UNIVERSITE DE PARIS VII

STRUCTURES ALGEBRIQUES ORDONNEES

SEMINAIRE 1986-1987

F. DELON, M. DICKMANN, D. GONDARD

SEMINAIRE DE STRUCTURES ALGEBRIQUES ORDONNEES.

F. Delon - M. Dickmann - D. Gondard

1986-87, Université Paris VII

-=-=-=-=-=-

7 et 14.10.86 - **F.Delon** et **F. Lucas.**

Groupes abéliens ordonnés et paires de groupes abéliens ordonnés divisibles. (*)

4.11.86 - **D. Gondard.**

Ordres de niveau supérieur et extensions.

18.11.86 - **M. Dickmann.**

Corps chaîne-clos.

25.11.86 - **L. Bélair.**

Mesures sur les groupes de Galois ; côté cours. (*)

02.12.86 - **J.L. Duret.**

Idem ; côté Jarden. (*)

16.12.86 - **M. Giraudet, F. Lucas** et **F. Oger.**

$G \times G \# H \times H \overset{?}{\Longrightarrow} G \# H$, où G et H sont des groupes abéliens ordonnés.

20.01.87 - **L. Bélair.**

Equivalence élémentaire et codimension dans les corps p-adiques.

27.01.87 - **D. Gondard.**

Axiomatisations à la "Artin-Schreier" des corps chaînables et des corps chaîne-clos.

03.02.87 - **J. Heintz** (Frankfurt (R.F.A.) et Nice).

Elimination des quantificateurs rapide dans les réels clos.

10.02.87 - **C. Michaux** (Mons, Belgique).

Corps différentiels ordonnés.

3.03. 87 - **F. Delon** et **F. Lucas.**

Constructions variées sur les groupes abéliens ordonnés.

10.03.87 - **L. Bélair.**

Spectre p-adique : aspects topologiques et géométriques.

16.03.87 - **F. Delon** et **D. Gondard.**

Sommes de puissances 2^n de fonctions rationnelles à coefficients dans un corps chaîne-clos.

17.03.87 - **F.V. Kuhlmann** (Heidelberg, R.F.A.).

Maximality properties of valued fields : new results.

24.03.87 - **E. Becker** (Dortmund, R.F.A.).

On Galois groups of formally real fields.

7.04.87 - **M. Giraudet.**

Une classe de groupes réticulés avec des invariants de Schmidt.

28.04.87 - **L.M. Pardo** (Santander (Espagne) et Rennes.

Rubin's width of a complete proof and the width of a semi-algebraic set. (*)

4 et 5.05.87 - **D. Mundici** (Florence, Italie).

Approximately finite-dimensional C^*-algebras, abelian ℓ-groups and Lukasiewicz's infinitely valued logic.

12 et 19.05.87 - **R. Bouscaren.**

Version modèle-théorique du théorème de Weil.

02.06.87 - **M. Gautier.**

Simplification pour les produits d'ordres totaux.

09.06.87 - **C. Steinhorn** (Vassar College et Notre Dame, Etats-Unis).

Expansions of $< \mathbb{R}, +, < >$.

19.06.87 - **A. Prestel** (Konstanz, R.F.A.).

An application of quantifier elimination to the space of orders of Hilbertian fields.

23.06.87 - **E. Dubuc** (Buenos-Aires, Argentine - Montréal, Canada).

La sémantique de Kripke et la logique des topos.

(*) Pas de manuscrit pour cet exposé.

ORDRES DE NIVEAU SUPERIEUR, EXTENSIONS ET CORPS CHAINE-CLOS

par

Danielle GONDARD

(Université de Paris VI)

I - NOTIONS PRELIMINAIRES

1 - Notion d'ordre de niveau supérieur.

Il s'agit de la notion d'ordre de niveau supérieur définie par E. Becker, en 1978 dans [Be 2] à l'I.M.P.A., sur un corps commutatif K ,

C'est un préordre T de niveau 2^n (i.e. $T+T \subset T$, $T.T \subset T$, $K^{2^n} \subset T$), propre (i.e. $-1 \notin T$ ou de manière équivalente $T \cap -T = \{0\}$ ou encore car $K = 0$ et $T \neq K$), maximal.

L'ordre sera dit de niveau exact 2^n si de plus $K^{2^{n-1}} \notin T$.

De tels ordres ne peuvent exister que si car $K = 0$.

En fait on a une première caractérisation des corps qui admettent des ordres de niveau supérieur :

Les trois propriétés ci-dessous sont équivalentes

(i) K *admet des ordres de niveau* 2^n

(ii) $-1 \notin \Sigma K^{2^n}$ (*où* $\Sigma K^{2^n} = \bigcup_{p=1}^{\infty} \{ \sum_{i=1}^{p} x_i^{2^n} , (x_1, \ldots, x_p) \in K^p \}$)

(iii) *car* $K = 0$ *et* $\Sigma K^{2^n} \neq K$

(iv) $-1 \notin \Sigma K^2$

Par la propriété (iv) *on déduit que* *les corps admettant des ordres de niveau* 2^n *sont exactement les corps ordonnables*.

On peut alors étudier le niveau d'ordre n , s_n d'un corps non ordonnable : on appellera s_n le plus petit entier tel que -1 soit somme de s_n puissances 2^n-ièmes dans le corps. Les problèmes sont alors de déterminer le niveau d'ordre n d'un corps non ordonnable donné et de déterminer en général quels types de nombres peuvent être des niveaux d'ordre n de corps non ordonnables (pour $n=1$ on sait que les s_1 sont des puissances de 2).

Les ordres de niveau supérieur sont en relation avec les sommes de puissances 2^n dans le corps, plus précisément on a :

$\Sigma K^{2^n} = \cap p$ où p décrit l'ensemble des ordres de niveau 2^n . (de niveau exact ou non, donc en fait tous les ordres de niveau exact 2^m avec $m \leqslant n$).

Théorème Fondamental -

Les ordres de niveau 2^n *sont donnés par les parties* $p \subset K$ *telles que :*

$p \neq K$, $0 \in p$, $p+p \subset p$;

$\dot{p} = p - \{0\}$ *est un sous groupe de* $\dot{K}$ *et* $\dot{K}/\dot{p}$ *est cyclique avec* $|\dot{K}/\dot{p}|$ *divise* 2^n .

L'ordre est de niveau exact 2^n *si* $|\dot{K}/\dot{p}| = 2^n$.

DANS TOUTE LA SUITE, K SERA UN CORPS COMMUTATIF, DE CARACTERISTIQUE 0 , ORDONNABLE ET ΣK^{2^n} DESIGNERA L'ENSEMBLE $\bigcup_{p=1}^{\infty} \{ \sum_{i=1}^{p} x_i^{2^n} \ / \ (x_1, \ldots, x_p) \in K^p \}$.

2 - Exemples

a) $K = \mathbb{R}((X))$

pour tout $i \geqslant 2$:

$$P_i = \{ \sum_{j=m}^{\infty} a_j t^j : a_m > 0 \text{ et } m \equiv 0 \ (2^i) \text{ ou } a_m < 0 \text{ et } m \equiv 2^{i-1} \ (2^i) \}$$

est un ordre de niveau 2^i de K .

Théorème

Soit K *un corps ordonnable, alors*

ou tout ordre de niveau supérieur est un ordre

ou pour tout $n \in \mathbb{N}$ *il existe des ordres de niveau exact* 2^n .

Il s'agit alors de déterminer quels corps rentrent dans l'un ou l'autre des cas ci-dessus.

b) Parmi les corps n'ayant pas d'ordre de niveau supérieur distincts des vrais ordres on peut citer

- Les corps ordonnables n'ayant qu'un seul ordre
- Les corps ordonnables dont tous les vrais ordres sont archimédiens
- Les extensions algébriques de corps n'ayant pas d'ordre de niveau supérieur.

On a donc par exemple les corps réels clos, et les corps de nombres algébriques réels qui ne peuvent admettre d'ordre de niveau supérieur distinct des ordres usuels.

Les résultats ci-dessus découlent en fait du théorème suivant :

Théorème :

Soit K *un corps ordonnable.*

Les propriétés ci-dessous sont équivalentes :

(i) *Tout ordre de niveau supérieur est un ordre*

(ii) *Tout semi-ordre normé de niveau supérieur est un ordre*

(iii) *Tout anneau de valuation réel a un groupe des valeurs 2-divisible*

(iv) $\Sigma K^2 = \Sigma K^{2^n}$ *pour tout* n

(v) $\Sigma K^{2^n} = \Sigma K^{2^{n+1}}$ *pour un* n

On peut donc dans les corps n'admettant pas d'ordre de niveau supérieur non trivial s'intéresser à la décomposition des éléments totalement positifs en sommes de puissances 2^n (nombres de puissances intervenant, constructibilité,...

c) Corps admettant des ordres de niveau supérieur non triviaux

- Tous les corps non de Pasch (ou non S.A.P.) par exemple $\mathbb{Q}(X)$
- Mais certains corps de Pasch peuvent admettre des ordres de niveau supérieur non triviaux par exemple $\mathbb{R}((X))$
- $\mathbb{Q}((X))$.

Enfin si un corps K admet exactement deux ordres (vrais) et des ordres de niveau supérieur non triviaux, alors il existe $\alpha \in \dot{K}$ tel que

(i) $p^+ = \Sigma K^2 \cup \alpha \Sigma K^2$

$p^- = \Sigma K^2 \cup -\alpha \Sigma K^2$ sont les deux ordres de K .

(ii) $p_n = \Sigma K^{2^n} \cup -\alpha^{2^{n-1}} \Sigma K^{2^n}$ est pour $n \geq 2$ l'unique ordre de niveau exact 2^n .

(iii) $\Sigma K^{2^{n-1}} = \Sigma K^{2^n} \cup \alpha^{2^{n-1}} \Sigma K^{2^n}$ pour tout $n \geq 2$

(iv) ΣK^{2^n} est un préordre de niveau supérieur tel que pour tout sous groupe maximal U , sur $\Sigma \dot{K}^{2^n}$, $U \cup \{0\}$ est un ordre.

3 - Relations avec la théorie des valuations.

Soit K un corps ordonnable, p un ordre de niveau n .

Remarquons que $\mathbb{Q} \subset K$, $\mathbb{N}^* \subset \dot{p}$ et donc $\mathbb{Q}^+ \subset p$.

On pose :

$$A(p) = A(\mathbb{Q},p) = \{a \in K : \exists\, b \in \mathbb{Q}^+ \ , \ b \pm a \in p\}$$

$$I(p) = I(\mathbb{Q},p) = \{a \in K : \forall b \in \mathbb{Q}^+ \ , \ b \pm a \in p\} \quad .$$

On a alors le théorème dû à Becker suivant.

Théorème

1) $A(p)$ *est un anneau de valuation de* K *d'idéal maximal* $I(p)$.

2) p *induit sur le corps résiduel* $k = A(p)/I(p)$ *un ordre (vrai)* $\bar{p}$ *archimédien.*

$A(p)$ *est donc réel puisque* k *est ordonnable*

($\bar{p} = \{a + I(p)$ *avec* $a \in A(p) \cap p\}$) .

On dira qu'un anneau de valuation A est compatible avec p et on notera $A \sim p$ si $1+I \subset p$.

Alors $\bar{p}$ est un ordre de niveau supérieur de $k = A/I$ et le niveau de $\bar{p}$ est inférieur ou égal au niveau de p .

(Donc A est réel car k ayant un ordre de niveau supérieur est ordonnable).

Un théorème relie alors $A(p)$ et les anneaux de valuation compatibles avec p :

Théorème :

Un anneau de valuation A *est compatible avec* p *si et seulement si* $A(p) \subset A$.

4 - Une autre présentation des ordres de niveau supérieur

Dans le cas des ordres vrais, si p est un ordre donné sur un corps K on peut définir un homomorphisme σ_p du groupe $\dot{K}$ dans le groupe $\{\pm 1\}$ par $\sigma_p(x) = 1$ si $x \in p$ est $\sigma_p(x) = -1$ si $x \in -p$.

On remarque que le noyau de cet homomorphisme est additivement fermé, i.e. si $\sigma_p(x_1) = 1$ et $\sigma_p(x_2) = 1$ alors $\sigma_p(x_1+x_2) = 1$.

Inversement si σ est un homomorphisme de $\dot{K} \to \mu_2 = \{+1, -1\}$, avec $\operatorname{Ker} \sigma$ additivement fermé alors

$p = \operatorname{Ker} \sigma \cup \{0\}$ est un ordre sur K .

On peut effectuer une présentation analogue pour les ordres de niveau 2^n .

Définition

On appelle signature de niveau 2^n un homomorphisme du groupe $\dot{K}$ dans $\mu_{2^n} = \{z \in \mathbb{C} \ / \ z^{2^n} = 1\}$, dont le noyau est additivement fermé.

La signature χ sera de niveau exact 2^n si 2^n est l'ordre de $\operatorname{Im} \chi$.

Théorème [B - Ha - R] .

Un sous-ensemble $p \subset K$ *est un ordre de niveau (Resp. de niveau exact)* 2^n *si et seulement si* p *est le noyau d'une signature de niveau (Resp. de niveau exact)* 2^n .

Remarquons que χ n'est unique que dans le cas des ordres vrais ; dans les autres cas χ_1 et χ_2 déterminent le même ordre de niveau supérieur si et seulement si il existe τ , automorphisme de μ_{2^n} , tel que $\tau \circ \chi_1 = \chi_2$.

Notations - On pose alors pour toute signature χ de K :

$$A(\chi) = A(\mathrm{Ker}\ \chi \cup \{0\}) = A(p)$$

$$I(\chi) = \{a \in K \mid \forall n \in \mathbb{N} : \frac{1}{n} \pm a \in \mathrm{Ker}\ \chi\}$$

(i) Alors $A(\chi)$ est un anneau de valuation d'idéal maximal $I(\chi)$. Le corps résiduel $A(\chi)/I(\chi)$ est ordonnable.

(ii) χ induit la signature d'un ordre archimédien p de $A(\chi)/I(\chi)$ via

$$\varepsilon + I(\chi) \to \chi(\varepsilon) \ , \ \varepsilon \in A(\chi) \quad \text{(unités de } A(\chi)) \ .$$

II - Ordres de Niveau Supérieur et Extensions

Soit L/K une extension du corps K.

Soit p un ordre de niveau supérieur de L ;

Alors $p \cap K$ est un ordre sur K et le niveau exact de $K \cap p$ est inférieur ou égal au niveau exact de p.

En effet on a $\dot{K}/\dot{K \cap p} \hookrightarrow \dot{L}/\dot{p}$ donc $\dot{K}/\dot{K \cap p}$ ext cyclique.

Le niveau des ordres ne peut donc que croître lors des extensions de (K,p).

Définition II-1

On dit que p *est une* ***extension fidèle*** *de* $K \cap p$ *si les niveaux exacts de* p *et* $K \cap p$ *sont égaux donc si* $[\dot{L} : \dot{p}] = [\dot{K} : \dot{K \cap p}]$.

Si on adopte la présentation avec les signatures on obtient : Soit K un corps muni de l'ordre de niveau supérieur p_K. Soit χ une signature telle que $\dot{p}_K = \text{Ker } \chi$, alors pour toute extension fidèle (L,p_L) de (K,p_K) il existe une signature χ_L de L telle que :

$$\chi_L(\dot{L}) = \chi(\dot{K}) \quad , \quad \text{Ker } \chi_L = \dot{p}_L \text{ et}$$

$$\chi_L|_{\dot{K}} = \chi \ .$$

Toutes les extensions ne sont pas fidèles :

Exemple II-2 - $K = \mathbb{Q}(X)$ est non de Pasch et a donc des ordres de niveau exact 2^r pour tout n. Notons p_{2^n} un tel ordre alors tous les $p_{2^n} \cap \mathbb{Q}$ sont l'ordre usuel de $\mathbb{Q}$ donc de niveau 2^1 , puisque $\mathbb{Q}$ n'a que l'ordre usuel comme ordre de niveau supérieur.

Exemple II-3 - Soit $K = \mathbb{R}((X))$ et $L = K(\sqrt{X})$ (ou $L = \mathbb{R}((X^{1/2}))$).

Sur K il existe deux ordres usuels p_o et p_1 tels que $X \in p_o$ et $-X \in p_1$ et p_o et p_1 étendent l'ordre de $\mathbb{R}$.

p_o s'étend en deux ordres vrais sur L , mais p_1 ne s'étend pas en un ordre sur L .

p_1 s'étend au seul ordre de niveau 2^2 de L qui est explicitement :

$$P_2^L = \{ \sum_{j=m}^{\infty} a_j (\sqrt{X})^j \ : \ a_m > 0 \quad \text{et} \quad m \equiv 0 \ (4) \quad \text{ou} \quad a_m < 0 \quad \text{et} \quad m \equiv 2 \ (4) \} \ .$$

Ici de manière générale l'ordre p_m de niveau 2^m , $m \geq 1$, s'étend à l'unique ordre de niveau 2^{m+1} de L ; le niveau ne peut que croître.

La théorie des extensions des ordres de niveau supérieur a été développée par Becker [Be 2] puis simplifiée et améliorée par Harman et Rosenberg [H-R] .

Théorème II-4 -

Soit p *un ordre de niveau exact* 2^n *sur le corps* K .

Soit L *une extension quelconque de* K .

Les conditions suivantes sont équivalentes :

(i) p *admet une extension fidèle* $\tilde{p}$ *à* L

(ii) $T = \{ \sum_{\text{finies}} a_i x_i^{2^n} \mid a_i \in p \ , \ x_i \in L \}$ est un préordre propre

(iii) $-1 \notin \{ \sum_{\text{finies}} a_i x_i^{2^n} \mid a_i \in p \ , \ x_i \in L \}$.

Démonstration

(ii) $\Leftrightarrow$ (iii) est évident car T est toujours un préordre.

(i) $\Rightarrow$ (ii) car T est le préordre de niveau 2^n engendré par p et donc $T \subset \tilde{p}$. Si T n'était pas propre alors $T = K$ et aussi $\tilde{p} = K$ ce qui est impossible.

(ii) $\Rightarrow$ (i) Si T préordre de niveau 2^n est propre alors tout ordre $\tilde{p}$ tel que $T \subset \tilde{p}$ est une extension fidèle à cause du plongement

$$\dot{K}/\dot{p} \hookrightarrow \dot{L}/\dot{\tilde{p}} \quad .$$

Remarque sur (iii)

On a donc $-1 \notin \Sigma x_i^{2^n}$, donc il existe bien un ordre de niveau (non forcément exact) 2^n sur L, mais c'est en fait beaucoup plus car les a_i ne sont pas forcément dans ΣK^{2^n} (ΣK^{2^n} est seulement contenu dans p) et p est un ordre de niveau exact 2^n.

Dans la suite de ce § nous allons chercher quand il peut exister des extensions fidèles de (K,p) pour une extension algébrique L de K.

Théorème II-5

Soit K *un corps muni d'un ordre de niveau* 2^n, p.

Soit L *une extension algébrique de* K.

Les propriétés suivantes sont équivalentes :

(i) *il existe une extension fidèle* $(L,\tilde{p})$ *de* (K,p)

(ii) *pour toute sous extension finie* F, $K \subset F \subset L$, *il existe une extension fidèle* (F, p_F) *de* (K,p).

(i) $\Rightarrow$ (ii) est évident (s'il existe F tel que $-1 \in \Sigma\, a_i\, x_1^{2^n}$, $a_i \in p$ et $x_i \in F$ alors c'est aussi vrai dans L).

(ii) $\Rightarrow$ (i) En effet d'après le Théorème II-4 si $-1 \in \sum_{\text{finie}} a_i\, x_i^{2^n}$ avec $a_i \in p$ et $x_i \in L$ alors $-1 \in \sum_{i \in I \text{ fini}} a_i\, x_i^{2^n}$ avec $a_i \in p$ et $x_i \in F_I$, F_I extension finie de K telle que les $\{x_i\}_{i \in I}$ soient dans F_I, ce qui est impossible.

Théorème II-6

Soit p *un ordre de niveau* 2^n *du corps* K .

Soit L *une extension algébrique de* K .

Alors (K,p) *admet une extension fidèle* $(L,\tilde{p})$ *dans les cas suivants*

(1) $[L : K]$ *est impair*

(2) L *est contenu dans la clôture pythagoricienne de* K

(clôture pythagoricienne $\tilde{K}$ *de* K *est définie par*

si a *et* b *sont dans* $\tilde{K}$, $\sqrt{a^2+b^2}$ *est dans* $\tilde{K}$)

De plus dans ces deux cas on a clairement :

$$\Sigma L^{2^n} \cap K = \Sigma K^{2^n} .$$

La démonstration utilise dans les deux cas
le lemme donné ci-après et dont la preuve très technique peut être trouvée dans [Be 2] .

Lemme II-7

Soit p un ordre de niveau supérieur de K , compatible avec la valuation v ; soit $\bar{p}$ l'ordre induit sur le corp résiduel k .

Soit $(L,\tilde{v})$ une extension de (K,v) avec corps résiduel ℓ .

Si (i) $e(\tilde{v}/v)$ est impair

(ii) $\bar{p}'$ est une extension fidèle à ℓ de $\bar{p}$,

Alors p admet une extension fidèle $\tilde{p}$ à L et $\tilde{\bar{p}} = \bar{p}'$.

Démonstration

Par le théorème II-5 il suffit de faire la démonstration pour L/K algébrique finie.

Cas 1 . Soit v la valuation associée à $A(p)$.

On sait déjà que $\tilde{p}$ est un ordre de k .

Les extension $\tilde{v}_i$ de v à L satisfont

$$\Sigma\, e_i\, f_i = [L : K] \text{ donc}$$

$$\Sigma\, e_i\, f_i \equiv 1 \text{ modulo } 2 \ .$$

On peut donc trouver une extension $\tilde{v}$ avec e et f impairs.

Alors $(L, \tilde{v})$ satisfait les conditions du lemme II.7 et donc p peut être étendue à un ordre de l'extension impaire ℓ .

Cas 2 . D'après la construction de la clôture pythagoricienne il est suffisant de considérer le cas $L = L(\sqrt{1+a^2})$.

On prend v la valuation associée à $A(p)$ et k le corps résiduel correspondant.

Soit $(\tilde{K}, \tilde{v})$ la clôture hensélienne de (K,v) .

Alors si $1+a^2 \in \tilde{K}^2$, v est totalement décomposée dans L c'est-à-dire que $e = 1$, $f = 1$, $g = 2$.

Autrement a doit être une unité de $\tilde{K}$, et $1+\bar{a}^2 \notin k^2$.

Dans ce cas L est une extension non ramifiée et $\ell = k(\sqrt{1+\bar{a}^2})$. On a alors les conditions du lemme II.7 qui sont vérifiées.

Pour terminer ce paragraphe donnons l'énoncé ci-dessous qui montre une limitation dans le nombre possible des extensions fidèles.

Théorème II.8

Soit L *une extension algébrique finie de* K *avec* p *ordre de niveau supérieur donné sur* K .

Alors le nombre d'extensions fidèles de (K,p) *à* L *est inférieur ou égal à* $[L : K]$.

La démonstration très longue et technique peut être trouvée dans [Be 2] .

III - CORPS REELS CLOS GENERALISES

Par le lemme de Zorn il existe une extension algébrique réelle maximale admettant une extension fidèle de l'ordre de niveau supérieur p, soit $(R,\tilde{p})$ clôture réelle généralisée de (K,p).

Bien sûr si p est un ordre habituel, on retrouve la clôture réelle usuelle et $\tilde{p} = R^2$.

Théorème III-1 (énoncé de Lam [L]).

Soit $(R,\tilde{p})$ *la clôture réelle généralisée de* (K,p) *avec* p *ordre de niveau exact supérieur ou égal à* 2^2. *Alors on a les propriétés suivantes :*

① R *a exactement deux (vrais) ordres* Q *et* Q' *et pour tout* $m \geqslant 2$ *un ordre unique de niveau exact* 2^m.

② *Si* R_1 *et* R_2 *sont des clôtures réelles (des vraies) de* (R,Q) *et* (R,Q') *respectivement alors*

$$R = R_1 \cap R_2 .$$

③ R *a une valuation hensélienne avec corps résiduel réel clos.*

④ R *est pythagoricien pour tout* m $(R^{2^m} + R^{2^m} = R^{2^m})$

⑤ R *n'a pas d'extension de degré impair.*

Donnons quelques indications sur la démonstration des propriétés ③ et ④, le reste pouvant être trouvé dans [Be 2].

pour ③ :

Soit $\tilde{p}$ une extension fidèle de p à R, et soit v la valuation sur R associé à $A(\tilde{p})$. D'après les maximalité de $(R,\tilde{p})$, v est henselienne et le corps résiduel correspondant est réel clos.

pour ④ :

Soit $x^{2^n} + y^{2^n} \in R$. Pour montrer que ceci est une puissance 2^n on peut supposer $x = 1$ et $y \in A(\tilde{p})$. Si $y \in I(\tilde{p})$, c'est terminé puisque $1 + I(\tilde{p})$ est 2-divisible. Supposons donc $y \notin I(\tilde{p})$. Le corps résiduel

étant réel clos il existe une unité z telle que $1+y^{2^n} = i+z^{2^n}$ avec $i \in I(\tilde{p})$. Alors $1+y^{2^n} = z^{2^n}(1+z^{-2^n} i) \in z^{2^n}(1+I(\tilde{p})) \subset R^{2^n}$ et ceci termine la démonstration.

Remarque : on aurait pu tenter de déduire ④ de ② mais ② n'entraîne pas ④ . Si R_1 et R_2 sont des sous corps réels clos de $\bar{\mathbb{Q}}$ induisant des ordres différents sur $R_1 \cap R_2$, Rosenberg a pu montrer que $R_1 \cap R_2$ n'est pas pythagoricien pour tout $m \geqslant 2$.

La question naturelle qui se pose alors est de regarder s'il y a une certaine unicité de ces clôtures réelles. Malheureusement en général deux clôtures réelles généralisées de (K,p) ne sont pas K-isomorphes. Aux paragraphes suivant nous introduisons d'autres notions pour essayer d'obtenir une sorte d'unicité.
Pour terminer cette partie nous allons citer quelques caractérisations qui permettent d'obtenir des clôtures réelles K-isomorphes.

Théorème III-2

Soit K *un corps muni d'un ordre de niveau supérieur* p. *Soit* R_1 *et* R_2 *deux clôtures réelles généralisées de* (K,p).
Alors R_1 *et* R_2 *sont* K*-isomorphes si et seulement si pour tout* $n \in \mathbb{N}$, $R_1^{2^n} \cap K = R_2^{2^n} \cap K$.

Remarquons que si P est un ordre usuel (niveau 2^1) alors les clôtures réelles R_1 et R_2 vérifient $R_1^{2^n} = R_1^2$ et $R_2^{2^n} = R_2^2$, pour tout $n \geqslant 1$. Donc $R_1^{2^n} \cap K = R_1^2 \cap K = p$ et $R_2^{2^n} \cap K = R_2^2 \cap K = p$ ce qui montre bien l'unicité des clôtures réelles dans la théorie classique d'Artin-Schreier.

Théorème III-3

Soit K *un corps,* p *un ordre de niveau* 2^n *avec* $n \geqslant 2$ *donné, alors deux clôtures réelles généralisées de* (K,p) *sont* K*-isomorphes si et*

seulement si $|\beta/\beta^2|=2$ *où* β *désigne le groupe des valeurs de la valuation* v *associée à* A(p).

Théorème III-4

Soit K *un corps. Un ordre* p *de niveau arbitraire a une clôture réelle généralisée unique à* K*-isomorphisme près si et seulement si pour toute valuation réelle sur* K *de groupe des valeurs* β *on a* $|\beta/\beta^2|\leqslant 2$.

Un corps de Pasch vérifiant entre autres conditions celle du théorème III-4, on en déduit que tout corps de Pasch, admet pour tout ordre de niveau supérieur une clôture réelle généralisée unique .

(on rappelle que d'après 10-11 de [L] un corps ordonnable K est de Pasch si et seulement si les deux conditions suivantes sont réalisées :

(1) pour toute valuation réelle sur K de groupe des valeurs β, on a $|\beta/\beta^2|\leqslant 2$

(2) si $|\beta/\beta^2|=2$ alors le corps résiduel correspondant doit avoir un seul ordre ;

et on rappelle que pour un corps ordonnable être de Pasch équivaut à être sap).

On obtient donc ainsi que $\mathbb{R}((X))$ par exemple qui est ordonnable et de Pasch admet pour tout ses ordres de tout niveau une clôture réelle généralisée unique à $\mathbb{R}((X))$-isomorphisme près.

Théorème III-5

Si le corps K *muni de l'ordre de niveau* 2^n , $n\geqslant 2$, *admet plus d'une classe d'isomorphisme de clôtures réelles généralisées alors il en admet une infinité.*

C'est par exemple le cas de R(X,Y) qui admet donc une infinité de clôtures réelles généralisées pour chaque ordre de niveau supérieur 2^n avec $n\geqslant 2$.

IV - CHAINES D'ORDRES DE NIVEAU SUPERIEUR ET EXTENSIONS DE CHAINES

Les notions et résultats de cette partie sont essentiellement dus à Harman et peuvent être trouvés dans [Ha].

Définition IV-1

Soit K un corps ordonnable. On définit une chaîne de K, notée $(p_i)_o^\infty$ par :

(1) p_o et p_1 sont des ordres (vrais) distincts.

(2) pour tout $i \geq 2$, p_i est un ordre de niveau exact 2^i.

