, il n'y a changement de signe d'aucun des polynômes $G_1, \ldots, G_m$). Comme Ψ est vraie pour $+\infty$, Ψ doit être vraie dans l'intervalle $]\alpha, +\infty[$, et par conséquent il suffit de borner la plus grande racine réelle des polynômes $G_1, \ldots, G_m$ pour obtenir le rayon R cherché.

La borne sur les degrés et la longueur binaire des coef-

ficients des polynômes $G_1, \ldots, G_m$ produit directement une borne $R \in \mathbb{N}$ pour leurs racines réelles, telle que $\ell(R) = (sd)^{O(n)}\ell$ (on applique par exemple l'inégalité de Cauchy, [8]).

Ainsi s'achève la preuve du Théorème 1. ■

Preuve du Corollaire - Celle-ci est immédiate puisque, sachant que si l'ensemble $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ est non vide, il contient un point dans la boule $B(0,R)$, où R est tel que $\ell(R) = (sd)^{O(n)}\ell$, il suffit de vérifier si un point entier $x \in \mathbb{Z}^n$, de longueur binaire majorée par cette borne vérifie les conditions $F_1(x) \leq 0, \ldots, F_s(x) \leq 0$ Cela peut bien sûr s'effectuer en temps $(sd)^{O(n)}\ell$, en tenant compte du degré de $F_1, \ldots, F_s$ et de $\ell(\{F_1, \ldots, F_s\})$. (Observons qu'une borne déterministe est de l'ordre de $2^{(sd)^{O(n)}\cdot\ell}$ puisqu'il faut évaluer les polynomes $F_1, \ldots, F_s$ en tous les points entiers de la boule $B(0,R)$). ■

Preuve du Théoreme 2 - On applique ici à nouveau les méthodes utilisées pour montrer le Théoreme 1: suppression des contraintes superflues et réduction à un ensemble compact. Nous ne fournirons pas ici une preuve complète mais simplement une esquisse de la démonstration, nous remettant à [7] pour les détails.

(i) Etant donné que $M \cap \mathbb{Z}^n \neq \emptyset$, il existe $x_0 \in M \cap \mathbb{Z}^n \cap B(0,R)$ où $\ell(R) = (sd)^{O(n)}\ell$ (Théorème 1), et $\ell(F(x_0)) = (sd)^{O(n)}\ell$.

(ii) Etant donné que $m := \inf\{F(x) : x \in M \cap \mathbb{Z}^n\} > -\infty$, $F(x_0) \geq m$, et, par conséquent, si $N := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0, F(x) \leq F(x_0)\}$, $N \cap \mathbb{Z}^n$ est non vide et $m = \inf\{F(x) : x \in M \cap \mathbb{Z}^n\}$.

On procède alors à la suppression des contraintes superflues de la succession $F_1, \ldots, F_s, F-F(x_0)$, de manière à obtenir un ensemble N', défini par éventuellement moins de

contraintes, comme dans la Proposition de la preuve du Théoreme 1. (ii) implique que dans cette procédure, on n'élimine jamais la contrainte $F-F(x_0)$, et par conséquent : $\inf\{F(x): x\in N\cap\mathbb{Z}^n\} = \inf\{F(x): x\in N'\cap\mathbb{Z}^n\}$

Comme auparavant, on a la décomposition:

$$N' = W + (N'\cap W^{\perp})$$

où W est un sous-espace linéaire de $\mathbb{R}^n$, qui admet une base entière $\mathcal{B}$ telle que $\ell(\mathcal{B}) = (sd)^{O(n)}\ell$, et $N'\cap W^{\perp}$ est un sous-ensemble compact de $\mathbb{R}^n$ qui vérifie: $N'\cap W^{\perp}\subseteq B(0,R)$, avec $\ell(R) = (sd)^{O(n)}\ell$.

On montre ensuite que:

$$\inf\{F(x): x\in N'\cap\mathbb{Z}^n\} = \inf\{F(x): x\in (N'\cap W^{\perp}+B)\cap N'\cap\mathbb{Z}^n\}$$

où $B := \{\sum_{v\in\mathcal{B}}\beta_v.v\ ,\ 0\le\beta_v<1\}$

et on achève la démonstration en récupérant à partir du point entier x' de $N'\cap\mathbb{Z}^n$ qui se trouve dans l'ensemble $N'\cap W^{\perp}+B$ et tel que $F(x') = m$, un point entier $x\in M\cap\mathbb{Z}^n$ qui vérifie $\ell(x) = (sd)^{O(n)}\ell$ et $F(x) = m$.

Observons, avant de conclure, que l'hypothèse du théorème, $\inf\{F(x): x\in M\cap\mathbb{Z}^n\} = m > -\infty$ entraîne que le résultat ne fournit pas une procédure de recherche de m, mais il est facile de montrer que dans nos conditions particulières, si $M\cap\mathbb{Z}^n$ est non vide, alors

$$\inf\{F(x): x\in M\cap\mathbb{Z}^n\} > -\infty \iff \inf\{F(x): x\in M\} > -\infty$$

et par conséquent, étant donné qu'on peut vérifier rapidement à l'aide de l'élimination des quantificateurs ([5]) si $\inf\{F(x): x\in M\} > -\infty$, on obtient une procédure de recherche de m. ■

REFERENCES BIBLIOGRAPHIQUES

[1] B.Bank, R.Mandel: Parametric integer optimization. Akademie-Verlag, Berlin (1988).

[2] B.Bank, R.Mandel: (Mixed-) Integer solutions of quasiconvex polynomial inequalities. Mathematical Research Advances in Mathematical Optimization, Akademie-Verlag, Berlin, Vol.45 (1988) 20-34.

[3] J.Heintz, M.-F.Roy, P.Solernó: On the complexity of semialgebraic sets (Extended abstract). Proc. IFIP Congress'89, IX World Computer Congress, North-Holland (1989).

[4] J.Heintz, M.-F.Roy, P.Solernó: Complexité du principe de Tarski-Seidenberg. C.R.Acad.Sci.Paris, t. 309, Série I (1989) 825-830.

[5] J.Heintz, M.-F.Roy, P.Solernó: Sur la complexité du principe de Tarski-Seidenberg. A paraître dans Bull.Soc.Math.France (1990).

[6] L.G.Khachiyan: Convexity and complexity in polynomial programming. Proc.Int.Congress Math., Varsovie (1983).

[7] T.Krick: Complejidad para problemas de geometría elemental. Thèse, Université de Buenos Aires (1990)

[8] M.Mignotte: Some useful bounds. Computer Algebra (Symbolic and Algebraic Computation). Springer-Verlag (1982) 259-264.

[9] J.Renegar: On the computational complexity and geometry of the first order theory of the reals. Part III. Quantifier elimination. Technical Report 856, Cornell University (1989).

[10] R.T.Rockafellar: Convex Analysis. Princeton Mathematical Series n°28 (1970).

[11] A.Schrijver: Theory of linear and integer programming. Wiley Interscience Series in Discrete Mathematics (1989).

[12] P.Solernó: Complejidad de conjuntos semialgebraicos. Thèse, Université de Buenos Aires (1989).

[13] S.P.Tarasov, L.G.Khachiyan: Bounds of solutions and algorithmic complexity of systems of convex diophantine inequalities. Soviet.Math.Adel., vol. 22, n°3 (1980).

THE FUNCTIONAL DECOMPOSITION OF POLYNOMIALS

JAIME GUTIERREZ
Departamento de Matemáticas, Estadística y Computación.
Facultad de Ciencias, Universidad de Cantabria, 39071-Santander, Spain
E-mail: gutierrez@ccucvx.unican.es

§.1 INTRODUCTION

If F is a field and $g(X),h(X)\in F[X]$, then $f(X)=g(X)\circ h(X)= g(h(X))\in F[X]$ is their (functional) composition, and $(g(X),h(X))$ is a functional decomposition of $f(X)$. Given $f(X)\in F[X]$, there exists a complete decomposition in the form:

$f(X)=f_1(X)\circ f_2(X)\circ.....\circ f_r(X)$, where "$\circ$" denotes substitution of polynomials and $f_i(X)$ are indecomposable polynomials over F[X], see *Pilz* .

The functional decomposition problem over F[X] can be stated as follows: given $f(X)\in F[X]$ of degree n=rs, to determine whether there exist $g(X),h(X)\in F[X]$ of degrees r,s respectively, such that $f(X)=g(X)\circ h(X)=g(h(X))$ and, in the affirmative case, to compute them. For some time, this problem was considered to be *computationally hard*, but since 1986 there are several polynomial-time algorithms working in the "tame" case, i.e. when the characteristic of F does not divide r, (see *Kozen & Landau* presented the first polynomial-time algorithm, in 1986, *Gathen el al.* , *Gutiérrez el al.*).

Regarding extensions of this important problem, recently *Kozen & Landau* have found (in the tame case) a solution when the polynomial f(X) has coefficients in a commutative ring, but assuming that the polynomials involved are monic.

On the other hand several generalizations of the decomposition problem have been posed for multivariate polynomials. *Barton & Zippel* proposes the following: given a polynomial $f(\underline{X})\in F[X_1,..,X_n]$ they wish to know if there exist a $g(\underline{Y})\in F[Y_1,..,Y_m]$ and $h_1(\underline{X}),..., h_m(\underline{X})\in F[X_1,..,X_n]$ such that:

$f(X_1,...,X_n)=g(h_1(\underline{X}),...,h_m(\underline{X}))$. This seems more difficult than the decomposition of univariate polynomials; but even partial solutions would be an aid to algebraic simplification and evaluation problemns. *Gathen* and *Dickerson* solve the following problem: given $f(X) \in F[X_1,...,X_m]$ of (total) degree n=rs, and r not divisible by the characteristic of the field F, to determine when there exist $g(X)\in F[X]$ and $h(X)\in F[X_1,.....,X_m]$ of degrees r,s respectively, such that $f(X_1,...,X_m)=g(h(X_1,...,X_m))$ and, in the affirmative case, to compute them. *Dickerson* presented the first polynomial-time algorithm in 1987 and *Gathen* (1990) presented a conceptually simple Newton approach that yields polynomial-time algorithms for densely presented inputs, and random

polynomial time for imputs given by arithmetic circuits.

Now, we remark that solving *in all generality* the problem of decomposition of polynomials in one vari able over a factorial domain will imply the solution of the decomposition problem forpolynomiials in several variables over a field, in a sense different to the one above stated by *Gathen*, namely, considering the given polynomial as a polynomial having as coefficients polynomials in one less variable and proceeding to an iterative decomposition, once an ordering has been choosen in the variable (c.f.Definition 2.1 below). Moreover, every decomposition in the sense of *Gathen* is also a decomposition in the new sense of definition 2.1, but no conversely, as shown by the following example:

$f(X,Y) = ((X^3+1)Y^2+ 2XY+ X^2+1)\circ(Y^2+Y+X) =$

$= (X^3+1)(Y^2+Y+X)^2 + 2X(Y^2+Y+X)+ X^2+1$

is a decomposition in our sense but the polynomial f(X,Y) is "indecomposable" according to Gathen's criterion. The solution of the decomposition problem for factorial domains is precisely the content of §3 of this paper. Besides we survey bri efly the algorithm of *Gutiérrez & Ruiz de Velasco* working in a field F; we also study and solve the more general problem of finding (and defining) a complete decomposition in indecomposable elements, stating some uniqueness results concerning this decomposition. As a consequence we can recover *Gathen's* decomposition and clarify also some of the concepts of *Kozen & Landau* with regard to complete decompositions (which were obscure to us as they were stated over non neccessarily integrity domains, see Remark 2.3).

In section 4 we coment very briefly some applications of the functional decomposition of polynomials.

§2 SOME GENERAL CONCEPTS AND RESULTS

Let R be a commutative ring with identity. It is very useful, in order to work with the functional decomposition of polynomials to consider the near-ring $(R[X],+,\circ)$, see *Pilz* . If R is a domain the units in the near-ring R[X] are the linear polynomials aX+b, where a is an unit. As usual $R_0[X]$ will denote the set of all polynomials over R whose constant term is zero, that is

$$R_0[X] := \{f(X)\in R[X] \,/\, f(X)\circ 0 = f(0) = 0\}.$$

$R_0[X]$ is a subnear-ring and agrees with the zero-symmetric part of R[X].

Given a polynomial f(X), we denote the degree of f(X) by deg(f(X)).

Firstly, we need some definitions.

Definitions 2.1. As in ring theory, we say that an element $f(X)\in R[X]$ is *indecomposable* provided that :

i) f(X) is non-constant and non-unit

ii) $f(X)= g(X)\circ h(X)$, $(g(X),h(X)\in R[X])$ implies g(X) or h(X) is an unit.

Otherwise we say f(X) is *decomposable*.

Of course, if R=F a field, then $f(X) \in F[X]$, non-zero and non-unit is indecomposable if and only if $f(X)=g(X) \circ h(X)$, implies $\deg(g(X))=\deg(f(X))$ or $\deg(h(X))=\deg(f(X))$.

A *decomposition* of f(X) is a set of polynomials $f_1(X), f_2(X), \ldots, f_r(X) \in R[X]$ such that: $f(X) = f_1(X) \circ f_2(X) \circ \ldots \circ f_r(X)$.

The $f_i(X)$ are componentes of the decomposition. If R is a domain the product of the degrees of the $f_i(X)$ is the degree of f(X).

A *complete decomposition* is one where all the $f_i(X)$ are indecomposable. ♦.

Remark 2.2.

If D=F is a field, every polynomial f(X) has complete decomposition in F[X], with a strong uniqueness property :

First of all, given a polynomial f(X) over any field, with n=deg(f(X)) prime to the characteristic (therefore without any restriction if the characteristic is zero) in order to find a decomposition of f(X) we can assume that f(X) is monic and n>1, let say

$$f(X) = X^n + A^0_1 X^{n-1} + A^0_2 X^{n-2} + \ldots\ldots + A^0_i X^{n-i} + \ldots + A^0_{n-1} X + A^0_n$$

Then we are going to find indecomposable polynomials $g_1(X), g_2(X), \ldots\ldots, g_r(X)$ of degree > 1 such that:

(a) $f(X) = g_1(X) \circ g_2(X) \circ \ldots \circ g_r(X)$.

(b) $g_i(X)$ are monic polynomials for all i .

(c) $g_i(X) \in K_0[X]$ for $i = 2, \ldots\ldots, r$.

The main step is to find a polynomial h(X) and verifiying $f(X)=g(X) \circ h(X)$ for some polynomial g(X). Then we compute g(X) and proceed recursively.

Let m be a strict divisor of n and let h(X),

$h(X) = X^m + b_1 X^{m-1} + b_2 X^{m-2} + \ldots\ldots\ldots + b_{m-1} X \in F_0[X]$, then h(X) a good candidate for the decomposition of f(X) if and only if the remainders of the h(X)-adic divisions of f(X) in h(X) are constant elements of F, that is

$$\begin{aligned} f(X) &= q_1(X)\, h(X) + r_0(X) \\ q_1(X) &= q_2(X)\, h(X) + r_1(X) \\ &\vdots \\ q_{t-1}(X) &= q_t(X)\, h(X) + r_{t-1}(X) \\ q_t(X) &= 0 \,.\, h(X) + r_t(X). \end{aligned}$$

where tm=n and therfore $q_t(X) = 1$. Note that if h(X) is a good candidate for the decomposition of f(X) then the sequence of h(X)-adic divisions compute the coefficients r_i of g(X) ($r_i(X) = r_i =$

$q_i(0)$) such that $f(X) = g(X) \circ h(X)$, where tm=n and therfore $q_t(X) = 1$ and $r_{t-1}(X)$ must be constant. Imposing this last condition we obtain a system of equations in the b_i's. Actually (see the proof *Gutiérrez & Ruiz de Velasco* if

$q_k(X) = X^{n-km} + A^k{}_1 X^{n-km-1} + ... + A^k{}_i X^{n-km-i} + ... + A^k{}_{m-1} X^{n-km-(m-1)} + ...$ for all k then

$$b_1 = (A^0{}_1)/t$$

$$A^k{}_1 = A^{k-1}{}_1 - b_1 \text{ for all k} \qquad \text{and}$$

$$C_1 = A^1{}_1 + A^2{}_1 + ... + A^{t-1}{}_1$$

Moreover

$$b_2 = (A^0{}_2 - b_1 C_1)/t$$

$$A^k{}_2 = A^{k-1}{}_2 - b_1 A^k{}_1 - b_2 \text{ for all k} \qquad \text{and}$$

$$C_2 = A^1{}_2 + A^2{}_2 + ... + A^{t-1}{}_2$$

and so on until b_{m-1} is computed. The complexity is $O(n^{2+\delta})$, where δ is an arbitrary small positive constant (see Gutiérrez et al (1988).

Finally we note assuming that h(X) is monic and h(0)=0, then h(X) is unique, (see *Gutiérrez & Ruiz de Velasco* or *Gathen*) . ♦.

Remark 2.3. *Kozen & Landau* give a "similarity" definition for an arbitrary commutative ring but this one does not agree with Definition 2.1 when D is not an integral domain. In fact, if we take as $R=Z_4$, the ring of integers modulo 4: then

$$2X^4+X^3 = X^3 \circ (2X^2+X)$$

is a complete decomposition ("tame case") in the sense *Kozen & Landau*, but notice that is not a complete decomposition as definition 2.1, because $2X^2+X$ is an unit in the near-ring $Z_4[X]$:

$$X = (2X^2+X) \circ (2X^2+X)$$

Nevertheless *Kozen & Landau's* proof of their decomposition theorem over monic polynomials seems to use implicitly a concept of decomposable element that agrees with our Definition 2.1. ♦.

§.3 DE COMPOSITION OVER FACTORIAL DOMAINS

In this section we prove our main result, i.e. that if D is factorial domain, then every polynomial in D[X] has a complete decomposition. Throughout this paper, we denote by D an unique factorization domain and by F its field of fractions.