(3) pour tout $i \geq 1$, $p_i \cup -p_i = (p_{i-1} \cap p_o) \cup -(p_{i-1} \cap p_o)$.

Exemple IV-2

Soit $K = \mathbb{R}((t))$

$$p_o = \{ \sum_{j=m}^{\infty} a_j t^j \mid a_m > 0 \}$$

$$p_1 = \{ \sum_{j=m}^{\infty} a_j t^j \mid a_m > 0 \text{ si } m \equiv 0 \quad (2)$$

$$\text{ou } a_m < 0 \text{ si } m \equiv 1 \quad (2) \}$$

$\forall i, i \geq 2$

$$p_i = \{ \sum_{j=m}^{\infty} a_j t^j \mid a_m > 0 \text{ si } m \equiv 0 \quad (2^i)$$

$$\text{ou } a_m < 0 \text{ si } m \equiv 2^{i-1} \quad (2^i) \}$$

$\forall i \geq 2$ p_i est un ordre de niveau exact 2^i.

Il est clair que $p_o \supset p_o \cap p_{i-1} \supset p_o \cap p_i$.

Vérifions la condition (3).

Soit $x \in p_{i-1} \cap p_o$. Alors le premier terme non nul de la série a un coefficient $a_m > 0$ et $m \equiv 0 \quad (2^{i-1})$, donc $m = \lambda 2^{i-1}$.

Si $\lambda = 2p$ alors $m = 2p2^{i-1} \equiv 0 \quad (2^i)$ et $x \in p_i$.

Si $\lambda = 2p+1$ alors $m = (2p+1)\, 2^{i-1} \equiv 2^{i-1} \quad (2^i)$ et $-x \in p_i$ donc $x \in -p_i$.

On a donc bien $x \in p_{i-1} \cap p_o \Rightarrow x \in p_i$ ou $x \in -p_i$.

De même si $x \in -(p_{i-1} \cap p_o)$, $-x \in (p_{i-1} \cap p_o)$ et $-x \in (p_i \cup -p_i)$ par le raisonnement

précédent et finalement $x \in -p_i$ ou $x \in p_i$.

Donnons pour commencer quelques théorèmes montrant des cas où l'on peut avoir l'existence d'une chaîne d'ordres de niveau supérieur.

Théorème IV-3

Si p *est un ordre de niveau exact* 2^n *avec* $n \geqslant 2$ *alors il existe une chaîne* $(p_i)_0^\infty$ *avec* $p_n = p$.

Il existe donc des chaînes d'ordres de niveau supérieur dès qu'il existe de vrais ordres de niveau supérieur.

Théorème IV-4

Soit K *un corps muni de deux vrais ordres* p_0 *et* p_1 *tous deux compatibles avec une valuation* v *et tels que* $\bar{p}_0 = \bar{p}_1$ *dans le corps résiduel* k.
Alors il existe une chaîne $(p_i)_0^\infty$ *d'ordres de niveau supérieur commençant par* p_0 *et* p_1.

Ces deux théorèmes sont obtenus comme corollaires du théorème IV-5 suivant et dont les démonstrations se trouvent dans un preprint [Ha-R] apparemment impossible à obtenir...

Théorème IV-5

Soit K *un corps,* v *une valuation réelle sur* K *et* n *un entier supérieur ou égal à* 1.
Alors il existe un isomorphisme :

$$\Theta : \chi_{2^n}(\dot{K}/(1+I)) \simeq \chi_{2^n}(\dot{k}) \times \chi_{2^n}(\beta).$$

tel que si $\Theta(\chi) = (\pi, \mu)$ *alors* $\overline{\ker \chi} = \operatorname{Ker} \pi$.
De plus χ *détermine un ordre de* K *si et seulement si* π *détermine un ordre de* k.

(La notation $\chi_{2^n}(G)$ désigne le groupe des caractères de G dans $\mathbb{C}_{2^n}$ c'est-à-dire $\mathrm{Hom}(G,\mathbb{C}_{2^n})$ où $\mathbb{C}_{2^n}$ est le groupe cyclique multiplicatif d'ordre 2^n ; Rappelons que compte tenu de la présentation des ordres de niveau supérieur à l'aide des signatures, $P \subset K$ sera un ordre de niveau 2^n si et seulement si P est le noyau additivement fermé d'un χ de $\chi_{2^n}(K)$.)

Théorème Fondamental IV-6

Soit $(p_i)_0^\infty$ *une chaîne du corps* K. *Alors il existe une valuation* v *compatible avec chaque* p_i *telle que les* $\overline{p_i}$ *coïncident tous et sont un ordre archimédien de* k.

La démonstration est longue et technique (2 lemmes et 3 étapes...) et utilise signatures et valuations.
Remarquons que si $(p_0\ p_1\ p_2 \ldots)$ est une chaîne du corps K alors $(p_1, p_0, p_2, \ldots)$ en est une également.

Un des intérêts des chaînes sera de pouvoir obtenir au §.V une notion de clôture unique à K-isomorphisme près ; Mais on a aussi des résultats plus raffinés, par exemple sur les sommes de puissances comme le montre le théorème ci-dessous :

Théorème IV-7

Soit K *un corps ordonnable et* $n \geq 1$.
Alors $\Sigma K^{2^n} = \cap$ ({ordres de K} $\cup$ {ordres de niveau exact 2^n de K}).

Rappelons que pour un entier m quelconque Becker avait obtenu que

$$\Sigma\ K^{2m} = \cap\ (\{\text{ ordres de niveau } 2m \text{ de } K\})$$

mais ici de niveau exact ou non ce qui donne beaucoup d'ordres possibles.

Démonstration de IV-7

ⓐ L'inclusion $\Sigma K^{2^n} \subset \cap$ ({ordres de K} $\cup$ {ordres de niveau exact 2^n de K}) est évidente.

ⓑ Soit $a \in \Sigma K^2$ (donc à tout ordre de K) mais tel que $a \notin \Sigma K^{2^n}$.

On va montrer qu'il existe un ordre de niveau exact 2^n qui ne contient pas a.

D'après le résultat de Becker il y a un ordre p de niveau exact 2^m avec $1 < m \leq n$ tel que $a \notin p$ et par le théorème IV-3 il existe une chaîne $(p_i)_0^\infty$ avec $p_m = p$. Donc $a \in p_0$ et $a \notin p_m$. Par la condition sur les chaînes $p_{m+1} \cup - p_{m+1} = (p_m \cap p_0) \cup - (p_m \cap p_0)$ on déduit $a \notin p_{m+1}$. En itérant $a \notin p_n$. On a donc l'inclusion

$\Sigma K^{2^n} \supset \cap$ ({ordres de K} $\cup$ {ordres de niveau exact 2^n de K})

On peut alors définir une notion d'extension de chaîne comme suit.

Définition IV-8

Soit K *un corps muni d'une chaîne* $(p_i)_0^\infty$. *Soit* L *une extension de* K. *On dira que* $(L,(p_i^L)_0^\infty)$ *est une extension de chaîne fidèle de* $(K,(p_i)_0^\infty)$ *si on a*

1) $(p_i^L)_0^\infty$ *est une chaîne de* L.

2) $\forall i \in \mathbb{N}$, $p_i^L \cap K = p_i$

(Notons que chaque (L,p_i^L) sera une extension fidèle de (K,p_i) au sens donné par Becker).

Pour terminer cette partie donnons deux énoncés sur les extensions algébriques de chaînes.

Théorème IV-9

Soit L *une extension de degré impair du corps* K. *Alors pour toute chaîne* $(p_i)_0^\infty$ *de* K, *il existe une extension fidèle* $(L,(p_i^L)_0^\infty)$ *de* $(K,(p_i)_0^\infty)$.

Théorème IV-10

Soit $L = K(\sqrt{a})$ *avec* $a \in K \setminus K^2$. *Alors une chaîne* $(p_i)_0^\infty$ *de* K *peut s'étendre fidèlement à* L *si et seulement si* $a \in p_0 \cap p_1$. *De plus il y a alors exactement deux extensions fidèles.*

Remarque : on a volontairement omis la notion d'extension non fidèle et les théorèmes techniques permettant d'obtenir les résultats donnés ci-dessus.

V - CORPS CHAINE-CLOS

L'intérêt des clôtures de chaîne est d'obtenir une unicité à K-isomorphisme près de cette clôture.

En fait les corps chaîne-clos seront les mêmes que les corps réels clos généralisés mais le manque d'isomorphisme vient du fait qu'un ordre de niveau supérieur peut appartenir à plusieurs chaînes différentes.

Les théorèmes de Becker qui caractérisent quand des clôtures réelles généralisées sont isomorphes, reviendront en fait à dire que ces corps sont des clôtures de chaîne d'une même chaîne.

Définition V-1

Soit K *un corps et* $(p_i)_0^\infty$ *une chaîne de* K. $(R,(p_i^L)_0^\infty)$ *est une clôture de chaîne de* $(K,(p_i)_0^\infty)$ *si* R *est une extension algébrique de* K *maximale pour les propriétés d'être une extension fidèle de* $(K,(p_i)_0^\infty)$.

Définition V-2

Un corps R *sera dit chaîne-clos, s'il existe une chaîne de* R *qui ne s'étend fidèlement à aucune extension algébrique de* R.

L'existence de clôture de chaîne de $(K,(p_i)_0^\infty)$ est assurée par le lemme de Zorn.

On peut alors obtenir un premier théorème caractérisant les corps chaîne-clos.

Théorème V-3

Soit R *un corps et* $(p_i)_0^\infty$ *une chaîne de* R. *Alors* R *est chaîne-clos si et seulement si les deux conditions suivantes sont vérifiées :*

(1) $p_0 \cap p_1 = R^2$.

(2) R *n'a pas d'extension impaire dans sa clôture algébrique.*

Lemme V-4

Soit K un corps n'ayant pas d'extension impaire dans sa clôture algébrique. Alors toute extension finie non triviale de K contient une extension quadratique.

Démonstration du lemme V-4

Soit L une extension finie de K. Soit N la clôture normale de L sur K de groupe de Galois G. Soit H un 2-sous-groupe de Sylow de G. Si $H \neq G$ alors K aurait une extension impaire. Donc G est un 2-groupe. Soit alors V le groupe de Galois de N sur L ; V est contenu dans un sous-groupe d'indice 2 dans G. Ainsi on obtient une extension quadratique de K contenue dans L.

Démonstration du théorème V-3

- Supposons R chaîne-clos. Il existe donc une chaîne $(p'_i)_0^\infty$ de R qui ne s'étend fidèlement à aucune extension algébrique de R.

  D'après le théorème IV-9 R n'a pas d'extension algébrique de degré impair.

- D'après le théorème IV-10, si $a \in p'_0 \cap p'_1$ alors $a \notin R-R^2$ donc $a \in R^2$. Comme $p'_0 \cap p'_1 \supset R^2$ toujours, on a exactement $p'_0 \cap p'_1 = R^2$. On en déduit évidemment que p'_0 et p'_1 sont les seuls vrais ordres de R donc que $p_0 \cap p_1 = R^2$.

- Réciproquement :

  Supposons $p_0 \cap p_1 = R^2$ et R n'a pas d'extension algébrique de degré impair.

  D'après le lemme V-4 toute extension finie de R contient une extension quadratique. Mais si $a \in R-R^2$ alors $a \notin p_0 \cap p_1$ donc $(R,(p_i))$ n'a pas d'extension fidèle à une extension quadratique de R. Donc R est chaîne-clos.

Théorème V-5

Soit $(p_i)_0^\infty$ *une chaîne de* K.

Soit R_0 *une clôture réelle de* (K,p_0).

Alors R_0 *contient une unique clôture de chaîne de* $(K,(p_i)_0^\infty)$.

Corollaire V-6

Soit K *un corps et* $(p_i)_0^\infty$ *une chaîne de* K. *Alors deux clôtures de chaîne de* $(K,(p_i)_0^\infty)$ *sont* K-*isomorphes.*

Soient $(E,(p_i^E)_0^\infty)$ et $(F,(p_i^F)_0^\infty)$ les deux clôtures de chaînes de $(K,(p_i)_0^\infty)$ choisies.

Soit E_0 une clôture réelle de (E,p_0^E) et F_0 une clôture réelle de (F,p_0^F).

Il y a un K isomorphisme $\Phi : E_0 \to F_0$ et par le théorème V-5 on a $\Phi(E) = F$. (puisque une clôture réelle de (K,p_0) ne contient qu'une unique clôture de chaîne de $(K,(p_i)_0^\infty)$).

Théorème V-7

Un corps réel clos généralisé (au sens de Becker et pour un ordre de niveau exact 2^m*) est chaîne clos (au sens de Harman) et réciproquement.*

Soit K un corps et p un ordre de niveau exact 2^m sur K avec $m \geqslant 2$.

Soit (R,p^R) une clôture réelle de (K,p).

Donc R est une extension algébrique de K, p^R est de niveau exact 2^m, $p^R \cap K = p$ et p^R ne s'étend fidèlement à aucune extension algébrique.

Par le théorème IV-3 , R a une chaîne $(p_i)_0^\infty$ avec $p^R = p_m$. Donc R est chaîne-clos cette chaîne ne pouvant s'étendre fidèlement à aucune extension algébrique.

Réciproquement :

Soit K un corps et $(p_i)_0^\infty$ une chaîne de K. Soit $p = p_m$. Soit $(R,(p_i^R)_0^\infty)$ une clôture de chaîne de $(K,(p_i)_0^\infty)$.

Nous allons montrer que (R,p_m^R) est une clôture réelle généralisée de (K,p). En effet soit L une extension <u>finie</u> de R. Supposons que p_m^R s'étende fidèlement en p^L sur L. Alors soit $(p_i^L)_0^\infty$ avec $p^L = p_m^L$ une chaîne de L.

Puisque p_m^L est une extension fidèle de p_m^R la chaîne $(p_i^L)_o^\infty$ doit être une extension fidèle de la chaîne qu'elle détermine sur R. Comme R est chaîne-clos il faut que L = R, donc (R,p_m^R) est une clôture réelle généralisée de (K,p).

Théorème V-7

Soit R *un corps chaîne-clos. Alors* R *a exactement deux chaînes. Soit* $(p_i)_o^\infty$ *l'une des deux chaînes et soit* $v = v(p_i)$ *(c'est la même pour tous les* p_i*). Alors* v *est hensélienne et le corps résiduel est réel clos.*

Démonstration

R est chaîne clos et a donc deux chaînes, soit $(p_i)_o^\infty$ l'une d'elle et soit $v= v(p_i)$ la valuation associée à tous les p_i.

R a seulement deux vrais ordres, donc R a seulement un seul ordre de niveau exact 2^n pour $n\geq 2$.

Les deux chaînes sont donc $(p_0\ p_1\ p_2 \ldots p_i \ldots)$ et $(p_1,p_0,p_2,\ldots,p_i,\ldots)$.

Le Henselisé (R',v') de (R,v) contient p_0' et p_1' les uniques extensions fidèles de p_0 et p_1. Le corps résiduel de v' étant k le corps résiduel de v, alors $\overline{p_0'}$ et $\overline{p_1'}$ sont le même ordre p de k que $\overline{p_0}$ et $\overline{p_1}$. Donc il existe une chaîne $(p_i')_o^\infty$ de R', et p_i' étant extension fidèle de p_i pour 0 et 1 alors $(p_i')_o^\infty$ est extension fidèle de $(p_i)_o^\infty$. Donc R' = R.

$p_0 \cap p_1 = R^2$ entraîne $p = k^2$. Si k avait une extension impaire R en aurait aussi une donc k est finalement réel clos.

Théorème V-8

Soit K *un corps et* p *un ordre de niveau exact* 2^m, $m\geq 2$. *Alors deux clôtures réelles généralisées* (R,p^R) *et* (E,p^E) *sont* K*-isomorphes si et seulement si elles déterminent les mêmes deux chaînes de* K.

Démonstration

$\Rightarrow$ R est chaîne-clos donc a deux chaînes $(p_o^R, p_1^R, p_2^R, \ldots)$ et $(p_1^R, p_o^R, p_2^R, \ldots)$ avec $p_m^R = p^R$.

Cette extension étant fidèle pour p, les deux chaînes sont des extensions fidèles des chaînes qu'elles déterminent sur K, soient $(p_o, p_1, p_2, \ldots)$ et $(p_1, p_o, \ldots)$.

Si R et E sont K-isomorphes cet isomorphisme transformera les chaînes de R en les chaînes de E et donc E déterminera les deux mêmes chaînes sur K que R.

$\Leftarrow$ Réciproquement

Si R et E déterminent les mêmes chaînes $(p_o, p_1, \ldots)$ et $(p_1, p_o, \ldots)$ de K alors $(R, (p_i^R)_o^\infty)$ et $(E, (p_i^E)_o^\infty)$ sont deux clôtures de chaînes de $(K, (p_i)_o^\infty)$ donc elles sont K-isomorphes (corollaire V-6).

Bibliographie

[B1] E. Becker
"Hereditarily pythagorean fields, Infinite Harrison primes and sums of 2^n-th powers."
Bull. Amer. Math. Soc. Vol 84, number 2, march 1978.

[B2] E. Becker
"Hereditarily pythagorean fields and orderings of higher types"
Impa. Lecture notes, n°29, Rio de Janeiro, 1978.

[B3] E. Becker
"Summen n-ter potenzen in Körpern"
J. Reine angew. Math. 307/308, 1979, 8-30.

[B4] E. Becker
"Local global theorems for diagonal forms of higher degree"
J. Reine angew. Math. 318, 1980, 36-50.

[B5] E. Becker
"Extended Artin-Schreier theory of fields"
Rocky mountain Journal of Math. Fall 84, vol 14, number 4.

[B-HA-R] E. Becker, J. Harman, A. Rosenberg
"Signatures of fields and extension Theory"
J. Reine angew. Math. 330, 1982, 53-75.

[E] O. Endler
"Valuation Theory"
Universitext, Springer Verlag, 1972.

[G] D. Gondard
"Théorie des ordres de niveau supérieur pour les corps commutatifs"
Séminaire DDG, 1984-85, Université de Paris 7.

[Ha] J. Harman
"Chains of higher level orderings"
Contemporary mathematics. vol. 8, 1982.

[H-R] J. Harman et A. Rosenberg
"Extensions of orderings of higher level"
preprint.

[Har] D.K. Harrison
"Finite and infinite primes for rings and fields"
Mem. Amer. Math. Soc. 68, 1966, 1-62.

[Har-W] D.K. Harrison et H.D. Warner
"Intinite primes of fields and completions"
pacific J. Math. 45, 1973, 201-216.

[J] J.R. Joly
"Sommes de puissances d-ièmes dans un anneau commutatif"
Acta Arithmetica 17, 1970, 37-114.

[L] T.Y. Lam
"The Theory of ordered fields"
proceedings of the Algebra and Ring theory Conference
Oklahoma, Mars 1979, M. DEKKER 1980.

[p1] A. Prestel
"Quadratische semi-ordnungen und quadratisch Formen"
Math Z. 133, 1973, 319-342.

[p2] A. Prestel
"Lectures on formally real fields"
Impa. n°22, Rio de Janeiro, 1975.

[S] P. Serre
"Extension de corps ordonnés"
C.R.A.S. 12/9, 1949.

THE MODEL THEORY OF CHAIN-CLOSED FIELDS. (*)

M.A. Dickmann

CNRS - University of Paris VII

Paris - FRANCE

Introduction. The notion of a *higher level ordering* is a generalization of the usual notion of an order introduced by Becker in the study of sums of even-powers in a field ; see [1] for a general reference. A precise definition of an ordering of level 2^n (level n in the terminology of [1]) is given in Definition 1.1(II) below.

In [1] Becker worked out the extension theory of fields with a higher level ordering and introduced the notion of a (generalized) real closure for such fields. For a survey of (the analog of) Artin-Schreier's theory of fields with a higher level ordering, see [2]. In [10] Jacob proved decidability, completeness and model-completeness (in a suitable language) for the theory of generalized real closed fields. Jacob's results are in a sense optimal insofar the non-uniqueness of generalized real closures (see [1 ; Ch. IV, Thms. 12, 13]) prevents quantifier elimination results from holding in languages natural from an algebraic point of view.

The following remarkable fact stems from the work of Becker and Harman : a field having a proper ordering (i.e. one which is not just an order) of any level, necessarily has an ordering of (exact) level 2^n for each integer $n \geq 2$, plus two usual orders and, moreover, a tight connection holds between orderings of two consecutive levels (cf. [9 ; Cor. 1.4] and [1 ; Thm. 15, p. 37]). The typical example is the field $\mathbb{R}((X))$ of formal power series in one variable with real coefficients, [9, Example 1.2]. Thus,

(*) To be published in J.S.L..

it became clear that the natural object of study in this setting are fields together with two orders and a chain of orderings of each 2-power level, as above ; these are called *chain fields* (see Definition 1.1 below).

In [9] Harman extensively investigated the algebra of chain fields. He worked out a satisfactory extension theory ([9; §3]), proving, *inter alia*, that every chain field has an algebraic extension maximal for the property that the chain extends faithfully, i.e. preserving the level of each ordering; see [9; Thm. 4.6]. Furthermore, such a chain-closure is unique, that is, two chain-closures of a chain field are exchanged by an isomorphism which fixes the base field [9; Cor. 4.7]. He also gave an Artin-Schreier type characterization of chain-closed fields [9; Thm. 4.3]. He established as well the connection between chain-closed fields and generalized real closed fields by showing that, for $n \geq 2$, the n^{th} ordering of a chain-closed field makes it into a generalized real closed field of level 2^n and that, conversely, given a generalized real closed field $\langle K,P \rangle$ of level 2^n , K is chain-closed for some chain whose n^{th} term is P [9 ; p. 167 and Cor. 1.4].

In this paper we draw the model-theoretic consequences of this algebraic theory and, using techniques pertaining to the model theory of valued fields, establish the following results :

(1) Completeness of the first-order theory of chain-closed fields. (Theorem 1.11).

Chain-closed fields are naturally endowed with a family of henselian valuations with real closed residue fields. Drawing from Becker's work, Harman [9; Thm. 1.8 and Prop. 4.4] exhibits one such valuation, having an archimedean residue field, while another example (originating in Ax) comes from Jacob [10; Thm. 1]; the latter has, in addition, the good taste of being first-order definable. We prove:

(2) Model-completeness of the theory of chain-closed valuation fields in the language for fields plus unary predicates for the members of the chain, and a unary predicate for the (Jacob) valuation ring. (Theorem 2.3).

(3) Quantifier elimination for the theory of (2) in the language enlarged by yet one individual constant (needed to distinguish the two orders). (Theorem 3.1).

In § 4 we establish some connections between the preceding results and previous work in the model theory of real fields, showing the following:

(4) The theory of chain-closed valuation fields is the model-companion of the theory of valued fields with precisely two orders compatible with the valuation and inducing the same order on the residue field. (Proposition 4.1).

These orders are called *superdependent*. Their theory was investigated in B. Laslandes' dissertation [13] (see [11], [12]), who established the existence of a model-companion and gave an explicit axiomatization for it. We also prove:

(5) The theory of chain-closed fields is identical with the theory of Rolle fields with exactly two orders. In particular, the latter is complete and decidable. (Proposition 4.2, Corollary 4.3).

Thus, chain-closed fields constitute the simplest example of Rolle fields beyond the real closed case.

I wish to thank D. Gondard whose expositions in the Paris DDG seminar aroused my interest on chain-closed fields and introduced me to the work of Becker and Harman. Thanks are also due to L. Bélair, F. Delon and F. Lucas whose comments helped to clarify some points, and to the referee for suggestions helping to improve the presentation of this paper.

§1. Completeness.

For the sake of readability we begin with the following definition from Harman [9; 1.1, 3.1 and 4.1].

Definition 1.1. Let K be a field.

(A) A sequence $\langle P_i \rangle_{i \in \omega}$ is a *chain* of K if:

(I) P_0, P_1 are different orders.

(II) For $n \geq 2$, P_n is an ordering of exact level 2^n, that is:

i) $\dot{P}_n + \dot{P}_n \subseteq \dot{P}_n$ (where $\dot{P} = P - \{0\}$);

ii) $\dot{P}_n \cdot \dot{P}_n \subseteq P_n$;

iii) $1 \in P_n$;

iv) $\dot{P}_n^{-1} \subseteq \dot{P}_n$

v) The group $\dot{K}/\dot{P}_n$ is cyclic of order 2^n.

(III) For $n \geq 1$, $P_n \cup -P_n = (P_{n-1} \cap P_0) \cup -(P_{n-1} \cap P_0)$.

(B) Let L be a field extension of K and $\langle P_i \rangle_{i\in\omega}$ a chain of L. $\langle P_i \rangle_{i\in\omega}$ is a *faithful extension* (of $\langle P_i \cap K \rangle_{i\in\omega}$) iff $\langle P_i \cap K \rangle_{i\in\omega}$ is a chain of K. [Note: since the sequence $\langle P_i \cap K \rangle_{i\in\omega}$ automatically satisfies II. (i)-(iv) and $\dot{K}/\dot{P}_n \cap K$ is a cyclic group of order 2^m, $m \leqslant n$, then we have a faithful extension iff $[\dot{K} : \dot{P}_n \cap K] = 2^n$, for $n \geqslant 2$, iff the orders $P_o \cap K$, $P_1 \cap K$ are distinct (cf. [9; Lemma 1.7])].

(C) A chain field $\langle K, P_i \rangle_{i\in\omega}$ is *chain-closed* if the chain $\langle P_i \rangle_{i\in\omega}$ does not extend faithfully to any proper algebraic extension of K. A field is *chain-closed* if there is a chain with respect to which it is chain-closed. □

Notation. $L_F = \{+,-,.,^{-1},0,1\}$ denotes the usual language for fields (with inverse for multiplication), and $L_{CF} = L_F \cup \{P_o, P_1, P_2, \ldots\}$ its expansion by countably many unary predicates; L_{CF} is the language for *chain fields*. □

We shall consider the following additional conditions on a chain field $\langle K, P_i \rangle_{i\in\omega}$:

(IV) $P_o \cap P_1 = K^2$.

(V) Every polynomial in $K[X]$ of odd degree has a root in K.

We call CCCF the set of L_{CF}-sentences which formalize conditions (I)-(V) together with the axioms for fields. We have:

Result 1.2 (Harman [9; Thm. 4.3]).
The models of CCCF are exactly the chain-closed chain fields. □

It is clear from the work of Harman (cf. specially [9; §§1, 4]) that the orderings P_n, $n \geq 2$, are (implicitly) definable from P_o, P_1. Using Result 1.3 below one can dispense with P_o, P_1 as well, and obtain an explicit axiomatization of chain-closed fields in the language for fields.

Result 1.3. (Becker [1; Cor. 2, p. 43]).
Let K be a Pythagorean field having exactly two orders P_o, P_1, and such that $K^{2^n} \neq K^{2^{n+1}}$ for some $n \geq 1$. Then:

(a) Let a be any element in $P_o \cap -P_1$; then

$$P_o = K^2 \cup aK^2, \qquad P_1 = K^2 \cup -aK^2.$$

(b) Let a be any element so that $a, -a \notin K^2$. Then, for $n \geq 2$ $P_n = K^{2^n} \cup -a^{2^{n-1}} K^{2^n}$ is the unique ordering of level 2^n, and $K^{2^{n-1}} = K^{2^n} \cup a^{2^{n-1}} K^{2^n}$.

In particular, these identities hold for $\langle K, P_i \rangle_{i \in \omega} \models CCCF$. □
Thus, replacing $P_n(x)$ $(n \geq 2)$ for

$$(\dagger) \quad \exists z (x = z^{2^n}) \vee \forall y \exists z \, [\forall w (y \neq \pm w^2) \rightarrow x = -y^{2^{n-1}} z^{2^n}],$$

the axioms of CCCF can be translated into the language of fields. The neatest Artin-Schreier type axiomatization for this translation was obtained by D. Gondard [7], [8]:

Proposition 1.4. Chain-closed fields are exactly the models of the following set of axioms in L_F (which we call CCF):

- Axioms for commutative fields.
- Pythagorean axioms:

  "A sum of two squares is a square",

  "A sum of two fourth-powers is a fourth-power".

- $\exists y\,[\forall w(y \neq w^2 \wedge y \neq -w^2) \wedge \forall x\,\exists z(x = z^2 \vee x = -z^2 \vee x = yz^2 \vee x = -yz^2)]$.
- "Every polynomial of odd degree has a root". □

Remarks. (a) The third axiom just says that the sets P_o, P_1 of 1.3 (a) are positive cones for *total* orders.

(b) For several alternatives to the Pythagorean axioms, see [8] and [9; Cor. 2.4].

(c) Result 1.3 shows that a chain-closed field K has exactly two chains, differing only in the order of the first two terms. They begin with the two orders of K, and their n^{th} term, $n \geq 2$, is uniquely determined by (†); cf. also Harman [9; Prop. 4.4].

Definition 1.5. (Jacob [10; p. 214]). Let K be a field and P an ordering of level $n \geq 2$ in K. Let:

$$J'(K,P) = \{x \in K \mid x \notin \pm \dot{P} \text{ and } 1 + x \in P\},$$

$$J''(K,P) = \{x \in K \mid x \in \pm P \text{ and } x.J'(K,P) \subseteq J'(K,P)\},$$

$$J(K,P) = J'(K,P) \cup J''(K,P).$$

For a chain field $\langle K, P_n \rangle_{n \in \omega}$ we set $J_n = J_n(K) = J(K,P_n)$, $n \geq 2$. □

Jacob [10; Thms. 1,2] proves :

Result 1.6. (a) $J(K,P)$ is a valuation ring of K, and $\overline{P \cap J(K,P)}$ is the positive cone of an order on the residue field $\overline{J(K,P)}$.