In order to get a complete decomposition of f(X), we can assume -without loss of generality- that f(X) is in $D_0[X]$; in fact, $f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 =$

$(X+a_0)\circ(a_nX^n+a_{n-1}X^{n-1}+.....+a_1X)$ is indecomposable if and only if

$a_nX^n+ a_{n-1}X^{n-1} +.....+ a_1X$ is indecomposable.

The key lemma for proving the complete decomposition of f(X) is:

Lemma 3.1. Let $g(X),h(X)\in D_0[X]$ be primitive polynomials, then their composition is primitive.

Proof. Suppose $g(X),h(X)\in D_0[X]$ are primitive but $f(X)=g(X)\circ h(X)$ is not. Then there exist an irreducible element $p\in D$ such that p does not divide g(X) and h(X) but p divide f(X). We consider the domain $\underline{D} = D_{/(p)}$. We now apply the composition ring homomorphism (i.e. ring and near-ring homomorphism) see *Pilz & So*) of D[X] onto $\underline{D}[X]$. We arrive to a contradiction with the fact that if D is a domain and g(X) and h(X) are polynomials in D[X] with positive degree then $g(X)\circ h(X)$ is a polynomial with positive degree. ♦

Theorem 3.2. If $f(X)\in D_0[X]$ is primitive then f(X) is indecomposable in D[X] iff f(X) is indecomposable in F[X].

Proof. Suppose that f(X) is decomposable in F[X]: $f(X)=g(X)\circ h(X)$ where $g(X),h(X)\in F[X]$ and $\deg(g(X))>1$, $\deg(h(X))>1$. We can find $a\in F$ such that:

$f(X)= aX \circ g'(X) \circ h'(X)$ with $h'(X),g'(X)\in D[X]$ primitives. Using the lemma, we have $a\in D$ and hence f(X) is decomposable in D[X]. Conversely, if f(X) is indecomposable in F[X] but f(X) decomposable in D[X], then $f(X)=l(X)\circ h(X)$ or $f(X)=g(X)\circ m(X)$ where $\deg(l(X))=\deg(m(X))=1$ and l(X), m(X) are not units in the near-ring D[X]. If $f(X) =(aX+b)\circ h(X)$, we observe that a divides f(X). Likewise we proceed in the case $f(X)= g(X)\circ m(X)$. ♦

Proposition. 3.3. The subnear-ring $RX:=\{rX/r\in R\}$ is isomorphic to ring R.

Proof. The map $rX \to r$ is a ring isomorphism . ♦

An immediate consequence of Theorem 3.2 and Proposition 3.3 is the complete decomposition:

Corollary 3.4. Given $f(X)\in D[X]$ non-constant, there exist indecomposable polynomials $f_1(X),f_2(X),....,f_r(X)\in D[X]$ such that: $f(X) = f_1(X)\circ f_2(X)\circ....\circ f_r(X)$. ♦

Remark. 3.5. To determine a complete decomposition of a polynomial f(X) over a

domain R, we observe that the assumption "R factorial domain" can not be omitted as shows Proposition 3.3 ♦.

Algorithm 3.6.

Input: $f(X)=a_nX^n+a_{n-1}X^{n-1}+.....+a_1X+a_0 \in D[X]$ of degree n=rs, and r not divisible by the characteristic of D.

Output: $g(X),h(X)\in D[X]$ with $f(X)=g(X)\circ h(X)$ and $\deg(g(X))=r$, if such a decomposition exits; and "*no decomposition*" otherwise.

A.1. Find $\alpha,\beta\in D$ such that $f(X)= (\alpha X+\beta)\circ f'(X)$ where f'(X) is primitive. Take $\alpha = G.c.d(a_n,a_{n-1},.....,a_1)$, $\beta= a_0$.

A.2. Use the standard algorithm decomposition over F[X], with input f'(X). If no decomposition of f'(X) in F[X] exist, return "no decomposition".

If $f'(X)=g'(X)\circ h'(X)$ is returned with $h'(X)\in F_0[X]$ and monic,

$h'(X)= X^s + (b_{s-1}/c_{s-1})X^{s-1}+.....+(b_1/c_1)X$, return

$g(X)= (\alpha X+\beta)\circ g'(X)\circ(1/\delta)X$ and $h(X)= \delta X \circ h'(X)$, where

$\delta= L.c.m.(c_{s-1}, c_{s-2},.....,c_1)$.

Using Lemma 3.1 and Theorem 3.2 we see that the algorithm correctly determines whether $f(X)\in D[X]$ has a decomposition with the required degrees, and if so, computes a decomposition.

If we suppose that G.c.d.(deg(f(X)),characteristic(D))=1, since the number of divisors of deg(f(X) is finite and using Proposition 3.3, we obtain an algorithm to decompose f(X) into indecomposable polynomials. ♦.

We end with some interesting results about the "uniqueness" of a decomposition of f(X).

Corollary 3.7. Let $f(X)\in D[X]$ be of degree n=rs; with G.c.d.(deg(f(X)), char(D))=1. The following holds:

(i) If $f(X)=g(X)\circ h(X)=g'(X)\circ h'(X)$ with $\deg(h(X))=\deg(h'(X))=r$ and $h(X),h'(X)\in D_0[X]$, then h(X) and h'(X) are associated in F[X]. In particular, if they are indecomposable polynomials, then they are associated in D[X].

(ii) Let $f(X)=m_1(X)\circ m_2(X)\circ...\circ m_r(X)\circ g_1(X)\circ g_2(X)\circ...\circ g_u(X)$ and

$f(X)=n_1(X)\circ n_2(X)\circ...\circ n_s(X)\circ h_1(X)\circ h_2(X)\circ...\circ h_v(X)$ are

two complete decomposition of f(X) with $\deg(m_i(X))=\deg(n_i(X))=1$ and $\deg(g_j(X))>1$, $\deg(h_j(X)>1$, then,

$m_1(X)\circ m_2(X)\circ....\circ m_r(X)=n_1(X)\circ n_2(X)\circ....\circ n_s(X)$ and r=s. Moreover,

$g_1(X)\circ g_2(X)\circ....\circ g_u(X) = h_1(X)\circ h_2(X)\circ....\circ h_v(X)$, u=v and the sequences $<\deg(g_j(X))>$, $<\deg(h_j(X))>$ are permutations of each other.

Proof. (i) It is a consequence of a strong uniqueness property (see *Gutiérrez & Ruiz de Velasco or Gathen*) and the algorithm.

(ii) Use Theorem 3.2. and the results about the "uniqueness" of a decomposition of a polynomial over a field, see *Schinzel* . ♦

More results about the "uniqueness" of a decomposition of polynomials over a field appear in the book of *Schinzel.*

§ 4. APPLICATIONS.

Solving polynomial equations 4.1.

Let f(X) be a decomposable polynomial, $f(X) = g(X) \circ h(X)$. Then to compute the zeroes of f(X), first compute those of g(X), z_i; so the zeroes of f(X) are the zeroes of the polynomials

$h_i(X) = h(X) - z_i$. For example, the polynomial $f(X) \in Q[X]$

$f(X)= X^{12} +3X^{11}+ 3X^{10} - 5X^9 - 12X^8 - 6X^7 +12X^6 +12X^5 - X^4 - 9X^3 +2X + 5$, is an irreducible polynomial over the rational integers, but

$f(X) = (X^3 - X + 5) \circ (X^4 + X^3 - 2X)$.

So we have reduced the problem to compute the zeroes of an irreducible polynomial of degree 12 to compute the zeroes the polynomials of degree 3 and 4. Of course f(X) is a polynomial resoluble by radicals.

The operator SOLVE in the REDUCE System does not give any solution for $f(X)= X^{12} +3X^{11}+ 3X^{10} - 5X^9 - 12X^8 - 6X^7 +12X^6 +12X^5 - X^4 - 9X^3 +2X + 5$, but it resolves the equation by appliying the above comment. ♦.

Determining polynomial factors 4.2.

(i) Let $f(X) \in F[X]$ such that Xf(X) is a decomposable polynomial, then f(X) is a reducible polynomial.

We have $Xf(X) = g(X) \circ h(X)$, then

$Xf(X) = c_0h(X)^t + c_1h(X)^{t-1} + c_2h(X)^{t-2} +.....+ c_{t-1}h(X)$, so h(X) is a factor of Xf(X) and since $\deg(h(X)) > 2$ we can get (trivialy) a factor of f(X).

(ii) Let $f(X) \in F[X]$, such that a primitive g(X) of f(X) (i.e. $g'(X) = f(X)$, $g'(X)$ is the

formal derivative of f(X)) is a decomposable polynomial, then f(X) is a reducible polynomial.

We have $g(X) = g(X) \circ h(X)$, applingthe properties of the formal derivate, $f(X) = (g'(X) \circ h(X)) h'(X)$, since $\deg(h'(X)) \geq 1$, $h'(X)$ is a factor of f(X).

(iii) Finally, to determine when the polynomial $(f(X) - f(Y))_{/(X-Y)} \in F[X,Y]$ is a reducible polynomial. (See *Fried*) ♦.

The N-Partition Problem 4.3.

There is a similar application of polynomial decomposition to the n-partition problem. Given a set $A=\{a_1,..., a_{mn}\}$ and a rational-valued function $q: A \rightarrow Q$, we want to compute a partition of A into m disjoints subsets $B_1,...., B_m$ of of n elements each such that for $1 \leq i \leq m$ we have:

$$\sum_{a_j \in B_i} q(a_j) = \frac{1}{m} \sum_{a_j \in A} q(a_j)$$

In certain instances, we can use polynomial decomposition to solve this problem:
we construct the polynomial f(X) as follows:

$$f(X) = \prod_{i=1}^{mn} (X - q(a_i)).$$

Assume that f(X) has a decomposition $f(X) = g(X) \circ h(X)$, with $\deg(g(X))=m$ and $\deg(h(X))=n$ and let g(X) factor in an extension of Q as:

$$g(X) = \prod_{i=1}^{m} (X - \beta_i).$$

Then

$$f(X) = g(h(X)) = \prod_{i=1}^{m} (h(X) - \beta_i).$$

It follows that the roots of the $h(X)-\beta_i$ give us the values of an n-partitioning of A (for details see *Dikerson(1989)*. ♦.

Permutation polynomials 4.4.

In this section we consider polynominals f(X) with coefficients over a finite field $\mathbb{F}_q$ of order $q=p^{\alpha}$ where p is a prime number and $\alpha \geq 1$, then f(X) is called permutation polynomial of $\mathbb{F}_q$ if the associatedpolynomial function from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Permutation polynomials have been studied since *Hermite* and *Dickson* , and recent interest stems from possible applications in public-key crytography (see *Lidl & Mullen*). A very good sumary concerning with permutation polynomials of $\mathbb{F}_q$ is Lidl& Niederreiter. In their survey paper, *Lidl & Mullen* pose as an open problems:

P2. Find new classes of permutation polynomials.

P3. Find news classes of permutation polynomials that are useful crytographically.
Our question is:

characterize polynomials $h(X) \in \mathbb{F}_q[X]$ such that $X + ((X^q - X)h(X)$ is decomposable. So we obtain permutation polynomials and its inverse. ♦.

Endormorphism Invertibility 4.5.

This last application of multivariate polynomial decomposition is to the problem of endomorphism invertibility:

Given $\sigma \in End_F F[X_1,..,X_n]$, determine if σ is invertible, and if it is, compute its inverse.

Let σ be an automorphism definided as follows:

$$\sigma(X_i) \rightarrow h_i(X_1,..,X_n).$$

Suppose the inverse of s is given by:

$$\sigma^{-1}(X_i) \rightarrow g_i(X_1,..,X_n) \quad \text{where}$$

$$X_i = g_i(\, h_1(X_1,..,X_n),.....,h_n(X_1,..,X_n)) \text{ for all i. } \blacklozenge.$$

Finally we only want to remark that the algorithms presented here - for one a multivariate case - are implemented in REDUCE and they are avalaible upon request.

References

[1] Barton, R. & Zippel, R.: *Polynomial Decomposition algorithms.* J.Symbolic Computation 1, 159-168 (1985)

[2] Dickerson, M.: *Polynomial decomposition algorithms for multivariate polynomials.* Tech. Rep. 87-826, Dep. of Computer Science, Cornell University, Ithaca NY (1987)

[3] Dickerson, M.: *The Functional Decompositttion of Polynomials.* Tech. Rep. 89-1023, Dep. of Computer Science, Cornell University, Ithaca NY (1989)

[4] Dickson,L.E. *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group.* Ann. of Math.11, 65-120,161-183 (1897)

[5] Fried, M D. (1970). *On a conjeture of Schur.* Michigan Mth. J. 17, 41-50.

[6] Gathen, J. von zur.: *Functional decomposition of polynomials: the tame case.* Tech. Rep. 13/1987, SFB 124, Universität Saarbrücken (1987) J. Symbolic Computation 9, 281-299 (1990)

[7] Gathen,J.von zur&Kozen,D.&Landau,S.: *Functional decomposition of*

polynomials. Proc. 28th Ann. IEEE Symp.Found. Comp. Sci.,127-131 (1987)

[8] Gutiérrez, J.&Ruiz de Velasco,C.: *A polynomial decomposition algorithm*. Proc. of II SBWAG. Alxebra, 54 , 75-91(1989)

[9] Gutiérrez, J. & Recio, T. & Ruiz de Velasco, C.: *Polynomial decomposition algorithm of almost quadratic complexity*. Proc. of AAECC-6 (1988) L.N.Comp. Science, 357. Springer-Verlag,471-476(1989)

[10] Hermite,C.: Sur les fonctions de sept lettres. C.R. Acad. Sci. Paris 57, 750-757(1863)

[11] Kozen, D. & Landau, S.: *Polynomial Decomposition Algorithms*. .Tech. Rep. 86-773, Dep. of Computer Science, Cornell University, Ithaca NY(1986). J. Symbolic Computation 7, 445-456 (1989)

[12] Lidl,R.&Mullen,G.L.: When Does a Polynomial over a Finite Permute the elements of the Field ?. Amer. Math. Monthly, 95, 243-246 (1988)

[13] Lidl,R.&Niederreiter,H.: Finite Fields. Encyclopedia Meth. Appl. Vol 20, Addison-Wesley ReadingMA, (now distributed by Cambridge Univ. Press) (1983)

[14] Pilz, G.:*Near-Rings*. 2nd revised Ed. Amsterdam, North- Holland Pub. Co. (1983)

[15] Pilz, G. & So, Y-S.: *Near-rings of polynomials and polynomials functions*. J. Austral. Math. Soc.(Series A) 29,61-70 (1980)

[16] Schinzel, A.: *Selected Topics on polynomials*. Ann. Arbor, University of Michigan Press, (1982).

A COMBINATORIAL GEOMETRIC STRUCTURE ON THE SPACE OF ORDERS OF A FIELD

M. A. Dickmann

CNRS – Université Paris VII

Note. This is a draft of the introduction to a paper in preparation under the title above. Even at this early stage, it may be useful to some readers, insofar the underlying intuitions and many of the ideas are explained in detail; we include exact statements of the main results, but proofs are omitted. □

Notation.

— A total order $\leq$ on a field K is identified with its positive cone: $P = \{x \in K \mid x \geq 0\}$.

— $\chi(K)$ denotes the set of all (total) orders on the field K. In using this notation we do assume that the field K is formally real (= orderable; abbreviated, *f.r.*), whence the set $\chi(K)$ is non–empty.

INTRODUCTION.

In the extensive literature on formally real fields the set $\chi(K)$ has hitherto been considered as a topological space, endowed with the so–called Harrison topology generated by the family of sets

$$H_K(a_1,\dots,a_n) = \{P \in \chi(K) \mid a_1,\dots,a_n \in P\} ,$$

for all finite sequences $a_1,\dots, a_n \in K$, as a base of open (in fact, clopen) sets.

The purpose of this paper is to introduce another —combinatorial— way of looking at $\chi(K)$ and develop at some length the ensuing theory. This yields many new (and, we hope, interesting) results, but a part of our task consists also in recasting in terms of the new concepts a part of the existing theory; the most fruitful aspects of this reinterpretation lie in the link with the combinatorial theory of quadratic forms, developed essentially by Marshall and Bröcker (see [8], [9], [10], [11], [2], [3]).

An informal notion of an "independent" set of orders has been around for some time, specially in some papers by Bröcker, see [2; p. 149]. However, this notion never was used as any more than a terminology. It never was the object of systematic investigation using the concepts and tools of the theory where it belongs, namely the theory of matroids. The idea of checking whether this vague notion of independence —or rather the corresponding notion of closure— did satisfy the matroid axioms occurred to me in November 1988. The immediate positive answer provided the impetus to continue (in particular, to become familiar with the theory of matroids). In a few months I essentially had the contents of §§ 1, 2 and one–half of § 3 below. The link with the work of Marshall contained in § 5 came later, in December 1989, after a conversation with E. Becker. The results of § 4 and its appendix, giving a geometric interpretation to, and generalizing the Baer–Krull theorem were obtained in the spring and summer of 1990.

Since most likely only few readers will be familiar with both sides of the link established in this paper, I have decided to precede it by a lengthy and somewhat leisurely introduction, intended to anchor the intuitions behind the main notions and results.

In § 1 we introduce the closure operator on $\chi(K)$ and show that it satisfies the axioms for a combinatorial geometry. Further, we show it verifies rather special axioms such as:

(i) "Lines consist of two points",

as well as the following properties, particularly significant when $\chi(K)$ is infinite, a case which by no means we want to exclude:

(ii) "A point in the closure of a set is in the closure of some finite subset",

(iii) (Local finiteness) "The closure of a finite set is finite".

Moreover, it is easily checked that the closure of an n–element set has cardinality $\leq 2^{n-1}$. The possible cardinalities that the closure of a finite set may take on have been determined, as a function of its rank, by Bröcker [3].