(b) If $K \models CCF$ and $\langle P_i \rangle_{i \in \omega}$ is a chain of K, then the valuation rings J_n, $n \geq 2$, are henselian with real closed residue field. □

Notation. We denote by $\mathcal{V}(K)$ the family of all henselian valuations on a field K with real closed residue field. For $v \in \mathcal{V}(K)$, A_v, M_v, Γ_v, $\bar{A}_v$ denote the ring, maximal ideal, value group and residue field corresponding to v. We denote by j_n the valuation defined by the ring J_n, and $M_n = M_{j_n}$, $\Gamma_n = \Gamma_{j_n}$, etc.

The next Proposition summarizes the basic properties of valuations in $\mathcal{V}(K)$.

Proposition 1.7. Let $K \models CCF$, $\langle P_i \rangle_{i \in \omega}$ be a chain of K, and $v \in \mathcal{V}(K)$. Then:

(a) Let u be a residually positive (resp. negative) unit of A_v. Then $u \in K^{2^n}$ (resp. $u \in -K^{2^n}$) for all $n \in \omega$.
In particular:
(b) $1 + M_v \subseteq K^{2^n}$ for $n \geq 1$. Hence the valuation v is compatible with every P_n (i.e. $1 + M_v \subseteq P_n$).
(c) The ring A_v is convex with respect to each P_n, $n \in \omega$ (i.e., $a \in P$, $b-a \in P$ and $b \in A_v$ imply $a \in A_v$).
(d) The group Γ_v is divisible by every prime $p \neq 2$.
(e) $\Gamma_v/2\Gamma_v \simeq \mathbb{Z}/2\mathbb{Z}$.
(f) Γ_v is dense. □

Remark 1.8. In the case $v = j_n$, Proposition 1.7 yields: let $z \notin \pm \dot{P}_n$; then $j_n(z) \neq 0$. Moreover:

(i) $z \notin \pm \dot{P}_n$ and $1 + z \in P_n$ imply $j_n(z) > 0$.

(ii) $z \notin \pm \dot{P}_n$ and $1 + z \notin P_n$ imply $j_n(z) < 0$.

Proof. The first assertion follows at once from 1.7 (a).

(i) We show that $J'(K,P_n) \subseteq M_n$. If $x \in J'(K,P_n)$ and $j_n(x) = 0$, then $x^{-1} \notin \pm \dot{P}_n$ and $x^{-1} \in J'(K,P_n)$; it follows that $1 + x$, $1 + x^{-1} \in P_n$, whence $x^{-1} = (1+x)^{-1}(1+x^{-1}) \in P_n$, a contradiction.

(ii) If $j_n(z) > 0$, i.e. $z \in M_n$, then $1 + z \in \bigcap_i K^{2^i} \subseteq P_n$, by 1.7 (b). □

A field is called a *Rolle field* (Delon [5]) if it is orderable and Rolle's theorem for polynomials holds in one (equivalently, each) of its orders. Brown, Craven and Pelling [3] characterized Rolle fields as those fields carrying a henselian valuation with real closed residue field and odd-divisible value group. Thus 1.6 and 1.7(d) yield:

Corollary 1.9. Any chain-closed field is a Rolle field. □

We are now in a position to use Delon's analysis of valuations in Rolle fields, [5; Prop. 1], in order to prove the main properties of the valuations j_n and their groups.

Proposition 1.10. Let $K \models CCF$ and $\langle P_n \rangle_{n \in \omega}$ be a chain of K. Then:

(a) The valuations j_n, $n \geq 2$, are minima in $\mathcal{V}(K)$, i.e. $J_n \supseteq A_v$ for every $v \in \mathcal{V}(K)$. In particular,

(b) $J_n = J_m$ for $n, m \geq 2$.

(c) Γ_n contains no non-trivial 2-divisible convex subgroup.

(d) Γ_n is regularly dense, that is, $m\Gamma_n$ is dense in Γ_n for every $m \geq 1$ (cf. Robinson-Zakon [15; Def. 3.3]).

(e) $\{\gamma \in \Gamma_n \mid \gamma \notin 2\Gamma_n\}$ is dense in Γ_n.

Proof. (a) Delon [5; Prop. 1] shows that $\mathcal{V}(K)$ is totally ordered (by reverse inclusion of the valuation rings) with first and last elements. The largest valuation ring, B, is first-order definable in the language of fields;

$$B = \{x \in K \mid \forall t[\forall z(t \neq \pm z^2) \wedge A(t) \text{ closed under multiplication} \rightarrow x \in A(t^{-1})]\},$$

where $A(t) = \{x \in K \mid \exists y(1+tx^2 = y^2)\}$.

It suffices to show that $B \subseteq J_n$. Let $x \notin J_n$; since $x^{2^\ell} \notin J_n$ for all $\ell \in \omega$, we may assume $x \in P_n$. By 1.5, there is $y \notin \pm \dot{P}_n$ such that $1 + y \in P_n$ and $1 + x^2y \notin P_n$; by 1.8 we have $j_n(y) > 0$ and $j_n(x^2y) < 0$. Clearly $y \notin \pm \dot{K}^{2^n}$ and, by the proof of Lemma 2.4 below, $2^n \nmid j_n(y)$. Hence $j_n(y) = 2^k j_n(a)$ for some $0 \leq k \leq n$ and some a such that $2 \nmid j_n(a)$; clearly we also have $j_n(a) > 0$ and $j_n(x^2a) < 0$. Hence $2 \nmid j_n(x^2a) = j_n(1+x^2a)$. Putting $b = a^{-1}$ we conclude that $x \notin A(b^{-1})$. By [5; Prop. 1(3)] we also have that $A(b)$ is closed under multiplication. Thus we have shown that $x \notin B$.

(b) Trivial.

Equivalently, P_2 can be replaced by any P_n, $n>2$ (1.10(b)), by $P_o \cap P_1$ (Axiom (III)) or by K^2 (Axiom (IV)). Note that the condition $xy \notin \pm P_2$ is superfluous.

We will need the following result of Robinson-Zakon [15 ; prcof of Thm. 4.6] :

Result 2.2. The theory of regularly dense ordered abelian groups with specified invariants $[G : pG]$ (= a power of p, or ∞) for each prime p, is model-complete in the language $\mathcal{L}$ for ordered groups augmented by the divisibility predicates

$$D_m(\alpha) \leftrightarrow \exists_\beta (m \cdot \beta = \alpha) ,$$

for $m \geq 2$. □

By Proposition 1.7 (d), (e), the prime invariants of the (Jacob) value group $\Gamma(K)$ of a chain-closed field K are 1 for $p \neq 2$, and 2 for $p = 2$.

Theorem 2.3. The theory CCVF is model-complete (in $L_{CF}(A)$).

Proof. By the Ax-Kochen-Ershov transfer principle for model-completeness the problem gets reduced to showing that, whenever $\langle K, P_i, J(K) \rangle \subseteq \langle F, Q_i, J(F) \rangle$ are models of CCVF, the value group $\Gamma(K)$ is an $\mathcal{L}$-substructure of $\Gamma(F)$, which is done in Lemma 2.4 below.

Indeed, model-completeness of real closed fields and Result 2.2 imply, then, that the canonical inclusions of residue fields and value groups are elementary. □

Lemma 2.4. The (lifting of) divisibility predicates D_m, $m \geq 2$, are quantifier-free definable in L_{CF} modulo the axioms of CCVF. In particular, if $\langle K,P_i,J(K)\rangle \subseteq \langle F,Q_i,J(F)\rangle$ are models of CCVF, then $\Gamma(K) \underset{\mathfrak{L}}{\subseteq} \Gamma(F)$.

Proof. By odd-divisibility (1.7(d)) we need only consider the case $m = 2^n$. For $x \in \dot{K}$, where $\langle K,P_i,J(K)\rangle \models$ CCVF, we have:

$$\Gamma(K) \models D_{2^n}(j(x)) \text{ iff } \langle K,J(K)\rangle \models \exists y(j(x) = 2^n j(y)) \text{ iff}$$
$$\langle K,J(K)\rangle \models \exists yz(xz = y^{2^n} \wedge \text{"}z \text{ is a unit of } A\text{"}).$$

The units of $J(K)$ are in $\pm \dot{K}^{2^n}$ (1.7(a)). Hence the last term of the equivalence above implies

$$K \models \exists yz\ (z \neq 0 \wedge \pm(xz^{2^n}) = y^{2^n}),$$

showing that $x \in \pm \dot{K}^{2^n}$. Hence we obtain

$$\Gamma(K) = D_{2^n}(j(x)) \quad \text{iff} \quad x \in \pm \dot{K}^{2^n}.$$

Since $\dot{K}^{2^n}$ is quantifier-free definable in terms of the predicates P_n (namely, $\dot{K}^{2^n} = \bigcap_{i=0}^{n} \dot{P}_i$; cf. 1.3), the lemma is proved. □

Remark. Another model-completeness result for chain-closed fields, in a different language, was subsequently proved by Delon and Gondard ; see [6].

§3. Quantifier elimination.

In order to obtain a quantifier elimination result we enlarge the language $L_{CF}(A)$ with a new individual constant needed to distinguish the orders P_o and P_1. We call $CCVF^+$ the theory CCVF plus the axiom:

(VII) $\qquad P_o(c) \wedge \neg P_1(c),$

and prove:

Theorem 3.1. The theory $CCVF^+$ admits quantifier elimination in the language $L_{CF}(A,c)$.

Proof. The simplest way to proceed is using the quantifier elimination transfer theorem of Cherlin-Dickmann [4 ; Thm. 5]. We note the following facts:

(1) The theory of $\Gamma(K)$ - the value group of any model $(K,\ldots)$ of $CCVF^+$ - admits q.e. in the language for ordered groups augmented by the divisibility predicates D_m, $m \geq 2$.

This follows from Weispfenning [16 ; Thm. 2.6], 1.10 (d) and 1.7 (d), (e).

(2) The residue fields of models of $CCVF^+$, being real closed, admit q.e. in the language with a predicate for the order.

(3) $[\,U(K) : U(K)^m] = \begin{cases} 1 & \text{if } m \text{ odd} \\ 2 & \text{if } m \text{ even,} \end{cases}$

where $U(K)$ is the multiplicative group of units of $J(K)$.

Indeed, if $m = 2^n \cdot q$, $n \in \omega$, q odd, then 1.7(d) shows that $U(K)^m = U(K)^{2^n}$. Since $U(K) \subseteq \pm K^{\cdot 2^n}$ (1.7(a)), then $U(K)/U(K)^{2^n} \simeq \mathbb{Z}/2\mathbb{Z}$ if $n \geq 1$. In particular, this shows:

(4) The constant 1, if m is odd, and $1,-1$, if m is even, from a complete set of representatives of $U(K)/U(K)^m$.

In view of these remarks, [4; Thm. 5] shows that the 'auxiliary' theory Σ described below admits q.e. in the expansion $\mathcal{L}$ of the language $L_P(K)$ of valued fields by:

(a) Unary predicates D_m, P_r $(m,r \geq 2)$ denoting respectively the lifting of the divisibility predicates in the value group language, and the r^{th} powers.

(b) A binary predicate $<^R$ lifting the residual order.

Σ is the theory of Henselian valued fields K with real closed residue field, value group as in 1.7(2), (e) and 1.10 (d), $[U(K) : U(K)^m]$ as in (3) above, and axioms giving the predicates D_m, P_r and $<^R$ the meaning stated in (a), (b) above.

Returning to the theory $CCVF^*$, we remark:

(5) To every model $\langle K, P_1, J(K)\rangle$ of CCVF is associated a (unique) model $\mathcal{K}$ of Σ with same underlying valued field $\langle K, J(K)\rangle$.

(6) The chain predicates P_n are definable (with quantifiers!) in $L_P(C)$. (Result 1.3).

(7) The predicates D_m, P_r, are equivalent in CCVF to quantifier-free formulas of L_{CF}. (Lemma 2.4).

(8) The predicate $<^R$ is quantifier-free definable in $L_{CF}(A)$.

Indeed, by 1.6(a) we have, for $x \in \dot{K}$:

$$\overline{\mathcal{K}} \models \bar{x} >^R 0 \quad \text{iff} \quad \langle K, P_i, J(K) \rangle \models A(x) \wedge A(x^{-1}) \wedge P_2(x).$$

Quantifier elimination for $CCVF^+$ is now an easy consequence of that of Σ, as follows: given a formula $\varphi(\bar{v})$ of $L_{CF}(A,c)$, use (6) to transform it into a formula $\varphi'(\bar{v})$ of $\mathcal{L}(c)$; then, get a quantifier-free $\mathcal{L}(c)$-formula $\psi'(\bar{v})$ equivalent to $\varphi'(\bar{v})$ modulo Σ; finally, use (7) and (8) to get back a quantifier-free formula $\psi(\bar{v})$ of $L_{CF}(A,c)$. It is routine checking that $CCVF^+$ proves the equivalence of $\varphi(\bar{v})$ and $\psi(\bar{v})$. □

Remarks. (a) The theory $CCCF^+$ is not complete. Its two completions are obtained by fixing the sign of the Jacob valuation of c. In the language $L_{CF}(c)$ this amounts to adding as an axiom either one of the statements "$1+c \in P_2$" or "$1+c^{-1} \in P_2$".
(b) As pointed out by the referee, Theorem 3.1 can be improved to "$CCVF^+$ admits *primitive recursive* quantifier elimination". Indeed, in [17 ; Thm. 4.12] Weispfenning proves, under assumptions more stringent than those of [4 ; Thm. 5], that primitive recursive q.e. of the theory of the residue field (here real closed fields) and of the theory of the value group (here regularly dense ordered abelian groups with specific primitive recursive prime invariants, see [16 ; Thm. 2.6]) lift to primitive recursive q.e. of the

theory of the valued field. Proposition 1.10 (d) insures that the additional assumptions are fulfilled in the present case ; see [17 ; 4.1 and 4.13 (iv)]. Thus, the auxiliary theory Σ has primitive recursive q.e. ; the translation of $CCVF^+$ into Σ and back clearly is primitive recursive.

(c) It is an open question whether the additional constant c is really necessary to get quantifier elimination. □

§ 4. Chain-closed fields, superdependent orders and Rolle fields.

In [11, 12, 13] B. Laslandes investigated several theories of fields with finitely many orders. Among others he considered the theory $COSD_n$ of fields with n *superdependent* orders, namely n orders defining the same topology, provided with a valuation ring convex for all of them, and inducing the same order on the residue field. He proved that $COSD_n$ has a model-companion, $\overline{COSD_n}$, and gave an explicit axiomatization of it in the language with symbols for the n orders and the valuation ring; see [12; Prop. 1 and Thm. 5]. We have:

Proposition 4.1. The theory $\overline{COSD_2}$ is identical with the theory CCVF (or, to be precise, with the obvious reformulation of the latter in the language $L_F \cup \{P_o, P_1, A\}$).

Proof. Both are complete theories satisfying Laslandes axioms for $\overline{COSD_2}$, [12; Prop. 1] ; namely:

- P_o, P_1 are distinct orders;
- The valuation ring A is convex for both P_o, P_1, and these induce the same order on the residue field (Proposition 1.7 (e) and Result 1.6(a)).
- A is Henselian with real closed residue field (Result 1.6 (b)).
- The value group Γ of A is divisible by every odd prime, $\Gamma/2\Gamma \simeq \mathbb{Z}/2\mathbb{Z}$ (Proposition 1.7(d), (e)) and regularly dense (Proposition 1.10(d)). □

Laslandes goes on defining an expansion $\widetilde{COSD_n}$ of $\overline{COSD_n}$ which admits q.e. in a suitably enlarged language.
As in 4.1 it is easily checked that his theory $\widetilde{COSD_2}$ coincides with $CCVF^+$ modulo trivial changes in the languages involved; see [13, Ch. III, § 4].

Finally we prove:

Proposition 4.2. The theory CCF is identical with the theory of Rolle fields with exactly two orders.

Proof. After 1.9 it only remains to be proved that a Rolle field with two orders is chain-closed. Using the characterization of Rolle fields mentioned before 1.9, we infer form Harman [9; Cor. 1.5] that K carries a chain $\langle P_i \rangle_{i \in \omega}$. We only need to check Axioms (IV) and (V) of §1. Axiom (V) readily follows from Hensel's lemma and the fact that the residue field is real closed.

Axiom (IV). Since K has two orders, the value group Γ_v of any valuation $v \in \mathcal{V}(K)$ cannot be 2-divisible; otherwise K itself would be real closed. Further, $K^2 \neq K^4$, as $x^2 \notin K^4$ for any x such that $2 \nmid v(x)$. Since a Rolle field is Pythagorean (Becker [1; p. 66]), Result 1.3(a) shows that $P_1 = K^2 \cup aK^2$ and $P_1 = K^2 \cup -aK^2$ for any $a \in P_o \cap -P_1$. Hence $P_o \cap P_1 = K^2$. □

Corollary 4.3. The theory of Rolle fields with exactly two orders is complete and decidable. The theory CCVF of $\S 2$ is its model companion. □

Proposition 4.2 clearly establishes that CCF is the simplest theory of Rolle fields beyond the real closed ones (a Rolle field with only one order is necessarily real closed, as the value group of any of its valuations in $\mathcal{V}(K)$ is 2-divisible).

REFERENCES.

[1] Becker, E., *Hereditarily-Pythagorean Fields and Orderings of Higher Level*, Monografías de Matemática N° 29, IMPA, Rio de Janeiro, 1978.

[2] Becker, E., Extended Artin-Schreier theory of fields, Rocky Mountain J. Math. 14 (1984), 881-897.

[3] Brown, R., Craven, T., and Pelling, M. J., Ordered fields satisfying Rolle's theorem, Illinois, J. Math. 30 (1986), 66-78.

[4] Cherlin, G. and Dickmann, M. A., Real Closed Rings; II Model Theory, Ann. Pure Appl. Logic 25(1983), 213-231.

[5] Delon, F., Corps et anneaux de Rolle, Proc. Amer. Math. Soc. 97(1986), 315-319.

[6] Delon, F. and Gondard, D., 17ème problème de Hilbert pour les corps chaîne-clos, Séminaire DDG "Structures algébriques ordonnées", 1986-87, Paris (to appear).

[7] Gondard, D., Théorie des corps chaînables et chaîne-clos, C.R. Acad. Sc. Paris (1987), to appear.

[8] Gondard, D., Axiomatisations "à la Artin-Schreier" des corps chaînables et chaîne-clos, Séminaire DDG "Structures algébriques ordonnées", 1986-87, Paris (to appear).

[9] Harman, J. Chains of higher level orderings, Contemporary Math. 8 "Ordered Fields and Real Algebraic Geometry", AMS (1982), 141-174.

[10] Jacob, B., The model theory of generalized real closed fields, J. Reine Angew. Math. 323(1981), 213-220.

[11] Laslandes, B., Modèle-compagnons de théories de corps munis de n ordres, C. R. Acad. Sc. Paris 300 (1985), 411-414.

[12] Laslandes, B., Corps de Rolle portant un nombre fini d' ordres, C. R. Acad. Sc. Paris 302(1986), 401-404.

[13] Laslandes, B., Théorie des modèles des corps n-ordonnés, Thèse 3ème-cycle, Univ. Paris VII, 1984.

[14] Ribenboim, P., *Théorie des valuations*, Presses Univ. Montréal, 1964.

[15] Robinson, A. and Zakon, E., Elementary properties of ordered abelian groups, Transactions Amer. Math. Soc. 96(1960), 222-236.

[16] Weispfenning, V., Elimination of quantifiers for certain ordered and lattice-ordered abelian groups, Bull. Soc. Math. Belg. 33(1981), 131-155.

[17] Weispfenning, V., Quantifier elimination and decision procedures for value fields, in *Models and Sets, Proceedings, Logic Colloquium' 83*, 419-472, Lecture Notes Math. 1103, Springer-Verlag, 1984.

Equipe de Logique Mathématique
UA 753 - CNRS
Université Paris VII
Tour 45-55, 5ème étage
2, Place Jussieu
75251 PARIS CEDEX 05.

Cancellation and absorption of lexicographic powers of totally ordered abelian groups

by M. Giraudet.

(Survey)

Abstract: We prove that an ordered abelian group G is determined up to isomorphism by any of its finite lexicographic powers whenever, for any ordered abelian groups A and B, if the lexicographic product $A \to G \to B$ is isomorphic to G, then so are the lexicographic products $A \to G$ and $G \to B$; we give a list of ordered abelian groups with these properties. With similar techniques, we also prove that any finite lexicographical power of any ordered abelian group G determines the first order theory and the order type of G.

&0- Notations:

In this paper, "ordered abelian group" will stand for "totally ordered abelian group".

For any ordered abelian groups A and B:

$A \to B$ denotes the lexicographic product of A and B, read from left to right: for any a and $a' \in A$ and b and $b' \in B$, $(a,a') \leqslant (b,b')$ in $A \to B$ if either $a < a'$ or $a = a'$ and $b \leqslant b'$.

A^k, k a positive integer, denotes the lexicographic product of k copies of A, we refer to it as the k^{th} lexicographic power of G.

A×B is the (un-ordered) cartesian product of the (un-ordered groups) A and B.

$A \simeq B$ means A and B are isomorphic as ordered groups (in the language $\{+,<\}$).

$A \equiv B$ means A and B are elementary equivalent as ordered groups (still in the language $\{+,<\}$).

$A \simeq_+ B$ means A and B are isomorphic as groups (in the language $\{+\}$).

$A \simeq_< B$ means A and B are isomorphic as ordered sets (in the language $\{<\}$)

If X and Y are totally ordered sets (chains) we shall also use the notation X→Y to denote their lexicographic product defined as above.

§1-Problems and background

In [O-2], F. Oger gave an example of two non-isomorphic ordered abelian groups with isomorphic lexicographic squares which was a strong motivation to the present work. The following question arose:

Let # stand for "isomorphic as ordered groups", "elementary equivalent as ordered groups", or "isomorphic as chains", when should the following cancellation rule: (Can,#): "$G^k \simeq H^k$ implies G # H for any ordered abelian

group H"

be true, for a given group G, and a given integer k, $k \geq 2$, ?

Most of our proofs of an eventual satisfaction of a (can,#) (Theorems on isomorphism, elementary equivalence and order isomorphism in this paper) make use of the fact that the following absorbing rule happens to be satisfied:

(Abs,#): "$G \simeq A \to G \to B$ implies $G \# G \to B$ (or, equivalently $G \# A \to G$) for any ordered abelian groups A and B."

Obviously, in order to have (Abs,#), it is enought that any of the following (Σ,#,L) and (Σ,#R) holds:

(Σ,#,L): "$G \simeq A \to G$, A an ordered abelian group, implies $G \# A^{(\omega)} \to X$ for some ordered abelian group X."

(Σ,#,R): "$G \simeq G \to B$, B an ordered abelian group, implies $G \# X \to B^{(\omega^*)}$ for some ordered abelian group X."

From these observations follows a list of ordered abelian groups which are uniquely determined by any of their k^{th} lexicographical power (Examples in § 3 here).

In [O-1], F. Oger also proved that any ω_1-saturated ordered abelian group G satisfies:

(Π,$\simeq$,L): "$G \simeq A \to G$, A any ordered abelian group, implies $G \simeq A^{\omega} \to X$ for some ordered abelian group X."

which also implies (Abs,$\simeq$), hence, by our theorem on isomorphism, any ω_1-saturated ordered abelian group G is also characterized by any of its k^{th} lexicographic power .

From the fact that (Σ,$\equiv$,R) holds for any ordered abelian group (Proposition on elementary equivalence), follows that the theory of any ordered abelian group is uniquely

determined by any of the k^{th} lexicographic powers of this ordered abelian group (Theorem on elementary equivalence).

In [D-L-1] and [D-L-2], the fact that the theory of any ordered abelian group is uniquely determined by the theory of any of its k^{th} lexicographic powers (Corollary 4-14 in [D-L-1]) and Theorem 5 in [D-L-2], was established using the classification of theories of ordered abelian groups given in [S]. We get, from our techniques, a new proof of this result (indeed two proofs, one using and one not using the result of [O-1]).

The fact that the order type of a chain is not uniquely determined by the order type of its lexicographic square is established in [Si] (Exercise 9 p. 232). A very slight change in the example of [Si] shows that $Q \to Z$ and $(Q+1) \to Z$ (where Q is the chain of rationals and Z is the chain of integers) have isomorphic k^{th} lexicographic powers ($k>2$) whence $Q \to Z$ is groupable (=admits a structure of ordered abelian group, see [R] p.125) and $(Q+1) \to Z$ is not even transitive. The characterisation of countable groupable chains, given in [R] makes it easy to check that at least the unscattered ones are determined by any of their k^{th} lexicographic power. However, the problem does not seem quite so clear in the uncountable case, and the fact that the order type of any ordered abelian group is determined by the ordered group structure of any of its k^{th} lexicographic powers follows very easily from our techniques (Theorem on order isomorphism). Note that $(\Sigma, \simeq_*, R)$ holds for

every ordered abelian group but $(\Sigma, \simeq_{\ll}, L)$ does not (example at the end).

§2 Results and techniques

Our main tool is indeed the following lemma:

Main lemma:

Let G, G', H and H' be ordered abelian groups, the following are equivalent:

-i) $G \to G' \simeq H \to H'$

-ii) For some ordered abelian group A:

either: $G \simeq H \to A$ and $H' \simeq A \to G'$

or: $H \simeq G \to A$ and $G' \simeq A \to H'$

Proof:

-i)⇒ii): Let f be an isomorphism from $G \to G'$ onto $H \to H'$, let G'' denote $f(\{0\} \to G')$, which is a convex subgroup of $H \to H'$, and assume that G'' is a convex subgroup of $\{0\} \to H'$ (otherwise, consider f^{-1}).

Let H'' denote $\{0\} \to H'$. Since G'' is a direct summand of $H \to H'$, it is a direct summand of H''.

Set $A = H''/G''$: $H' \simeq H'' \simeq A \to G'' \simeq A \to G'$.

Now: $G \simeq (G \to G')/(\{0\} \to G') \simeq (H \to H')/G'' \simeq H \to (H''/G'') \simeq H \to A$.

-ii)⇒i) is easy to check.

Using the main lemma, the problem of (can,≃) can be completely settled for k=2:

Proposition on squares:

let G and H be ordered abelian groups, the following are equivalent:

-i) $G^{\simeq} \simeq H^{\simeq}$

-ii) For some ordered abelian group A:

either: $G \simeq H \to A$ and $H \simeq A \to G$

or: $H \simeq G \to A$ and $G \simeq A \to H$.

-iii) For some ordered abelian group A:

$G \simeq A \to G \to A$, and either $H \simeq A \to G$ or $H \simeq G \to A$.

Theorem on squares:

Let G be an ordered abelian group, the following are equivalent:

-1) For any ordered abelian group A, $G \simeq A \to G \to A$ implies $G \simeq G \to A$.

-2) $G^{\simeq} \simeq H^{\simeq}$ implies $G \simeq H$.

Note that, if G ≃ A→G→B, then G ≃ G→B is equivalent to G ≃ A→G, but if G and G→B are not isomorphic, G→B and A→G may or may not be isomorphic, even when A=B: they are not in [O-2], but it may happen that exactly two non-isomorphic ordered abelian groups have the same lexicographic square as can be seen from an example at the end of this paper

We now want to deduce (can,#) (for any integer k) from (abs,#), and the technique falls into two cases:

- Case 1: Since some ordered abelian groups do not satisfy (abs,$\simeq$) ((our theorememem on squares shows that the counter example in [O-2] is a counter example to this), it is not suitable, when considering $G^k \simeq H^k$ where G satisfies (abs,$\simeq$), to assume H satisfies (abs,$\simeq$) too. Fortunately, since the conclusion of (abs,$\simeq$), is concerned with $\simeq$ as well as the premices, the proof gets throught applying twice (abs,$\simeq$) to the same group G, and gives:

Theorem on isomorphism

Let G be an ordered abelian group and assume G satisfies:
(1) For any ordered abelian groups A and B, $G \simeq A \to G \to B$ implies $G \simeq A \to G$ (or, equivalently, implies $G \simeq G \to B$).
Then G satisfies:
(2) For any ordered abelian group H and for any positive integer k: $G^k \simeq H^k$ implies $G \simeq H$.

- Case 2: Prooving that (abs,$\equiv$) and (abs,$\simeq_c$) hold for every ordered abelian group is now the way to proove that so do (can,$\equiv$) and (can,$\simeq_c$), and we get:

Proposition on elementary equivalence:

Let G be any ordered abelian group, let A and B be (possibly trivial) ordered abelian groups, and let p be a positive integer.

If: $G \simeq A \to G \to B^p$

then: $G \equiv X \to B^{(\omega *)}$ *for some ordered abelian group X*

hence $G \equiv A \to G \equiv G \to B$

Theorem on elementary equivalence:

Let G and H be ordered abelian groups such that, for some positive integer k: $G^k \simeq H^k$

Then $G \equiv H$.

Proposition on order isomorphism:

If, for some ordered abelian groups A, G, and B and some positive integer n:

$G \simeq A \to G \to B^n$ *(as ordered groups)*

then: (as ordered sets)

-1) $G \simeq_s X \to B^{(\omega *)}$ *for some ordered abelian group X.*

-2) $G \simeq_s A \to G \simeq_s G \to B$.

Theorem on order isomorphism:

Let G and H be ordered abelian groups such that, for some positive integer k: $G^k \simeq H^k$

then:

G and H are isomorphic as ordered sets.

Both ceses 1 and 2 make use of the following technical lemma (case 1 using 1 zand 2, case 2 using 3):

Technical lemma:

let G and H be ordered abelian groups such that, for some integer k, k⩾2, $G^k \simeq H^k$, then:

-1) For some ordered abelian groups A, B, C, and D:

$G \simeq A \to H \to B$ and $H \simeq C \to G \to D$, where A or C is a trivial group.

-2) For some ordered abelian groups A', B', C', and D':

$G \simeq A' \to H \to B'$ and $H \simeq C' \to G \to D'$, where B' or D' is a trivial group.

-3) For some ordered abelian groups A, B, C, and D, one of the following four conditions holds:

-i) $G \simeq A \to H \simeq H \to B$ and $H \simeq C \to G \to D$

-ii) $G \simeq A \to H$ and $H \simeq G \to B$

-i') and ii') obtained from i) and ii), by exchanging G and H

However, none of the techniques described here have worked out the problem of (can, $\simeq_{ab}$), and wether all ordered abelian groups satisfy (abs, $\simeq_{ab}$) and (can, $\simeq_{ab}$) seems still unknown.

&3 Applications and examples:

Cases of cancellation of powers:

The following ordered abelian groups satisfy (abs,≃), hence are uniquely determined by any of their k™ lexicographic powers, k finite:

-1) ordered abelian groups in which every convex subgroup is a direct summand: divisible ordered abelian groups, (whatever the order relation they are provided with is), summs and Hahn products of archimedian ordered abelian groups .

-2) ordered abelian groups in which no chain of convex direct summands is of order type $\omega+\omega^*$.

-3) ordered abelian groups without proper direct summand, groups which are isomorphic to none of their proper direct summands (whatever the order relation they are provided with is), groups which are isomorphic to no proper homomorphic image of one of their proper convex direct summands.

-4) Any finite lexicographic product of the ordered abelian groups mentioned above (and, more generally, of groups satisfying (abs,≃)).

Remark 1:

By [O-1], Lemma 4-1, whenever G is An ω_1-saturated ordered abelian groups, $G \simeq A \to G$ implies $G \simeq A^\omega \to G$ for any ordered abelian groups A, where A^ω is the product of ω copies of A. We mentionned in &1 that it follows from this

copies of A. We mentionned in &1 that it follows from this and our Theorem on isomorphism that every ω_1-saturated ordered abelian groups is uniquely determined by any of its k^m lexicographical powers (and so is any finite lexicogaphic product of ω_1-saturated ordered abelian groups with groups mentionned above.

It also follows that any ordered abelian group which is not determined by its k^m powers is elementary equivalent to some ω_1-saturated one which is, whence, by corollary 8, in some elementary classes of ordered abelian groups (divisible ones for instance) every model is uniquely determined by any of its k^m powers.

Remark 2: One may reasonably wonder wether there is any simple relationship between (abs,≃) and the following absorption property (abs,squ.) considered in [O-1]:

(abs,squ.): $A^{\rightarrow 2}\rightarrow G \simeq G$ implies $A\rightarrow G \simeq G$ for any ordered abelian group A.

The answer is no: In [O-1], F. Oger gave two examples of groups G not satisfying (abs,squ.). In both cases, the order type of the set of convex subgroups of G is ω, hence, for any ordered abelian group B, $G \simeq A\rightarrow G\rightarrow B$ implies $B \simeq \{0\}$ and $G \simeq A\rightarrow G$, hence G satisfies (abs,≃). On the contrary, the example in [O-2] of an ordered abelian group G not determined by its lexicographic square, hence not satisfying (abs,≃) (by the Theorem on isomorphism), is such that, if

$A^{=}\to G \simeq G$ for some ordered abelian group A, then $A = \{0\}$, hence $A\to G \simeq G$.

Remark 3 (miscellaneous):

i- When $G \simeq A\to G$, there is not always a chain X such that $G \simeq_{\equiv} A^{<\omega>}\to X$.

ii- In [O-2], Oger's example is an ordered abelian group not determined by its square but determined by its cube:

ii- For any integer n ($n\geq 2$), there can be exactly n non-isomorphic ordered abelian groups with the same square (or infinitely many, like in [O-2]).

Bibliography:

[E-F] P.C. Eklof and E.R. Fisher. The elementary theory of abelian groups. Annals of Mathematical Logic. Volume 4. N° 2 (1972) p. 115-171.

[C-K] C.C. Chang and H. J. Keisler. Model Theory. Studies in Logic N° 73. North-Holland (1973).

[D-L-1] F. Delon and F. Lucas. Inclusions et produits de groupes abéliens étudiés au premier ordre. Preprint.

[D-L-2] F. Delon and F. Lucas. Quelques constructions sur les groupes abéliens ordonnés. Ce recueil.

[F-V] S. Feferman and R.L. Vaught. The first order properties of products of algebraic systems. Fundamentae Mathematicae. XLVII (1959) p. 57-103.

[O-1] F. Oger. Produits lexicographiques de groupes ordonnés. Isomorphisme et equivalence élémentaire: To appear in Journal of Algebra.

[O-2] F. Oger An example of two non-isomorphic countable ordered abelian groups with isomorphic lexicographic squares. Submitted.

[R] J.G. Rosenstein, Linear orderings, Academic press, New York (1982).

[S] P.H. Schmidt. Model theory of ordered abelian groups. Habilitationsschrift. Heidelberg. (1982).

[Si] W. Sierpinski. Cardinal and ordinal numbers. Warsaw. P.W.N. (1965).

Michèle Giraudet.
(U.A. 753-Paris 7 and université du Maine)
32 rue de la Réunion.
75020 Paris. France.

An example of two nonisomorphic countable ordered abelian groups with isomorphic lexicographical squares

F. Oger

If M and N are ordered groups, we denote by $M\vec{\times}N$ the group $M\times N$ equipped with the lexicographical order: $(a,b) < (a',b')$ if and only if $a<a'$ or $(a=a'$ and $b<b')$.

In [1], A.S.L. Corner gives an example of two countable abelian groups A,G such that G and $A\times A\times G$ are isomorphic while G and $A\times G$ are not isomorphic; he also gives an exemple of two nonisomorphic countable abelian groups G,H which satisfy $G\times G \cong H\times H$.

On the other hand, we can easily deduce from [5, Theorem 5.2] that, if A and G are abelian groups and if G and $A\times A\times G$ are elementarily equivalent, then, G and $A\times G$ are elementarily equivalent. It follows from the same theorem that two abelian groups G,H are elementarily equivalent as soon as $G\times G$ and $H\times H$ are elementarily equivalent.

We showed in [4] that, if A and G are ordered abelian groups and if G and $A\vec{\times}A\vec{\times}G$ are elementarily equivalent, then, G and $A\vec{\times}G$ are elementarily equivalent. We also gave an example of two countable ordered abelian groups A,G such that G and $A\vec{\times}A\vec{\times}G$ are isomorphic while G and $A\vec{\times}G$ are not isomorphic.

In [2, Corollary 4.7] and [3], F. Lucas and M. Giraudet prove that two ordered abelian groups G,H are elementarily equivalent as soon as $G\vec{\times}G$ and $H\vec{\times}H$ are elementarily equivalent. In the present paper, we give an exemple of two nonisomorphic countable ordered abelian groups G,H which satisfy $G\vec{\times}G \cong H\vec{\times}H$.

1. Notations; definition of the ordered groups G,H .

For each prime number p, $\mathbb{Z}_p$ is the ordered subgroup of $\mathbb{Q}$ which consists of the elements a/b with $a\in\mathbb{N}$, $b\in\mathbb{N}^*$ and b not divisible by p.

We consider a sequence $(p(n))_{n\in\mathbb{Z}}$ of prime numbers which are all different and we denote by A the direct sum $\bigoplus_{n\in\mathbb{Z}} \mathbb{Z}_{p(n)}$ equipped with the lexicographical order: $(a_n)_{n\in\mathbb{Z}} < (b_n)_{n\in\mathbb{Z}}$ if and only if there exists an integer n such that $a_n < b_n$ and $a_m = b_m$ for each integer $m<n$. For each $n\in\mathbb{Z}$, we consider the element $1_n = (a_m)_{m\in\mathbb{Z}} \in A$ with $a_n = 1$ and $a_m = 0$ for $m\neq n$.

We denote by I the ordered set which consists of the sequence $0+ < 1+ < 2+ < \ldots < 2- < 1- < 0-$. For each $n\in\mathbb{Z}$, we write

$u_n = (1_{2n}, 1_{2n+2}, 1_{2n+4}, \ldots, \ldots, 1_{2n+5}, 1_{2n+3}, 1_{2n+1})$ and

$v_n = (1_{2n}, 1_{2n+2}, 1_{2n+4}, \ldots, \ldots, 1_{2n+7}, 1_{2n+5}, 1_{2n+3})$.

We consider the subgroup M (respectively N) of $\bigotimes_{i\in I} A$ which is generated by $\bigoplus_{i\in I} A$ and the elements u_n (respectively v_n) and we denote by G (respectively H) the subgroup of $\bigotimes_{i\in I} A$ which consists of the elements x such that there exists an integer $s\geq 1$ for which $sx \in M$ (respectively N). We define an order on G (respectively H) as follows: for two different elements $u = (a_i)_{i\in I}$ and $v = (b_i)_{i\in I}$ which belong to G (respectively H), there exists an element $i\in I$ such that $a_i \neq b_i$ and $a_j = b_j$ for each $j<i$ (this property is true for G and H though it is false for $\bigotimes_{i\in I} A$); we write $u<v$ if and only if $a_i < b_i$.

2. $G\vec{\times}G$ and $H\vec{\times}H$ are isomorphic.

We define an isomorphism $f : G\vec{\times}G \to H\vec{\times}H$ by writing, for any sequences $(a_i)_{i\in I} \in G$ and $(c_i)_{i\in I} \in G$, $f((a_i)_{i\in I}, (c_i)_{i\in I}) = ((b_i)_{i\in I}, (d_i)_{i\in I})$ with

$b_{n+} = a_{n+}$ for each $n \in \mathbb{N}$, $b_{n-} = a_{(n+1)-}$ for each $n \in \mathbb{N}$, $d_{0+} = a_{0-}$, $d_{n+} = c_{(n-1)+}$ for each $n \in \mathbb{N}^*$ and $d_{n-} = c_{n-}$ for each $n \in \mathbb{N}$.

For each $n \in \mathbb{Z}$, we have

$$f((u_n,0)) = (v_n,0) + (0,(1_{2n+1},0,\ldots,0,\ldots)),$$

$$f((0,u_n)) = (0,v_{n-1}) - (0,(1_{2n-2},0,\ldots,0,\ldots)),$$

$$(v_n,0) = f((u_n,0) - ((\ldots,0,\ldots,0,1_{2n+1}),0)),$$

$$(0,v_n) = f((0,u_{n+1}) + ((\ldots,0,\ldots,0,1_{2n}),0)).$$

3. G and H are isomorphic as groups.

Let us write $E(m) = \{0-\}$, $E(-m) = \{0-,1-,\ldots,(2m)-\}$, $F(m) = \emptyset$ and $F(-m) = \{0-,1-,\ldots,(2m-1)-\}$ for each $m \in \mathbb{N}$. For each $n \in \mathbb{Z}$, let us consider the following subgroups in G and H :

$K(n) = \{x = (x_i)_{i\in I} \in G \mid$ for each $m \in \mathbb{N}$, $x_{m+} = (a_k)_{k\in\mathbb{Z}}$ with $a_k = 0$ for $k \neq 2(m+n)$ and $x_{m-} = (a_k)_{k\in\mathbb{Z}}$ with $a_k = 0$ for $k \neq 2(m+n)+1\}$,

$K'(n) = \{x = (x_i)_{i\in I} \in K(n) \mid x_i = 0$ for $i \in E(n)\}$,

$K''(n) = \{x = (x_i)_{i\in I} \in K(n) \mid x_i = 0$ for $i \in I - E(n)\}$,

$L(n) = \{x = (x_i)_{i\in I} \in H \mid$ for each $m \in \mathbb{N}$, $x_{m+} = (a_k)_{k\in\mathbb{Z}}$ with $a_k = 0$ for $k \neq 2(m+n)$ and $x_{m-} = (a_k)_{k\in\mathbb{Z}}$ with $a_k = 0$ for $k \neq 2(m+n)+3\}$,

$L'(n) = \{x = (x_i)_{i\in I} \in L(n) \mid x_i = 0$ for $i \in F(n)\}$ and

$L''(n) = \{x = (x_i)_{i\in I} \in L(n) \mid x_i = 0$ for $i \in I - F(n)\}$.

For each $n \in \mathbb{Z}$, we have $u_n \in K(n)$, $v_n \in L(n)$, $K(n) = K'(n) \oplus K''(n)$ and $L(n) = L'(n) \oplus L''(n)$. It follows $G = \bigoplus_{n\in\mathbb{Z}} K(n) = (\bigoplus_{n\in\mathbb{Z}} K'(n)) \oplus (\bigoplus_{n\in\mathbb{Z}} K''(n))$ and $H = \bigoplus_{n\in\mathbb{Z}} L(n) = (\bigoplus_{n\in\mathbb{Z}} L'(n)) \oplus (\bigoplus_{n\in\mathbb{Z}} L''(n))$.

We define an isomorphism $f : \bigoplus_{n\in\mathbb{Z}} K'(n) \to \bigoplus_{n\in\mathbb{Z}} L'(n)$ by writing $f((a_i)_{i\in I}) = (b_i)_{i\in I}$ with $b_{n+} = a_{n+}$ for each $n \in \mathbb{N}$ and $b_{n-} = a_{(n+1)-}$ for each $n \in \mathbb{N}$.

For each $m \in \mathbb{N}$, we have $K''(m) \cong \mathbb{Z}_{p(2m+1)}$, $L''(M) = \{0\}$, $K''(-m) =$

$\bigoplus_{k=-m}^{m} \mathbb{Z}_{p(2k+1)}$ and $L''(-m) = \bigoplus_{k=-m+1}^{m} \mathbb{Z}_{p(2k+1)}$. It follows $\bigoplus_{n\in\mathbb{Z}} K''(n) \cong \bigoplus_{n\in\mathbb{Z}} L''(n) \cong \bigoplus_{k\in\mathbb{N}} \left(\bigoplus_{n\in\mathbb{Z}} \mathbb{Z}_{p(2n+1)} \right)$.

4. G and H are not isomorphic as ordered groups.

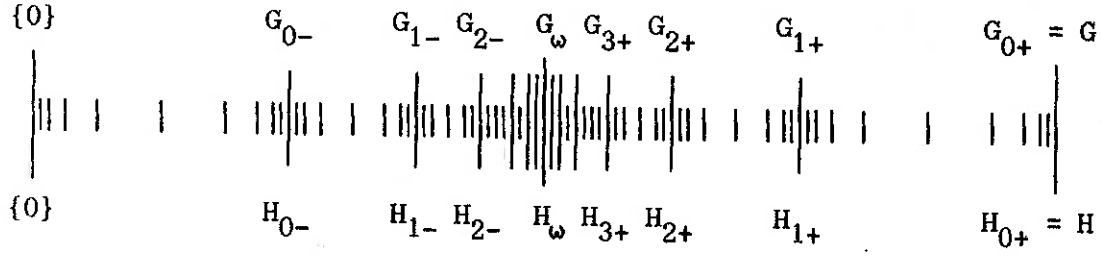
Convex subgroups.

The following subgroups are convex in G (respectively H):

- for each $i\in I$, $G_i = \{x = (a_j)_{j\in I} \in G \mid a_j = 0 \text{ for } j<i\}$, (respectively $H_i = \{x = (a_j)_{j\in I} \in H \mid a_j = 0 \text{ for } j<i\}$);
- $G_\omega = \{x = (a_j)_{j\in I} \in G \mid a_{n+} = 0 \text{ for each } n\in\mathbb{N}\}$ (respectively $H_\omega = \{x = (a_j)_{j\in I} \in H \mid a_{n+} = 0 \text{ for each } n\in\mathbb{N}\}$).

If $x = (a_j)_{j\in I}$ is an element of G_ω (respectively H_ω), we have $a_j = 0$ except for a finite number of values of j. It follows $G_\omega = \bigcup_{n\in\mathbb{N}} G_{n-} = \bigcap_{n\in\mathbb{N}} G_{n+}$ and $H_\omega = \bigcup_{n\in\mathbb{N}} H_{n-} = \bigcap_{n\in\mathbb{N}} H_{n+}$.

The set of all convex subgroups of G and the set of all convex subgroups of H, ordered by inclusion, can be described by the following diagram:



It follows from the structures of these isomorphic ordered sets that an isomorphism $f : G \to H$ necessarily satisfies $f(G_i) = H_i$ for each $i \in I \cup \{\omega\}$.

Arguments of divisibility.

For each $n\in\mathbb{Z}$, $A(n) = \{x = (a_m)_{m\in\mathbb{Z}} \in A \mid a_m = 0 \text{ for } m \neq n\}$ is the set of all elements of A which are divisible by each integer k which is not itself divisible by $p(n)$. Consequently, for each $n\in\mathbb{Z}$, $G(n) = \{x = (x_i)_{i\in I} \in G \mid x_i \in A(n) \text{ for each } i\in I\}$ (respectively $H(n) = \{x = (x_i)_{i\in I} \in H \mid x_i \in A(n) \text{ for each } i\in I\}$) is the set of all elements of G (respectively H) which are divisible by each integer k which is not itself divisible by $p(n)$. So, any isomorphism $f : G \to H$ satisfies $f(G(n)) = H(n)$ for each $n\in\mathbb{Z}$.

Moreover, for each each element

$x = (1/s)\ ((a_i)_{i\in I} + b_1\, u_{r(1)} + \ldots + b_k\, u_{r(k)}) \in G$

(respectively $x = (1/s)\ ((a_i)_{i\in I} + b_1\, v_{r(1)} + \ldots + b_k\, v_{r(k)}) \in H$),

with $s \in \mathbb{N}^*$, $a_i \in A$ for each $i\in I$, $a_i = 0$ except for a finite number of values of i , $b_1,\ldots,b_k \in \mathbb{Z}$ and $r(1),\ldots,r(k)$ elements of $\mathbb{Z}$ which are all different, we have $x \in G(n)$ (respectively $x \in H(n)$) if and only if $b_1 = \ldots = b_k = 0$ and $a_i \in A(n)$ for each $i\in I$. This implies $G(n) = H(n) = \bigoplus_{i\in I} A(n)$ for each $n\in\mathbb{Z}$ and $\sum_{n\in\mathbb{Z}} G(n) = \sum_{n\in\mathbb{Z}} H(n) = \bigoplus_{i\in I} A$. So, any isomorphism $f : G \to H$ satisfies $f(\bigoplus_{i\in I} A) = \bigoplus_{i\in I} A$.

End of the proof.

Here, we consider an isomorphism $f : G \to H$ and we prove that the elements v_n cannot belong to $f(G)$, whence a contradiction.

For each $j\in I$ and each $n\in\mathbb{Z}$, we write $1_{j,n} = (a_i)_{i\in I}$ with $a_i = 0$ for $i\neq j$ and $a_j = 1_n$. We consider the following subgroups in G and H : $G'_{0-} = \{0\}$; $G'_{n-} = G_{(n-1)-}$ for each $n\in\mathbb{N}^*$; $G'_{n+} = G_{(n+1)+}$ for each $n\in\mathbb{N}$; $H'_{0-} = \{0\}$; $H'_{n-} = H_{(n-1)-}$ for each $n\in\mathbb{N}^*$; $H'_{n+} = H_{(n+1)+}$ for each $n\in\mathbb{N}$. For each $j\in I$ and each $n\in\mathbb{Z}$, $f(1_{j,n})$ belongs to $H(n) \cap H_j$ since $1_{j,n}$

belongs to $G(n) \cap G_j$. Moreover, the image of $f(1_{j,n})$ in H_j/H'_j is not divisible by $p(n)$ since the image of $1_{j,n}$ in G_j/G'_j is not divisible by $p(n)$. So, we have $f(1_{j,n}) = (b_i)_{i\in I}$ with $b_i \in A(n)$ for each $i\in I$, $b_i = 0$ for $i<j$ and b_j not divisible by $p(n)$.

For each $n\in\mathbb{Z}$ and each $k\in\mathbb{N}$, $f(u_n) - f(1_{k+,2(n+k)})$ is divisible by $(p(2\ (n+k)))^t$ for each $t\in\mathbb{N}$ since $u_n - 1_{k+,2(n+k)}$ is divisible by $(p(2\ (n+k)))^t$ for each $t\in\mathbb{N}$. Similarly, $f(u_n) - f(1_{k-,2(n+k)+1})$ is divisible by $(p(2\ (n+k) + 1))^t$ for each $t\in\mathbb{N}$ since $u_n - 1_{k-,2(n+k)+1}$ is divisible by $(p(2\ (n+k) + 1))^t$ for each $t\in\mathbb{N}$.

It follows $f(u_n) = (x_i)_{i\in I}$ with, for each $k\in\mathbb{N}$, x_{k+} not divisible by $p(2\ (n+k))$, x_{k+} divisible by $(p(2\ (m+k)))^t$ for each integer $m>n$ and each $t\in\mathbb{N}$, x_{k-} not divisible by $p(2\ (n+k) + 1)$ and x_{k-} divisible by $(p(2\ (m+k) + 1))^t$ for each integer $m<n$ and each $t\in\mathbb{N}$.

Let us write $f(u_n) = (x_i)_{i\in I} = (1/s)\ [(a_i)_{i\in I} + \sum_{m\in\mathbb{Z}} c_m\ v_m]$ with $s\in\mathbb{N}^*$, $a_i \in A$ for each $i\in I$, $a_i = 0$ except for a finite number of values of i , $c_m \in \mathbb{Z}$ for each $m\in\mathbb{Z}$ and $c_m = 0$ except for a finite number of values of m .

For each $k\in\mathbb{N}$ such that $a_{k+} = 0$, we have $x_{k+} = (1/s) \sum_{m\in\mathbb{Z}} c_m\ 1_{2(m+k)}$. This implies $c_n \neq 0$ and $c_m = 0$ for $m>n$ since x_{k+} is not divisible by $p(2\ (n+k))$ and x_{k+} is divisible by $(p(2\ (m+k)))^t$ for each integer $m>n$ and each $t\in\mathbb{N}$.

For each $k\in\mathbb{N}$ such that $a_{k-} = 0$, we have $x_{k-} = (1/s) \sum_{m\in\mathbb{Z}} c_m\ 1_{2(m+k)+3}$. This implies $c_{n-1} \neq 0$ and $c_m = 0$ for $m < n-1$ since x_{k-} is not divisible by $p(2\ (n-1+k) + 3)$ and x_{k-} is divisible by $(p(2\ (m+k) + 3))^t$ for each integer $m < n-1$ and each $t\in\mathbb{N}$.

It follows $f(u_n) = (1/s)\ (c\ v_{n-1} + d\ v_n + y)$ with $s\in\mathbb{N}^*$, $c,d \in \mathbb{Z}^*$ and $y \in \bigoplus_{i\in I} A$.

Any element of $G = \bigoplus_{i\in I} A$ can be written $u = (1/s)\left(\sum_{k=m}^{n} a_k u_k + x\right)$ with $s \in \mathbb{N}^*$, $m,n \in \mathbb{Z}$, $m \leq n$, $a_k \in \mathbb{Z}$ for $m \leq k \leq n$, $a_m \neq 0$, $a_n \neq 0$ and $x \in \bigoplus_{i\in I} A$. There exists an integer $t \geq 1$ such that $t\, f(u_k) \in N$ for each integer k which satisfies $m \leq k \leq n$; we have $f(u_k) = (1/t)(c_k v_{k-1} + d_k v_k + y_k)$ with $c_k, d_k \in \mathbb{Z}^*$ and $y_k \in \bigoplus_{i\in I} A$ for $m \leq k \leq n$. It follows $f(u) = (1/st)\left[a_m c_m v_{m-1} + \sum_{m\leq k\leq n-1} (a_{k+1} c_{k+1} + a_k d_k) v_k + a_n d_n v_n + \left(t f(x) + \sum_{k=m}^{n} a_k y_k\right)\right]$ with $t f(x) + \sum_{k=m}^{n} a_k y_k \in \bigoplus_{i\in I} A$. The element $f(u)$ cannot be equal to any v_k since $a_m c_m$ and $a_n d_n$ are both non trivial.

On the other hand, for each $u \in \bigoplus_{i\in I} A$, we have $f(u) \in \bigoplus_{i\in I} A$ and $f(u)$ cannot be equal to any v_k. This achieves to prove that the elements v_k cannot belong to $f(G)$, whence a contradiction.

References

[1] A.S.L. Corner, On a conjecture of Pierce concerning direct decompositions of abelian groups, Proceedings of the Colloquium on Abelian Groups, Akadémiai Kiadó, Budapest, 1964.

[2] F. Delon and F. Lucas, Inclusions et produits de groupes abéliens ordonnés étudiés au premier ordre, preprint, Paris, 1986.

[3] M. Giraudet, Lexicographical squares of totally ordered abelian groups, preprint, Paris, 1986.

[4] F. Oger, Produits lexicographiques de groupes ordonnés: Isomorphisme et équivalence élémentaire, J. Algebra, to appear.

[5] W. Szmielew, Elementary properties of abelian groups, Fund. Math. 41, 1954.

OGER Francis, Unité Associée 753, Département de Mathématiques,
Université Paris VII, 2 Place Jussieu, 75251 PARIS Cedex 05

EQUIVALENCE ELEMENTAIRE & CODIMENSION DANS LES CORPS p-ADIQUES

L. Bélair

Résumé. Nous présentons le résultat d'une note avec A. Macintyre et L. van den Dries. On sait que tout corps algébriquement clos de caractéristique nulle possède un sous-corps réel clos d'indice 2 . Du point de vue de la théorie des corps réels clos ceci se traduit en ce qu'un corps élémentairement équivalent à une extension finie de $\mathbb{R}$ possède un sous-corps d'indice fini élémentairement équivalent à $\mathbb{R}$. Nous montrons qu'il n'en est pas de même pour le corps des nombres p-adiques, $\mathbb{Q}_p$ (p un nombre premier fixé). A savoir que, pour toute extension finie de $\mathbb{Q}_p$ donnée, il existe un corps élémentairement équivalent qui ne contient pas de sous-corps d'indice fini élémentairement équivalent à $\mathbb{Q}_p$. La théorie des modèles de $\mathbb{R}$ et $\mathbb{Q}_p$ diffère donc sur ce point. Nous soulignons que les exemples donnés possèdent le groupe de valuation le plus simple possible, i.e. $\mathbb{Z}$. On utilise des résultats élémentaires de la géométrie algébrique (réduite de Weil, dimension), le théorème de Baire dans $\mathbb{Q}_p$, et le fait que dans une extension finie de $\mathbb{Q}_p$, un sous-corps relativement algébriquement clos est élémentairement équivalent à l'extension elle-même. Les détails devraient paraître dans Manuscripta Mathematica.

L. Bélair
Université de Paris VII- C.N.R.S.
Equipe de logique mathématique, U.A. 753
2, place Jussieu
Paris, 5ième

AXIOMATISATIONS "A LA ARTIN SCHREIER" DES CORPS CHAÎNABLES ET DES CORPS CHAÎNE-CLOS

par Danielle GONDARD

(Université de Paris 6)

En 1982 Harman introduit la notion de chaîne d'ordres de niveau supérieur faisant ainsi suite aux travaux de Becker qui avait formalisé la notion d'ordre de niveau supérieur et obtenu divers résultats sur ce sujet.

La motivation fondamentale pour l'introduction de ces chaînes d'ordre de niveau supérieur par Harman était en fait que pour un corps K muni d'un ordre de niveau supérieur on ne pouvait trouver de notion de clôture réelle généralisée satisfaisante car on pouvait obtenir différentes clôtures non K-isomorphes.

Au contraire si on considère un corps K muni d'une chaîne d'ordres de niveau supérieur on aura une clôture de chaîne unique à K-isomorphisme près. Ceci s'explique par le fait qu'un ordre de niveau supérieur peut appartenir à plusieurs chaînes différentes.

Nous appellerons corps chaînable un corps K qui peut être muni d'une chaîne d'ordres de niveau supérieur et corps chaîne-clos un corps K admettant une chaîne d'ordres $(P_i)_{i\in\mathbb{N}}$ tel que $(K,P_i)_{i\in\mathbb{N}})$ n'admette pas d'extension algébrique fidèle au sens de Harman. Nous dirons qu'un corps $(K,(P_i)_{i\in\mathbb{N}})$ est un-chaîné lorsqu'il n'admet qu'une seule chaîne d'ordres de niveau supérieur, à échange de P_0 et P_1 près.

Les résultats de cet article consistent en des axiomatisations des diverses notions de corps chaînable, corps pythagoricien un-chaîné n'admettant

que deux ordres et corps chaîne-clos, parfaitement dans l'esprit des axiomatisations de corps ordonnable et de corps ordonné maximal dues à Artin-Schreier.

Rappelons tout d'abord les définitions d'un ordre de niveau supérieur et d'une chaîne d'ordres de niveau supérieur :

$P \subset K$ est un ordre de niveau supérieur si

(a) $\dot{P} = P - \{0\}$ est un sous groupe de $\dot{K} = K - \{0\}$.