Next, a well–known theorem of Bröcker (cf. Lam [6; Thm. 10.5]) is used to characterize the free matroids (i.e., those whose closure operator is trivial) of type $\chi(K)$ in terms of the field K :

Theorem 1. *$\chi(K)$ is a free matroid iff the field K has the strong approximation property (SAP).* □

With these basic facts established, the first question which comes to mind is: in which of the best known classes of matroids considered by combinatorists do the geometries $\chi(K)$ lie? We give a very satisfactory answer to this question in § 2 :

Theorem 2. *For every (f.r.) field K, the matroid $\chi(K)$ is binary.* □

Here $\chi(K)$ may be infinite (in which case the representing vector space over $\mathbb{Z}_2$ is infinite–dimensional). This result is proved in two steps:

— Firstly, if $M = \chi(K)$ is finite (or, more generally, M is a finite flat of $\chi(K)$), we use the following well–known criterion (cf. White [14; Thm. 2.2.1(8)]) : a (finite) matroid is binary iff no coline (= flat of corank 2) is contained in four or more hyperplanes (= flats of corank 1). The verification of this criterion is carried out by means of "dual basis" elements.

— Secondly, in order to pass from the finite to the infinite case, we use an ultraproduct construction to put together the binary representations of finite flats of $\chi(K)$ given by the previous step.

The existence of an obvious map

$$\chi(K) \longrightarrow \mathrm{Hom}(K^\times/_{\Sigma K^{\times 2}},\ \mathbb{Z}_2)$$

$$P \longrightarrow \mathrm{sgn}_P$$

where sgn_P is induced by the characteristic function of P, raises the question whether this is a matroid representation of $\chi(K)$ into the dual of the $\mathbb{Z}_2$–vector space $K^\times/_{\Sigma K^{\times 2}}$. We show that this is actually the case.

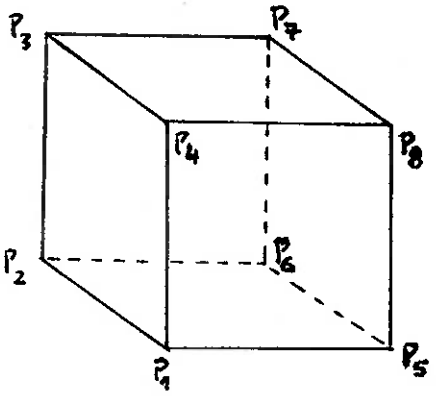
One way or another, the preceding theorem gives an invaluable piece of information, from a conceptual point of view, at this stage. Another important result is proved by the same type of "dual base" argument as in the previous theorem, namely:

Theorem 3. *Every circuit of $\chi(K)$ has even cardinality.* □

(Matroids with this property are called bipartite. A circuit is a minimal dependent set.) Notice that the results mentioned above show that circuits are finite (cf. (ii)), of cardinality ≥ 4 (since any three elements are independent, by (i)). A corollary of Theorem 3 is that finite spaces of orders of the form $\chi(K)$ have a coordinatization by odd vectors of $\mathbb{Z}_2^n$, that is, vectors with an odd number of non–zero coordinates.

Once we know that the matroids $\chi(K)$ are binary, the next basic question suggested by matroid theory is : which of them are unimodular ?. A point of caution is in order here: what do we mean by a unimodular, possibly infinite, matroid ?. We shall take it to mean that *every finite flat is unimodular* in the usual sense.

In fact, there is a simple example of a non–unimodular matroid $\chi(K)$, namely for $K = \mathbb{R}(X, Y, Z)$. This is shown as follows ; since it is known how all orders of a rational function field $k(X)$ which extend a given order of k are constructed (cf., f. ex., Dickmann [5; Ch. I, § 5]), by placing the elements $X, Y, Z,$ in suitable positions with respect to one another, we construct eight orders $P_1,\ldots,P_8$ of $\mathbb{R}(X, Y, Z)$ whose dependencies can be explicitly computed. The resulting configuration is a three–dimensional cube (= 3–dimensional affine space) over $\mathbb{Z}_2$:



The presence of this configuration as a minor in $\chi(\mathbb{R}(X, Y, Z))$ makes it non–unimodular, by Tutte's famous excluded minor characterization of unimodular (binary) matroids : Fano's plane $\mathbb{F}$ is obtained from the cube by contraction of any (one) vertex, and its dual, $\mathbb{F}^*$, by deletion. (If the presence of many other orders in $\mathbb{R}(X, Y, Z)$ bothers you, consider instead the formal power series field $\mathbb{R}((X))((Y))((Z))$, which only has eight orders.)

Which is, then, an example (at least a non–trivial one) of a field K so that $\chi(K)$ is unimodular?. Familiarity with the example above shows that the argument proving non–unimodularity depends essentially on having three variables, since the cube has rank four; it breaks down for $\mathbb{R}(X, Y)$. Another candidate is $\mathbb{Q}(X)$. (We exclude $\mathbb{R}(X)$ since it is unimodular for trivial reasons: it is SAP and hence its closure operator is trivial.)

Before explaining the general solution to this problem, let us take a further look at the cube above. Such a configuration is an example of a notion crucial in quadratic form theory: that of a fan. This notion is defined as follows:

Definition. Let K be a f.r. field. A fan of K is a preorder T such that any multiplicative subgroup S of $K^\times$ so that $T \subseteq S$, $[K^\times : S] = 2$, and $-1 \notin S$, is an order. □

The following characterization of fans brings us to our point:

Proposition (Bröcker [2; p. 149, (a)]). *A preorder T of K is a fan iff for every three different orders P_0, P_1, P_2 containing T, the closure $cl_K(\{P_0, P_1, P_2\})$ has cardinality four (this is the largest cardinality it can have).* □

In this case, $cl_K(P_0, P_1, P_2)$ is necessarily a four–element circuit of $\chi(K)$. In our geometric language it is more telling to redefine this notion as follows: a subset $\mathfrak{F} \subseteq \chi(K)$ is a fan iff any three distinct elements of $\mathfrak{F}$ are contained in a four–point circuit contained in $\mathfrak{F}$.

It is an easy matter to show that there is a unique fan of rank n for every integer $n \geq 1$; it has 2^n elements. In terms of the coordinatization by odd vectors mentioned above, the fan of rank n is exactly the geometry of all odd vectors of $\mathbb{Z}_2^n$. Concrete examples: (i) If K is a field with a unique order, then the fan of rank $n \geq 2$ is isomorphic to the matroid $\chi(K((X_1,...,X_{n-1})))$. (ii) If L is a Rolle field with 2^n orders, $\chi(L)$ is the fan of rank $n+1$. Lam [7; Ch. 5] contains a comprehensive analysis of fans (in their disguise as preorders) and their role in quadratic form theory.

Returning to the problem of characterizing the fields K such that $\chi(K)$ is unimodular, we obtain a very satisfactory solution in terms of the so–called stability index of K, a magnitude considered in quadratic form theory, the meaning of which we explain below:

Theorem 4. *Let K be a f.r. field. Then $\chi(K)$ is unimodular iff the reduced stability index of K is at most 2.* □

One–half of the proof, the implication $(\Leftarrow)$, is based on Bröcker's local–global principle for stability indices [1; Thm. 3.19], which reduces the question to an analysis of the structure of the order spaces $\chi(\overline{K_v})$ of the residue fields $\overline{K_v}$ of K, for all real valuations v of K. For the other implication, $(\Rightarrow)$, we use a characterization of the (reduced) stability index in terms of fans, cf. [7; Thm. 13.7] and [12]:

$$st(K) = \max \{n \in \mathbb{N} \mid \chi(K) \text{ contains a fan of cardinality } 2^n\}$$

($st(K) = \infty$ if $\chi(K)$ contains fans of arbitrarily large finite cardinality). Thus, if $st(K) \geq 3$, then $\chi(K)$ contains a fan of at least 8 elements, hence a fan of 8 elements, i.e. the affine cube designed above. By Tutte's criterion again, $\chi(K)$ is not unimodular.

Examples. Here are some examples of fields K such that $st(K) \leq 2$:

(a) $st(K) = 0$ iff K has a unique order.

(b) $st(K) \leq 1$ iff K is SAP (iff $\chi(K)$ is free); cf. [1; Satz 3.20].

(c) $st(\mathbb{Q}(X)) = 2$, $st(\mathbb{R}(X, Y)) = 2$. □

(For an explicit "drawing" of $\chi(\mathbb{Q}(X))$, see below.)

The same technique can be used to improve the preceding result in a way which underlines the sharp dichotomy between the spaces of orders of 2–stable fields (stability index ≤ 2) and those with a larger stability index. The result is as follows:

Theorem 5. *Let K be a f.r. field. Each of the following conditions is equivalent to $st(K) \leq 2$:*

(a) *$\chi(K)$ is a graphical matroid.*

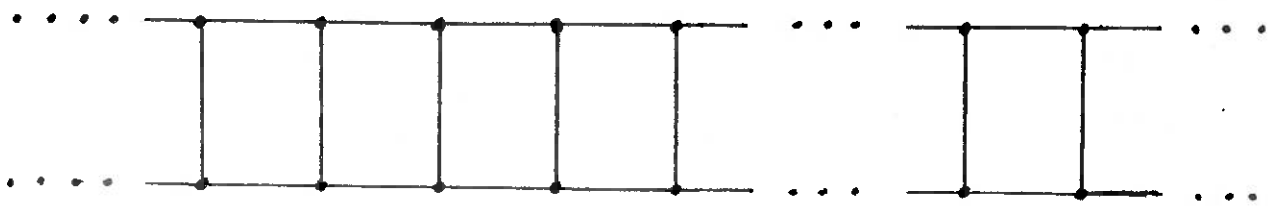
(b) *$\chi(K)$ is a cographical matroid.*

(c) *$\chi(K)$ is a planar graphical matroid.*

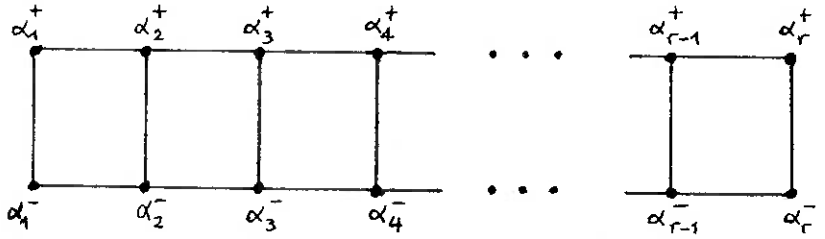
(d) *$\chi(K)$ is a series–parallel matroid.* □

As in the case of unimodular matroids, the meaning of these notions for infinite $\chi(K)$ is that every finite flat has the stated property. Well–known excluded minor characterizations for each of these classes of matroids (cf. White [13; pp. 146–147]) are used in the proof.

The point in the proof of Theorems 4 and 5 is that Brõcker's local–global principle, together with Theorem 1, implies that the space $\chi(K)$ has a very simple structure if the field K is 2–stable. Indeed, each connected component of $\chi(K)$ (in the matroid sense) is either a single point or it is a (possibly infinite) slab of the form:



A particularly transparent example is that of $\chi(\mathbb{Q}(X))$, where the components are either single points (corresponding to Archimedean orders or, equivalently, transcendental cuts on $\mathbb{Q}$), or slabs as above containing $2r$ points (i.e., of rank $r+1$). For each $r \geq 1$ there are countably many such slabs, classified by the polynomials $F \in \mathbb{Q}[X]$ with exactly r real roots, say $\alpha_1 < \ldots < \alpha_r$. The $2r$ orders are those obtained by placing X infinitesimally near each real root α_i of F, either to the left $(= \alpha_i^-)$, or to the right $(= \alpha_i^+)$.



A (non–trivial) component of $\chi(\mathbb{Q}(X))$

It is widely known that any inclusion of fields $i : K \hookrightarrow L$ induces a dual map $\rho : \chi(L) \longrightarrow \chi(K)$ given by the restriction of orders from L to K. The map ρ is just the (real) spectral dual of the inclusion i. From a combinatorial point of view, ρ is a <u>strong map</u> of the geometry $\chi(L)$ into $\chi(K)$, i.e. a map preserving closures $(P \in cl_L(\mathfrak{X}) \Longrightarrow \rho(P) \in cl_K(\rho[\mathfrak{X}])$; cf. White [13; Prop. 8.1.3]). The interpretation of a well–known result from valuation theory (cf. Lam [7; Prop. 3.17]) in our geometric language yields:

<u>Theorem 6</u>. *Let $< K, v > \subseteq < L, w >$ be an extension of valued fields, where w is a real valuation. Let $\chi(K, v)$ denote the set of all orders of K compatible with v; similarly for L, w. If $< L, w >$ is an immediate extension of $< K, v >$, then $\rho \restriction \chi(L, w) : \chi(L, w) \longrightarrow \chi(K, v)$ is a matroid isomorphism. In particular, if $K^{v,h}$ denotes the*

henselization of $< K, v >$, *then* ρ *is an isomorphism of* $\chi(K^{v,h})$ *onto* $\chi(K, v)$. □

(Recall that an immediate extension is an extension of valued fields such that the canonical inclusions of the value groups $\Gamma_v \rightarrowtail \Gamma_w$ and of the residue fields $K_v \rightarrowtail L_w$ are isomorphisms.)

The preceding theorem implies that a subset of $\chi(K)$ of the form $\chi(K, v)$, v a real valuation of K, is itself the space of orders of a field, namely that of the henselization $K^{v,h}$.

As a motivation for our next theme, we recall a result of Baer and Krull (cf. Lam [7; Thm 3.10 and Notes on Ch. 3]). Let v be a real valuation of a f.r. field K. Two objects are associated to each $P \in \chi(K, v)$:

1) The push–down order $\overline{P}$ of P on the residue field $\overline{K_v}$, defined by:

$$\overline{P} = \{x/_{M_v} \mid x \in A_v \cap P\}.$$

2) A character $P^* \in \mathrm{Hom}(\Gamma_v/_{2\Gamma_v}, \mathbb{Z}_2)$, essentially induced by the sign function on $K^\times/_{\Sigma(K^\times)^2}$; Γ_v denotes the value group of v. Actually, P^* is in the dual of the $\mathbb{Z}_2$–vector space $\Gamma_v/_{2\Gamma_v}$, but is not intrinsically defined.

The formal definition of P^* is as follows. Denote by v' the composition of the valuation $v : K^\times \longrightarrow \Gamma_v$ and the canonical quotient map $\Gamma_v \longrightarrow \Gamma_v/_{2\Gamma_v}$. Let us choose a system of representatives $\bar{a} = \{a_i \mid i \in I\} \subseteq K^\times$ such that $\{v'(a_i) \mid i \in I\}$ forms a $\mathbb{Z}_2$–base of $\Gamma_v/_{2\Gamma_v}$. We define $P^*_{\bar{a}}$ by specifying its action on the chosen base, as follows:

$$P^*_{\bar{a}}(v'(a_i)) = \mathrm{sgn}_P(a_i) = \begin{cases} 0 & \text{if } a_i \in P \\ 1 & \text{if } a_i \notin P \end{cases}$$

and extending to all of $\Gamma_v/_{2\Gamma_v}$ by linearity.

The result we have in mind is:

Theorem (Baer–Krull) *The map*

$$g_{\underline{a}} : \chi(K, v) \longrightarrow \chi(\overline{K_v}) \times Hom(\Gamma_v/2\Gamma_v, \mathbb{Z}_2)$$
$$P \longrightarrow < \overline{P}, P^*_{\underline{a}} >$$

is a bijection. □

A refinement of the technique employed in proving the surjectivity of this map (lifting a residual order along a character $\chi \in \mathrm{Hom}(\Gamma_v/2\Gamma_v, \mathbb{Z}_2)$) suffices to prove the following result:

Theorem 7 (The rank formula). *Let* v *be a real valuation of a field* K. *Then :*

$$r_K(\chi(K, v)) = r_{\overline{K_v}}(\chi(\overline{K_v})) + dim_{\mathbb{Z}_2}(Hom(\Gamma_v/2\Gamma_v, \mathbb{Z}_2)) = r_{\overline{K_v}}(\chi(\overline{K_v}) + dim_{\mathbb{Z}_2}(\Gamma_v/2\Gamma_v)\,.$$ □

The proof shows that lifting a base of $\chi(\overline{K_v})$ along the constant character 0 plus lifting, e.g., any residual order along each member of the dual base of $\{v'(a_i) \mid i \in I\}$ results in a base for $\chi(K, v)$.

All along the proof of Theorem 7 the subgroup $2\Gamma_v$ $(= v[\Sigma(K^\times)^2])$ can be replaced by the subgroup $v[T]$, where T is an arbitrary preorder of K; we obtain:

Theorem 7* (The rank formula, sharpened). *Let* v *be a real valuation of a field* K. *Let* $\mathfrak{X} \subseteq \chi(K, v)$, $T = \cap\{P \mid P \in \mathfrak{X}\}$, *and* $\overline{\mathfrak{X}} = \{\overline{P} \mid P \in \mathfrak{X}\}$. *Then :*

$$r_K(\mathfrak{X}) = r_{\overline{K_v}}(\overline{\mathfrak{X}}) + dim_{\mathbb{Z}_2}(Hom(\Gamma_v/v[T], \mathbb{Z}_2)) = r_{\overline{K_v}}(\overline{\mathfrak{X}}) + dim_{\mathbb{Z}_2}(\Gamma_v/v[T])\,.$$ □

The rank formula allows to compute, inductively, the rank of an arbitrary (finite) subset of $\chi(K)$, whether it is included in $\chi(K, v)$ for some real valuation v, or not.

A further question suggested by the foregoing results is whether the set–theoretic bijection between $\chi(K, v)$ and $\chi(\overline{K_v}) \times \mathrm{Hom}(\Gamma_v/2\Gamma_v, \mathbb{Z}_2)$ established by the Baer–Krull theorem has a geometric interpretation. Since $\chi(\overline{K_v})$ and $\mathrm{Hom}(\Gamma_v/2\Gamma_v, \mathbb{Z}_2)$ each have a natural matroid

structure, we may ask, for instance, whether these structures induce on the cartesian product a matroid structure which makes the Baer–Krull map $g_{\bar{a}}$ into a matroid isomorphism. The answer is positive whenever $\chi(K, v)$ is finite; more generally, we show:

Theorem 8 (Geometric form of the Baer–Krull theorem).