(b) $\dot{P} + \dot{P} \subset \dot{P}$

(c) $\dot{K}/\dot{P}$ est un groupe cyclique fini.

On dira que P est un ordre de niveau q si $|\dot{K}/\dot{P}|$ divise q , et que P est un ordre de niveau exact q si $|\dot{K}/\dot{P}| = q$.

$(P_i)_{i \in \mathbf{N}}$ est une chaîne d'ordres de niveau supérieur si

(i) P_o et P_1 sont deux ordres (au sens usuel) distincts

(ii) Pour tout $i \geq 2$, P_i est un ordre de niveau exact 2^i.

(iii) Pour tout $i \geq 1$:

$$P_i \cup -P_i = (P_{i-1} \cap P_o) \cup -(P_{i-1} \cap P_o) .$$

Dans nos démonstrations nous reverrons le lecteur à nos articles [G1] et [G2] pour les résultats utilisés concernant les théories des ordres de niveau supérieur et des chaînes d'ordres de niveau supérieur quoique ces résultats soient le plus souvent dus à Becker [Be] ou à Harman [Ha] , puisque les premières références sont directement utilisables dans ce même volume du séminaire.

Dans toute la suite du texte la notation ΣK^{2^n} représentera $\bigcup_{i=1}^{\infty} (\sum_{p=o}^{i} x_p^{2^n})$ et de même ΣK^{2^n} notera $\bigcup_{i=1}^{\infty} (\sum_{p=o}^{i} x_p^{2^n})$.

I CORPS CHAÎNABLES

Soit $\mathfrak{L}(0,1,+,.,-,=,\alpha)$ le langage formé de

0,1 et α comme symboles de constante

+ et . comme symboles fonctionnels à 2 variables

- comme symbole fonctionnel à 1 variable

= comme symbole relationnel.

THEOREME I-1 : *Un corps* K *est chaînable si et seulement si on peut y trouver un élément* $\bar{\alpha}$ *tel que* $(K,\bar{\alpha})$ *satisfasse le système d'axiomes* T_1 *du langage* $\mathfrak{L}$.

T_1 :

- *Axiomes de corps commutatif ordonnable* :
  - *Axiomes de corps commutatif* :
    - *Axiomes de Groupe commutatif* :
      - $\Lambda x\, \Lambda y\, \Lambda z((x+y)+z = x + (y+z))$
      - $\Lambda x\, \Lambda y\, (x+y = y+x)$
      - $\Lambda x\, (x + 0 = x)$
      - $\Lambda x\, (x + (-x) = 0)$
    - $\Lambda x\, \Lambda y\, \Lambda z\, (x.(y.z) = (x.y).z)$
    - $\Lambda x\, \Lambda y\, (x.y = y.x)$
    - $\Lambda x\, (x.1 = x)$
    - $\Lambda x\, \Lambda y\, (x = 0 \vee x.y = 1)$
    - $\Lambda x\, \Lambda y\, \Lambda z\, (x.(y+z) = x.y + x.z)$
    - $\neg(0 = 1)$
  - *pour chaque* $n \geq 1$ *l'axiome* $\Lambda x_1 \ldots \Lambda x_n\, \neg(-1 = x_1^2 + \ldots + x_n^2)$
- *pour chaque* $n \geq 1$ *l'axiome* $\Lambda x_1 \ldots \Lambda x_n\, \neg(\alpha^2 = x_1^4 + \ldots + x_n^4)$.

Démonstration.

Les premiers axiomes assurent qu'un modèle de T_1 est un corps commutatif ordonnable (Artin-Schreier). Le dernier schéma d'axiome montre qu'il existe un élément α du corps K tel que α^2 n'est pas une somme de puissances quatrièmes.

Ceci entraîne que $\Sigma K^2 \neq \Sigma K^4$ et donc que le corps K admet des ordres de niveau supérieur non triviaux, (voir [G1] , th. 4-4) et donc que pour tout n il existe un ordre de niveau exact 2^n soit P_n (voir [G1], th. 4-3). Il passe alors par cet ordre P_n une chaîne d'ordres $(P_i)_{i \in \mathbb{N}}$ ([G2], th. IV-3). Un modèle de T_1 est donc bien un corps chaînable. Réciproquement : tout corps chaînable est un modèle de T_1 . En effet si K est un corps chaînable il admet des ordres de niveau exact 2^n pour tout n et donc $\Sigma K^2 \neq \Sigma K^4$ ([G1], th. 4-4). Si pour tout $\alpha \in K$ on a $\alpha^2 \in \Sigma K^4$ alors toute somme de carrés d'éléments de K est une somme de puissances quatrièmes ce qui est impossible ; Donc il existe α tel que $\alpha^2 \notin \Sigma K^4$. Un corps chaînable étant nécessairement ordonnable ([G1], th. 4-1), K est bien un modèle de T_1 .

CONJECTURE I-2.

On ne peut pas trouver une axiomatisation du premier ordre de la théorie des corps chaînables dans le langage des corps $\mathcal{L}"(0,1,+,.,-,=)$, *c'est-à-dire* $\mathcal{L}$ *privé du symbole de constante* α .

II CORPS UN-CHAINE, PYTHAGORICIEN N'AYANT QUE DEUX ORDRES USUELS.

Soit $\mathcal{L}'(0,1,+,.,-,=,\alpha, \underset{0}{>}, \underset{1}{>})$ le langage formé à partir de $\mathcal{L}$ en ajoutant $\underset{0}{>}$ et $\underset{1}{>}$ comme symboles relationnels.

THEOREME II-1 : Un corps K *est un-chaîné, pythagoricien et a seulement deux ordres vrais si et seulement si on peut y trouver un élément* $\bar{\alpha}$ *tel que* $(K,\bar{\alpha})$ *satisfasse le système d'axiomes* T_2' *du langage* $\mathcal{L}'$.

(On peut remarquer que le théorème II-1. reste valable en remplaçant un-chainé par chaînable).

T'_2 { T'_1 (*corps chaînable: lemme II-2*) { *Axiomes de corps ordonné pour* $\geq_0$ et *pour* $\geq_1$ { *Axiomes de corps ordonné pour* $\geq_0$ { *Axiomes de corps commutati (cf. théorème I-1)*; $\Lambda x\ \Lambda y (x \geq_0 0) \wedge (y \geq_0 0) \to x+y \geq_0 0)$; $\Lambda x\ \Lambda y (x \geq_0 0) \wedge (y \geq_0 0) \to x.y \geq_0 0)$; $\Lambda x\ \ (x \geq_0 0) \vee (-x \geq_0 0)$; $\Lambda x\ \ (\neg((x \geq_0 0) \wedge (-x \geq_0 0)) \vee x=0)$ }; *Les 4 axiomes obtenus en substituant* $\geq_1$ *à* $\geq_0$ *dans les 4 axiomes ci-dessus* }; *pour chaque* $n \geq 1$ *l'axiome* $\Lambda x_1 \ldots \Lambda x_n \neg(\alpha^2 = x_1^4 + \ldots + x_n^4)$ }; $(\alpha \geq_0 0) \wedge (\alpha \leq_1 0)$; $\Lambda x\ \forall y\ ((x = y^2) \vee (x = -y^2) \vee (x = \alpha y^2) \vee (x = -\alpha y^2))$ }

LEMME II-2 : Un corps K *est chaînable si et seulement si on peut y trouver un élément* $\bar{\alpha}$ *tel que* $(K,\bar{\alpha})$ *satisfasse le système d'axiomes* T'_1 *du langage* £' .

C'est clair : Un modèle de T'_1 est ordonnable donc est aussi modèle de T_1 et est un corps chaînable.

Réciproquement un corps chaînable est un modèle de T_1 et comme il a toujours deux ordres vrais au moins il est aussi modèle de T'_1 .

Démonstration du théorème : Soit K un modèle de T'_2 . Par le lemme nous savons qu'un modèle de T'_2 est un corps chaînable.

Posons $P_0 = K^2 \cup \alpha K^2$ et $P_1 = K^2 \cup -\alpha K^2$ et montrons que P_0 et P_1 sont des ordres :

(1) $P_0 \cup -P_0 = K$, est clair d'après le dernier axiome.

(2) $P_0 . P_0 \subset P_0$ est évident.

(3) $P_0 \cap -P_0 = \{0\}$: En effet soit $x \in P_0 \cap -P_0$, on a donc $x \in (K^2 \cup \alpha K^2) \cap (-K^2 \cup -\alpha K^2)$. Alors :

. Si $x \in K^2$ et $x \in -K^2$, clairement $x = 0$.

. Si $x \in K^2$ alors $x \underset{0}{\geq} 0$, et si $x \in -\alpha K^2$ alors $0 \underset{0}{\leq} x$, car $\alpha \underset{0}{\geq} 0$. Donc $x = 0$.

. Si $x \in \alpha K^2$ alors $x \underset{0}{\geq} 0$ car $\alpha \underset{0}{\geq} 0$, et si $x \in -\alpha K^2$ alors $0 \underset{0}{\leq} x$ car $\alpha \underset{0}{\geq} 0$. Donc $x = 0$.

. Enfin si $x \in \alpha K^2$ alors $x \underset{0}{\geq} 0$, et si $x \in -K^2$, alors $x \underset{0}{\leq} 0$, donc $x = 0$.

Dans tous les cas $x \in P_0 \cap -P_0$ entraîne $x = 0$.

(4) $P_0 + P_0 \subset P_0$:

Soit $x \in P_0 = K^2 \cup \alpha K^2$ et $y \in P_0 = K^2 \cup \alpha K^2$.

$x \underset{0}{\geq} 0$ car K^2 est formé d'éléments positifs pour $\underset{0}{\geq}$ et $\alpha \underset{0}{\geq} 0$.

$y \underset{0}{\geq} 0$ de même donc $x + y \underset{0}{\geq} 0$.

Mais $x + y \in K = K^2 \cup -K^2 \cup \alpha K^2 \cup -\alpha K^2$.

Les éléments de $-K^2$ et de $-\alpha K^2$ étant négatif pour $\underset{0}{\geq}$ on a $x+y \in K^2 \cup \alpha K^2 = P_0$.

Les propriétés (1) à (4) montrent que P_0 est un ordre sur K.

On démontrerait de même que P_1 est un ordre sur K.

Si $P_0 = K^2 \cup \alpha K^2$ et $P_1 = K^2 \cup -\alpha K^2$, il est clair que $\underline{P_0 \cap P_1 = K^2}$

Si on considère tous les ordres possibles de K on sait que

$\Sigma K^2 = \cap_{P \text{ ordre de } K} P \subset P_0 \cap P_1 = K^2$ donc $\Sigma K^2 = K^2$ et le corps $\underline{K \text{ est un corps pythagoricien}}$.

Enfin P_0 et P_1 sont évidemment les seuls ordres de K : en effet si P est un autre ordre de K on a $\alpha \in P$ ou $\alpha \in -P$.

Si $\alpha \in P$ alors $P \supset K^2 \cup \alpha K^2 = P_0$ et donc $P = P_0$.

Si $-\alpha \in P$ alors $P \supset K^2 \cup -\alpha K^2 = P_1$ et $P = P_1$.

Le corps $\underline{K \text{ n'admet donc que deux vrais ordres}}$ P_0 et P_1 (correspondant en fait aux symboles $\underset{0}{\geq}$ et $\underset{1}{\geq}$ finalement).

Dans un tel corps il n'existe pour tout $n \geq 2$ qu'un seul ordre de niveau 2^n, et celui-ci est donné par

$$P_n = \Sigma K^{2^n} \cup -\alpha^{2^{n-1}} \Sigma K^{2^n}$$

(voir [G1], th. 5-3) ; Le corps K est donc un-chaîné. Les modèles de T_2' sont donc bien les corps un-chaîné, pythagoricien n'admettant que deux ordres vrais.

Réciproquement, soit K un corps un-chaîné, pythagoricien n'admettant que deux ordres. C'est d'abord un corps chaînable qui vérifie donc les axiomes T_1' avec $\underset{0}{\geq}$ et $\underset{1}{>}$ pour ses deux seuls ordres.

Il est pythagoricien donc $\Sigma K^2 = K^2$ et les éléments totalement positifs de K sont ceux de K^2. Si $\alpha^2 \notin \Sigma K^4$ alors $\alpha \notin K^2$ et $\alpha \notin -K^2$ donc α n'est ni totalement positif ni totalement négatif et on a bien $\alpha \underset{0}{\geq} 0$ et $\alpha \underset{1}{<} 0$.

Il suffit alors de montrer qu'un β convenant au dernier axiome est bien tel que $\beta^2 \notin \Sigma K^4$. Dans un corps chaînable n'ayant que deux ordres P_0 et P_1, il existe β tel que $P_0 = \Sigma K^2 \cup \beta \Sigma K^2$ et $P_1 = \Sigma K^2 \cup -\beta \Sigma K^2$ ([G1], Ex. 5-3). K étant pythagoricien c'est en fait $P_0 = K^2 \cup \beta K^2$ et $P_1 = K^2 \cup -\beta K^2$, et β est donc bien convenable pour le dernier axiome. Montrons que $\beta^2 \notin \Sigma K^4$:

Si $\beta^2 \in \Sigma K^4$ alors puisque P_2 l'unique ordre de niveau 2^2 de K est donné par

$P_2 = \Sigma K^4 \cup -\beta^2 \Sigma K^4$, alors on a $P_2 = \Sigma K^4 \cup -\Sigma K^4$, donc aussi $P_2 \cup -P_2 = \Sigma K^4 \cup -\Sigma K^4$.

Or d'après la définition d'une chaîne d'ordres de niveau supérieur $P_2 \cup -P_2 = (P_1 \cap P_0) \cup -(P_1 \cap P_0) = \Sigma K^2 \cup -\Sigma K^2 = K^2 \cup -K^2$.

En comparant les éléments totalement positifs et totalement négatifs de $P_2 \cup -P_2$ on aurait $\Sigma K^4 = K^2$ ce qui est impossible dans un corps chaînable. Donc $\beta^2 \notin \Sigma K^4$. K est bien un modèle de T_2'.

III. CORPS CHAÎNE-CLOS

Un corps chaîne-clos étant en particulier un-chaîné, pythagoricien et ayant seulement deux vrais ordres une axiomatisation de sa théorie pourra contenir une axiomatisation de la théorie étudiée au II .

THEOREME III-1 : Un corps K *est chaîne-clos si et seulement si on peut y trouver un élément* $\bar{\alpha}$ *tel que* $(K,\bar{\alpha})$ *satisfasse le système d'axiomes* T'_3 *du langage* $\mathcal{L}'$.

T'_3 :

- *corp commutatif un-chaîné pythagoricien 2 ordres seul*^{t} T'_2
- *corps chaînable* T'_1 :
  - *Axiomes de corps commutatif ordonné pour* $\geq_0$ *et pour* $\geq_1$ *(cf. th. II-1).*
  - *pour tout* $n \geq 1$ *l'axiome* $\Lambda x_1 \ldots \Lambda x_n \neg(\alpha^2 = x_1^4 + \ldots + x_n^4)$
  - $(\alpha \geq_0 0) \wedge (\alpha \leq_1 0)$
  - $\Lambda x \, \forall y (x = y^2 \vee x = -y^2 \vee x = \alpha y^2 \vee x = -\alpha y^2)$
- *pour tout* $n \geq 0$ *l'axiome* $\Lambda x_0 \ldots \Lambda x_{2n+1} \, \forall y \, (x_0 + x_2 y + \ldots + x_{2n+1} y^{2n+1} = 0 \vee x_{2n+1} = 0)$

Les modèles K de T'_3 sont des corps chaîne-clos. Il est clair qu'étant modèles du T'_2 ils sont un-chainé, pythagoricien et n'ont que deux ordres vrais. On sait qu'alors $P_0 \cap P_1 = K^2$ (où P_0 et P_1 représentent l'ensemble des éléments positifs pour chacun des deux ordres). Le dernier schéma d'axiome assure alors que tout polynôme de degré impair a une racine. Par la caractérisation des corps chaîne-clos comme corps chaîné tel que $P_0 \cap P_1 = K^2$ et K n'a pas d'extension algébrique de degré impair non triviale ([G2], th. V-3) il est clair qu'un modèle de T'_3 est chaîne-clos.

Inversement, tout corps chaîne-clos étant un-chaîné pythagoricien avec deux ordres seulement est modèle de T'_2 et puisqu'il n'admet pas d'extension algébrique de degré impair il est modèle de T'_3 .

Lors d'un entretien avec Max Dickmann, qui souhaitait lui une axiomatisation des corps chaîne-clos dans le langage des corps, nous avons pu obtenir

à partir du théorème III-1 l'axiomatisation suivante où $\mathcal{L}''(0,1,+,.,-,=)$ est le langage $\mathcal{L}$ privé du symbole de constante α .

THEOREME III-2. Dans le langage $\mathcal{L}''$ le système d'axiomes qui suit est une axiomatisation T_3'' de la théorie des corps chaîne clos.

$$T_3'' \begin{cases} T_2'' \begin{cases} \left\{ \text{Axiomes de corps commutatif ordonnable} \right. \\ \Lambda x\, \Lambda y\, \forall z (x^2+y^2 = z^2) \\ \Lambda x\, \Lambda y\, \forall z (x^4+y^4 = z^4) \\ \forall \alpha\, \Lambda x (\neg(\alpha^2 = x^4) \wedge \forall y (x = y^2 \vee x = -y^2 \vee x = -\alpha y^2 \vee x = \alpha y^2)) \end{cases} \\ \text{Pour tout } n \geq 0 \text{ l'axiome} \\ \Lambda x_0\, \Lambda x_2 \ldots \Lambda x_{2n+1}\, \forall y (x_0 + x_2 y + \ldots + x_{2n+1} y^{2n+1} = 0 \vee x_{2n+1} = 0) \ . \end{cases}$$

LEMME III.3. T_2'' est une axiomatisation de la théorie des corps urchaîné, pythagoricien, n'ayant que deux ordres.

Démonstration du lemme III.3 : Soit K un modèle de T_2'' . Si on pose $P_0 = K^2 \cup \alpha K^2$ et $P_1 = K^2 \cup -\alpha K^2$ où α vérifie le dernier axiome de T_2'' alors on peut vérifier que P_0 et P_1 sont des ordres sur K .

(1) $P_0 \cup -P_0 = K$ découle immédiatement du dernier axiome de T_2''

(2) $P_0 . P_0 \subset P_0$ est clair

(3) $P_0 \cap -P_0 = \{0\}$. Soit $x \in P_0 \cap -P_0$, alors

$x \in K^2 \cup \alpha K^2$ et $x \in -(K^2 \cup \alpha K^2)$.

. $x \in K^2$ et $x \in -K^2$ entraîne $x = 0$.

. $x \in \alpha K^2$ et $x \in -\alpha K^2$ entraîne aussi $x = 0$ immédiatement.

. Si $x \in K^2$ et $x \in -\alpha K^2$, alors il existe y et z , non nuls si $x \neq 0$, tels que $y^2 = -\alpha z^2$, donc $-\alpha = (\frac{y}{z})^2$ ce qui est impossible, car $\alpha^2 \notin K^4$; donc $x = 0$.

. De même si $x \in -K^2$ et $x \in \alpha K^2$ on obtient si $x \neq 0$ l'existence de y et z non nuls tels que $-y^2 = \alpha z^2$ et $\alpha = -(\frac{y}{z})^2$ ce qui est impossible ; Donc $x = 0$.

(4) $P_o + P_o \subset P_o$: soient x et y appartenant à $P_o = K^2 \cup \alpha K^2$.

. Si x et y sont dans K^2 , $x + y$ est aussi car K est pythagoricien, donc $x + y \in P_o$.

. Si x et y sont dans αK^2 , de même $x + y \in \alpha K^2$.

. Si $x \in K^2$ et $y \in \alpha K^2$, $x + y \in K^2 \vee -K^2 \cup \alpha K^2 \cup -\alpha K^2$.

a) Si $x + y \in -K^2$, en supposant $y \neq 0$ (sinon $x = 0$ aussi) il existe x', y' et z avec $y' \neq 0$ tels que

$x'^2 + \alpha y'^2 = -z^2$ d'où $-\alpha y'^2 = x'^2 + z^2$

et $-\alpha y'^2 = T^2$ car K est pythagoricien. On en déduit $-\alpha = (\frac{I}{y'})^2$ ce qui est impossible.

b) Si $x + y \in -\alpha K^2$ alors de même on peut supposer $y \neq 0$ (sinon $x = 0$) et il existerait x', $y' \neq 0$ et z tels que

$x'^2 + \alpha y'^2 = -\alpha z^2$. On en déduit

$\alpha(y'^2+z^2) = - x'^2$ et puisque K est pythagoricien

$\alpha T^2 = - x'^2$ et $\alpha = - (\frac{x'}{T^2})$ ce qui est impossible (T est non nul car $T^2 = y'^2+z^2$ et $y' \neq 0$) .

Donc finalement $x + y \in K^2 \cup \alpha K^2 = P_o$ et (4) est bien vérifié.

Les relations (1) à (4) montrent que P_o est un ordre de K ; On montrerait de même que $P_1 = K^2 \cup -\alpha K^2$ est un ordre sur K .

Le dernier axiome de T_2'' assure que $\alpha^2 \notin K^4$ et puisque $K^4 + K^4 = K^4$, on a $\alpha^2 \notin \Sigma K^4$. Un modèle K de T_2'' étant donc ordonnable et tel qu'il existe $\alpha \in K$ avec $\alpha^2 \notin \Sigma K^4$ est donc un corps chaînable (th. I-1).

K est pythagoricien d'après l'un des axiomes. Par un raisonnement déjà effectué au II, K n'a que les deux ordres P_o et P_1 , $P_o \cap P_1 = K^2$ et toujours de même il existe un unique ordre P_n de niveau 2^n donné par $P_n = \Sigma K^{2^n} \cup - \alpha^{2^{n-1}} \Sigma K^{2^n}$. K est donc bien un-chaîné.

Inversement un corps K pythagoricien un-chaîné et n'ayant que deux ordres et automatiquement pythagoricien à tout niveau donc $K^4 + K^4 = K^4$ et il

possède un élément $\alpha \notin \Sigma K^4$ et qui est tel que $K = K^2 \cup -K^2 \cup \alpha K^2 \cup -\alpha K^2$ (cf. démonstration à la fin du II). C'est donc bien un modèle de T_2'' .

Le théorème III-4 découle alors immédiatement du lemme et du théorème III-1.

Remarque III-4.

Dans T_2'' on peut supprimer l'axiome assurant que $K^2 + K^2 = K^2$, car dans un corps ordonnable $K^4 + K^4 = K^4$ entraîne $K^2 + K^2 = K^2$, (voir [Ha]) .

En conclusion l'axiomatisation la plus adaptée pour l'étude des corps chaînables et chaîne-clos apparaît à l'auteur être celle écrite dans le langage $\mathfrak{L}(0,1,+,.,-,=,\alpha)$ et énoncée dans le théorème ci-dessous :

THEOREME III-5 : Un corps K *est chaîne-clos si et seulement si on peut y trouver un élément* $\bar{\alpha}$ *tel que* $(K,\bar{\alpha})$ *satisfasse le système d'axiomes* T_3 *du langage* $\mathfrak{L}$.

corps chaîne-clos T_3 :

- *corps un-chaîné pythagoricien 2 ordres seulement* T_2 :
  - *corps chaînable* T_1 :
    - *Axiomes de corps commutatif ordonnable.*
    - *pour tout* $n \geq 1$ *l'axiome* $\Lambda x_1 \ldots \Lambda x_n \neg(\alpha^2 = x_1^4 + \ldots + x_n^4)$
  - $\Lambda x \Lambda y \forall z \quad x^2 + y^2 = z^2$
  - $\Lambda x \forall y \; (x = y^2 \vee x = -y^2 \vee x = \alpha y^2 \vee x = -\alpha y^2)$
- *pour tout* $n \geq 0$ *l'axiome* $\Lambda x_0 \ldots \Lambda x_{2n+1} \forall y (x_0 + x_2 y + \ldots + y_{2n+1} y^{2n+1} = 0 \vee x_{2n+1} = 0)$.

LEMME III-6 : Un corps K *est un-chaîné, pythagoricien et a seulement deux ordres vrais si et seulement si on peut y trouver un élément* $\bar{\alpha}$ *tel que* $(K,\bar{\alpha})$ *satisfasse le système d'axiomes* T_2 *du langage* $\mathfrak{L}$.

Le théorème III-5 découle alors immédiatement du lemme III-6.

Démonstration de lemme III-6.

Un modèle de T_2 est un corps chaînable puisque modèle de T_1. Il est pythagoricien puisque c'est dans les axiomes. Il suffit de vérifier que un modèle K de T_2 n'a que deux ordres.

Posons $P_0 = K^2 \cup \alpha K^2$ et $P_1 = K^2 \cup -\alpha K^2$. Les propriétés (1) $P_0 \cup -P_0 = K$ et (2) $P_0.P_0 \subset P_0$ sont évidentes.

Puisque $\alpha^2 \notin \Sigma K^4$ alors $\alpha \notin \Sigma K^2$ et les démonstrations faites dans le lemme III-3 sont valables et montrent que (3) $P_0 \cap -P_0 = \{0\}$ et (4) $P_0 + P_0 \subset P_0$.

Donc P_0 est un ordre sur K. De même pour P_1. Puisque $P_0 \cap P_1 = K^2$, K n'a que les deux ordres P_0 et P_1 et donc un unique ordre P_n donné par $P_n = \Sigma K^{2^n} \cup -\alpha^{2^{n-1}} \Sigma K^{2^n}$. K est donc bien un corps un-chaîné.

Réciproquement tout corps K un-chaîné pythagoricien n'ayant que deux ordres est modèle de T_2 : s'il est un-chainé il est chaînable donc modèle de T_1. Il est pythagoricien donc vérifie l'axiome suivant, enfin puisqu'il n'a que deux ordres ces deux ordres sont donnés par $P_0 = K^2 \cup \beta K^2$ et $P_1 = K^2 \cup -\beta K^2$ et le raisonnement fait à la fin de II assure que ce β est bien tel que $\beta^2 \notin \Sigma K^4$.

BIBLIOGRAPHIE

[Be] E. BECKER. - *"Hereditarily pythagorean fields and orderings of higher types"*.
I.M.P.A. Lectures notes, n° 29, Rio de Janeiro, 1978.

[Ha] J. HARMAN. - *"Chains of higher level orderings"*.
contemporary Mathematics, vol 8, 1982. pp. 141-174.

[G1] D. GONDARD. - *"Théorie des ordres de niveau supérieur pour les corps commutatifs"*.
Séminaire D.D.G., 1984-85, Université de Paris 7.

[G2] D. GONDARD. - *"Ordres de niveau supérieur, extensions et corps chaîne-clos"*.
Séminaire D.D.G., 1986-87, Université de Paris 7.
(à paraître).

[G3] D. GONDARD. - *"Theorie des corps chaînables et des corps chaîne-clos"*.
A paraître : C.R.A.S., Paris, 1987.

Algorithmes rapides en séquentiel et en parallele pour l'élimination de quantificateurs en géométrie élémentaire

Noaï Fitchas[1] , André Galligo[2,3] , Jacques Morgenstern[2,3]

1: Groupe de travail: Leandro Caniglia, Silvia Danón, Joos Heintz, Teresa Krick, Pablo Solernó. Instituto Argentino de Matemática Viamonte 1636 2°A, -1055- Buenos Aires, Argentina.

2: Institut de Mathématique et de Sciences Physiques, Université de Nice, Nice.

3: INRIA, Sophia Antipolis, Valbonne, France.

I. INTRODUCTION:

Dans cet article, nous traitons le problème de l'élimination de quantificateurs dans la théorie élémentaire des corps réel et algébriquement clos (de charactéristique arbitraire) du point de vue des complexités séquentielle et parallèle.

L'intérêt du cas des corps algébriquement clos est plus théorique que pratique (par exemple la détermination de la dimension d'une variété algébrique) et nous le traitons ici de manière succinte.

Nous travaillons plus en détail le cas des corps réel clos pour deux raisons: la première est qu'en général la littérature sur le sujet est de lecture difficile et nous proposons ici des démonstrations accessibles à un public moins familiarisé avec les notions de complexité. D'autre part, dans le domaine de la Robotique, une tendance moderne essaye de réduire les problèmes de mouvement à des problèmes de géométrie semi-algébrique où apparaissent des formules très intriquées dans le langage de premier ordre du corps réel $\mathbb{R}$. Une manière d'attaquer ce problème du point de vue calculatoire est d'essayer d'éliminer effectivement et efficacement les quantificateurs de la formule donnée. Ceci ne veut pas dire que nous proposons cette attaque du problème: nous essayons simplement d'examiner les possibilités qu'offrent les bornes obtenues. Il existe de sérieux doutes quant à l'efficacité de cette méthode, vu les bornes inférieures doublement exponentielles en séquentiel. La seule solution que nous voyons pour résoudre ce problème inhérent à l'élimination des quantificateurs est de considérer un modèle de complexité qui permet de travailler en parallèle, sans augmenter plus que nécessaire le nombre de processeurs. Il faut aussi tenir compte du fait que dans la réalité un processeur physique peut s'utiliser

plus d'une fois alors que notre modèle prévoit un usage unique de chaque processeur. Ceci se manifeste par les résultats de complexité séquentielle (nombre de noeuds du réseau arithmétique en jeu.) C'est pour celà que nous serions aussi intéressés par la possibilité de créer un modèle qui permettrait d'économiser le nombre de processeurs physiques. Comme nos bornes en parallèle sont optimales,nous laissons le lecteur juger si le rapprochement de l'élimination de quantificateurs avec le problème de la Robotique est viable ou non.