Let T be a preorder of K and v be a valuation fully compatible with T. Assume $\chi(K, T)$ is finite. Let $d = \dim_{\mathbb{Z}_2}(Hom(\Gamma_v/_{v[T]}, \mathbb{Z}_2)$ and $r = r(\chi(\overline{K_v}, \overline{T}))$. Let $\bar{a} = \{a_1,...,a_d\} \subseteq K^\times$ be such that $\{v'(a_1),...,v'(a_d)\}$ is a basis of the $\mathbb{Z}_2$–vector space $\Gamma_v/_{v[T]}$.

The set $\chi(\overline{K_v}, \overline{T}) \times Hom(\Gamma_v/_{v[T]}, \mathbb{Z}_2)$ can be endowed with a matroid structure so that the Baer–Krull map

$$\begin{array}{rccc} g_{\bar{a}} : & \chi(K, T) & \longrightarrow & \chi(\overline{K_v}, \overline{T}) \times Hom(\Gamma_v/_{v[T]}, \mathbb{Z}_2) \\ & P & \longrightarrow & < \overline{P}, P^*_{\bar{a}} > \end{array}$$

is a matroid isomorphism. This matroid structure is defined by taking as bases all families of sets of the form

$$\{<R_i, \chi_i> \mid i = 1,...,d\} \cup \{<Q_s, \psi_s> \mid s = 1,...,r\}$$

such that :

(i) $\{\chi_1,...,\chi_d\}$ *is a basis of the* $\mathbb{Z}_2$*–vector space* $Hom(\Gamma_v/_{v[T]}, \mathbb{Z}_2)$.

(ii) $\{Q_1,...,Q_r\}$ *is a basis of* $\chi(\overline{K_v}, \overline{T})$.

(iii) $\{R_1,...,R_d\}$ *is a non–empty subset of* $\chi(\overline{K_v}, \overline{T})$ *of cardinality* $\leq d$ *and* $\{\psi_1,...,\psi_r\}$ *is a non–empty subset of* $Hom(\Gamma_v/_{v[T]}, \mathbb{Z}_2)$ *of cardinality* $\leq r$ *(repetitions allowed).*

(iv) *The matrix* $I_r - NE$ *is non–singular, where*

— I_r *is the* $r \times r$ *identity matrix.*

— N *is the* $r \times d$ *matrix (with entries in* $\mathbb{Z}_2$*) of linear dependencies of* $\{\psi_1,...,\psi_r\}$ *with respect to the basis* $\{\chi_1,...,\chi_d\}$, *i.e.*

$$\begin{bmatrix} \psi_1 \\ \vdots \\ \psi_r \end{bmatrix} = N \begin{bmatrix} \chi_1 \\ \vdots \\ \chi_d \end{bmatrix}.$$

— *E is the $d \times r$ incidence matrix of $\{R_1,...,R_d\}$ with respect to the basis $\{Q_1,...,Q_r\}$ in $\chi(\overline{K_v}, T)$, i.e., the matrix with entries e_{ij} $(1 \le i \le d,\ 1 \le j \le r)$ in $\mathbb{Z}_2$ defined as follows : e_{ij} is 1 or 0 according to whether Q_j belongs or not to the fundamental circuit of R_i with respect to $\{Q_1,...,Q_r\}$ (cf. White [13; p. 129]).* □

Section § 5, is devoted to the decomposition theory of the matroids $\chi(K)$. The main tool used in this part is the approximation theorem for V–topologies, a very efficient instrument in dealing simultaneously with orders and valuations.

Matroids are naturally split in connected components by the circuit–connectivity relation: for $p, q \in M$,

$p \overset{c}{\sim} q$ iff either $p = q$ or there is a circuit containing both p and q.

The circuit axioms (see White [13; p. 301–302]) imply that $\overset{c}{\sim}$ is an equivalence relation; the equivalence classes modulo $\overset{c}{\sim}$ are the connected components of M. A corresponding external operation of direct sum of a (possibly infinite) family of matroids can be defined in such a way that a matroid is isomorphic to the direct sum of its connected components (considered themselves as matroids under the induced closure operator).

In [3] Bröcker introduced a natural way of splitting the spaces $\chi(K)$; for $P, Q \in \chi(K)$,

$P \overset{v}{\sim} Q$ iff either $P = Q$ or there is a non-trivial valuation of K compatible with both P and Q.

Since Archimedean orders are characterized by the fact that only the trivial valuation is compatible with them, the class $\mathrm{Arch}(K)$ of such orders, if non–empty, gets split into singletons modulo $\overset{v}{\sim}$. The approximation theorem for V–topologies implies that the classes modulo $\overset{v}{\sim}$ are flats of $\chi(K)$. Furthermore, it implies:

Theorem 9. *Let K be a f.r. field. Then:*

(a) *The operator cl_K is trivial on $\mathrm{Arch}(K)$, i.e. $cl_K(\mathfrak{X}) = \mathfrak{X}$, for $\mathfrak{X} \subseteq \mathrm{Arch}(K)$.*

(b) *$\mathrm{Arch}(K)$ is a separator of $\chi(K)$ (cf. White [14; pp. 175–176]). Hence*

$$\chi(K) \simeq Arch(K) \oplus (\chi(K) - Arch(K)) .$$

(c) *Every* $P \in Arch(K)$ *is an isthmus of* $\chi(K)$ *(cf. White [14; pp. 128–130]).* □

The connection between the relations $\underset{c}{\sim}$ and $\underset{v}{\sim}$ is as follows:

Proposition 10. (a) *Circuit–connectivity implies Bröcker (valuation) –equivalence.*

(b) *Every Bröcker class of* $\chi(K)$ *is the direct sum of the connected components of* $\chi(K)$ *contained in it.* □

Circuit–connectivity admits a characterization in valuation–theoretic terms, namely :

Theorem 11. *Let* $P_1, P_2 \in \chi(K)$. *Then :*

$P_1 \underset{c}{\sim} P_2$ *iff* $P_1 = P_2$ *or there is* $P_3 \neq P_1, P_2$ *and a non–trivial valuation* v *compatible with* P_1, P_2, P_3 *such that* Γ_v *is not 2–divisible.* □

The main technical tool used in proving this result (as well as Theorem 12 below) is the Baer–Krull theorem mentioned above.

This characterization suggests that circuit–connectivity is a finer relation than Bröcker–equivalence. In fact, this is the case, and there are well–known examples: the field $\mathbb{R}((X))$, or any chain–closed field, has a Bröcker–connected space of orders of cardinality 2 which necessarily splits into two one–point (i.e., trivial) components (cf. Dickmann [4]) . We present a non–trivial example of the same situation by constructing a field K with Bröcker–connected order space $\chi(K)$ of cardinality 8 which splits into two 4–element connected components.

Our main result concerning circuit–connectivity in order spaces is:

Theorem 12. *Let* K *be a f.r. field, and* $P, Q \in \chi(K)$. *Then :*

$P \underset{c}{\sim} Q$ *iff* $P = Q$ *or there is a 4–element circuit containing both* P *and* Q. □

This turns out to be the crucial property of the geometries $\chi(K)$. In order to understand its significance (and its origin), let us recall that Marshall [8] considered, in the context of a generalization of the spaces $\chi(K)$ called by him abstract order spaces, a relation equivalent to that on the right–hand side of the statement of Theorem 12. We shall denote this relation by $\tilde{m}$; obviously, it is reflexive and antisymmetric. Showing that it is transitive is a non–trivial matter requiring the use of yet poorly understood notions pertaining to the combinatorics of quadratic forms. Of course, Theorem 12 yields at once:

Corollary 13 (Marshall [10; Thm 2.3]). *The relation* $\tilde{m}$ *is an equivalence relation.* □

I think that the point of Theorem 12 is that it offers an elucidation of Marshall's relation $\tilde{m}$ and puts the heart of his work in a natural and, hopefully, fruitful perspective. Of course, Marshall's work takes place in the more general context of abstract order spaces, and is of a more difficult technical nature due to the absence of valuation–theoretic tools. However:

1) In spite of its usefulness (for example, in the investigation of the stability index of real varieties and related matters, cf. [12]), it is not known whether abstract order spaces yield anything different from the concrete spaces $\chi(K)$, at least as far as isomorphism types is concerned (in the finite case it does not, see [8; Thm. 4.10]).

2) Our combinatorial geometric approach works equally well for Marshall's abstract order spaces; in fact, I do not (yet?) know of any property of these abstract spaces which is not shared by the concrete order spaces of fields.

3) Our approach helps to elucidate other, ill understood, points of Marshall's work, as well (for example, the Basic Lemma 3.1 of [8]).

The interaction of the combinatorial geometric approach presented here with Marshall's work is the subject of joint work in progress with A. Lira, to which the present paper serves as background.

REFERENCES.

[1] Bröcker, L., Zur Theorie der quadratischen Forme über formal reellen Körper, Math. Ann. 210 (1974), 233–256.

[2] Bröcker, L., Characterizations of fans and hereditarily pythagorean fields, Math. Z. 151 (1976), 149–163.

[3] Bröcker, L., Uber die Anzahl der anordnungen eines kommutativen Körpers, Arch. Math. 29 (1977), 458–464.

[4] Dickmann, M. A., The model theory of chain–closed fields, J. Symb. Logic 53 (1988), 921–930.

[5] Dickmann, M. A., **Model–theoretic Methods in Real Algebraic Geometry**, approx. 450 pp., Math. Library, North–Holland Publ. Co., to appear.

[6] Lam, T. Y., The theory of ordered fields, in **Ring Theory and Algebra III** (B. Mc Donald, ed.), Lect. Notes Pure Appl. Math. 55, M. Dekker, N. York, 1980, 1–152.

[7] Lam, T. Y., **Orderings, Valuations and Quadratic Forms**, Regional Conf. Series Math. 52, A. M. S., 1982.

[8] Marshall, M., Classification of finite spaces of orderings, Can. J. Math. 31 (1979), 320–330.

[9] Marshall, M., Quotients and inverse limits of spaces of orderings, Can. J. Math. 31 (1979), 604–616.

[10] Marshall, M., Spaces of orderings IV, Can. J. Math. 32 (1980), 603–627.

[11] Marshall, M., The Witt ring of a space of orderings, Trans. Amer. Math. Soc. 258 (1980), 505–521.

[12] Scheiderer, C., Stability index of real varieties, Invent. Math. 97 (1989), 467–483.

[13] White, N. (ed.), **Theory of Matroids**, Encyclopedia Math. and Appl., vol. 26, 1986, Cambridge Univ. Press.

[14] White, N. (ed.), **Combinatorial Geometries**, Encyclopedia Math. and Appl., vol. 29, 1988, Cambridge Univ. Press.

M. A. Dickmann
Equipe de logique mathématique
UFR de Mathématiques
Université Paris VII
75251 Paris Cedex 05 – FRANCE

Constructing models by games for infinitary languages

Tapani Hyttinen

In the model theory of infinitary languages one of the main problems is the almost total lack of methods of constructing models. For example elementary chains does not work, Ehrenfeucht-Mostowsky models work only in some very limitted cases, ultraproducts need large cardinals and so on. In this paper we demonstrate one construction, namely generalized Henkin construction (sometimes called also Hintikka game), that does work for languages like $L_{\kappa\kappa}$, $L_{\kappa^+\kappa}$ and also for infinitely deep languages like $M_{\kappa\kappa}$ and $M_{\kappa^+\kappa}$ (for the definition see [Ka] or [H1]). For this paper one needs to know about M-languages only that $L_{\lambda\kappa}$ is a sublanguage of $M_{\lambda\kappa}$.

The history of the generalized Henkin construction is roughly the following. The idea of generalizing inductive constructions by long games is due to J. Väänänen and J. Oikkonen. First formulations of generalized Henkin games are due to J. Oikkonen and first succesful applications of the method are due to the author.

We demostrate the method by proving an old and easy theorem (Hanf, Scott) that if $2^\lambda < \kappa$ for all $\lambda < \kappa$ and κ has the tree property then $L_{\kappa\kappa}$ is weakly compact. Here we use large cardinals but it is the theorem that needs them not the method. In this example we end up with a proof more or less similar to the proof of this theorem in [Je]. So are these games needed? In this example no but in more untrivial cases, especially with infinitely deep languages, yes.

By this construction we can prove for example that if $\kappa^{<\kappa} = \kappa$ and κ is regular then the separation theorem is true for $M_{\kappa^+\kappa}$ (this is not true for $L_{\kappa^+\kappa}$) and "there is no decending κ-sequences" is not expressable in $M_{\kappa^+\kappa}$ ([H1], stronger form in [Tu]). With the construction we can also instead of one model construct two models and some morphism between them and prove preservation theorems and normal form theorems for $M_{\kappa\kappa}$ ([H2]).

1 Definition. *Let Σ be a set of $L_{\kappa^+\kappa}$-sentences of similarity type μ. Assume $|\Sigma| \leq \kappa$. Let $C = \{c_\alpha | \alpha < \kappa\}$ be a set of new constant symbols. The generalized Henkin game $H(\Sigma)$ is a game of length κ played by A and E. During the game E interprets symbols of μ to the set C to make C a model of Σ. This is done so that at every move $\alpha < \kappa$ first A asks a question and then E answers the question by choosing some set S_α of $L_{\kappa^+\kappa}$-sentences. There are eight different ways to form the question: Assume game is in move $\alpha < \kappa$ and let $S'_\alpha = \bigcup_{\beta<\alpha} S_\beta$.*

1. A chooses some $\phi \in \Sigma$; then E must choose $S_\alpha = S'_\alpha \cup \{\phi\}$.

2. *A chooses a closed term t; then E must choose $S_\alpha = S'_\alpha \cup \{t = t, t = c\}$ for some $c \in C$.*
3. *A chooses $t = t' \in S'_\alpha$, where t and t' are closed terms; then E must choose $S_\alpha = S'_\alpha \cup \{t' = t\}$.*
4. *A chooses $\exists \overline{x} \phi(\overline{x}) \in S'_\alpha$; then E must choose $S_\alpha = S'_\alpha \cup \{\phi(\overline{c})\}$ for some $\overline{c} \in C$.*
5. *A chooses $\forall \overline{x} \phi(\overline{x}) \in S'_\alpha$ and some sequence $\overline{t}$ of closed terms; then E must choose $S_\alpha = S'_\alpha \cup \{\phi(\overline{t})\}$.*
6. *A chooses $\bigvee \Phi \in S'_\alpha$; then E must choose $S_\alpha = S'_\alpha \cup \{\phi\}$ for some $\phi \in \Phi$*
7. *A chooses $\bigwedge \Phi \in S'_\beta$ and $\phi \in \Phi$; then E must choose $S_\alpha = S'_\alpha \cup \{\phi\}$.*
8. *A chooses $t = t'$ and $\phi(t)$ from S'_α, where t and t' are closed terms; then E must choose $S_\alpha = S'_\alpha \cup \{\phi(t')\}$.*

Furthermore E must obey the following rules.

9. *For all atomic sentences ϕ either ϕ or $\neg\phi$ does not belong to S_α.*
10. *If E, in her answer, uses new constants from C that do not appear in the sentences of S'_α then E must choose them so that they are minimal (in the ordering $c_\alpha < c_\beta$ iff $\alpha < \beta$) among such constants.*

A wins if for some $\alpha < \kappa$ E cannot find S_α satisfying the rules. Otherwise E wins.

2. Theorem. *Let Σ be a set of $L_{\kappa^+\kappa}$-sentences of cardinality $\leq \kappa$. Then Σ has a model if and only if A does not have a winning strategy for $H(\Sigma)$.*

Proof. " $\Rightarrow$ " If Σ has a model $\mathcal{A}$ then E always wins $H(\Sigma)$ by playing according to $\mathcal{A}$ in an obvious way and so A has no winning strategy.

" $\Leftarrow$ " Let τ be a strategy of A for $H(\Sigma)$ such that if κ moves are played then A has asked all the possible questions. Such a strategy is for example the following. Let $g : \kappa \to \kappa \times \kappa$ be one-one and onto such that always if $g(\alpha) = (\beta, \gamma)$ then $\beta \leq \alpha$. At each move α A lists all the possible questions he can ask at this move, let the list be q^α_β, $\beta < \kappa$, and asks the question q^γ_ν, where $(\gamma, \nu) = g(\alpha)$. By assumption this is not a winning strategy and so there is a play in which A has used τ and lost. Let S_α, $\alpha < \kappa$, be the answers of E in this play. Let $S = \bigcup_{\alpha<\kappa} S_\alpha$. As in the usual Henkin construction we now make a model for Σ out of the new constants by using S as a set of instructions. □

3. Theorem. *(Hanf, Scott) Assume $2^\lambda < \kappa$ for all $\lambda < \kappa$ and κ has the tree property. Then $L_{\kappa\kappa}$ is weakly compact.*

Proof. Let Σ be a set of $L_{\kappa\kappa}$-sentences of cardinality $\leq \kappa$. Assume that if $\Sigma' \subseteq \Sigma$ has cardinality $< \kappa$ then Σ' has a model. For a contradiction assume Σ has not a model Then by the Theorem 2 A has a winning strategy τ for $H(\Sigma)$. Let T be a set of all sequences $(q_0, S_0, ..., q_\alpha)$, $\alpha < \kappa$, such that $q_\beta = \tau(S_0, ..., S_\gamma, ...)_{\gamma<\beta}$ and for all $\beta < \alpha$ S_β satisfies, as a move of E in $H(\Sigma)$, all the conditions of the Definition 1. In other words let T be the set of all initial segments of plays in which A has used τ and E has not lost yet. We order T by

the initial segment relation. Then T is a tree. Because τ is a winning strategy T has no branches of lenght κ. Because of 10 in the Definition 1 and the assumption that $2^\lambda < \kappa$ for all $\lambda < \kappa$, all the levels of T are of cardinality $< \kappa$. By the tree property $|T| < \kappa$. Let Σ' be the set of all sentences of Σ that belong to some S_β from some sequence in T. Then τ is a winning strategy of A for $H(\Sigma')$, too and by the Theorem 2 Σ' has no model. On the other hand, because $|T| < \kappa$, $|\Sigma'| < \kappa$ and so by the assumption Σ' has a model. A contradiction. □

Almost exactly the same proof would show that if $2^\lambda < \kappa$ for all $\lambda < \kappa$ and κ has the tree property then $M_{\kappa\kappa}$ is weakly compact (originally proved by using ultraproducts in [Ka]).

References

[H1] Hyttinen, T.: Model theory for infinite quantifier languages. -Fundamenta Matematicae, to appear.

[H2] Hyttinen, T.: Preservation in homomorphisms and infinitary languages. -Notre Dame Journal of Formal Logic, to appear.

[Je] Jech, T.: Set Theory. -Academic Press, New York, San Francisco, London, 1978.

[Ka] Karttunen, M.: Model theory for infinitely deep languages, Ann. Acad. Sci. Fenn. Ser. A I Math. Diss., vol 50 (1984).

[Tu] Tuuri, H.: Infinitary languages and long Ehrenfeucht-Fraisse games. -Ph.D. Thesis, University of Helsinki, to appear.

Department of mathematics
University of Helsinki
Hallituskatu 15
00100 Helsinki
Finland

UN EXEMPLE DE CORPS INDECIDABLE DONT TOUTES LES EXTENSIONS FINIES PROPRES SONT DECIDABLES

(D'après une remarque de L. van den Dries)

Zoé Chatzidakis

Cet exposé a pour but de montrer l'existence d'un corps dont la théorie élémentaire est indécidable tel que toutes ses extensions algébriques finies propres ont une théorie décidable. Cette observation a été faite par Van den Dries et se démontre facilement à partir des résultats de Jarden [J], et Van den Dries, Smith [DS].

Nous commençons par rappeler plusieurs définitions qui seront utilisées dans l'énoncé des théorèmes.

Définitions

Rappelons d'abord qu'un corps K est dit **pseudo-algébriquement clos (PAC)** si toute variété absolument irréductible définie sur K a un point K-rationnel.

Un corps K est **hilbertien** s'il satisfait la propriété suivante: Si un polynôme $f(T,X) \in K[T,X]$ est irréductible, alors il existe une infinité d'éléments a de K tels que $f(a,X)$ soit irréductible.

Bien évidemment, aucun corps algébriquement clos n'est hilbertien. Les exemples les plus connus de corps hilbertiens sont le corps des nombres rationnels $\mathbf{Q}$ et les corps de fonctions rationnelles $K(t)$. Notons aussi que toute extension algébrique finie d'un corps hilbertien est hilbertienne; ceci ne se généralise pas aux extensions algébriques infinies. Pour plus d'informations sur ces corps, on pourra consulter le livre de Fried et Jarden [FJ].

Le **groupe de Galois absolu** d'un corps K, que nous dénoterons par $G(K)$, est le groupe de Galois de la clôture séparable K_s de K sur K. C'est un groupe profini, et donc compact.

Si σ est un ensemble d'éléments de $G(K)$, nous dénotons par $K_s(\sigma)$ le sous-corps de K_s fixé par les éléments de σ; le groupe de Galois absolu de ce corps est alors le sous-groupe fermé de $G(K)$ engendré par les éléments de σ.

Le **corps des nombres absolus** d'un corps K est l'intersection de K avec la clôture algébrique du corps premier. Nous le dénotons par $K^{\mathbf{abs}}$.

Enfin, le groupe $\hat{\mathbf{F}}_\omega$ est le groupe profini libre sur un ensemble générateur infini dénombrable. Il peut être obtenu de la façon suivante:

Considérons le groupe discret libre F sur un ensemble générateur infini dénombrable X. Si $N \subset M$ sont deux sous-groupes normaux de F, il y a un épimorphisme canonique $\pi_{NM} : F/N \to F/M$. On définit alors

$$\hat{\mathbf{F}}_\omega = \varprojlim F/N$$

où N parcourt l'ensemble des sous groupes normaux d'indices fini de F qui contiennent un ensemble cofini de X, et les morphismes sont les épimorphismes π_{NM}.

Résultats que nous utiliserons.

Les théories élémentaires de corps PAC sont maintenant bien connues et ont fait l'objet de plusieurs artides, voir par exemple [A], [JK], [J], [CDM] et [E]. Le résultat le plus général étant un peu long à énoncer, nous nous contenterons du résultat suivant, dû à Jarden [J], et qui est une généralisation au cas infini des résultats de Ax [A] et de Jarden, Kiehne [JK]:

Théorème A. Soient K et L des corps PAC dont les groupes de Galois absolus sont isomorphes à $\hat{\mathbf{F}}_\omega$. Alors

$$K \equiv L \quad \Longleftrightarrow \quad K^{\mathrm{abs}} \simeq L^{\mathrm{abs}}.$$

De plus, la théorie des corps PAC de groupe de Galois absolu isomorphe à $\hat{\mathbf{F}}_\omega$ est décidable.

Théorème B. [J] Soit K un corps hilbertien dénombrable. L'ensemble des ω-uplets $\sigma \in G(K)^\omega$ tels que $K_s(\sigma)$ soit PAC et ait groupe de Galois absolu isomorphe à $\hat{\mathbf{F}}_\omega$ a mesure 1.

Nous ne donnerons pas la définition de la mesure utilisée, qui est un produit de mesures de Haar. Il nous suffit ici de savoir qu'il existe beaucoup de corps avec les propriétés qui nous intéressent.

Théorème C. Soit N un sous-groupe normal fermé de $\hat{\mathbf{F}}_\omega$. Alors tout sous-groupe ouvert propre de N est isomorphe à $\hat{\mathbf{F}}_\omega$.

Ce résultat est dû à Van den Dries et Smith [DS], et à Mel'nikov [M]. Il peut être en fait enoncé de manière bien plus générale. Notons aussi que Mel'nikov définit des invariants qui décrivent complètement les sous-groupes normaux de $\hat{\mathbf{F}}_\omega$.

Lemme. Soit S un ensemble de nombres premiers, et considérons l'intersection N de tous les sous-groupes ouverts normaux de $\hat{\mathbf{F}}_\omega$ dont l'index est produit d'éléments de S. Alors, pour tout nombre premier p l'on a: $p \in S$ si et seulement si N n'a aucun sous-groupe normal ouvert d'indice p.

Démonstration: Supposons d'abord que p n'appartienne pas à S, et soit U un sous-groupe normal ouvert de $F = \hat{\mathbf{F}}_\omega$ d'indice p. Puisque U n'est contenu dans aucun sous-groupe ouvert de F contenant N, il n'est pas contenu dans N, et donc $U \cap N$ est un sous-groupe normal ouvert de N d'indice p.

Pour la réciproque, soit U un sous-groupe normal ouvert de N d'indice p; puisque N est fermé dans F, il existe un sous-groupe ouvert V de F tel que

$$U = V \cap N.$$

Définissons ensuite

$$V_0 = \bigcap_{g \in F} V^g \qquad \text{et} \qquad U_0 = V_0 \cap N = \bigcap_{g \in F} U^g.$$

Comme $[F : V]$ est fini, V n'a qu'un nombre fini de conjugués distincts, et donc V_0 est un sous-groupe normal ouvert de F, et U_0 est un sous-groupe ouvert de N. Pour tout $g \in G$, U^g est un sous-groupe normal ouvert de N d'indice p, ce qui implique que $[N : U_0] = p^e$ pour un entier $e > 1$. Nous avons alors

$$\begin{aligned}[F : V_0] &= [F : V_0N][V_0N : V_0] \\ &= [F : V_0N][N : V_0 \cap N] \\ &= [F : V_0N][N : U_0] \\ &= [F : V_0N]\, p^e\end{aligned}$$

La définition de N implique alors que p n'appartient pas à S.

Démonstration du résultat

Comme $\tilde{\mathbf{Q}}(t)$ est hilbertien, $\tilde{\mathbf{Q}}(t)$ possède une extension algébrique E qui est PAC et dont le groupe de Galois absolu est isomorphe à $\hat{\mathbf{F}}_\omega$ (Théorème B). Choisissons un ensemble non-récursif S de nombres premiers, soit N le sous-groupe fermé de $\hat{\mathbf{F}}_\omega = G(E)$ défini dans le lemme, et soit K le sous-corps de $\tilde{E}$ laissé fixe par N. Observons ensuite que pour tout nombre premier p, K a une extension de Galois de degré p si et seulement si $K \models \exists x \forall y\ y^p \neq x$. Cela provient du fait que K contient toutes les racines primitives de l'unité. Nous avons alors:

$$K \models \exists x \forall y\ y^p \neq x \iff p \notin S,$$

et donc $\mathrm{Th}(K)$ est indécidable. Soit L une extension algébrique finie propre de K. Par le Théorème C nous avons $G(L) \simeq \hat{\mathbf{F}}_\omega$. Théorème A nous donne alors la décidabilité de $\mathrm{Th}(L)$: en effet, $\mathrm{Th}(L)$ est obtenue en adjoignant à la théorie des corps PAC de groupe de Galois absolu $\hat{\mathbf{F}}_\omega$ une collection d'énoncés exprimant que L contient la clôture algébrique de $\mathbf{Q}$.

Bibliographie

[A] J. Ax, The elementary theory of finite fields, Ann. of Math. 88 (1968), 239 – 271.

[CDM] G. Cherlin, L. van den Dries, A. Macintyre, The elementary theory of regularly closed fields, ms. (1980).

[DS] L. van den Dries, R.L. Smith, Decidable regularly closed fields of algebraic numbers, JSL 50 (1985), 468 – 475.

[E] Ju.L. Ershov, Regularly closed fields, Sov. Mat. Doklady 31 (1980), 510 – 512.

[FJ] M. Fried, M. Jarden, Field arithmetic, Springer-Verlag, Berlin Heidelberg 1986.

[J] M. Jarden, The elementary theory of ω-free Ax fields, Inv. math. 38 (1976), 187 – 206.

[JK] M. Jarden, U. Kiehne, The elementary theory of algebraic fields of finite corank, Inv. Math. 30 (1975), 275 – 294.

[M] O.V. Mel'nikov, Normal subgroups of free profinite groups, Math. USSR Izvestija 12 (1978), 1 – 20.

THE ELEMENTARY CLASS OF PRODUCTS OF TOTALLY ORDERED ABELIAN GROUPS[1]

by Daniel Gluschankof - (Universidad de Buenos Aires, Université d'Angers)

§ 0. Introduction. A basic goal in model-theoretic algebra is to obtain the classification of the complete extensions of a given (first-order) algebraic theory.

Results of this type, for the theory of totally ordered abelian groups, were obtained first by A.Robinson and E.Zakon [5] in 1960, later extended by Yu.Gurevich [4] in 1965 and further clarified by P.Schmitt in [6].

Within this circle of ideas, we give in this paper an axiomatization of the first-order theory of the class of all direct products of totally ordered abelian groups, construed as lattice-ordered groups (ℓ-groups)

We write *groups* for abelian ℓ-groups construed as structures in the language $\langle \vee, \wedge, +, -, 0\rangle$ ("-" is an unary operation). For definitions, the reader is refered to [1].

§ 1. First-order products. We recall that a group G is called *projectable* if, for all $g \in G$ we have $g^{\perp} \times g^{\perp\perp} = G$. *Basic* if for all strictly positive g there exists b such that $0 < b \leq g$, and the interval $[0, b]$ is totally ordered. The element b is called *basic*. A group is *laterally complete* if any orthogonal subset of G has a least upper bound. It is known that a group is isomorphic to a product of totally ordered groups if and only if it is projectable, basic and laterally complete.

We shall define some predicates to be used in the sequel:

$x \perp y$ iff $|x| \wedge |y| = 0$ (x and y are orthogonal);

$\mathrm{Bas}(x)$ iff $\forall yz(x>0 \ \& \ (0 \leq y, z \leq x \Longrightarrow y \leq z \text{ or } z \leq y))$ (x is basic);

$\mathrm{Mbas}(x,y)$ iff $\forall z(\mathrm{Bas}(x) \ \& \ x \leq |y| \ \& \ (\mathrm{Bas}(z) \ \& \ z \wedge x > 0 \ \& \ z \leq |y| \Longrightarrow z \leq x))$
(x is maximal in the set of basic elements bounded by $|y|$);

$\mathrm{Ext}(x,y)$ iff $\forall z(\mathrm{Mbas}(z,x) \Longrightarrow \mathrm{Mbas}(z,y) \ \& \ (y+(-x)) \perp z)$
(y "extends" x; in case G is a product of totally ordered groups, this means that x and y coincide in all coordinates where x is not zero).

$x = y_{|z}$ iff $x \in z^{\perp\perp} \ \& \ \exists x'(x' \in z^{\perp} \ \& \ y = x + x')$.

---

[1] A paraître en version complète dans The Journal of Symbolic Logic.

The notions of basicity and projectability are first order but lateral completeness is essentially a second-order notion. For the time being we will consider a first-order version of it, namely, the notion of "definable lateral completeness": if $\varphi(x_1,..,x_n)$ is a formula such that, for given $g_1,..,g_{n-1}$, the set $\{x_n \;/\; G \models \varphi(g_1,..,g_{n-1},x_n)\}$ is orthogonal, then it has a least upper bound. Explicitly:

$$(\forall\varphi):\ \forall x_1\ldots x_{n-1}(\forall xy(\varphi(x_1,..,x_{n-1},x)\ \&\ \varphi(x_1,..,x_{n-1},y) \Longrightarrow x\perp y) \Longrightarrow$$
$$\Longrightarrow \exists y\forall xw((\varphi(x_1,..,x_{n-1},x) \Longrightarrow x\le y)\ \&\ ((\varphi(x_1,..,x_{n-1},x) \Longrightarrow x\le w) \Longrightarrow$$
$$\Longrightarrow y\le w))).$$

For later use we recall three corollaries of a result of S.Feferman and R.Vaught on products of models (see [3]):

Let $\mathcal{L}$ be a first-order language and $(\mathfrak{U}_i)_{i\in I}$ a family of models for $\mathcal{L}$ where the set I is infinite:

Corollary 1: There exists a countable subset J of I such that the products $\prod_I \mathfrak{U}_i$ and $\prod_J \mathfrak{U}_i$ are elementary equivalent.

Corollary 2: For any given sentence φ of the language $\mathcal{L}$ such that $\prod_I \mathfrak{U}_i \models \varphi$ there exists a finite subset J of I such that, for any K ($J\subseteq K\subseteq I$), $\prod_K \mathfrak{U}_i \models \varphi$ holds.

Corollary 3: Suppose $I=\mathbb{N}$. Given a sentence φ of the language $\mathcal{L}$ such that $\prod_{i\le n} \mathfrak{U}_i \models \varphi$ for each $n\in\mathbb{N}$, then φ also holds in $\prod_I \mathfrak{U}_i$.

Returning to the theory of abelian ℓ-groups, for a projectable group G, a formula φ and $g\in G$, since $g^{\perp\perp}$ is a definable ℓ-subgroup of G, we write the relativization of φ to $g^{\perp\perp}$ by φ_g. Observe that this can be done in general with a variable replacing the element g. If $\varphi=\varphi(x_1,..,x_n)$ and $g_1,..,g_n\in G$, we shall understand $\varphi_g(g_1,..,g_n)$ as $\varphi_g(g_1\,|\,g,..,g_n\,|\,g)$.

Now, for a formula $\varphi(x_1,..,x_n)$ define the new formula $\varphi'(x_1,..,x_n,w)$ by:
"$x_n\in w^{\perp\perp}$ & $\varphi_w(x_1,..,x_n)$ & $\forall x'w'z(\mathrm{Ext}(w,w')$ & $\mathrm{Bas}(z)$ & $z\notin w'^{\perp\perp}$ & $x_n = x'\,|\,w$ & & $\varphi_{w'}(x_1,..,x_{n-1},x') \Longrightarrow \exists x''(x''\in (w'+z)^{\perp\perp}$ & $x = x''\,|\,w$ & $\varphi_{w'+z}(x_1,..,x_{n-1},x'')))$"

The meaning of $\varphi'(x_1,..,x_n,w)$ is: "$\varphi(x_1,..,x_n)$ holds in $w^{\perp\perp}$ and whenever it holds for a suitable x' in an extension $w'^{\perp\perp}$ of $w^{\perp\perp}$, it holds for some x'' in any extension of the form $(w'+z)^{\perp\perp}$ by a basic element z ".

Now we are ready to add, for each formula $\varphi(x_1,..,x_n)$ of our language, a new axiom for our class of ℓ-groups:

$$(*\varphi)\ \forall x_1..x_n w \exists x \forall y(\varphi'(x_1,..,x_n,w)\ \&\ \mathrm{Ext}(w,y) \Longrightarrow$$
$$\Longrightarrow \varphi(x_1,..,x_{n-1},x)\ \&\ \varphi_y(x_1,..,x_{n-1},x)).$$

This axiom states that, whenever $\varphi'(x_1,..,x_n,w)$ holds, there exists an element x such that $\varphi(x_1,..,x_{n-1},x)$ holds. Moreover, for any extension y of w, the relativization $\varphi_y(x_1,..,x_{n-1},x)$ holds.

Lemma 1: Let $(L_i)_{i\in I}$ be a family of totally ordered abelian groups. For any formula $\varphi(x_1,..,x_n)$, we have $\prod_I L_i \models (*\varphi)$.

Now we shall characterize the elementary class generated by the products of totally ordered abelian groups.

Definition: A group is called a *fo-product* (first-order-product) if and only if it is projectable, basic, definably laterally complete and, for any formula φ satisfies the axiom $(*\varphi)$.

The subgroup $G = \{z \,/\, z(n)$ is eventually constant$\}$ of $\mathbb{Z}^\omega$ is an example of a fo-product group which is not laterally complete (and hence not isomorphic to a product of totally ordered groups).

Lemma 2: Let G be an fo-product, $x, b \in G$, $x \neq 0$.

i) If $\mathrm{Bas}(b)$ and $b \leq |x|$ there exists and unique b_2 such that $\mathrm{Bas}(b_2)$, b and b_2 are comparable and $\mathrm{Mbas}(b_2, |x|)$;

ii) $x = \vee B - \vee B'$ where $B = \{b \,/\, \mathrm{Mbas}(b, x_+)\}$ and $B' = \{b \,/\, \mathrm{Mbas}(b, x_-)\}$.