Le fait que la théorie élémentaire des corps réel clos admet l'élimination de quantificateurs a été démontré par Tarski dans les années 30 (voir [42]). Dans cet article, Tarski donne un algorithme effectif, mais impraticable dans la réalité car il fonctionne en temps $2^{2^{2^{\ell}}}$, où ℓ est la longueur de la formule d'entrée, écrite sur un ruban de machine de Turing.

La recherche d'algorithmes rapides provient de l'idée d'appliquer l'élimination de quantificateurs à des problemes concrets de géométrie élémentaire. En 1975, dans [14] on trouve un algorithme qui fonctionne en temps $2^{2^{2\ell \log\log\ell}}$,où log désigne le logarithme en base 2. Le même genre de bornes est obtenu dans [44] , inspiré sur [37],[41] (algorithmes rapides en séquentiel pour la décision de la théorie élémentaire des corps réel clos.) Dans le cas des corps algébriquement clos, des résultats analogues sont donnés dans [30],[29],[11]. Les bornes les plus intéressantes pour les corps réel clos sont obtenues dans [28][27] où les résultats généraux ne sont pas essentiellement modifiés mais sont plus précis quant aux paramètres qui mesurent la taille de la formule d'entrée, ce qui permet dans certains cas des applications pratiques. (Toutes ces bornes correspondent au temps séquentiel.)

Les méthodes utilisées jusqu'a présent pour l'élimination des quantificateurs dans la théorie des corps réel clos sont toutes fondées sur des sous-algorithmes qui peuvent être considérés comme des calculs de fonctions de Skolem semi-algébriques, ce qui en soi n'est pas efficacement parallélisable: c'était là l'obstacle principal pour trouver des algorithmes rapides en parallèle. Pour le problème de la décision, il existe par contre un résultat précurseur [6], un algorithme qui fonctionne en temps parallèle simplement exponentiel avec un nombre doublement exponentiel de processeurs (c'est-à-dire de type doublement exponentiel en séquentiel)

Pour préciser un peu les concepts, disons que nous considérons le langage de premier ordre de R, avec les symboles non-logiques suivants : $\{a,\ a \in Q\}$,+,-,.,=, > et les variables $X_1, \ldots, X_n, \ldots$. Les termes de notre langage sont écrits sous forme de polynômes à coefficients dans Q (représentation dense). Dans le cas d' un corps algébriquement clos k, les symboles seront $\{a,\ a \in \Omega\}$,+,-, . ,= où Ω est

le corps premier de k.

Pour le modèle séquentiel, il est naturel de représenter les mots du langage L sur un alphabet fini,convenablement choisi,et de codifier la formule sur un ruban de machine de Turing. La formule Φ d'entrée a alors une longueur $|\Phi|$ qui correspond au nombre de cases du ruban qu'elle occupe, et les notions de temps et d'espace de l'algorithme qui découlent de ce modèle sont le nombre de pas qu'effectue la machine de Turing pour réaliser l'algorithme et la quantité de cases occupée pendant ce processus.

La présentation que nous choisissons dans ce travail est plus simple. Nous utilisons le modele algébrique où additionner et multiplier deux éléments du corps de base coûte toujours un, indépendemment de la longueur binaire de ces éléments. Il n'y a pas de perte de généralité dans le cas séquentiel car les bornes qui s'obtiennent sont exactement du même type que si l'on travaille avec le modèle de la machine de Turing. Il nous semble que le modèle algébrique proposé ici est plus en accord avec le genre de problème que nous traitons: la raison est que la notion de machine de Turing n'est guère parallélisable.

Nous cherchons donc un modèle qui est à la fois déterministe et où la notion de parallélisme a un sens. Le modèle adéquat, quant au travail qui s'effectue sur les polynômes (termes de notre langage) est celui de réseau arithmétique, que nous définirons ensuite. En résumé, l'algorithme est décrit par un graphe où le nombre de noeuds représente la complexité séquentielle et la profondeur du graphe (chemin le plus long) la complexité parallèle.

Une partie du modèle qui n'est pas explicitée est celle de la manipulation des lettres de la formule. Mais le chemin à suivre est clair et n'est d'ailleurs pas essentiel pour les bornes supérieures et inférieures, comme le lecteur verra.

Avec ce modèle, nous obtenons des bornes supérieures pour la complexité parallèle de l'élimination de quantificateurs dans la théorie des corps réel et algébriquement clos, sans augmenter essentiellement la complexité séquentielle. Le lecteur intéressé pourra aisément traduire les résultats pour la complexité séquentielle au modèle de machine de Turing, afin d'aboutir au même genre de bornes qu'en [44]

De plus, nous démontrons que les bornes sont optimales, tant en séquentiel qu'en parallèle dans les deux cas (pour les résultats antérieurs, voir [29][43][19])

Le problème des bornes inférieures pour la complexité parallèle des corps réel clos avait été esquissé dans [5] où les auteurs pensaient appliquer, apparemment sans résultat (Voir [10]), les techniques de [35] en combinaison avec le théoreme des zéros de Hilbert; c'est un tout autre chemin que nous suivons ici.

II. LES RESULTATS :

Soit k un corps réel clos ou algébriquement clos. Comme nous considérons la théorie élémentaire de k, dans le cas réel clos, nous écrirons simplement k= $\mathbb{R}$.

Pour parler de k, nous considérons le langage de premier ordre L, avec les symboles non logiques: $\{a,\ a \in \Omega\}$,+,-,.,=, où Ω est le corps premier de k. Dans le cas réel clos, nous avons en plus un symbole relationnel >.

Nous considérons les variables de L comme indéterminées $X_1,\ldots,X_n,\ldots$ sur k. Les termes de L sont représentés par des polynômes à plusieurs variables, à coefficients dans Ω (représentation dense). Par conséquent, un terme typique a l'aspect $F \in \Omega[X_1,\ldots,X_n]$ et une formule typique est du genre F=0, et si k= $\mathbb{R}$, aussi F>0. Pour la négation de ces formules nous écrivons $F \neq 0$ (et $F \leqslant 0$, pour k= $\mathbb{R}$).

Notre langage L est construit à partir des formules atomiques en utilisant les connectifs logiques $\vee, \wedge, \neg$ et aussi par convenance $\rightarrow$, et les quantificateurs $\exists$, $\forall$ qui s'appliquent aux éléments de k (pas à des sous-ensembles, ni à des relations). Chaque formule Φ de L contient alors des polynômes, disons $F_1,\ldots,F_s$ de $\Omega[X_1,\ldots,X_n]$, et $X_1,\ldots,X_n$ sont les variables de Φ .

Nous considérons le langage L comme un ensemble de mots sur l'alphabet (infini) des symboles de L (variables, symboles non logiques et connectifs logiques, quantificateurs et parenthèses.) A toute formule Φ de L correspond alors une longueur naturelle $|\Phi|$ (nombre de symboles utilisés pour écrire Φ)

Les autres paramètres que nous utilisons sont:

$$\sigma(\Phi) := 2 + \sum_{1 \leqslant i \leqslant s} \deg(F_i)$$

n:= le nombre total de variables qui apparaissent dans la formule Φ . Et si Φ est une formule prénexe, c'est-à-dire tous les quantificateurs se trouvent au début de Φ), nous tenons compte aussi de:

r:= le nombre d'alternations de blocs de quantificateurs $\exists, \forall$.

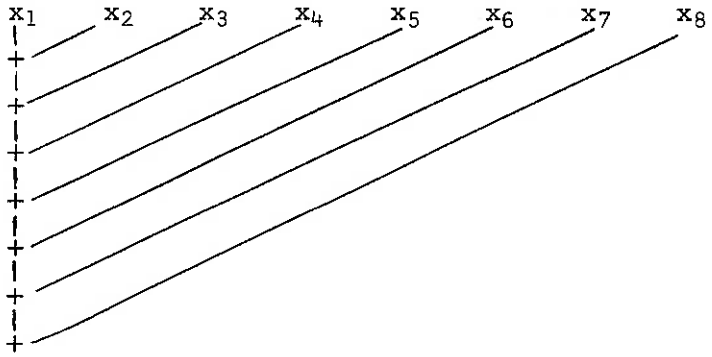
(Une formule Φ peut etre ramenée en temps séquentiel linéaire $O(\Phi)$ à une formule équivalente Ψ prénexe; ce processus ne modifie guère $|\Phi|$, $\sigma(\Phi)$ et n.

Nous allons maintenant donner les notions de complexité nécessaires à la compréhension des résultats.

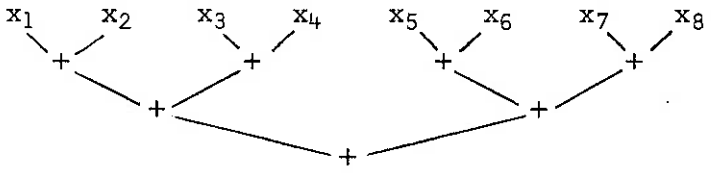
Le noyau de notre algorithme correspond à faire des opérations arithmétiques avec des polynômes $F \in \Omega[X_1,\ldots,X_n]$ (représentés par le vecteur des coefficients, écrits de manière dense), et dans certains cas, nous nous posons la question F=0? (selon si la réponse est Vrai ou Faux nous suivons un chemin ou l'autre.)

Le modèle le plus convenable pour ce genre d'algorithmes arithmétiques est celui de "réseau arithmétique" [25], qui utilise comme entrées les constantes du corps k et qui permet les opérations +,-,. . Pour la question F=0 (et F>0, dans le cas de $\mathbb{R}$), nous admettons aussi les comparaisons. Cette notion de réseau arithmétique peut être décrite par un graphe, où chaque noeud représente une opération (entre deux éléments) à réaliser.

Par exemple, additionner $x_1,\ldots,x_8$, $x_i \in \mathbb{R}$ peut être représenté par l'algorithme (I) suivant:



On peut aussi exécuter ce calcul par l'algorithme (II):



la manière de calculer une fonction n'étant pas unique en général.

Nous pouvons définir, pour un algorithme donné décrit par un graphe, deux notions de complexité:

1) La complexité séquentielle de l'algorithme: C'est le nombre de noeuds du graphe (dans les exemples (I) et (II), 7). Si l'on suppose que chaque opération de l'algorithme se réalise en une unité de temps fixe, la complexité séquentielle

représente le temps nécessaire à un processeur pour effectuer l'algorithme.

2) La complexité parallèle de l'algorithme, ou profondeur du graphe: C'est le nombre d'"étages" du graphe, c'est-à-dire le chemin le plus long à suivre pour arriver aux résultats (Dans l'exemple (I) la profondeur est 7, alors que dans l'exemple (II) qui décrit le même calcul, la profondeur est 3.) Cette notion de complexité parallèle correspond au temps minimum nécessaire pour réaliser l'algorithme, si nous disposons d'une quantité arbitraire de processeurs qui fonctionnent en parallèle, c'est-à-dire si tous les processeurs peuvent effectuer des opérations en même temps, et les processeurs sont intégrés de manière telle que le résultat obtenu par un processeur peut être transmis à un autre processeur qui réalise alors l'opération suivante. Comme la profondeur du graphe décrit le nombre d'opérations qui doivent attendre les résultats d'opérations précédentes, cette notion correspond clairement au temps indispensable pour effectuer l'algorithme, même si l'on dispose d'un nombre illimité de processeurs.

Si nous observons l'exemple (I), la quantité nécessaire de processeurs pour effectuer l'algorithme en temps 7 est 1, alors que dans l'exemple (II) qui fonctionne plus rapidement en parallèle, il en faut 4 (qui correspondent aux quatre premières opérations à faire.) Malheureusement, comme en général les graphes ne sont pas aussi réguliers que ceux de ces exemples, la seule borne dont nous disposons pour le nombre de processeurs est la quantité de noeuds du graphe, c'est-à-dire la complexité séquentielle de l'algorithme. Ceci veut dire que nous "jetons" un processeur après l'avoir utilisé une seule fois. Bien évidemment, dans la réalité, un processeur peut être réutilisé après avoir effectué une opération; il serait donc intéressant d'obtenir des bornes sur le nombre de processeurs nécessaires, en fonction du nombre de noeuds et de la profondeur du graphe. Comme nous n'avons pas ce genre de bornes, nous présupposons ici un usage unique de chaque processeur, et le nombre de processeurs sera représenté par la complexité séquentielle de l'algorithme.

Généralement, les algorithmes qui donnent la meilleure complexité séquentielle ne sont pas ceux qui fonctionnent le plus rapidement en parallèle, et un "bon" algorithme en parallèle fait augmenter le nombre de processeurs nécessaires (complexité séquentielle.) On cherche à obtenir des algorithmes rapides en parallèle qui ne font pas "exploser" le nombre de processeurs, c'est-à-dire qui n'empirent pas essentiellement la complexité séquentielle. Ceci signifie que les résultats qui s'obtiennent pour la complexité séquentielle de ces algorithmes doivent être dans le même ordre que ceux qui se connaissent déja par d'autres algorithmes représentant le même calcul, rapides en séquentiel. Par

exemple, si nous savons que les meilleurs algorithmes séquentiels pour calculer une fonction donnée en n variables s'exécutent en temps $2^{O(n.\log n)}$, un autre algorithme décrivant le même résultat qui fonctionne en temps parallèle $O(n.\log n)$ avec $2^{O(n^3)}$ processeurs est "bon" alors que s'il utilise $2^{2^{O(n)}}$ processeurs, l'ordre de complexité séquentielle est modifié et cet algorithme n'est pas utile.

Dans le paragraphe précédent, nous avons sans le préciser esquissé la notion de complexité de calcul de fonctions. On désire calculer une fonction F. La complexité séquentielle de F est la plus petite des complexités séquentielles des algorithmes qui donnent comme résultat F. De la même manière, la complexité parallèle de F est la plus petite des complexités parallèles des algorithmes qui calculent F. Par exemple on peut démontrer que dans le cas de $F= x_1+\ldots+ x_8$, $x_i \in \mathbb{R}$, la complexité séquentielle L(F) est 7 alors que la complexité parallèle, D(F) ,est 3.

La partie du modèle que nous ne décrirons pratiquement pas est celle qui correspond à la manipulation de la formule d'entrée pour obtenir la famille de polynômes sur laquelle nous travaillons, ou pour décrire la formule de sortie (sans quantificateurs) à partir de polynômes. Nous admettons le même genre d'opérations avec les lettres (symboles) qu'avec les éléments de k: par exemple, joindre des mots, interchanger ou insérer des lettres. Ces opérations permettent par exemple en temps linéaire $O(|\Phi|)$ de construire a partir d'une formule Φ une formule équivalente Ψ prénexe, ou de savoir à quels polynômes il faut appliquer la décomposition cylindrique. Nous laissons le lecteur créer le modèle le plus convenable pour représenter ce travail.

Nous abordons dans cet article deux problèmes différents: le problème des bornes supérieures et le problème des bornes inférieures pour la complexité parallèle de l'élimination de quantificateurs dans la théorie élémentaire des corps réel et algébriquement clos.

1) Les bornes supérieures: Dans ce cas, selon ce qui a été dit auparavant, il suffit d'exhiber un algorithme qui fonctionne rapidement en parallèle sans faire exploser le nombre de processeurs.

Dans le cas de $\mathbb{R}$, pour la complexité séquentielle, les meilleures bornes sont obtenues dans [14], [44], [37], [41] et [27] et sont doublement exponentielles : $\sigma(\Phi)^{2^{O(n)}} + O(|\Phi|)$, les plus précises étant celles de [27] (Voir aussi [28]) où le facteur doublement exponentiel dépend uniquement du nombre d'alternations de blocs de quantificateurs r : $\sigma(\Phi)^{n^{O(r^2)}} + O(|\Phi|)$. Dans ce cas, comme le modèle adéquat (pour la complexité séquentielle) est celui de la Machine de Turing, le terme $\sigma(\Phi)$ controle aussi la longueur

binaire des coefficients des polynômes de la formule Φ, et n est le nombre de variables de Φ. Le terme $O(|\Phi|)$ provient du fait que la formule d'entrée Φ doit subir un processus de préparation, qui la ramène à une formule prénexe, qui contrôle raisonnablement les connectifs et qui donne explicitement les polynômes; en général, les auteurs présupposent ce travail préparatoire déja fait et donnent directement leurs résultats en fonction de $\sigma(\Phi)$, n et r. Bien évidemment, les mêmes bornes supérieures s'appliquent aussi pour le problème de la décision de la théorie élémentaire des corps réel clos.

En ce qui concerne la complexité parallèle, on trouve dans [6] un algorithme, pour le problème de la décision, qui fonctionne en temps parallèle $n^{O(n)}.\log(\sigma(\Phi))^{O(1)} + O(|\Phi|)$ en utilisant $\sigma(\Phi)^{n^{O(n)}} + O(|\Phi|)$ processeurs (complexité séquentielle).

Dans le cas des corps algébriquement clos de charactéristique arbitraire, des bornes supérieures pour l'élimination de quantificateurs et la décision équivalentes à celles de $\mathbb{R}$ sont données dans [30][29][11], ce dernier article, fondé sur [13] donnant des résultats plus différenciés quant aux paramètres (le facteur doublement exponentiel dépend uniquement de r) mais avec la restriction suivante: le corps des constantes n'est pas tout le corps k mais un certain corps arithmétique de base.

Nos résultats pour les bornes supérieures de la complexité parallèle sont les suivants:

Soit k un corps réel ou algébriquement clos (de charactéristique arbitraire):

Théoreme 1 : Pour tout $\ell \in \mathbb{N}$, il existe un réseau N_ℓ sur les symboles de L, langage de premier ordre de k, de profondeur (complexité parallèle) $\ell^{O(\ell)}$ et de complexité séquentielle $\ell^{\ell^{O(\ell)}}$ avec la propriété suivante:
Pour toute formule d'entrée $\Phi \in L$, avec $|\Phi| = \ell$, N_ℓ calcule une formule sans quantificateurs équivalente à Φ (modulo la théorie élémentaire de k)

Autrement dit , il existe un algorithme (la famille de réseaux $N_\ell, \ell \in \mathbb{N}$) qui élimine les quantificateurs en temps parallèle (profondeur de N_ℓ) $|\Phi|^{O(|\Phi|)}$ et temps séquentiel $|\Phi|^{|\Phi|^{O(|\Phi|)}}$, où $\Phi \in L$ est une formule d'entrée arbitraire de longueur ℓ.

Corollaire : Il existe un algorithme qui décide la théorie élémentaire de k en temps parallèle simplement exponentiel et temps séquentiel doublement exponentiel, la formule d'entrée étant mesurée par sa longueur.
(Ceci est le résultat principal de [6], pour les corps réel clos et les corps

algébriquement clos de caractéristique 0.)

Pour le théorème 1 nous avons utilisé comme seul parametre la longueur de la formule d'entrée Φ . Pour les théorèmes suivants nous allons supposer que Φ est une formule prénexe et convenablement "préparée" (les polynômes de Φ sont donnés explicitement). Comme le modèle adéquat est ici le modèle algébrique, les paramètres que nous utilisons sont $\sigma(\Phi)$ qui controle la quantité et le degré des polynômes de Φ , n -le nombre de variables de Φ -,et r -la quantité d'alternations de blocs de quantificateurs.

Théorème 2 : i) Il existe un algorithme qui élimine les quantificateurs, modulo la théorie élémentaire de k, en:

temps parallèle: $2^{n^{O(1)}} \log \sigma(\Phi) + O(\log|\Phi|)$

temps séquentiel: $\sigma(\Phi)^{n^{O(n)}} + O(|\Phi|)$

ii) Les mêmes bornes s'appliquent pour le problème de la décision.

Le théorème 2 implique que l'élimination de quantificateurs et le problème de la décision de la théorie élémentaire des corps réel et algébriquement clos appartiennent à la classe NC (complexité séquentielle polynômiale et complexité parallèle polylogarithmique) si le nombre de variables n de la formule d'entrée Φ est fixé.

Dans le cas des corps algébriquement clos de caractéristique 0, on obtient aussi le résultat plus différencié suivant:

Théorème 3 : Soit k un corps algébriquement clos de caractéristique 0,

i) Il existe un algorithme qui élimine les quantificateurs (modulo la théorie élémentaire de k)

en temps parallèle: $n^{O(r)} \log \sigma(\Phi)^{O(1)} + O(\log|\Phi|)$

et temps séquentiel: $\sigma(\Phi)^{n^{O(r)}} + O(|\Phi|)$

ii) Les mêmes bornes s'appliquent pour le problème de la décision.

2) Les bornes inférieures: Le but de cette section est de démontrer que nos algorithmes sont optimaux en tant que mesure générale de complexité. C'est-à-dire que le problème général de l'élimination de quantificateurs sur $\mathbb{R}$ ou sur un corps algébriquement clos est de complexité inhérente doublement exponentielle en séquentiel (nombre de processeurs) et simplement exponentielle en parallèle. Cela n'empêche pas que les bornes supérieures puissent être données d'une manière plus précise quant aux paramètres dans le futur. En ce sens le Théorème 3 est seulement une première approximation aux résultats possibles

en parallèle, puisque vu [11] on s'attend à un résultat qui ne dépend pas de la charactéristique de k, et dans le cas de $\mathbb{R}$ on pourrait aussi obtenir en parallèle des bornes plus différenciées comme celles qui se trouvent pour la complexité séquentielle dans [27]. Ceci est une des tâches que nous nous proposons.

En ce qui concerne les bornes inférieures, il existe le résultat de [24] pour le problème de la décision élémentaire de k. Ces bornes sont données pour le modèle séquentiel et sont simplement exponentielles, alors que les bornes supérieures connues sont doublement exponentielles: ce déphasage n'indique donc pas si les bornes supérieures obtenues sont optimales ou non.

Pour la complexité séquentielle de l'élimination de quantificateurs, des bornes inférieures doublement exponentielles sont données dans [43], [19] et [29] dans le cas des corps réel ou algébriquement clos. La méthode suivie dans ces travaux est la suivante: on exhibe une succession de formules $\Psi_k \in L$, $k \in \mathbb{N}$ (en 1 ou 2 variables libres, de longueur $|\Psi_k| = O(k)$ et avec 6k quantificateurs) qui a la propriété suivante: Ψ_k définit 2^{2^k} points isolés du corps k dans la topologie de Zariski si k est algébriquement clos (respectivement de $\mathbb{R}$, dans la topologie forte si $k = \mathbb{R}$.) ; ensuite on démontre que n'importe quelle formule Θ_k sans quantificateurs équivalente a Ψ_k contient des polynômes $F_1, \ldots, F_s$, tels que $\sum_{1 \le i \le s} \deg(F_i) = 2^{2^k}$, ce qui entraine $|\Theta_k| \geq 2^{2^k}$. Si nous supposons que les polynômes de Θ_k sont codifiés de manière dense dans le langage de L, n'importe quel algorithme pour l'élimination de quantificateurs doit nécessairement utiliser un temps doublement exponentiel pour produire le résultat. Cette dépendance de la codification (dans ce cas, représentation dense des polynômes) pour les bornes inférieures est habituelle dans les articles écrits sur le sujet, elle existe aussi dans les résultats de [24]. Les résultats les plus importants jusqu'à présent, quant aux bornes inférieures en Calcul Formel, sont ceux de [35], (voir aussi [20] et [4]) qui sont indépendants de la codification choisie et traitent le probleme de l'appartenance d'un polynôme à un idéal.

Pour la décomposition cylindrique algébrique, il existe aussi une borne inférieure indépendante de la codification, doublement exponentielle, dans [19] qui pourrait avoir des conséquences pour la recherche en Robotique: dans [39] et [40], les auteurs réduisent le probleme de construire des robots (qui "déménagent des pianos"-Piano Movers Problem-) au probleme de décomposition d'ensembles semi-algébriques en composantes semi-algébriques connexes de dimension constante. Notons, en passant, que la décomposition cylindrique four

nit une notion de dimension. Cette notion est équivalente aussi bien a la notion algébrique de dimension qu'a celle obtenue par le biais du spectre réel (voir [17], [8], [22]).

Si la construction d'un robot entraîne la nécessité d'effectuer une décomposition cylindrique algébrique, il est évident qu'il ne faut pas attaquer ce problème par un algorithme général et séquentiel, vu sa complexité inhérente, doublement exponentielle; ceci est dû au fait qu'il n'est guère possible de se restreindre à des espaces ambiants de dimension "petite".

L'idée qui apparait alors est celle d'utiliser des machines qui fonctionnent en parallèle (réseaux). Dans ce cas, les bornes pour la complexité parallèle obtenues sont simplement exponentielles, nous allons démontrer qu'elles sont optimales et qu'elles ne dépendent guère de la codification.

Nous pouvons aussi considérer un point de vue différent: Supposons que les bornes supérieures pour la complexité parallèle des problèmes traités sont des bornes qui s'appliquent pour une notion réaliste de l'espace (Voir [6]) et que l'ordre des bornes en parallèle est toujours le logarithme des bornes séquentielles, supposons aussi que la complexité séquentielle intinsèque des problèmes "géométriques" est simplement exponentielle([21])tandis que celle des problèmes "algébriques" et de l'élimination des quantificateurs est doublement exponentielle, il existe alors vraiment une possibilité d'obtenir pour la Robotique des bornes polynômiales (en fixant le nombre d'alternations de blocs d'$\exists$, $\forall$) grâce aux processeurs qui fonctionnent en parallèle.

Un mot final sur notre modèle "éliminateur de quantificateurs": Ce modèle consiste en une machine qui fait le "travail intellectuel" (et dont nous ne savons pas donner des bornes inférieures de complexité) et en une "imprimante" (ou bien, dans le cas parallèle, en une machine qui contient un réseau arithmétique qui évalue les polynômes) et nous avons pour lui des bornes inférieures, soit pour l'élimination de quantificateurs, soit, dans le cas k= $\mathbb{R}$, pour la décomposition cylindrique algébrique. Ce modèle est raisonnable puisque jusqu'à présent, en éliminant des quantificateurs, l'"intelligence naturelle" (non-mesurable) a toujours gagné contre l'"intelligence artificielle"([36], [34], [1], [2]). Pour faire faillir l'intelligence naturelle, il faudrait restreindre la mémoire qui permet de réaliser les calculs, ou la quantité de papier nécessaire pour écrire les résultats obtenus grace à cette mémoire.

Théorème 4 : Il existe une succession de formules (avec des quantificateurs et en 1 ou 2 variables libres) $\Psi_k \in L$, $k \in \mathbb{N}$ avec les propriétés suivantes:
i) $|\Psi_k| = O(k)$
ii) Pour chaque formule $\theta \in L$ sans quantificateurs et équivalente a Ψ_k, composée de formules atomiques qui contiennent les polynômes $F_1,\ldots,F_s$, on a: $\sum_{1\leq i\leq s} \deg(F_i) \geq 2^{2^k}$ et il existe j, $1\leq j\leq s$ tel que $\deg(F_j)\geq 2^{2^{ck}}$, où c>0 est une constante appropriée.

L'énoncé (ii) implique que $|\theta| \geq 2^{2^k}$ et que chaque réseau qui construit θ contient un réseau arithmétique de profondeur 2^{ck} parce qu'il doit évaluer un F_i ($1\leq i\leq s$) de degré $\geq 2^{2^{ck}}$ (Voir [25])

Corollaire: L'élimination de quantificateurs de la théorie élémentaire de k est doublement exponentielle en temps séquentiel et simplement exponentielle en temps parallèle.

N'importe quel algorithme de décomposition algébrique cylindrique sur $\mathbb{R}$ entraine un algorithme d'élimination de quantificateurs pour la théorie élémentaire de $\mathbb{R}$. Alors, comme notre algorithme d'élimination de quantificateurs de R est basé sur la décomposition algébrique cylindrique, les bornes du Corollaire s'appliquent aussi à la décomposition algébrique cylindrique. Révisant notre démonstration, on peut procéder directement, car la décomposition algébrique cylindrique de $\mathbb{R}^{6k+2}$ induite par Ψ_k conduit à au moins $2^{2^{k+1}}$ régions de dimension 0. Cela entraine:

Théorème 5 : Le temps séquentiel pour décomposer cylindriquement $\mathbb{R}^{6k+2}$ a partir de 8k+2 polynômes de degré ≤ 4 est au moins $2^{2^{k+1}}$. Le temps parallèle nécessaire pour la même tâche est au moins $2^k - 3$.

III. DEMONSTRATIONS:

1) Bornes supérieures pour l'élimination de quantificateurs dans la théorie élémentaire des corps réels clos:

Nous suivrons le raisonnement de [44] , qui se base sur la Décom-

position cylindrique algébrique (Voir aussi [14]). Ces algorithmes sont en partie aisément parallélisables, grâce à l'existence de calculs rapides de déterminants en parallèle ([7],[18]). La difficulté essentielle pour paralléliser complètement ces processus consiste en la manière de déterminer le signe que prend un polynôme sur un vecteur de nombres algébriques (ce que nous faisons en détail dans (B)).