Now we are ready to prove the main theorem of the paper:

Theorem: Given a fo-product group G there exists a family $\mathcal{L}=(L_s)_{s\in S}$ of totally ordered groups such that G is elementary equivalent to the product $\prod_S L_s$.

Proof: First, using the downward Löwenheim-Skolem theorem, we can assume that G is countable (any non-trivial ℓ-group is always infinite).
Observe that the maximal totally ordered subgroups of G are exactly those of the form $g^{\perp\perp}$ with $g \in G$ and $\mathrm{Bas}(g)$; furthermore there are at most countably many of them. Let $\mathcal{L}$ denote the family of those subgroups. If $\mathcal{L}$ is finite, it is easy to verify that G is isomorphic to the product of the members of $\mathcal{L}$. We may assume $\mathcal{L}$ countable, indexed by $\mathbb{N}$. Define $f: G \longrightarrow \prod_{\mathbb{N}} L_s$ by

$$f(g)(s) = \begin{cases} b_s & \text{if } b_s \in L_s,\ \mathrm{Mbas}(b_s, g_+); \\ -b_s & \text{if } b_s \in L_s,\ \mathrm{Mbas}(b_s, g_-); \\ 0 & \text{if for all } b \in L_s\ \mathrm{Mbas}(b, |g|) \text{ does not hold.} \end{cases}$$

It is not hard to verify that f is well defined, and a one-one homomorphism.

We shall show that f is an elementary embedding. To check this, it is enough to show that for every formula $\varphi(x_1,\ldots,x_n)$ with free variables among $x_1,\ldots,x_n$, and $g_1,\ldots,g_{n-1} \in G$, if $\prod_N L_s \models \exists x_n \varphi(f(g_1),\ldots,f(g_{n-1}),x_n)$ then there exists an element g_n in G such that $\prod_N L_s \models \varphi(f(g_1),\ldots,f(g_{n-1}),f(g_n))$. For notational simplicity we shall identify G with its image in $\prod_N L_s$ and assume $n = 2$. Since $\prod_N L_s \models \exists x_2 \varphi(g_1, x_2)$, exists g_2 in $\prod_N L_s$ such that $\prod_N L_s \models \varphi(g_1, g_2)$ and, expanding our language with new constant symbols for g_1 and g_2, by corollary 2, there exists $m_0 \in \mathbb{N}$ such that, for all $K \subseteq \mathbb{N}$ with $\{0,..,m_0\} \subseteq K$ we have $\prod_K L_s \models \varphi(g_{1|K}, g_{2|K})$ (where with $g_{|K}$ we denote the projection of g to the subgroup $\prod_K L_s$). Choosing positive elements $h_s \in L_s$ $(0 \le s \le m_0)$ and defining $h \in G \subseteq \prod_N L_s$ by $h(s) = h_s$ if $s \le m_0$ and $h(s) = 0$ otherwise, we have that $\varphi_h(g_1, g_2)$, hence $\varphi'(g_1, g_2, h)$, holds in G. Now, since $(*\varphi)$ is an axiom for G we can find a $g_2' \in G$ such that $G \models \varphi(g_1, g_2')$ and for all $h' \in G$ such that $\mathrm{Ext}(h, h')$, $h'^{\perp\perp} \models \varphi(g_{1|h'}, g'_{2|h'})$; in particular, since we can chose h' such that $\{s \,/\, h'(s) \neq 0\}$ is finite, we have that, for all finite $J \supseteq K$, $\prod_J L_s \models \varphi(g_{1|J}, g'_{2|J})$ implying, by corollary 3, that $\varphi(g_1, g_2)$ holds in $\prod_N L_s$ ■

Remark: Observe that the property of being definably laterally complete is implied by the axiom-scheme $(*\varphi)$, so we may dispense of that property in the definition of fo-products.

§ 2. Final remarks. Since a fundamental result of P.Conrad, J.Harvey and C. Holland [2] states that any abelian ℓ-group is isomorphic to an ℓ-subgroup of a Hahn product of totally ordered (archimedean) abelian groups, it is an interesting problem to find an axiom-scheme which implies that the embedding is elementary. The direct approach which consists in rewriting the axiom $(*\varphi)$ does not work because corollaries 2 and 3 do not hold for Hahn products.

References

[1] Bigard,A.,Keimel,K. and Wolfenstein,S., *Groupes et anneaux réticulés*, Springer LNM 608, 1978.

[2] Conrad,P.,Harvey,J. and Holland,C., *The Hahn embedding theorem for lattice-ordered groups*, Trans.Am.Math.Soc., 108 (1963), 143-169.

[3] Feferman,S. and Vaught,R.L., *The first order properties of algebraic systems*, Fund. Math., XLVII (1959), 57-103.

[4] Gurevich,Yu., *Elementary properties of ordered abelian groups*, Transl. A. M.S. 46 (1965), 165-192.

[5] Robinson,A. and Zakon,E., *Elementary properties of ordered abelian groups* Trans. A.M.S. 96 (1960), 222-236.

[6] Schmitt,P.H., *Model- and substructure complete theories of ordered abelian groups*, Proc. Logic Coll. Aachen 1983, LNM 1103 (Models and Sets), Springer, 1984.

GÉOMÉTRIE LOCALE DES POLYNÔMES HYPERBOLIQUES

Ivan Meguerditchian

Résumé : *Si P est un polynôme hyperbolique (cad ayant toutes ses racines réelles) de degré n , et s un entier plus petit que n , on détermine dans quels cas il existe un polynôme de degré s qu'on puisse ajouter à P sans sortir des polynômes hyperboliques. Cette question, en partie traitée par Arnol'd, est ici résolue complètement dans le cas local.*

Local geometry of hyperbolic polynomials

Abstract : *Given P a hyperbolic polynomial(that is all its roots are real) of degree n and $s < n$, is it possible to find a polynomial Q of degree s such that $P+Q$ remains hyperbolic ? This question, partly treated by Arnol'd, is here completely solved in the local case.*

Définitions :

Un polynôme unitaire à coefficients réels est dit *hyperbolique* si toutes ses racines sont réelles.
Étant donnés deux entiers n et s tels que $0 \leq s < n$, un polynôme hyperbolique $P = x^n + \lambda_1 x^{n-1} + \cdots + \lambda_n$ est dit *localement s-maximal* (respectivement *localement s-minimal*) s'il existe dans $\mathbf{R}^n$ un voisinage de P – P étant identifié au n-uplet $(\lambda_1, \ldots, \lambda_n)$ – dans lequel aucun polynôme de la forme $P+c_0x^s+c_1x^{s-1}+\cdots+c_s$ avec $c_0 > 0$ (respectivement $c_0 < 0$) n'est hyperbolique .
Si P est un polynôme hyperbolique il s'écrit de manière unique $P = (X - x_1)^{m_1} \ldots (X - x_k)^{m_k}$ avec $x_1 > x_2 > \cdots > x_k$ et le k-uplet $(m_1, \ldots, m_k)$ s'appelle *vecteur-multiplicité* de P.
A tout vecteur-multiplicité d'un polynôme P on associe l'entier s_P défini de la manière suivante :

i) si P n'a que des racines simples, $s_P = -1$.

ii) sinon on pose $s_P = \sum_{i/m_i \geq 2} (m_i - 2) + l$ où l est le nombre de de séquences impaires de 1 consécutifs dans le vecteur-multiplicité, en ne tenant compte que des séquences comprises entre deux multiplicités supérieures ou égales à 2.

Un polynôme hyperbolique est dit *droit* lorsque son vecteur-multiplicité commence par une séquence paire de 1, et gauche dans le cas contraire.

Théorème : Un polynôme hyperbolique P est :

. localement s-maximal et localement s-minimal si $0 \leq s < s_P$
. localement s_P-maximal mais non localement s_P-minimal si P est droit
et localement s_P-minimal mais non localement s_P-maximal si P est gauche
. il n'est ni localement s-maximal ni localement s-minimal pour $s > s_P$

Ce résultat s'exprime plus lisiblement sur le tableau suivant, pour un polynôme droit (respectivement pour un polynôme gauche) :

s	localement s-maximal	localement s-minimal
$n-1$	non	non
$\cdots$	$\cdots$	$\cdots$
s_P+1	non	non
s_P	oui (respectivement non)	non (respectivement oui)
s_P-1	oui	oui
$\cdots$	$\cdots$	$\cdots$
0	oui	oui

On désigne par *propriété A* l'ensemble des réponses négatives de ce tableau et par *propriété B* l'ensemble des réponses positives.

On remarquera que le résultat ne dépend que du vecteur-multiplicité, c'est à dire de l'ordre des racines et de leur multiplicité, mais pas des racines elles-mêmes.

Soient P de degré n et $s < n$. Notons que trouver $Q = c_0X^s + \cdots + c_s$ tel que $P + Q$ soit hyperbolique revient à trouver une courbe $y = -Q(x)$ coupant n fois la courbe $y = P(x)$.

Exemples : Soient A (fig.1) et B (fig.2) deux polynômes hyperboliques de degré 6, respectivement de vecteur-multiplicité $(2,1,1,2)$ et $(1,2,1,2)$.

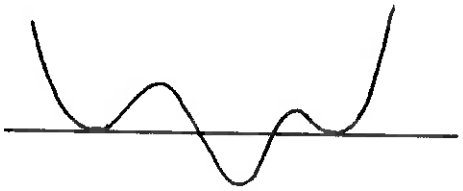


fig 1

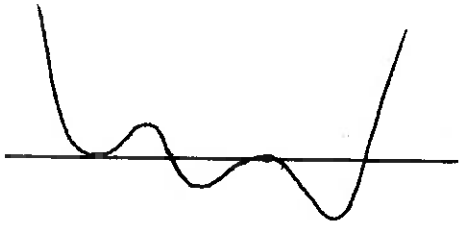


fig 2

Il existe des courbes $y = c$ avec $c > 0$ et $y = cx + d$ avec $c \neq 0$ coupant 6 fois le graphe de A ce qui est impossible pour $y = c$ avec $c < 0$, ce qui signifie que A est 0-maximal mais ni 0-minimal, ni 1-maximal, ni 1-minimal. Semblablement il existe des courbes $y = cx + d$ avec $c < 0$ coupant 6 fois le graphe de B ce qui est impossible pour $y = c$ avec $c \neq 0$ et $y = cx + d$ avec $c > 0$, ce qui signifie que B est 0-maximal, 0-minimal, et 1-minimal, mais non 1-maximal.

DEMONSTRATION DE LA PROPRIETE A :

Proposition 1 :

La propriété A est vérifiée pour P tel que $s_P = 0$.

Démonstration :

L'hypothèse signifie que P ne possède que des racines simples ou doubles et que son vecteur-multiplicité ne contient que des séquences paires de racines simples. Dans le cas où P est droit, ses racines doubles sont des minima locaux de la courbe $y = P(x)$ et ses maxima locaux sont nécessairement au-dessus de l'axe Ox. On notera η le minimum des valeurs prises par P en ces maxima locaux. On a bien entendu $\eta > 0$. Cela nous permet d'affirmer que pour $\varepsilon \in]0, \eta[$ la droite $y = \varepsilon$ coupe la courbe n fois, ce qui assure que P n'est pas localement 0-minimal. Appelons a le minimum de l'ensemble des racines de P et des abscisses des points d'intersection de la courbe avec la droite $y = \eta$ et b le maximum de cet ensemble. Soit R un polynôme non constant, on sait que $\exists\ m < M\ /\ \forall\ x \in [a,b]\ m \leq R(x) \leq M$. Dès lors, si on pose $Q(x) = \varepsilon \dfrac{R(x) - m}{M - m}$ avec $0 < \varepsilon < \eta$ on aura $\forall\ x \in [a,b]\ 0 \leq Q(x) \leq \eta$. Par conséquent la courbe $y = Q(x)$ coupe n fois la courbe $y = P(x)$ ce qui montre que, pour $s \geq 1$, P n'est ni localement s-maximal ni localement s-minimal.
On procède de manière semblable pour un polynôme gauche.

Proposition 2 :

La propriété A est vérifiée pour P quelconque.

Démonstration :

Au polynôme $P = (X - x_1)^{m_1} \ldots (X - x_p)^{m_p}$ on associe donc l'entier $s_P = \sum_{i/m_i \geq 2}(m_i - 2) + l$. Dans chacune des l séquences impaires on choisit une racine simple que l'on désigne par x_{j_k} pour k allant de 1 à l . Formons le polynôme $Q(X) = \prod_{i/m_i \geq 2} (X - x_i)^{m_i - 2} \prod_{k=1}^{l} (X - x_{j_k})$. On a $degQ = s_P$, Q divise P , et, en notant P_1 le quotient, $s_{P_1} = 0$. En utilisant le fait que si $P_1 + R$ est hyperbolique alors $Q(P_1 + R) = P + QR$ également et en appliquant la proposition 1 à P_1 on a la proposition 2 pour P .

DEMONSTRATION DE LA PROPRIETE B :

Définition :

On note $X_k(c)$ (respectivement $X_k^{\mathbf{C}}(c)$) et on appelle *variété de Vandermonde réelle* (respectivement *complexe*) *d'ordre* k , l'ensemble algébrique de $\mathbf{R^n}$ (respectivement $\mathbf{C^n}$) défini par les k équations suivantes :

$$\begin{cases} x_1 + \cdots + x_n = c_1 \\ \cdots \quad \cdots \quad \cdots \\ x_1^k + \cdots + x_n^k = c_k \end{cases}$$

Proposition 3 :

Les variétés de Vandermonde complexes d'ordre k sont de codimension k.

Démonstration :

Notons $s_j = \sum_{i=1}^{n} x_i^j$ la j-ième somme de Newton et φ : $\mathbf{C}^n \longrightarrow \mathbf{C}^n$

$(x_1, \ldots, x_n) \longmapsto (s_1, \ldots, s_n)$

L'application φ est surjective et à fibres finies. Soit Y le $(n-k)-plan$ de $\mathbf{C}^n$ obtenu en fixant les valeurs des k premières coordonnées. La préimage X par φ de Y est une variété de Vandermonde d'ordre k . La restriction à X de φ est encore une application polynomiale , à fibres finies et surjective sur Y de même que la restriction à une composante irréductible X_i de X : $\varphi_{/X_i} : X_i \to Y_i = \varphi(X_i)$. Sachant que, X_i étant irréductible , Y_i l'est aussi, on peut affirmer que dans un ouvert non vide de Y_i la dimension des fibres vaut $dimX_i - dimY_i$, donc que $dimX_i = dimY_i$. Par ailleurs, de $Y_i \subset Y$ on déduit d'abord $dimY_i \leq n-k$ puis $dimX_i \leq n-k$ pour tout i, et enfin $dimX \leq n-k$. On achève la démonstration en remarquant que k polynômes dans $\mathbf{C}^n$ définissent un ensemble algébrique de dimension au moins $n-k$.
Remarque : La dimension de la variété réelle correspondante est inférieure ou égale à $n-k$. (en passant de $\mathbf{C}$ à $\mathbf{R}$ la dimension peut chuter mais en aucun cas elle n'augmente).

Proposition 4 :

Si $X_k(c)$ contient un point ayant au moins k coordonnées distinctes, alors $dimX_k(c) = n-k$.

Démonstration :

Soient f l'application de $\mathbf{R}^n$ dans $\mathbf{R}^k$ associant à un n-uplet ses k premières sommes de Newton , $a = (a_1, \ldots, a_n)$ un point de $\mathbf{R}^n$ ayant k coordonnées distinctes, et c l'image de a par f.

$$Jac_{\,a}\,(f) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 2a_1 & 2a_2 & \ldots & 2a_n \\ \vdots & \vdots & \ddots & \vdots \\ ka_1^{k-1} & ka_2^{k-1} & \ldots & ka_n^{k-1} \end{pmatrix}$$

Les mineurs d'ordre k de la matrice jacobienne sont proportionnels à des déterminants de Vandermonde , il y en a donc au moins un non nul , celui correspondant à k coordonnées distinctes de a . La matrice jacobienne est donc de rang maximal k au point a et f est une submersion en ce point. La dimension locale en a de la variété $X_k(c) = f^{-1}(c)$ vaut dans ce cas $n-k$. Comme sa dimension globale est inférieure ou égale à $n-k$, elle est exactement $n-k$.

Proposition 5 :

Supposons $X_k(c)$ de codimension k exactement , alors :

i) Les points singuliers de $X_k(c)$ sont les points de $X_k(c)$ ayant moins de k coordonnées distinctes .

ii) Les points critiques de s_{k+1} sur la partie régulière de $X_k(c)$ sont les points de $X_k(c)$ ayant exactement k coordonnées distinctes .

Démonstration :

i) La matrice jacobienne de $X_k(c)$ est identique à la matrice jacobienne de f .

ii) On sait que si $x = (x_1, \ldots, x_n)$ est un point critique de s_{k+1} sur $RegX_k(c)$ alors il existe k nombres $p_1, \ldots, p_k$, appelés nombres de Lagrange , tels que $ds_{k+1} = p_1 ds_1 + \cdots + p_k ds_k$ au point x . Si L est la fonction de Lagrange associée , $L = s_{k+1} - p_1(s_1 - c_1) - \cdots - p_k(s_k - c_k)$, on obtient les points critques cherchés en résolvant le système : $dL = 0, s_1 = c_1, \ldots, s_k = c_k$. Notant $F(z) = (k+1)z^k - kp_k z^{k-1} - \cdots - p_1$ on a : $dL_x = 0 \Longleftrightarrow F(x_i) = 0$, $\forall i \in \{1, 2, \ldots, n\}$.

Maintenant si x est un point critique , ses n coordonnées sont racines de F , c'est à dire d'un polynôme de degré k ,et donc x a au plus k coordonnées distinctes , en réalité k exactement puisque c'est un point régulier.