Nous décrirons brèvement l'algorithme (récurrent) de [44] :

Si $\Phi(X_1 \ldots X_r)$ est une formule, à variables libres $X_1 \ldots X_r$ et variables liées, du langage de 1er. ordre de $\mathbb{R}$, on décompose $\mathbb{R}^r$ en sous-ensembles où Φ a une valeur de vérité fixée. Pour déterminer si la formule Φ est vraie sur un sous-ensemble donné, il suffit alors de l'évaluer en un point choisi de ce sous-ensemble (ces points se choisissent algorithmiquement et définissent un système de représentants). Finalement, on décrira par des formules sans quantificateurs les sous-ensembles de $\mathbb{R}^r$ où Φ est vraie.

Ce chapitre est divisé en trois parties:

A) La décomposition cylindrique de $\mathbb{R}^r$ et le choix du système de représentants.

B) La détermination du signe d'un polynôme évalué en un vecteur de nombres algébriques.

C) Le calcul total des complexités.

A. Décomposition cylindrique de $\mathbb{R}^r$ et choix du système de représentants:

Comme nous suivons l'algorithme proposé dans [44], nous éviterons d'entrer dans les détails. Le lecteur intéressé peut trouver toutes les démonstrations dans l'article mentionné.

Les calculs de complexité parallèle seront réalisés dans (C).

- Soit $\mathbb{P} \subseteq Z[X_1, \ldots X_n]$ fini

$\mathbb{U}(\mathbb{P})$ est la partition de $\mathbb{R}^n$, où chaque élément de la partition

est une composante connexe d'une condition de signe fixée sur les polynômes de $\mathbb{P}$.

- $E_{X_n}(\mathbb{P}) \subseteq \mathbb{Z}[X_1,\ldots X_{n-1}]$ fini, est un ensemble construit de manière telle que si $U \in \mathbb{U}(\mathbb{P}))$, $V \in \mathbb{U}(E_{X_n}(\mathbb{P}))$ et $\Pi(U) \cap V \neq \emptyset$, alors $V \subseteq \Pi(U)$

($\Pi: \mathbb{R}^n \longrightarrow \mathbb{R}^{n-1}$ est la projection définie par $\Pi(y_1,\ldots,y_n) = (y_1,\ldots,y_{n-1})$ $\forall (y_1,\ldots,y_n) \in \mathbb{R}^n$)

La définition de $E_{X_n}(\mathbb{P})$ est la suivante:

Soit $C_{X_n}(\mathbb{P})$: = l'ensemble des coefficients des polynômes de $\mathbb{P}$, considérés comme polynômes en X_n

Soient $P, Q \in \mathbb{Z}[X_1,\ldots,X_{n-1}][X_n]$

$$P = \sum_{j=0}^{m} (p_j X_n^j) \quad \text{et} \quad Q = \sum_{j=0}^{t} (q_j X_n^j)$$

Si $h \leq m$, $\ell \leq t$, et $1 \leq g \leq \min\{h,\ell\}$ on définit:

$$M_{X_n}(P,Q,h,\ell,g) := \begin{bmatrix} p_h & p_{h-1} & \cdots & p_o & & \\ & \ddots & \ddots & & \ddots & \\ & & p_h & p_{h-1} & \cdots & p_o \\ q_\ell & q_{\ell-1} & \cdots & q_o & & \\ & \ddots & \ddots & & \ddots & \\ & & q_\ell & q_{\ell-1} & \cdots & q_o \end{bmatrix}$$

$\ell - (g-1)$ lignes de p, $h - (g-1)$ lignes de q; $\ell + h - (g-1)$ colonnes.

et $S_{X_n}(P, Q, h, \ell, g) := \det(M.M^t)$ où $M := M_{X_n}(P, Q, h, \ell, g)$

Alors:

$$E_{X_n}(\mathbb{P}) := C_{X_n}(\mathbb{P}) \cup \left\{ S_{X_n}(P, Q, h, \ell, g) : P, Q \in (\mathbb{P} \cup \frac{\partial}{\partial X_n}\mathbb{P});\ h \leq \deg_{X_n}(P),\ \ell \leq \deg_{X_n}(Q) \text{ et } 1 \leq g \leq \min\{h, \ell\} \right.$$

La propriété précédente est fondamentale pour la récurrence de la décomposition cylindrique algébrique. La démonstration est une conséquence du Saucissonage de Cohen.

- Si $\Phi(X_1, \ldots, X_r)$ est une formule en r variables libres et s variables liées (de $\mathbb{R}$), on travaille sur la famille de polynômes $\mathbb{P}_\Phi$ définie par:

i) $\mathbb{P}_{p(X_1,\ldots,X_r)>0} := \{P(X_1, \ldots, X_r)\}$

ii) $\mathbb{P}_{(\Phi \vee \Psi)(X_1,\ldots,X_r)} := \mathbb{P}_\Phi \cup \mathbb{P}_\Psi$

iii) $\mathbb{P}_{\neg\Psi(X_1,\ldots,X_r)} := \mathbb{P}_\Psi$

iv) $\mathbb{P}_{\exists\, \Psi(X_1,\ldots,X_r,Y)} := E_Y \mathbb{P}_\Psi$

On a alors la propriété: $\forall\, U \in \mathbb{U}(\mathbb{P}_\Phi)$, Φ a une valeur de vérité constante sur U.

- Pour des raisons techniques, il ne suffit pas de calculer $\mathbb{U}(\mathbb{P}_\Phi)$ mais il faut prendre des nouvelles sous-partitions.

On définit, pour $\mathbb{P} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ un ensemble fini:

$$\mathbb{V}(\mathbb{P}) := \begin{cases} \mathbb{U}(D_{X_1}(\mathbb{P})) \text{ si } n = 1 \\ (W \times R) \cap U \quad \text{où } W \in \mathbb{W}(E_{X_n} D_{X_n} \mathbb{P}),\ U \in \mathbb{U}(D_{X_n}\mathbb{P}) \text{ et} \\ \qquad (W \times R) \cap U \neq \emptyset \quad \text{si } n > 2 \end{cases}$$

ou $D_{X_i}(\mathbb{P}) := \left\{ \dfrac{\partial^j P}{\partial X_i^j} : P \in \mathbb{P},\ 0 \leq j < \deg_{X_i}(P) \right\}$

et on considère alors $\mathbb{V}(\mathbb{P}_\Phi)$.

Cette partition a, entre autres, l'avantage suivant: deux composantes d'une même condition de signe pour les polynômes de $\mathbb{P}_\Phi$ ont des projections dans $\mathbb{R}^{n-1}$ disjointes.

- Soit $\mathbb{W}$ une partition de $\mathbb{R}^n$. Un système de représentants de $\mathbb{W}$ est un ensemble fini $S \subseteq \mathbb{R}^n$, de vecteurs algébriques (i.e $a = (a_1,\ldots, a_n)$ et a_i algébrique sur $\mathbb{Q}$), tel que $\forall\ W \in \mathbb{W}, \exists\ a \in S$ et $a \in W$.

Dans [44] , on donne un algorithme qui construit des systèmes de représentants pour $\mathbb{U}(\mathbb{P}_\Phi)$ et $\mathbb{V}(\mathbb{P}_\Phi)$.

- Soient $\mathbb{P} \subseteq \mathbb{Z}[X_1,\ldots X_r]$ un ensemble fini, et $a \in \mathbb{R}^r$; on définit a partir de $\mathbb{P}$ une formule:

$$\varphi_a(\mathbb{P}) := \begin{cases} \bigwedge_{P \in D_{X_1}(\mathbb{P})} \operatorname{sg} P = \operatorname{sg} P(a) & \text{si } r = 1 \\ \varphi_{(a_1,\ldots,a_{r-1})}(E_{X_r}(D_{X_r}(\mathbb{P}))) \wedge \bigwedge_{P \in D_{X_r}(\mathbb{P})} (\operatorname{sg} P = \operatorname{sg} P(a)) & \text{si } r > 1 \end{cases}$$

Où $a = (a_1,\ldots,a_r)$ et $\operatorname{sg} P = \operatorname{sg} P(a)$ signifie $P \gtreqless 0$ selon $P(a) \gtreqless 0$

La propriété fondamentale de la formule $\varphi_a(\mathbb{P})$ est qu'elle est sans quantificateurs et qu'elle définit exactement la composante $V \in \mathbb{V}(\mathbb{P})$ qui contient a.

- Elimination de quantificateurs

Soit $\Phi(X_1,\ldots,X_r)$ une formule avec r-variables libres et s liées.

Soit S un système de représentants pour $\mathbb{V}(\mathbb{P}_\Phi)$.

Alors: Φ est équivalente, modulo les axiomes de la théorie élémentaire de $\mathbb{R}$, à une formule sans quantificateurs $\Psi(X_1,\ldots,X_r)$ définie par :

$$\Psi(X_1,\ldots,X_r) = \bigvee_{\substack{a \in S \\ \Phi(a) \text{ est vraie}}} \varphi_a(\mathbb{P}_\Phi)$$

- Il faut par conséquent savoir évaluer la valeur de vérité de la formule Φ sur un élément a du système de représentants S: on procède de la manière suivante:

i) Si $\Phi = P > 0$, alors $\Phi(a)$ est vraie $\Leftrightarrow P(a) > 0$

ii) Si $\Phi = \varphi \vee \Psi$, alors $\Phi(a)$ est vraie $\Leftrightarrow \varphi(a)$ est vraie ou ou $\Psi(a)$ est vraie.

iii) Si $\Phi = \neg\Psi$, alors $\Phi(a)$ est vraie $\Leftrightarrow \Psi(a)$ est fausse.

iv) Si $\Phi = (\exists Y)(\Psi(X_1,\ldots,X_r,Y))$, et S est un système de représentants pour $\mathbb{U}(\mathbb{P}_\Psi(a,Y))$, alors $\Phi(a)$ est vraie $\Leftrightarrow$ $\Leftrightarrow \exists b \in S \ / \ \Psi(a,b)$ est vraie.

Donc, déterminer la valeur de vérité de la formule Φ en $(a_1,\ldots,a_r)$ se réduit a évaluer le signe que prennent certains polynômes sur des vecteurs $(a_1,\ldots,a_r,b_1,\ldots,b_s)$ de nombres algébriques.

B. Détermination du signe:

a) Selon ce qui a été montré auparavant, décider de la valeur de vérité d'une formule évaluée en un vecteur $(x_1,\ldots,x_r)$ de nombres algébriques se réduit à décider le signe d'un certain polynôme en $(x_1,\ldots,x_r,y_{r+1},\ldots,y_n)$ pour des nombres algébriques adéquats, $y_{r+1},\ldots,y_n$. Pour décrire ces nombres algébriques on a le lemme suivant:

Lemme (Thom): Soit $P(x) \in \mathbb{R}[X]$, $\deg(P)=n$.
Soit $P^{(i)}$ la i-ème dérivée de P
Si $A=\{ x \in R \ / \ P(x)\delta_0 0$ et $P^{(1)}(x)\delta_1 0$ et ... et $P^{(n)}(x)\ \delta_n 0$, où $\delta_i \in \{ >, <, = \} \}$
Alors $A=\emptyset$, ou $A=\{ a \}$, ou $A=(a,b)$, $a,b \in \mathbb{R}$.

Corollaire: Une racine de P peut être distinguée par des conditions déterminées de signe sur les dérivées.

b) Notre méthode pour déterminer le signe d'un polynôme sur des nombres algébriques est essentiellement différente de celle utilisée dans [44]. Les racines des polynômes ne sont pas ici approchées par des nombres rationnels. Nous nous basons principalement sur une généralisation des successions de Sturm [6], et sur des résultats de sous-résultantes, pour être "rapides" en parallèle.

Notation et Définitions:
- Soit $a \in \mathbb{R}$, sg(a) (le signe de a) sera noté par +1,-1 ou 0 selon si a est positif, négatif ou nul.
- Si $P,Q_1,\ldots,Q_k \in \mathbb{R}[X]$,et $\varepsilon=(\varepsilon_1,\ldots,\varepsilon_k)$ est une succession de signes, appartenant à $\{+1,-1,0\}$ on définit:

$$C_\varepsilon(P,Q_1,\ldots,Q_k) := \#\{ x \in \mathbb{R} \ / \ P(x)=0 \text{ et } sg(Q_j(x))=\varepsilon_j \ \forall j \}$$

- La succession de Sturm de P et Q est définie par:

$$P_0 := P$$
$$P_1 := Q$$
et si $P_{i-1} = Q_i . P_i + R_i$, $P_{i+1} := - R_i$

- On note par $V_{P,Q}(-\infty)$ et $V_{P,Q}(+\infty)$ le nombre de changements de signe (stricts) qui apparaissent dans la succession des signes des P_i évalués respectivement en $-\infty$ et $+\infty$.

Alors, si $S(P,Q) := V_{P,Q}(-\infty) - V_{P,Q}(+\infty)$, on a le théoreme suivant:

Théorème (Sturm): Soit $P \in \mathbb{R}[X]$, un polynôme libre de carrés. Alors:

$S(P,P^{(1)}) = \#\{x \in \mathbb{R} \;/\; P(x)=0\}$ (nombre de racines réelles de P)

Lemme (Tarski): Soit P comme auparavant, $Q \in \mathbb{R}[X]$

$S(P,P^{(1)}.Q) = C_1(P,Q) - C_{-1}(P,Q)$

c) Soit $P(x_1,\ldots,x_n) \in \mathbb{Z}(X_1,\ldots,X_n)$. On désire calculer le signe de $P(\xi_1,\ldots,\xi_n)$, connaissant ξ_i par : $B_i(\xi_i)=0$ ($B_i \in \mathbb{Z}[X]$) et des conditions de signe déterminées sur les dérivées de B_i. L'on procédera par récurrence sur le nombre de variables n pour effectuer cette évaluation.

Cas n=1: Nous suivrons,sans faire les démonstrations, le raisonnement par étapes montré dans [16]

(E1): Soient $P,B \in \mathbb{R}[X]$, libres de carrés. Soit PGDC(P,B)=1.

Alors, $S(B,B^{(1)}) = C_1(B,P) + C_{-1}(B,P)$ (Théorème de Sturm)

$S(B,B^{(1)}.P) = C_1(B,P) - C_{-1}(B,P)$ (Lemme de Tarski)

Et en calculant $S(B,B^{(1)})$ et $S(B,B^{(1)}.P)$ grâce aux successions de Sturm, il suffit de résoudre un système d'équations pour obtenir les valeurs de $C_1(B,P)$ et $C_{-1}(B,P)$

(E2): Calcul de $C_1(B,P)$, $C_{-1}(B,P)$ et $C_0(B,P)$: (Cas où $PGDC(B,P)\neq 1$)

Si B et P sont premiers entre eux, on applique (E1). Sinon,

$C_0(B,P)$= nombre de racines réelles de PGDC(B,P), selon le Th. Sturm,

et en remplacant B par S:=B/PGDC(B,P), on applique (E1):

$C_1(B,P) = C_1(S,P)$ et $C_{-1}(B,P) = C_{-1}(S,P)$.

(E3): Soit $B \in \mathbb{R}[X]$ comme auparavant.

Soient $Q_1,\ldots,Q_k \in \mathbb{R}[X]$ / $PGDC(B,Q_i)=1$, $1 \leqslant i \leqslant k$

On cherche à déterminer $C_\varepsilon(B,Q_1,\ldots,Q_k)$, où $\varepsilon=(\varepsilon_1,\ldots,\varepsilon_k)$ fixe les conditions de signe sur $Q_1,\ldots,Q_k$.

Le cas k=1 correspond à (E1).

Le cas général est démontré dans [6] et réduit le problème a résoudre un système d'équations non homogène: la matrice du système s'obtient de faire 2^k produits de Kronecker de la matrice $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ (qui provient du système de (E1)) et la constante est composée par des expressins du genre $S(B,B^{(1)}.Q)$, ou $Q=\prod_{i\in I} Q_i$, et $I \subseteq \{1,\ldots k\}$. Comme ce système, du point de vue des complexités est trop "cher" a résoudre, [6] réduit le problème à travailler par étapes sur des systèmes plus petits (2k systèmes d'ordre k^2).

Cette méthode est ici essentielle pour la rapidité de notre algorithme.

(E4): Cas où $Q_1,\ldots,Q_k$ ne sont pas forcément premiers avec B:
Soient $B,Q_1,\ldots,Q_k \in \mathbb{R}[X]$, B libre de carrés. L'on déterminera les vecteurs $\varepsilon=(\varepsilon_1,\ldots,\varepsilon_k)$ de conditions de signe sur les Q_i telles que $C_\varepsilon(B,Q_1,\ldots,Q_k)\neq 0$.
Si $\varepsilon_{j_1},\ldots,\varepsilon_{j_\ell}$ sont les ε_i non nuls du vecteur ε, on construit un polynôme S, $S \mid B$ et $PGDC(S,Q_{j_i})=1$ $(1\leqslant i\leqslant \ell)$ de telle manière que:
$C_{\varepsilon'}(S,Q_{j_1},\ldots,Q_{j_\ell}) = C_\varepsilon(B,Q_1,\ldots,Q_k)$, où $\varepsilon'=(\varepsilon_{j_1},\ldots,\varepsilon_{j_\ell})$ (et on applique (E3))
La construction de S se fait par récurrence sur k (remplacant B par $PGDC(B,Q_i)$ ou $B/PGDC(B,Q_i)$ suivant si $\varepsilon_i=0$ ou non.)

(E5): Détermination du signe d'un polynôme évalué en un nombre algébrique: (donné par le polynôme qui l'annule et les conditions de signe sur les dérivées)
Soit $\xi\in\mathbb{R}$ tel que $B(\xi)=0$ ($B\in\mathbb{Z}[X]$ libre de carrés, $deg(B)=s$)
Soit $P\in\mathbb{Z}[X]$. On cherche a déterminer le signe de $P(\xi)$.
On sait que: $\{\xi\}=\{y\in\mathbb{R}/B(y)=0 \text{ et } sg(B^{(i)}(y))=\varepsilon_i\}$ pour un vecteur $\varepsilon=(\varepsilon_1,\ldots,\varepsilon_{s-1})$ fixé. Il suffit alors d'appliquer (E4) pour la succession de polynômes:
$B,B^{(1)},\ldots,B^{(s-1)},P$ et la succession respective de signes: $(0,\varepsilon_1,\ldots,\varepsilon_{s-1},\nu)$ où $\nu\in\{+1,-1,0\}$ selon si l'on cherche à savoir si $P(\xi)>0, P(\xi)<0$ ou $P(\xi)=0$.

Cas général ($n>1$):

Soient $\xi_i\in\mathbb{R}$ $(1\leqslant i\leqslant n)$ des nombres algébriques déterminés par $B_i\in\mathbb{Z}[X]$ et des conditions de signe fixées sur les dérivées. On cherche à évaluer le signe de $P(\xi_1,\ldots,\xi_n)$, où $P\in\mathbb{Z}[X_1,\ldots,X_n]$ La difficulté provient ici du fait que les racines $\xi_1,\ldots,\xi_n$ ne sont pas données explicitement: on peut essayer de reproduire le raisonnement fait dans le cas précédent pour $P(\xi_1,\ldots,\xi_{n-1},X)$ mais il faut alors construire certaines successions de Sturm, c'est-à-dire donner $R(\xi_1,\ldots,\xi_{n-1})(X)$ de telle manière que:

*) $B^*(\xi_1,\ldots,\xi_{n-1})(X) = Q(\xi_1,\ldots,\xi_{n-1})(X).P(\xi_1,\ldots,\xi_{n-1})(X) + R(\xi_1,\ldots,\xi_{n-1})(X)$

(Algorithme de division)

Puisque nous ne connaissons pas $\xi_1,\ldots,\xi_{n-1}$, nous cherchons une méthode qui permet de diviser $B^*(X_1,\ldots,X_{n-1})(X)$ par $P(X_1,\ldots,X_{n-1})(X)$ et qui, si nous remplacons $X_1,\ldots,X_{n-1}$ par $\xi_1,\ldots,\xi_{n-1}$ représente (*) .

Etant donné que $\mathbb{Q}[X_1,\ldots,X_{n-1}]$ n'est pas un corps, il n'y a pas d'algorithme de division général dans $\mathbb{Q}[X_1,\ldots,X_{n-1}][X]$. La division est permise seulement dans quelques cas particuliers, par exemple si le coefficient directeur du diviseur vérifie certaines conditons (ce que nous utiliserons dans nos algorithmes). Ce problème de la division n'a pas été explicitement considéré dans [6] ni dans [16] et nous ne savons pas comment les auteurs surmontent cet obstacle. Une manière naturelle de travailler serait ou de multiplier B^* par un facteur adéquat ou de diviser le diviseur par son coefficient directeur.

Ces méthodes, appliquées directement, sont pour nous trop chères, car nous ne pouvons pas controler suffisemment les degrés des restes qui apparaissent. en d'autres termes, comme la division doit s'effectuer récursivement autant de fois que le degré de B^* l'indique, si le coût d'une division est élevé, le coût total pour obtenir la succession de Sturm sera hors des bornes que nous cherchons à obtenir.

L'algorithme que nous proposons ici pour effectuer la division est plus intriqué mais a l'avantage d'être plus controlé du point de vue de la croissance des degrés, ce qui permet d'obtenir les bornes supérieures cherchées pour la complexité parallèle, sans faire exploser la complexité séquentielle. Il existe certainement une méthode plus élégante pour effectuer bon marché cette division, mais de toute manière nous pensons qu'il est utile d'avoir pour une fois écrit en détail un algorithme qui permet de surmonter les obstacles (Algorithme STURM).

Pour en revenir au problème, nous cherchons à analyser les conditions ν de signe consistantes dans la formule:

$$sg(B_n(X))=0 \wedge \bigwedge_{i=1}^{s-1} sg(B_n^{(i)})= \varepsilon_i \ \wedge\ sg(P(\xi_1,\ldots,\xi_{n-1},X))= \nu$$

où $\{\xi_n\}= \{y\in \mathbb{R} \ / \ sg(B_n(y))=0 \wedge \bigwedge_{i=1}^{s-1} sg(B_n{}^{i}(y))= \varepsilon_i \}$, $s=\deg(B_n)$

et $\nu \in \{+1,-1,0\}$

Nous suivrons un raisonnement similaire au cas n=1, et (E4') et (E3') noterons les analogues à (E4) et (E3).

(E4'): Il faut transformer la famille de polynômes $\{ B_n^{(j)},\ 0\leqslant j\leqslant s-1 \} \cup \{ P(\xi_1,\ldots,\xi_{n-1},X) \}$ en une famille qui respecte les conditions de (E4).

Travailler avec les $B_n^{(j)}$, $1 \leq j \leq s-1$, n'est guère problématique car $B_n^{(j)} \in \mathbb{Z}[X]$. On suit l'algorithme SIMPLE, qui a comme OUTPUT $B_n^*(X)$, tel que $\forall$ j, $PGDC(B_n^*, B_n^{(j)})=1$.

Pour rendre $B_n^*(X)$ et $P(\xi_1,\ldots,\xi_{n-1},X)$ premiers entre eux, nous utilisons des résultats sur les sous-résultantes et les algorithmes PSEUDOPGDC et PSEUDODIV. Ces algorithmes ne calculent pas exactement le PGDC ni le quotient de la division (Les résultats apparaissent modulo un coefficient en $(X_1,\ldots,X_{n-1})$ qui ne s'annule pas en $(\xi_1,\ldots,\xi_{n-1})$) mais l'OUTPUT a des propriétés équivalentes au polynôme S de (E4).

(E3'): Il faut savoir calculer exactement les restes (*). Notre idée est de diviser dans $\mathbb{Q}[X_1,\ldots,X_{n-1}][X]$, en "inversant" le coefficient principal du diviseur, qui correspond à un polynôme non nul en $(\xi_1,\ldots,\xi_{n-1})$. Cette partie apparait dans l'algorithme INVERSE. L'algorithme qui décrit le processus pour obtenir la succession des restes est l'algorithme STURM, qui se base principalement en [26]; cet algorithme comprend la division exacte mentionnée auparavant. Constemment, dans INVERSE et STURM, nous utiliserons l'évaluation du signe de polynômes en $(\xi_1,\ldots,\xi_{n-1})$, en particulier pour évaluer le signe des coefficients directeurs des restes qui apparaissent dans la succession de STURM. Notre résultat final est l'algorithme SIGNE, qui décide si $P(\xi_1,\ldots,\xi_n)$ est positif ou non.

c1) ALGORITHMES POUR LA DETERMINATION DU SIGNE:

i) Algorithme SIGNE $(P,B_1,\ldots,B_n,I_1,\ldots,I_n)$

INPUT: $P \in \mathbb{Q}[X_1,\ldots,X_n]$

$B_i \in \mathbb{Z}[X]$, $B_i \neq 0$, $1 \leq i \leq n$, $\deg(B_i)=s_i$; $B_i^{(j)}$ $(\forall i,\ 1 \leq j \leq s_i)$

(B_i donné par l'OUTPUT de SIMPLE.)

I_i= s_i-uple formée par 1 et -1 qui représente les conditions de signe pour l'OUTPUT de SIMPLE (L'OUTPUT de SIMPLE décrit un nombre algébrique ξ_i racine du polynôme B_i)

OUTPUT: Vrai ou faux, suivant si $P(\xi_1,\ldots,\xi_n)$ est positif ou non.

a- Faire:

$M := \mathrm{PSEUDOPGDC}(B_n(X), P(\xi_1,\ldots,\xi_{n-1},X))$

$B_n^* := \mathrm{PSEUDODIV}(B_n, M)$

(B_n^* et P , comme polynômes en X, sont premiers entre eux: cela correspond a (E4').)

b- Soit $F = \{B_n^{(j)},\ 0<j<\deg(B_n)\} \cup \{ P \}$, où les dérivées se prennent seulement sur les $B_n^{(j)}$ qui apparaissent avec un signe strict ($\neq 0$) dans l'INPUT.

Pour les sous-ensembles $\mathcal{J}$ de F, déterminés par (E3) ([16]), calculer:

$$\mathrm{STURM}\left(B_n^*(\xi_1,\ldots,\xi_{n-1},X),\ \frac{\partial}{\partial X} B_n^*(\xi_1,\ldots,\xi_{n-1},X).\prod_{Q\in\mathcal{J}} Q\right)$$

(Ici, on produit les restes R_k de la succession de Sturm.)

c- Pour $\mathcal{J} \subseteq F$ fixé et pour tout R_k, faire (par récurrence):

$\mathrm{SIGNE}(\mathrm{CDIR}(R_k), B_1,\ldots,B_{n-1},I_1,\ldots,I_{n-1})$,où $\mathrm{CDIR}(R_k)$ note le coefficient directeur de R_k, considéré comme polynôme en $X_1,\ldots,X_{n-1}$.

Grace aux signes obtenus, on calcule :

$$S\left(B_n^*,\ \frac{\partial B_n^*}{\partial X}.\prod_{Q\in\mathcal{J}} Q\right)$$, qui correspond à la notation de B.b)

d- En utilisant le processus rapide de [ ] on détermine si $P(\xi_1,\ldots,\xi_{n-1})$ est positif, en utilisant au plus $2.\deg_X(B_n^*)$ sous-ensembles $\mathcal{J}$.)

ii) Algorithme PSEUDOPGDC $(P,Q,B_1,\ldots,B_{n-1},I_1,\ldots,I_{n-1})$

INPUT: $P,Q \in \mathbb{Q}[X_1,\ldots,X_{n-1}][X]$, $\deg_X(P) = m$, $\deg_X(Q) = t$;

$B_i \in \mathbb{Z}[X]$, $1\leq i\leq n-1$

I_i ($1\leq i\leq n-1$) comme dans l'OUTPUT de SIMPLE (apparaissent seulement les dérivées avec des conditions de signe non nulles sur ξ_n.)

OUTPUT: $M(X_1,\ldots,X_{n-1})(X) \in \mathbb{Q}[X_1,\ldots,X_{n-1}][X]$ tel que:

$M(\xi_1,\ldots,\xi_{n-1})(X) = H(\xi_1,\ldots,\xi_{n-1})(X).\mathrm{PGDC}(P(\xi_1,\ldots,\xi_{n-1})(X),$

$Q(\xi_1,\ldots,\xi_{n-1})(X))$, où $H \in \mathbb{Z}[X_1,\ldots,X_{n-1}]$, $H(\xi_1,\ldots,\xi_{n-1})\neq 0$

(PGDC désigne le Plus Grand Diviseur Commun.)

a- Soit P_i la i-ème sous-résultante principale entre $P(X_1,\ldots,X_{n-1})(X)$ et $Q(X_1,\ldots,X_{n-1})(X)$ (Voir[9],[15] et[26])

Si $k=\min\{i \;/\; Det(P_i)$ évalué en $(\xi_1,\ldots,\xi_{n-1})$ est non nul $\}$, alors:

$\deg(PGDC(P(\xi_1,\ldots,\xi_{n-1})(X),Q(\xi_1,\ldots,\xi_{n-1})(X))) = k.$

(Ici, on évalue le signe de $Det(P_i)(\xi_1,\ldots,\xi_{n-1})$ avec l'algorithme SIGNE appliqué a (n-1) variables.)

b- Soient $y = (y_{t-k-1},\ldots,y_0)$ et $z = (z_{m-k-1},\ldots z_0)$

Résoudre:

$$P_k \cdot \begin{pmatrix} y^t \\ z^t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ Det(P_k) \end{pmatrix} \quad \text{(C'est-à-dire } \begin{pmatrix} y^t \\ z^t \end{pmatrix} = Adj(P_k) \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \text{)}$$

Faire: $Y = y_{t-k-1}.X^{t-k-1} +\ldots+ y_0$ et $Z = z_{m-k-1}.X^{m-k-1} +\ldots+ z_0$

c- Soit $M = P.Y + Q.Z$,

Alors $M(\xi_1,\ldots,\xi_{n-1})(X) = Det(P_k)(\xi_1,\ldots,\xi_{n-1}).$

$$.PGDC(P(\xi_1,\ldots,\xi_{n-1})(X),Q(\xi_1,\ldots,\xi_{n-1})(X))$$

(Pour la démonstration, voir [26])

iii) Algorithme PSEUDODIV: (P,Q)

INPUT: $P,Q \in \mathbb{Q}[X_1,\ldots,X_{n-1}][X]$

$Q(\xi_1,\ldots,\xi_{n-1})(X)$ divise exactement $P(\xi_1,\ldots,\xi_{n-1})(X)$,

$\deg_X(P)=m$, $\deg_X(Q)=t$

Si $q_t(X_1,\ldots,X_{n-1})$ est le coefficient directeur de Q, comme polynôme en X, on a $q_t(\xi_1,\ldots,\xi_{n-1}) \neq 0$

Si $p_m(X_1,\ldots,X_{n-1})$ est le coefficient directeur de P, comme polynôme en X, on a $p_m(\xi_1,\ldots,\xi_{n-1}) \neq 0$.