Réciproquement soit $x \in X_k(c)$ ayant exactement k coordonnées distinctes $z_1, \ldots, z_k$ à l'aide desquelles nous formons le polynôme $F(z) = (k+1)(z - z_1)(z - z_2) \cdots (z - z_k)$. Le développement de F détermine de manière unique k nombres de Lagrange $p_1, \ldots, p_k$. Alors x vérifie bien le système précédent.

Proposition 6 :

Etant fixé un point critique x de s_{k+1} sur $X_k(c)$ on ordonne ses k coordonnées distinctes $z_1 > \ldots > z_k$, on note m_i le nombre de fois où z_i apparait dans $x = (x_1, \ldots, x_n)$ et on pose $r_i = m_i - 1$.
Alors la différentielle seconde de s_{k+1} sur $X_k(c)$ au point x est la somme d'une forme définie positive sur $\mathbf{R}^a$ (où $a = r_1 + r_3 + \cdots$) et d'une forme définie négative sur $\mathbf{R}^b$ (où $b = r_2 + r_4 + \cdots$).

Démonstration :

Toutes les données étant invariantes par permutation des coordonnées on peut supposer que x s'écrit :

$$x = (\underbrace{z_1, \ldots, z_1}_{r_1 \text{ fois}}, \underbrace{z_2, \ldots, z_2}_{r_2 \text{ fois}}, \ldots, \underbrace{z_k, \ldots, z_k}_{r_k \text{ fois}}, z_1, \ldots, z_k)$$

Dans la matrice jacobienne de $X_k(c)$ un mineur non nul d'ordre k est obtenu en sélectionnant les k dernières colonnes. Cela signifie en particulier que les $n-k$ premières coordonnées forment un système de coordonnées locales de $X_k(c)$ au voisinage de x . Dans ce système on a toujours $dL_x = 0$. De $\frac{\partial^2 L}{\partial x_i \partial x_j} = 0$ si $i \neq j$ et de $\frac{\partial^2 L}{\partial x_i^2} = F'(x_i)$ on déduit :

$$d^2 L_x(h_1, \ldots, h_{n-k}) = (h_1^2 + \cdots + h_{r_1}^2)F'(z_1) + \cdots + (h_{n-k-r_k}^2 + \cdots + h_{n-k}^2)F'(z_k)$$

C'est bien une forme quadratique non dégénérée puisque, F n'ayant que des racines simples , $F'(z_i) \neq 0$ pour tout i . On obtient la signature en remarquant que $F'(z_1) > 0, F'(z_2) < 0, F'(z_3) > 0$ etc.
La proposition 6 a pour corollaire immédiat la proposition suivante :

Proposition 7 :

Un point critique x sera un minimum local de s_{k+1} sur $X_k(c)$ si son vecteur-multiplicité est de la forme $(r, 1, s, 1, \ldots)$ et un maximum local si son vecteur-multiplicité est de la forme $(1, r, 1, s, 1, \ldots)$

Définition :

Un polynôme hyperbolique de vecteur-multiplicité $(m_1, \ldots, m_k)$ est dit *alterné droit* si $m_{2i} = 0$ pour tout i et *alterné gauche* si $m_{2i+1} = 0$ pour tout i.

Proposition 8 :

Un polynôme hyperbolique P alterné droit (respectivement alterné gauche) est localement s_P-maximal (respectivement localement s_P-minimal).

Démonstration :

Soient P un polynôme alterné droit ayant exactement k racines réelles distinctes et $X_k(c)$ la variété de Vandermonde réelle d'ordre k à laquelle appartient le n-uplet des racines de P . Ce dernier, noté $x = (x_1, \ldots, x_n)$, a pour vecteur-multiplicité $(r, 1, s, 1, \ldots)$ et est par conséquent minimum local de s_{k+1} sur $X_k(c)$. Supposons maintenant que Q soit un polynôme hyperbolique dont les k premières sommes de Newton sont égales à celles de P , ce que l'on notera $s_i(P) = s_i(Q)$ pour $i \in \{1, \ldots, k\}$. De la relation classique entre

sommes de Newton et fonctions symétriques élémentaires on déduit que les k premières fonctions symétriques élémentaires des racines de P sont égales à celles des racines de Q ce que l'on notera $\sigma_i(P) = \sigma_i(Q)$ pour $i \in \{1, \ldots, k\}$. Si Q est suffisamment proche de P on aura la relation $s_{k+1}(P) \leq s_{k+1}(Q)$ qui traduite en termes de fonctions symétriques élémentaires s'écrit : $(-1)^{k+1}\sigma_{k+1}(P) \geq (-1)^{k+1}\sigma_{k+1}(Q)$ c'est à dire que le coefficient de X^{n-k-1} dans Q est plus petit que le même dans P . Ceci montre bien que P est $(n-k-1)$-maximal. On vérifie alors aisément que $s_P = n-k-1$.

Proposition 9 :

Soient $a_1, \ldots, a_q$ des nombres réels et P un polynôme hyperbolique. Si $P(X-a_1)\ldots(X-a_q)$ est localement $(s+q)$-maximal (respectivement minimal) alors P est localement s-maximal (respectivement minimal)

Démonstration :

Il est clair que si $P+Q$ est hyperbolique alors $P(X-a_1)\ldots(X-a_q) + Q(X-a_1)\ldots(X-a_q)$ l'est aussi ce qui se traduit encore par : si P n'est pas localement s-maximal alors $P(X-a_1)\ldots(X-a_q)$ n'est pas localement $(s+q)$-maximal. La proposition 9 est la contraposée de celle-ci.

Proposition 10 :

La propriété B est vraie pour les polynômes hyperboliques alternés.

Démontrons-la pour un polynôme alterné droit, P, de vecteur-multiplicité $(r, 1, s, 1, \ldots)$. On sait, par la proposition 8 , que P est localement s_P-maximal et on souhaiterait montrer que P est localement s-maximal pour $0 \leq s < s_P$. Soit q l'entier non nul tel que $s+q = s_P$. On construit $Q_1 = P(X-a_1)\ldots(X-a_q)$ avec $a_q < \ldots < a_1 < min\{$ racines de P $\}$ ce qui revient à ajouter des 1 à la fin du vecteur-multiplicité de P pour obtenir celui de Q_1 . Le polynôme Q_1 est hyperbolique alterné droit et $s_{Q_1} = s_P$. D'après la proposition 8, Q_1 est localement s_P-maximal, donc P est localement s-maximal d'après la proposition 9.
On construit Q_2 en gardant $a_2, \ldots, a_q$ comme ci-dessus mais a_1 est choisi tel que $a_1 > max\{racines\ de\ P\}$. On applique alors la propositon 8 au polynôme alterné gauche Q_2 pour obtenir que P est localement s-minimal.

Proposition 11 :

La propriété B est vraie pour tout polynôme hyperbolique.

Démonstration :

Soit $P = (X-x_1)^{m_1}\ldots(X-x_p)^{m_p}$ avec $x_1 > x_2 > \cdots > x_p$. On peut toujours transformer chacune des séquences paires de 1 consécutifs comprises entre deux multiplicités supérieures ou égales à 2 en une séquence impaire par la multiplication de P par $(X-a_k)$, a_k étant un nombre réel non racine de P . Après un nombre fini d'opérations on obtient $Q = P(X-a_1)\ldots(X-a_q)$ polynôme alterné avec $s_Q = s_P + q$. La propriété B étant vraie pour Q on la déduit pour P à l'aide, une fois encore, de la proposition 9 .

RÉFÉRENCES BIBLIOGRAPHIQUES :

[1]:V.I. ARNOL'D : Hyperbolic polynomials and Vandermonde mappings, Funktsional. Anal. i Prilozhen. 20:2 (1986),52-57 = Functional Anal. Appl. 20 (1986),125-127.

[2]:A.B. GIVENTAL' : Moments of random variables and the equivariant Morse lemma, Uspekhi Mat. Nauk 42 (1987) n° 2 (254),221-222 =(english translation) Russian Math. Surveys 42 (1987) n° 2,275-276.

Laboratoire de Mathématiques, Université de Rennes 1
Campus de Beaulieu, 35042 Rennes Cedex

SUR LA PROJECTION DE VARIÉTÉS ALGÉBRIQUES RÉELLES

Daniel Pecker

§I. Introduction.

Dans ce travail nous nous intéressons au problème de trouver un ensemble algébrique, si possible irréductible, se projetant sur un ensemble semi-algébrique donné.

Notre résultat principal est de nature géométrique :

Théorème 2. Un semi algébrique de $\mathbb{R}^n$ est la projection d'un ensemble algébrique irréductible de $\mathbb{R}^{n+1}$ si et seulement si son adhérence de Zariski est un ensemble algébrique irréductible.

On commencera par le résultat algébrique suivant d'élimination relative des inégalités. (On note $\underline{x}=(x_1,\ldots,x_n)$).

Théorème 1. Soit S un ensemble semi-algébrique contenu dans V une variété irréductible de $\mathbb{R}^N$ non réduite à un point.

Il existe un polynôme $P(\underline{x},t)\in\mathbb{R}[x,t]$ dont la réduction modulo I(V) est un polynôme irréductible de $\mathbb{R}(V)[t]$ tel que :

$$\underline{x}\in S \iff x\in V \text{ et } \exists t\in\mathbb{R},\ P(\underline{x},t) = 0.$$

Comme un ensemble algébrique réel d'équation irréductible n'est pas forcément irréductible on utilisera, pour déduire le théorème 2 du théorème 1, une généralisation du critère de changement de signe (qui permet de déduire sous certaines conditions l'irréductibilité d'un ensemble algébrique réel de l'irréductibilité de ses équations).

Dans le cas où le semi-algébrique est localement fermé d'intérieur non

vide, une démonstration plus explicite des théorèmes 1 et 2 figure dans $[P_1]$, $[P_2]$ et $[P_3]$. Dans le cas général abordé ici, on utilise un argument de densité déduit du théorème d'irréductibilité de Hilbert qu'on rappelle au paragraphe 2.

Le cas où S est fermé pour la topologie euclidienne est plus simple, toutes les projections peuvent alors être choisies propres, et les équations des ensembles algébriques unitaires (cf.[P4]).

En général, ce n'est plus le cas, mais les fibres des projections obtenues dans cet article sont finies.

Enfin, on donne des réponses à la plupart des questions posées dans les premiers travaux sur ce sujet (cf.[Mot1], [Mot2], [A.G1], [A.G2]). Pour d'autres détails, on pourra se reporter à [P2] ou à [P3] .

§2. L'élimination relative des inégalités.

Si $\underline{x}=(x_1, x_2,\ldots)\in\mathbb{R}^\infty=\bigcup_{n=1}^{\infty}\mathbb{R}^n$ on note $\underline{x}\geq 0$ si et seulement si tous les $x_i\geq 0$.

Soit $a_k(\underline{x})=x_{k+1}(x_1+x_2+\ldots+x_k)$ $k=1,2\ldots$ et $a(\underline{x})=(a_1(\underline{x}), a_2(\underline{x}),\ldots)$.

Remarquons que $\underline{a}(\underline{x})\geq 0$ si et seulement si $\underline{x}\geq 0$ ou $-\underline{x}\geq 0$.

Définissons les polynômes $P_n(\underline{x},u)$ et $A_n(\underline{x})$ par récurrence :

$P_1(\underline{x},u)=u-x_1$ $\quad A_1(\underline{x})=x_1$

$P_{n+1}(\underline{x},u)=P_n(a_1(\underline{x}),\ldots,a_n(\underline{x}),\ (u-(x_1+\ldots+x_{n+1}))^2)$

$A_{n+1}(\underline{x})=A_n(a_1(\underline{x}),\ldots,a_n(\underline{x}))$. A_n est une somme positive de monômes.

Proposition 1.

(i) P_n et A_n sont homogènes de degré 2^{n-1}

(ii) P_n est unitaire en chaque variable.

(iii) Si $\underline{x}\in\mathbb{R}^n$, $\underline{x}\geq 0 \iff \exists t\in\mathbb{R},\ P_n(\underline{x},t^2)=0$

(iv) Si $\underline{x}\in\mathbb{R}^n$, $\underline{x}\geq 0$ et $u\notin]0,2(x_1+\ldots+x_n)[$ alors $|P_n(\underline{x}_1 u)|\geq A_n(\underline{x})$

(v) Si $\underline{x}\in\mathbb{R}^n$ et l'un des $x_i<0$, alors $P_n(\underline{x},t^2)\geq|A_n(\underline{x})|$

Démonstration. (i) et (ii) sont faciles, (iii) est démontré dans [P2]. Démontrons (iv) par récurrence.

Le cas n=1 est clair, $|P_1(x,u)|=|u-x|\geq x$ si $u\notin]0,2x[$. Supposons la propriété vraie pour n, et montrons la pour n+1.

On a : $P_{n+1}(\underline{x},u)=P_n(a_1(\underline{x}),\ldots a_n(\underline{x}),(u-(x_1+\ldots+x_{n+1}))^2)$

or $(u-(x_1+\ldots+x_{n+1}))^2>(x_1+\ldots+x_{n+1})^2\geq 2(a_1(\underline{x})+\ldots+a_n(\underline{x}))$

D'où par l'hypothèse de récurrence :

$$|P_{n+1}(\underline{x},u)|\geq A_n(a_1(\underline{x}),\ldots,a_n(\underline{x}))=A_{n+1}(\underline{x})$$

(v) par récurrence : pour n=1 c'est vrai.

On a : $P_{n+1}(\underline{x},t^2)=P_n(a_1(\underline{x}),\ldots,a_n(\underline{x}),((t^2-(x_1+\ldots+x_{n+1}))^2)$.

Si $\underline{a}(\underline{x})\geq 0$, par la remarque on voit que $-\underline{x}\geq 0$.

On a alors en utilisant (iv) :

$$|P_{n+1}(\underline{x},t^2)|=P_{n+1}(-\underline{x},-t^2)|\geq|A_n(a_1(-\underline{x}),\ldots,a_n(-\underline{x}))|=|A_{n+1}(\underline{x})|$$

ce qui montre l'affirmation dans ce cas, $P_{n+1}(\underline{x},t^2)$ étant unitaire en t et ne pouvant s'annuler, son signe est constamment positif.

Sinon c'est que l'un des $a_i(\underline{x})<0$, et par récurrence :

$$P_{n+1}(x,t^2)\geq|A_n(a_1(\underline{x}),\ldots,a_n(\underline{x}))|=A_{n+1}(\underline{x}) \quad \blacksquare$$

Dans la suite de ce travail, on notera V un ensemble algébrique irréductible non réduit à un point contenu dans $\mathbb{R}^N$, I(V) son idéal, $k=\mathbb{R}(V)$ le corps des fractions de $\mathbb{R}[V]=\mathbb{R}[\underline{x}]/I(V)$ et $k'=\mathbb{C}(V)=k[i]$.

Proposition 2. Soit S un sous-ensemble semi-algébrique de V donné par la formule : $S=\{\underline{x}\in V \mid C_1(\underline{x})\geq 0,\ldots,C_n(\underline{x})\geq 0, B_1(\underline{x})>0,\ldots B_m(\underline{x})>0\}$.

Supposons qu'il existe un point de V où tous les polynômes A_i et B_j prennent une valeur strictement positive.

Alors il existe un polynôme $P(\underline{x},t)$ de $\mathbb{R}[\underline{x},t]$, et un polynôme $a(\underline{x})$ de $\mathbb{R}[\underline{x}]-I(V)$ tels que

(i) si $\underline{x}\in V$, $\underline{x}\in S \Leftrightarrow \exists t\in\mathbb{R},\ P(\underline{x},t)=0$

(ii) si $\underline{x}\in V$ et $\underline{x}\notin S$ $\quad P(\underline{x},t)\geq|a(\underline{x})|$

(iii) si $\underline{x}\in V$, $P(\underline{x},\infty)\geq 1$

(iv) P ne peut être constant pour $\underline{x}\in\mathbb{C}^n$ que si $a(\underline{x})=0$, et $P(\underline{x},t)=1$.

Démonstration.

$$\text{Soit } P(\underline{x},t)=(B_1\ldots B_m)^{2^{m+n-1}} P_{m+n}\left(C_1,\ldots,C_n,B_1,\ldots,B_{m-1},\frac{1}{B_1\ldots B_m},t^2\right).$$

Par la proposition 1 $P(\underline{x},t)$ a une racine réelle si et seulement si $C_1(\underline{x})\geq 0,\ldots\ C_n(\underline{x})\geq 0,\ B_1(\underline{x})>0,\ldots\ B_m(\underline{x})>0$. De plus on a $P(\underline{x},t)\geq|a(\underline{x})|$ si l'un des $C_i<0$ ou l'un des $B_i=0$, avec $a(\underline{x})$ donné par :

$$a(\underline{x})=(B_1\ldots B_m)^{2^{m+n-1}} A_{m+n}\left(C_1,\ldots,C_n,B_1,\ldots,B_{m-1},\frac{1}{B_1B_2\ldots B_m}\right).$$

En effet si l'un des B_i est égal à zéro, A_{n+m} n'étant pas unitaire on a $a(\underline{x})=0$. Dans le cas où aucun des B_i ne s'annule on utilise directement la proposition 1.

On voit que $a(\underline{x})\notin I(V)$ car $a(\underline{x})$ est une somme positive de monômes en les C_i et B_j qui sont tous strictement positifs en un certain point de V.

Enfin, P ne peut être constant que si $B_1\ldots B_m=0$ et à ce moment-là $a(\underline{x})=0$ et $P(\underline{x},t)=1$. ∎

Dans la démonstration du théorème suivant, on va utiliser le *théorème d'irréductibilité de Hilbert* (cf. [L1] p.225, 236 et 239). Rappelons-le sous la forme qui nous intéresse ici :

Si A est un anneau de type fini sur $\mathbb{R}$, k son corps des fractions qui n'est pas algébrique sur $\mathbb{R}$, k' une extension algébrique finie de k, et $P(\lambda,t)$ un polynôme irréductible dans $k[\lambda,t]$. Alors il existe $\lambda_0 \in A$, tel que $P(\lambda_0,t)$ soit irréductible dans $k'[t]$.

Théorème 1 (Elimination relative des inégalités).

Soit $V \subset \mathbb{R}^N$ un ensemble algébrique irréductible non réduit à un point, I(V) son idéal, $k=\mathbb{R}(V)$; $k'=k[i]$, et S un ensemble semi-algébrique contenu dans V. Alors il existe un polynôme $P(\underline{x},t) \in \mathbb{R}[\underline{x},t]$ tel que :

(i) Si $\underline{x} \in V$, $\underline{x} \in S \Leftrightarrow \exists t \in \mathbb{R}$, $P(\underline{x},t)=0$

(ii) La réduction de $P(\underline{x},t)$ modulo I(V) est irréductible dans $k'[t]$

(iii) $P(\underline{x},t)$ n'est identiquement nul pour aucune valeur de $\underline{x} \in \mathbb{C}^N$.

Démonstration.

Soit $S=\bigcup_1^M S_i$, $S_i=\{x \in V \mid C_1^i \geq 0, \ldots, C_{n_i}^i \geq 0, \quad B_1^i>0, \ldots, B_{m_i}^i>0\}$. Quitte à décomposer chaque S_i en une réunion d'ensembles du même type, on peut supposer que pour chaque i il existe un point $\underline{x}_i \in V$ tel que : $C_j^i(\underline{x}_i)>0$, $B_k^i(\underline{x}_i)>0$, $j=1,\ldots,n_i$, $k=1,\ldots,m_i$.

Pour chaque i, soit $P_i(\underline{x},t)$ et $a_i(\underline{x})$ des polynômes donnés par la proposition 2.

Soit $H(\underline{x})=a_1^2(\underline{x})\cdot\ldots\cdot a_M^2(\underline{x})$, et $\lambda(\underline{x})$ un polynôme quelconque.

Définissons P par la formule :

$$P(\underline{x},t)=(1+H+H\cdot\lambda^2(\underline{x}))P_1^2\ldots P_M^2-H(\underline{x})$$

Démontrons que le polynôme P a les propriétés voulues :

(i) Si $\underline{x} \in \bigcup_1^M S_i$ l'un des P_i s'annule pour une certaine valeur de t, et $P(\underline{x},t)$ prend une valeur négative ou nulle. Quand t tend vers l'infini $P(\underline{x},t)$ prend des valeurs strictement positives. P s'annule donc pour une

valeur réelle de t. D'autre part si $\underline{x} \notin \bigcup_1^M S_i$, $P_i^2(\underline{x},t) \geq a_i^2(x)$, d'où $P_1^2 \ldots P_M^2 \geq H(\underline{x})$ et cela implique que $P(\underline{x},t) \geq H^2(\underline{x})$ et par suite $P(\underline{x},t)>0$.
Ce polynôme P a donc les bonnes propriétés de projection.

(ii) En vertu du théorème d'irréductibilité de Hilbert, pour montrer qu'il existe un polynôme λ de $\mathbb{R}[V]$ tel que P soit irréductible dans k[V] il suffit de démontrer le lemme suivant :

Lemme. Soit k un corps, B,H,K des éléments non nuls de k, $A \in k[t]$ un polynôme non constant, alors $P=(K+H\lambda^2)A^2-B^2$ est irréductible dans $k[\lambda,t]$.

Démonstration du lemme.

P n'a pas de diviseur non constant dans k[t], en effet ce diviseur diviserait A, et par soustraction B ce qui est impossible puisque $B \in k$.
Si $P=(\alpha\lambda+\beta)(\gamma\lambda+\delta)$ avec $\alpha,\beta,\gamma,\delta$ dans k[t] on a $\alpha\cdot\beta\cdot\gamma\delta \neq 0$ et $\alpha\gamma=HA^2$, $\alpha\delta+\gamma\beta=0$ et $\beta\delta=KA^2-B^2$.
De la deuxième relation on tire par le lemme de Gauss : $\alpha=r\gamma$, $\beta=-r\delta$ avec $\delta \in k$, en reportant dans la troisième relation on obtient $B^2=KA^2+r\delta^2$ avec $K,r \in k$. Comme B est un polynôme constant de k[t] et que A ne l'est pas, on voit en identifiant que $r=-v^2K$ où $v \in k$, et par suite $B=K(A-v\delta)(A+v\delta)$ d'où $A+v\delta \in k$, $A-v\delta \in k$ ce qui implique que $A \in k$ ce qui n'est pas vrai.
La démonstration du lemme, et donc de (ii) est achevée.

(iii) Montrons enfin que le polynôme obtenu $P(\underline{x},t)$ ne s'annule identiquement en aucun point $\underline{x}$ de $\mathbb{C}^N$. Sinon, si $(1+H+H\lambda^2)=0$ en ce point, alors H=0 et par suite $P_1^2 \ldots P_M^2=0$ ce qui est impossible, ce polynôme ayant une limite au moins égale à 1 quand t tend vers l'infini.
Par suite la seule possibilité c'est que $P_1^2 \ldots P_M^2$ soit de degré 0 en t, c'est-à-dire que chaque polynôme P_i le soit, mais alors c'est que chaque

$a_i=0$ et chaque $P_i=1$ et par suite $P=P_1^2\ldots P_M^2=1\neq 0$ ∎

Remarques. L'utilisation du théorème de Hilbert, si elle permet un énoncé beaucoup plus général que celui trouvé en [P2] et [P3] ne fournit pas vraiment d'indications sur la manière de trouver le polynôme $\lambda(\underline{x})$. D'autre part les degrés (même en t) des polynômes obtenus sont plus élevés que ceux qu'on obtient en [P2] pour des ensembles semi-algébriques localement fermés.Enfin, dans le cas où S est fermé le polynôme P obtenu, contrairement à ceux de [P4] n'est pas unitaire. On pourrait en modifiant la définition de P faire en sorte qu'il le soit, mais au prix d'un degré plus élevé.

§3. Les projections de variétés algébriques réelles.

Dans ce paragraphe nous allons déduire de l'irréductibilité des équations de certains ensembles leur irréductibilité géométrique. Une telle déduction nécessite évidemment quelques précautions : $X^2+Y^2(Y+1)^2=0$ est bien une équation irréductible, mais l'ensemble de ses zéros ne l'est pas. (D'après le théorème 1 cet ensemble a même une équation $\mathbb{C}$-irréductible). Notre outil sera une généralisation du critère de changement de signe.
Commençons par rappeler quelques notations : $V\subset\mathbb{R}^N$ est un ensemble algébrique irréductible, I(V) l'idéal de $\mathbb{R}[x_1,\ldots,x_N]=\mathbb{R}[\underline{x}]$ formé de tous les polynômes qui s'annulent sur V, $\mathbb{R}[V]=\mathbb{R}[\underline{x}]/I(V)$ et $k=\mathbb{R}(V)$ le corps des fractions de $\mathbb{R}[V]$. On suppose que V n'est pas réduit à un point. Un polynôme de $\mathbb{R}[\underline{x},t]$ sera dit irréductible modulo I(V), s'il est irréductible, et si sa réduction modulo I(V) est un polynôme irréductible de k[t]. On dira enfin qu'un élément de $\mathbb{R}[\underline{x},t]$ est un polynôme réel.
Si W est un ensemble algébrique réel contenu dans $\mathbb{R}^m$ notons $W_{\mathbb{C}}$ le sous-ensemble de $\mathbb{C}^m$ où tous les polynômes de I(W) s'annulent : $W_{\mathbb{C}}\cap\mathbb{R}^m=W$.
Si W est irréductible, $W_{\mathbb{C}}$ l'est aussi.

On va utiliser un théorème classique en géométrie algébrique sur un corps algébriquement clos, qui n'a pas d'analogue en géométrie algébrique réelle (cf. [L2] page 36, ou aussi [Sam] ou [Sha]).

Théorème sur la dimension des intersections.

Soit $U \subset \mathbb{C}^n$ une variété affine irréductible de dimension h. Soit $P(\underline{x})$ un polynôme de $\mathbb{C}[\underline{x}]$. Si $U \cap \{P(\underline{x})=0\}$ est non vide, et si P ne s'annule pas sur U tout entier, alors toutes les composantes irréductibles de cette intersection ont la même dimension h-1. ∎

Corollaire. Soit $\tilde{W}=\{(\underline{x},t) \in V_{\mathbb{C}} \times \mathbb{C} \mid R(x,t)=0\}$ où R(x,t) est un polynôme ne s'annulant identiquement en aucun point $\underline{x} \in V_{\mathbb{C}}$. Soit $W' \subset \mathbb{C}^{N+1}$ un ensemble algébrique, et a(x) un polynôme non identiquement nul sur V, alors si $\tilde{W} - \{a(\underline{x})=0\} \subset W'$ on a aussi $\tilde{W} \subset W'$.

Démonstration. D'après le théorème sur la dimension des intersections, chacune des composantes irréductibles de $\tilde{W}$ est de dimension r, et aucune d'elles ne peut être contenue dans $\tilde{W} \cap \{a(\underline{x})=0\} = (\{a(\underline{x})=0\} \cap V_{\mathbb{C}} \times \mathbb{C}) \cap \{R(x,t)=0\}$ qui est de dimension r-1 (R(x,t) ne pouvant s'annuler identiquement sur aucune des composantes de $\{a(\underline{x})=0\} \cap V_{\mathbb{C}} \times \mathbb{C}$ puisque ces composantes sont des cylindres).

Soit W_i une composante irréductible de $\tilde{W}$, comme $W_i \subset W' \cup (\tilde{W} \cap \{a(\underline{x})=0\})$ et $W_i \subset (\tilde{W} \cap \{a(\underline{x})=0\})$, on a donc $W_i \subset W'$ et par suite $\tilde{W} \subset W'$. ∎

Proposition 3 (Généralisation du critère de changement de signe).

Soit $V \subset \mathbb{R}^n$ un ensemble algébrique irréductible, I(V) son idéal, $R(\underline{x},t)$ un polynôme réel irréductible modulo I(V) qui n'est identiquement nul pour aucune valeur de $\underline{x} \in V_{\mathbb{C}}$. Alors, si $W=\{(\underline{x},t) \in V \times \mathbb{R} \mid R(\underline{x},t)=0\}$ se projette verticalement sur un ensemble de même dimension que V, W est irréductible.

Démonstration. Le cas où V est un point étant trivial, on peut donc supposer que V n'est pas réduit à un point. On peut supposer aussi que R est de même degré que sa réduction modulo I(V). Montrons que cette hypothèse implique que R est de degré minimal au sens suivant : soit P un polynôme de $\mathbb{R}[\underline{x},t]$ non congru à zéro modulo I(V), nul sur un fermé $W_1 \subset W$ de dimension maximale, et de degré minimal en t parmi tous les polynômes ayant ces propriétés. Le coefficient $b(\underline{x})$ du terme de plus haut degré en t de $P(\underline{x},t)$ n'appartient pas à I(V). On a la division dans $\mathbb{R}[\underline{x},t]$:

$$b^M(\underline{x})R(\underline{x},t)=\lambda(\underline{x},t)P(\underline{x},t)+R_1(\underline{x},t).$$

Par la minimalité de P, on voit que R_1 est congru à zéro modulo I(V), et en réduisant modulo I(V) on obtient : $\overline{b^M(\underline{x})}\,\overline{R(\underline{x},t)}=\overline{\lambda(\underline{x},t)}\,\overline{P(\underline{x},t)}$. Comme $\overline{R(\underline{x},t)}$ est irréductible dans $\mathbb{R}(V)[t]$ et $\overline{P(\underline{x},t)}$ n'est pas de degré zéro en t, on en déduit que P et R ont même degré en t, c'est-à-dire que R est de degré minimal.

Supposons maintenant que le polynôme Q s'annule sur un fermé $W_1 \subset W$ de dimension maximale. Si $a(\underline{x}) \notin I(V)$ est le coefficient du terme de plus haut degré en t de $R(\underline{x},t)$, on a la division (d) dans $\mathbb{R}[\underline{x},t]$:

$$a^D(\underline{x})Q(\underline{x},t)=\mu(\underline{x},t)R(\underline{x},t)+R_2(\underline{x},t) \qquad (d)$$

Par la minimalité de R, on voit que $R_2 \in I(V)[t]$.

Soit $$\tilde{W}=\{(\underline{x},t)\in V_{\mathbb{C}}\times\mathbb{C} \mid R(\underline{x},t)=0\}$$

et $$W'=\{(\underline{x},t)\in\mathbb{C}^{n+1} \mid Q(\underline{x},t)=0\}$$

De l'égalité (d) on déduit que $\tilde{W}-\{a(x)=0\} \subset W'$. Par le corollaire, cela implique que $\tilde{W} \subset W'$, c'est-à-dire que le polynôme Q s'annule sur $\tilde{W}$ tout entier, donc sur $W \subset \tilde{W}$ ∎

Remarque. Si $V=\mathbb{R}^N$, la proposition 3 n'est autre que le critère de changement de signe (voir [BCR] page 85 ou [Mil] p.14).

Nous sommes maintenant en mesure de démontrer le résultat principal de ce travail :

Théorème 2. Un semi-algébrique de $\mathbb{R}^n$ est la projection d'un ensemble algébrique irréductible de $\mathbb{R}^{n+1}$ si et seulement si son adhérence de Zariski est un ensemble algébrique irréductible.

Démonstration. Soit S ce semi-algébrique et V son adhérence de Zariski qu'on suppose irréductible, par le théorème 1 et le critère de changement de signe généralisé (proposition 3) on voit que S est projection d'un ensemble algébrique irréductible de $\mathbb{R}^{n+1}$.

La réciproque est facile : si l'adhérence de Zariski de S n'est pas irréductible, on peut trouver deux polynômes P_1 et P_2 non identiquement nuls sur S, tels que leur produit soit identiquement nul sur S. Par suite si $W \subset \mathbb{R}^{n+1}$ se projette sur S, ces deux polynômes ne sont pas identiquement nuls sur W, mais leur produit l'est, ce qui montre que W n'est pas irréductible. ■

Remarque. Les projections obtenues ici sont quasi-finies, c'est-à-dire que leurs fibres sont des ensembles finis.

REFERENCES BIBLIOGRAPHIQUES

[A.G1] **C. Andradas et J.M. Gamboa**, *A note on projections of real algebraic varieties*, Pacific Journal of Mathematics, vol.115, n°1, 1984, p.1-11.

[A.G2] **C. Andradas et J.M. Gamboa**, *On projections of real algebraic varieties*, Pacific Journal of Mathematics, vol.121, n°2, 1986, p.281-291.

[B.C.R] **J. Bochnak, M. Coste & M.F., Coste Roy**, *Géométrie algébrique réelle*, Ergebnisse der Mathematik, vol.12, Springer-Verlag, 1987.

[L1] **S. Lang**, *Fundamentals of diophantine geometry*, Springer-Verlag, 1983.

[L2] **S. Lang**, *Introduction to algebraic geometry*, Interscience, 1958.

[Mil] **J. Milnor**, *Singular points of complex hypersurfaces*. Princeton, Princeton University Press, 1968.

[Mot1] **T.S. Motzkin**, *Elimination theory of algebraic inequalities*, B.A.M.S., 61, 1955, 326.

[Mot2] **T.S. Motzkin**, *The real solution set of a system of algebraic inequalities is the projection of a hypersurface in one more dimension*, Inequalities II, Academic Press, 1970, p.251-254.

[P1] **D. Pecker**, *Sur l'équation d'un ensemble algébrique de* R^{n+1} *dont la projection dans* R^n *est un ensemble semi-algébrique fermé donné*, C.R. Acad. Sci. Paris, t.306, série II, p.265-268, 1988.

[P2] **D.Pecker**, *L'elimination radicale des inégalités* Séminaire DDG 1987

[P3] **D. Pecker**, *On the elimination of algebraic inequalities*, à paraître au Pacific Journal of Mathematics.

[P4] **D. Pecker**, *Projections propres de variétés algébriques réelles*, C.R. Acad. Sci. Paris, t.309, série I, p.777-779, 1989.

[Sam] **P. Samuel**, *Méthodes d'algèbre abstraite en géométrie algébrique*, Berlin, Heidelberg, New York, Springer, 1967.

[Sha] **I.R. Shafarevich**, *Basic algebraic geometry*, Berlin, Heidelberg, New York, Springer, 1974.

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.

N° 4. **M. Giraudet.**
Groupes à moitié ordonnés. Première partie : Présentation axiomatique des groupes de permutations monotones de chaînes, février 1990.

N° 5. **M. Giraudet et F. Lucas.**
Groupes à moitié ordonnés. Deuxième partie : Sous–groupes de groupes à moitié réticulés, février 1990.

N° 6. **C. Michaux.**
Ordered rings over which output sets are recursively enumerable sets, février 1990.

N° 7. **V. Danos.**
Lambda–calculus and its dynamic algebra 1 : basic results, février 1990.

N° 8. **L. Regnier.**
A propos de l'équivalence opérationnelle.

N°9. **Ch. Berline.**
Rétrations et Interprétation interne du polymorphisme : Le problème de la rétraction universelle.

N° 10. **D. Gondard–Cozette.**
Axiomatisations simples des théories des corps de Rolle.

N° 11. **A. Fleury et C. Retoré.**
The MIX rule : a proofnet syntax for multiplicatives, their units and (A⊗B)-o(A&B).

N° 12. **P. Malacaria et L. Regnier.**
Lambda–calculus and its dynamic algebra 3 : Weak Nilpotency.

N° 13. **D. Lascar.**
Les automorphismes d'un ensemble fortement minimal.

N° 14. **D. Gluschankof and M. Tilli.**
On some extension theorems in functional analysis and the theory of boolean algebras.

N° 15. **U. Gropp.**
There is no sharp transitivity on q^6 when q is a type of Morley rank 2.

N° 16. **M.A. Dickmann.**
A combinatorial geometric structure on the space of orders of a field.

N° 17. **F. Delon, M. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées 1989–90, décembre 1990.

N° 18. **J.Y. Girard.**
Logic and exceptions : A few remarks.

Hors série. **Y.J. Ringard.**
Mustard watches : an integrated approach to time and food.