OUTPUT: $C(X_1,\ldots,X_{n-1})(X)$ qui est le quotient de la division entière de $q_t^{m-t+1} \cdot P$ par Q, dans $\mathbb{Q}[X_1,\ldots,X_{n-1}][X]$ de manière que si:

$P(\xi_1,\ldots,\xi_{n-1})(X) = Q(\xi_1,\ldots,\xi_{n-1})(X).\ C'(\xi_1,\ldots,\xi_{n-1})(X)$

alors $C(\xi_1,\ldots,\xi_{n-1})(X) = q_t(\xi_1,\ldots,\xi_{n-1})^{m-t+1}.C'(\xi_1,\ldots,\xi_{n-1})(X)$

a- Soient C et R le quotient et le reste de la division entiere de $q_t^{m-t+1}.P$ par Q (qui peut se faire dans $\mathbb{Z}[X_1,\ldots,X_{n-1}][X]$ car tous les coefficients du dividende sont divisibles par q_t^{m-t+1}) :

Le quotient C est déterminé, de manière unique, par les conditions:

$$q_t^{m-t+1}.P = C.Q + R \quad \text{et} \quad \deg_X(q_t^{m-t+1}.P - C.Q) < \deg_X(Q)$$

Si $q_t^{m-t+1}.P = q_t^{m-t+1}.(p_m.X^m +\ldots+ p_0)$ et $Q = q_t.X^t +\ldots+ q_0$,

il faut résoudre le système:

$$\begin{pmatrix} q_t & 0 & \cdots & 0 \\ q_{t-1} & q_t & & \vdots \\ \vdots & & \ddots & \vdots \\ q_{t-(m-t)} & \cdots & & q_t \end{pmatrix} \cdot \begin{pmatrix} c_{m-t} \\ \vdots \\ c_0 \end{pmatrix} = q_t^{m-t+1} \cdot \begin{pmatrix} p_m \\ \vdots \\ p_t \end{pmatrix}$$

C'est-à-dire:

$$\begin{pmatrix} c_{m-t} \\ \vdots \\ c_0 \end{pmatrix} = \mathrm{Adj} \begin{pmatrix} q_t & & 0 \\ \vdots & \ddots & \\ \vdots & * & \ddots \\ \vdots & \cdots & q_t \end{pmatrix} \cdot \begin{pmatrix} p_m \\ \vdots \\ p_t \end{pmatrix}$$

Et par conséquent, $C = c_{m-t}.X^{m-t} +\ldots+ c_0$

Algorithme INVERSE: $(P,B_1,\ldots,B_n,I_1,\ldots,I_n)$

INPUT: $P \in \mathbb{Z}[X_1,\ldots,X_n]$, $B_1,\ldots,B_n \in \mathbb{Z}[X]$, $I_1,\ldots,I_n$ conditions de signe définies comme dans l'OUTPUT de SIMPLE. $\{B_i,I_i\}_{1\leq i\leq n}$ définissent les nombres algébriques $\xi_1,\ldots,\xi_n$ tels que $P(\xi_1,\ldots,\xi_n) \neq 0$.

OUTPUT: $H \in \mathbb{Q}[X_1,\ldots,X_n]$ tel que $H(\xi_1,\ldots,\xi_n) = P(\xi_1,\ldots,\xi_n)^{-1}$.

a- Faire $M = \mathrm{PSEUDOPGDC}(P(\xi_1,\ldots,\xi_{n-1})(X),B_n(X))$ (Noter que $M(\xi_1,\ldots,\xi_n)\neq 0$)

$B_n^* = \mathrm{PSEUDODIV}(B_n,M)$

(B_n^* et M sont maintenant premiers entre eux. De plus, comme $B_n = M.B_n^*.T$ et $M(\xi_1,\ldots,\xi_n).T(\xi_1,\ldots,\xi_{n-1}) \neq 0$, $B_n^*(\xi_1,\ldots,\xi_n) = 0$ car $B_n(\xi_n) = 0$)

b- Soit $R(X_1,\ldots,X_{n-1}) := \text{Résultante}_X(P(X_1,\ldots,X_{n-1})(X), B_n^*(X_1,\ldots,X_{n-1})(X))$

$(R(\xi_1,\ldots,\xi_{n-1}) \neq 0$ car $\text{PGDC}(P(\xi_1,\ldots,\xi_{n-1})(X), B_n^*(\xi_1,\ldots,\xi_{n-1})(X)) = 1$)

c- Résoudre: $R(X_1,\ldots,X_{n-1}) = Q(X_1,\ldots,X_{n-1})(X).P(X_1,\ldots,X_{n-1})(X) + Q'(X_1,\ldots,X_{n-1})(X).B_n^*(X_1,\ldots,X_{n-1})(X)$

(comme polynômes en X, selon ce qui a été fait dans PSEUDOPGDC)

Si on évalue en $(\xi_1,\ldots,\xi_n)$ on a:

$$R(\xi_1,\ldots,\xi_{n-1}) = Q(\xi_1,\ldots,\xi_n).P(\xi_1,\ldots,\xi_n)$$

et on obtient donc:

$$P(\xi_1,\ldots,\xi_n)^{-1} = Q(\xi_1,\ldots,\xi_n).R(\xi_1,\ldots,\xi_{n-1})^{-1}$$

Par récurrence, on calcule $R(\xi_1,\ldots,\xi_{n-1})^{-1}$,

alors, si $H'(X_1,\ldots,X_{n-1})$ est tel que $H'(\xi_1,\ldots,\xi_{n-1}) = R(\xi_1,\ldots,\xi_{n-1})^{-1}$,

le résultat est: $H(X_1,\ldots,X_{n-1}) = Q(X_1,\ldots,X_{n-1}).H'(X_1,\ldots,X_{n-1})$

v) Algorithme STURM: $(P,Q,B_1,\ldots,B_{n-1},I_1,\ldots,I_{n-1})$

INPUT: $P,Q \in \mathbb{Z}[X_1,\ldots,X_{n-1}][X]$, $\deg_X(P) = m$, $\deg_X(Q) = t$;

$\{B_i,I_i\}_{1\leq i\leq n-1}$ comme dans les algorithmes précédents qui déterminent des nombres algébriques $\xi_1,\ldots,\xi_{n-1}$.

OUTPUT: $\{R_k(X_1,\ldots,X_n)\}_k \subseteq \mathbb{Q}[X_1,\ldots,X_n]$ tel que $\{R_k(\xi_1,\ldots,\xi_{n-1},X)\}_k$ correspond à la succession de Sturm de $P(\xi_1,\ldots,\xi_{n-1})(X)$ et $Q(\xi_1,\ldots,\xi_{n-1})(X)$.

a- Faire $R_0 := P$; $R_1 := Q$.

b- Pour tout $0\leq i\leq t$, soit $p_i = \text{Det}(P_i)$, où P_i est la i-ème sous-résultante principale entre $P(X_1,\ldots,X_{n-1})(X)$ et $Q(X_1,\ldots,X_{n-1})(X)$.

(Par [26], on sait que si $p_i(\xi_1,\ldots,\xi_{n-1}) \neq 0$ (Utilisation de l'algorithme SIGNE en (n-1) variables) il existe un reste R de degré i)

c- Soient $y = (y_{t-i-1},..,y_0)$ et $z = (z_{m-i-1},\ldots,z_0)$

Pour chaque i tel que $p_i(\xi_1,\ldots,\xi_{n-1}) \neq 0$, résoudre:

$$P_i \begin{pmatrix} y^t \\ z^t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

(en inversant $p_i(\xi_1,\ldots,\xi_{n-1})$ grâce à INVERSE)

(Comme y et z sont déterminés par la dernière colonne de P_i^{-1}, leurs coordonnées s'obtiennent de sous-déterminants de P_i, correspondant aux termes de $Adj(P_i)$ multipliés par p_i^{-1}.)

On a donc ℓ solutions $\begin{pmatrix} y^t \\ z^t \end{pmatrix}$ correspondant aux ℓ degrés des restes.

d- On ordonne les ℓ déterminants p_i non nuls en $(\xi_1,\ldots,\xi_{n-1})$ de manière décroissante: p_t est le premier.

Soit p_i le k-ème déterminant p_i non nul $(1\leq k\leq \ell)$ et soient:

$Y_k := y_{t-i-1}.X^{t-i-1} + \ldots + y_0$ et $Z_k := z_{m-i-1}.X^{m-i-1} + \ldots + z_0$

où y et z sont les solutions du système correspondant a P_i.

Faire: $M_k := Y_k.P + Z_k.Q$ (Ce sont les restes à coefficient directeur 1)

e- Pour $2\leq k\leq \ell$, résoudre:

$$M_{k-2} = M_{k-1}.C_{k-1} + D_k \quad , \text{ en prenant } M_0 = P .$$

(L'algorithme de division vaut dans $\mathbb{Q}[X_1,\ldots,X_{n-1}][X]$ car les M_k ont pour coefficient directeur 1)

f- Pour $1\leq k\leq \ell$, si $d_k :=$ coefficient directeur de D_k comme polynôme en X ($d_1 = q_t$)

calculer: $$e_k := \begin{cases} d_k.d_{k-2}\cdots d_2 & \text{si k est pair} \\ d_k.d_{k-2}\cdots d_1 & \text{si k est impair} \end{cases}$$

et soit $R'_k := e_k.M_k \quad (1\leq k\leq \ell)$

g- Pour tout $k\geq 1$, faire $R_k := -R'_k$; alors, $\{R_k\}_k$ est la succession de Sturm de P et Q.

(Pour cet algorithme, nous avons pratiquement suivi celui qui se trouve, pour une variable, dans [6], où toutes les démonstrations sont faites.)

vi) Algorithme SIMPLE: $(B,\{B^{(i)}\}_{1\leq i<deg(B)},I)$

INPUT: $B\in \mathbb{Z}[X]$, $deg(B) = s$, $\{B^{(i)}\}_{1\leq i<s}$;

I: un vecteur formé par 0,1 et -1 qui représente les conditions de signe sur les dérivées de B. Ces conditions caractérisent une racine ξ de B.

OUTPUT: $B^*\in \mathbb{Z}[X]$

$\{B^{(i)}\}_i$ tel que les conditions de signe données par I sont non nulles

(C'est-à-dire une nouvelle famille I' formée par 1,-1 et $\not 0$, où $\not 0$ indique que cette dérivée ne se considère plus)

tels que: $PGDC(B^*,B^{*\prime}) = 1$

et $PGDC(B^*,B^{(i)}) = 1$ si $I_i \neq \not 0$.

a- Faire: $B_1 := PGDC(B,B^{(j_1)},\ldots,B^{(j_\ell)})$ où $B^{(j_i)}$ est tel que $I_{j_i} = 0$.

Remplacer I_{j_i} par $\not 0$.

b- Calculer $A := PPMC(B^{(k_1)},\ldots,B^{(k_j)})$ où $B^{(k_i)}$ est tel que $I_k \neq \not 0$.

c- Faire $B_2 := B_1 / PGDC(B_1,A)$ et $B_3 := B_2 / PGDC(B_2,B_2^{(1)})$

d- Remplacer B_3 par $B^* := k.B_3$ $(k \in \mathbb{Z})$ de manière que $B^* \in \mathbb{Z}[X]$

(k est par exemple le plus petit multiple commun des dénominateurs de B_3)

(Nous utilisons dans cet algorithme les méthodes proposées dans [26] pour les calculs de PGDC et PPMC de plusieurs polynômes.)

C. Calcul des complexités:

Si Φ est une formule d'entrée, prénexe et convenablement préparée, en n variables (r libres et s liées), où interviennent les polynômes $F_1,\ldots,F_s$, nous avons défini dans l'introduction:

$$\sigma(\Phi) := \sum_{1 \leq i \leq s} (2 + \deg(F_i))$$

Ces deux paramètres, n et $\sigma(\Phi)$, sont ceux que nous considérons pour obtenir nos bornes différenciées pour les complexités parallèle et séquentielle.

Le modèle que nous utilisons étant le modèle algébrique, σ ne dépend pas de la longueur binaire des coefficients des polynômes F_i. Dans le cas de la complexité séquentielle, le modèle adéquat est celui de Machine de Turing (non parallélisable) et σ doit controler aussi la longueur binaire des coefficients. Tous les résultats obtenus pour la complexité séquentielle dans notre modèle peuvent se traduire sans peine au modèle de Machine de Turing, et on a des bornes supérieures essentiellement du même ordre que celles de notre théorème.

Dans tout ce qui suit, log désigne le logarithme en base 2 , et c est une constante universelle, qui ne dépend ni de n ni de σ .

1- Croissance de σ :

La plupart des algorithmes ont une complexité qui dépend du degré des polynômes qui interviennent. Nous définissons alors, de la même manière que pour la formule Φ :

$$\sigma(\mathbb{P}) := \sum_{1 \leq i \leq s} (2 + \deg(P_i)) \qquad \text{si} \quad \mathbb{P} = \{P_1, \ldots P_s\} \subseteq \mathbb{Z}[X_1, \ldots, X_n] \text{ fini.}$$

($\sigma(\mathbb{P})$ contrôle le nombre et le degré des polynômes de $\mathbb{P}$.)
Si $\mathbb{P} = \{P\}$, nous noterons directement $\sigma(\{P\}) = \sigma(P)$.

Soit $\mathbb{P} \subseteq \mathbb{Q}[X_1, \ldots, X_r]$ fini, $\sigma(\mathbb{P}) \leq \sigma$, on a les résultats suivants:

i) $\sigma(E_{X_r}(\mathbb{P})) \leq c.\ \sigma^7$ et $\sigma(D_{X_r}(\mathbb{P})) \leq \sigma^3$,

(Il suffit de modifier légerement, pour notre σ , les démonstrations de [44])

ii) $\sigma(E_{X_j} \ldots E_{X_r}(\mathbb{P})) \leq \sigma^{2^{c(r-j+1)}}$ et $\sigma(E_{X_2} \ldots E_{X_r}(\mathbb{P})) \leq \sigma^{2^{c(r-1)}}$

De la même manière:

$$\sigma(D_{X_j} E_{X_{j+1}} \ldots E_{X_r} D_{X_r}(\mathbb{P})) \leq \sigma^{2^{c(r-j+1)}} \quad \text{et} \quad \sigma(D_{X_1} E_{X_2} \ldots E_{X_r} D_{X_r}(\mathbb{P})) < \sigma^{2^{cr}}$$

iii) Le système de représentants de $\mathbb{V}(\mathbb{P}_\Phi)$ est l'ensemble des zéros de certains polynômes $\nu_1, \ldots, \nu_r$ ($\nu_i \in \mathbb{Z}[X]$) tels que:

$$\sigma(\nu_i) \leq \sigma(\mathbb{P}_\Phi)^{2^{cr^2}}$$

et pour évaluer Φ en ce système de représentants, il faut calculer un nouveau système de représentants, donné par $B_1, \ldots, B_s$ tels que:

$$\sigma(B_i) < \sigma(\mathbb{P}_\Phi)^{2^{cn^2}}$$

(Ceci provient de [44] , en modifiant à peine les démonstrations.)

iv) Croissance de σ pour les algorithmes de la détermination du signe:

Comme l'algorithme SIGNE dépend de tous les autres algorithmes, il est nécessaire de connaître la croissance des degrés totaux des polynômes qui interviennent dans ces algorithmes, quand on leur fait subir les changements proposés, pour pouvoir calculer les complexités. Les résultats sont dans tous les cas immédiats et ne seront pas démontrés.

Soient $P, Q \in \mathbb{Q}[X_1, \ldots, X_n]$ et $B_1, \ldots, B_n \in \mathbb{Z}[X]$ tels que:

$\sigma(P) \leq \sigma$, $\sigma(Q) \leq \sigma$, $\sigma(B_i) \leq \sigma$, $1 \leq i \leq n$

Alors:

$\sigma(\text{PSEUDOPGDC}(P,Q)) \leq 2\sigma^2 + 2\sigma = O(\sigma^2)$

$\sigma(\text{PSEUDODIV}(P,Q)) \leq \sigma^2 + 2\sigma = O(\sigma^2)$

$\sigma(\text{INVERSE}(P)) = O(\sigma^{2^{cn}})$ (Par induction sur n)

$\sigma(\text{STURM}(P,Q)) = O(\sigma^{2^{cn}})$

$\sigma(\text{SIMPLE}(B, B^{(i)}) \leq \sigma^2$ et $\sigma(B^*) \leq \sigma$

2- Calcul des complexités (séquentielle et parallèle)

Les calculs qui apparaissent dépendent en général de produits de polynômes et de déterminants (pour résoudre des systèmes d'équations). Nous calculerons d'abord la complexité de ces opérations.
Nous rappelons que nous travaillons avec des polynômes de $\mathbb{Q}[X_1,\ldots,X_n]$ qui sont représentés de manière dense, c'est-à-dire, donnés par les vecteurs des coefficients de tous les monômes possibles.

i) Les opérations entre polynômes se font par interpolation:
Soit $P \in \mathbb{Q}[X_1,\ldots,X_n]$ tel que $\deg(P) \leq \sigma$, alors P est bien déterminé par son évaluation en $(\sigma+1)^n$ points spéciaux, par exemple les points entiers du cube $[0,\sigma]^n$; et on récupere sans peine P de ces valeurs en résolvant un système d'équations de $(\sigma+1)^n \times (\sigma+1)^n$.

Par récurrence, et grâce aux résultats de [7] et [18] (le déterminant d'une matrice carrée d'ordre N, à éléments dans un anneau A, peut s'obtenir sans divisions en temps parallèle $O(\log^2 N)$ et temps séquentiel $N^{O(1)}$), on démontre que si $P \in \mathbb{Q}[X_1,\ldots,X_n]$, $\deg(P) \leq \sigma$ et si on ne compte pas ici le temps nécessaire pour évaluer P (complexité de P), on peut récupérer P, par interpolation, en temps parallèle $cn.\log^2\sigma$ et temps séquentiel σ^{cn}

- Soient $P_1,\ldots,P_m \in \mathbb{Q}[X_1,\ldots,X_n]$, $\sigma(P_i) \leq \sigma$ $(1 \leq i \leq m)$

  Alors: $D(\prod_{1\leq i\leq m}(P_i)) \leq \log(m) + cn^2\log^2(n\sigma)$ et $L(\prod_{1\leq i\leq m}(P_i)) < n\sigma^{cn}$

(Où D et L notent respectivement la complexité parallèle et la complexité séquentielle)

- Soient $(P_{i,j})_{1\leq i,j\leq N} \in \mathbb{Q}[X_1,\ldots,X_n]$, $\sigma(P_{i,j}) \leq \sigma$, $1\leq i,j\leq N$

Alors: $D(Det(P_{i,j})) \leq cn.\log^2(N\sigma)$ et $L(Det(P_{i,j})) \leq (N\sigma)^{cn}$

ii) Si $\mathbb{P}\subseteq \mathbb{Z}[X_1,\ldots,X_r]$ fini, et $\sigma(\mathbb{P}) \leq \sigma$

- Alors: $D(E_{X_r}(\mathbb{P})) \leq cn^2\log^2(\sigma)$ et $L(E_{X_r}(\mathbb{P})) \leq \sigma^{cn}$

(On applique directement la définition de $E_{X_r}(\mathbb{P})$ et les résultats précédents)

Par récurrence, on prouve aussi:

$$D(D_{X_1}E_{X_2}\ldots E_{X_r}D_{X_r}(\mathbb{P})) \leq 2^{cr}\log^2(\sigma)$$

et

$$L(D_{X_1}E_{X_2}\ldots E_{X_r}D_{X_r}(\mathbb{P})) \leq \sigma^{2^{cr}}$$

- Si nous parallélisons les calculs (directement) pour les systèmes de représentants $\{\nu_1,\ldots\nu_r\}$ et $\{B_1,\ldots,B_s\}$ effectués dans [44] , nous obtenons:

$$D(\{\nu_1,\ldots,\nu_r\}) \leq 2^{cr^2}\log^2\sigma \quad \text{et} \quad D(\{B_1,\ldots,B_s\}) \leq 2^{cn^2}\log^2\sigma$$

et

$$L(\{\nu_1,\ldots,\nu_r\}) \leq \sigma^{2^{cr^2}} \quad \text{et} \quad L(\{B_1,\ldots,B_s\}) \leq \sigma^{2^{cn^2}}$$

- Pour calculer $\mathbb{P}_\Phi$ à partir d'une formule Φ , on a:

$$D(\mathbb{P}_\Phi) \leq 2^{cn^2}\log^2\sigma(\Phi) \quad \text{et} \quad L(\mathbb{P}_\Phi) \leq \sigma(\Phi)^{2^{cn^2}}$$

iii) Pour calculer les complexités correspondant a (B) nous adopterons la notation suivante: ALGORITHME(a,b) indique qu'on fait appel a ALGORITHME pour des polynômes en " a " variables et où σ est controlé par " b ". Par exemple: SIGNE$(n-1,\sigma^2)$ signifie qu'on applique l'algorithme SIGNE a des polynômes P,B en (n-1) variables tels que $\sigma(P)\leq\sigma^2$ et $\sigma(B)\leq\sigma^2$.

a- Algorithme PSEUDOPGDC:

$P,Q \in \mathbb{Q}[X_1,\ldots,X_n]$, $\sigma(P) \leq \sigma$ et $\sigma(Q) \leq \sigma$

Si on suit l'algorithme en question, on observe que non seulement on doit effectuer des calculs, mais on doit aussi appliquer SIGNE$(n-1,4\sigma^2)$ (pour calculer le degré du PGDC). Les calculs a réaliser correspondent

a résoudre des systèmes d'équations. On obtient:

$D(PSEUDOPGDC(n,\sigma)) \leq cn^2\log^2\sigma + D(SIGNE(n-1,4\sigma^2)$

$L(PSEUDOPGDC(n,\sigma)) \leq \sigma^{cn^2} + \sigma L(SIGNE(n-1,4\sigma^2)$

b- Algorithme PSEUDODIV:

$P,Q \in \mathbb{Q}[X_1,\ldots,X_n]$, $\sigma(P) \leq \sigma$ et $\sigma(Q) \leq \sigma$

$D(PSEUDODIV(n,\sigma)) \leq cn.\log^2\sigma$

$L(PSEUDODIV(n,\sigma)) \leq \sigma^{cn}$

car l'algorithme PSEUDODIV résoud un système d'équations d'ordre $\sigma \times \sigma$.

c- Algorithme INVERSE:

$P \in \mathbb{Q}[X_1,\ldots,X_n]$, $\sigma(P) \leq \sigma$.

Selon les coûts des algorithmes PSEUDOPGDC et PSEUDODIV, et comme $INVERSE(n,\sigma)$ dépend d'$INVERSE(n-1,c\sigma^c)$, on obtient par récurrence:

$$D(INVERSE(n,\sigma)) \leq 2^{cn}\log^2\sigma + \sum_{1\leq k\leq n-1} D(SIGNE(n-k,4^{k+1}.\sigma^{2^k}))$$

$$L(INVERSE(n,\sigma)) \leq \sigma^{2^{cn}} + \sum_{1\leq k\leq n-1} 4^{k+1}.\sigma^{2^k}\, L(SIGNE(n-k,4^{k+1}.\sigma^{2^k}))$$

d- Algorithme STURM:

$P,Q \in \mathbb{Q}[X_1,\ldots X_n]$, $\sigma(P) \leq \sigma$ et $\sigma(Q) \leq \sigma$

Pour déterminer les degrés des restes R_k il faut appliquer l'algorithme $SIGNE(n-1,4\sigma^2)$. Une fois déterminés les degrés des restes, pour chaque degré on résoud un système d'équations en utilisant $INVERSE(n-1,4\sigma^2)$. Ayant obtenu les restes a coefficient directeur 1, l'algorithme PSEUDO-DIV permet d'exhiber les restes R_k: on applique $PSEUDODIV(n,\sigma^{2^{cn}})$. Comme les calculs proprement dit sont tous controlés en parallèle par $2^{cn}\log^2\sigma$ et en séquentiel par $\sigma^{2^{cn}}$, on obtient finalement:

$D(STURM(n,\sigma)) \leq 2^{cn}\log^2\sigma + D(INVERSE(n-1,4\sigma^2)) + D(SIGNE(n-1,4\sigma^2))$

$L(STURM(n,\sigma)) \leq \sigma^{2^{cn}} + \sigma(L(INVERSE(n-1,4\sigma^2)) + L(SIGNE(n-1,4\sigma^2)))$

e- Algorithme SIGNE:

$P \in \mathbb{Q}[X_1,\ldots,X_n]$, $B_i \in \mathbb{Z}[X]$ $(1\leq i\leq n)$, $\sigma(P) \leq \sigma$, $\sigma(B_i) \leq \sigma$ $(1\leq i\leq n)$

En suivant pas a pas l'algorithme SIGNE et les complexités obtenues pour les algorithmes précédents, on a:

$$D(STURM(B_n^*, \frac{\partial^{B_n^*}}{\partial X} \cdot \prod_{Q\in\mathcal{J}} Q)) \leq 2^{cn}\log^2(\sigma^{cn}) + D(INVERSE(n-1,\sigma^2)) +$$

$$+ D(SIGNE(n-1,\sigma^2)) + D(\frac{\partial^{B_n^*}}{\partial X} \cdot \prod_{Q\in\mathcal{J}} Q)) \leq$$

$$\leq 2^{cn}\log^2\sigma + D(INVERSE(n-1,\sigma^2)) + D(SIGNE(n-1,\sigma^2)) + D(SIGNE(n-1,4\sigma^2)) \leq$$

$$\leq 2^{cn}\log^2\sigma + \sum_{2\leq k\leq n-1} D(SIGNE(n-k,\sigma^{2^{cn}})) + 2D(SIGNE(n-1,4\sigma^2))$$

Et de la même manière:

$$L(STURM(B_n^*, \frac{\partial^{B_n^*}}{\partial X} \prod_{Q\in\mathcal{J}} Q)) \leq \sigma^{2^{cn}} + \sigma^{2^{cn}} \sum_{2\leq k\leq n-1} L(SIGNE(n-k,\sigma^{2^{cn}})) +$$

$$+ 2L(SIGNE(n-1,4\sigma^2))$$

Pour compléter l'algorithme SIGNE, il faut appliquer les résultats de [6] Dans ce travail les auteurs réduisent le problème de résoudre des systèmes d'équations d'ordre 2^σ (qui est pour nous trop cher) a la résolution de systèmes non-homogènes d'ordre σ^2 en $\log(\sigma)$ étapes consécutives. Dans la première étape, on a σ systèmes, dans la seconde $\sigma/2$ et ainsi successivement jusqu'a la derniere étape de $\sigma/2^{[\log\sigma]}$ systèmes. De plus, il faut ajouter le travail qu'implique calculer le signe des coefficients directeurs des restes R_k , pour obtenir le nombre de variations de signe mentionné en B-b) .

De cette manière, on obtient:

$$D(SIGNE(n,\sigma)) \leq 2^{cn}\log^2\sigma + \sum_{2\leq k\leq n-1} D(SIGNE(n-k,\sigma^{2^{cn}})) + 2D(SIGNE(n-1,4\sigma^2)) +$$

$$+ D(SIGNE(n-1,\sigma^{2^{cn}})) + \log(\sigma).\log^3\sigma \ ,$$

et par une borne grossière:

$$D(SIGNE(n,\sigma)) \leq 2^{cn}\log^3\sigma + 3 \sum_{1\leq k\leq n-1} D(SIGNE(n-k,\sigma^{2^{cn}})) <$$

$$\leq 2^{cn}\log^3\sigma + 3.2^{c(n-1)}\log^3(\sigma^{2^{cn}}) + 3.4.2^{c(n-2)}\log^3(\sigma^{2^{2cn}}) + \ldots$$

$$\ldots + 3.4^{n-2}.2^{c}\log^3(\sigma^{2^{cn^2}}) + 3.4^{n-2} D(SIGNE(1,\sigma^{2^{cn^2}}))$$

C'est-à-dire:

$$D(SIGNE(n,\sigma)) \leq 2^{cn^2}\log^3\sigma \ .$$

Analoguement, on prouve:

$$L(SIGNE(n,\sigma)) \leq \sigma^{2^{cn^2}} \ .$$

Observation: Nous n'avons pas compté dans ces résultats le coût de l'algorithme SIMPLE, qui est totalement négligeable face aux coûts des autres algorithmes (sachant que calculer des PGDC et des PPMC de familles de N polynômes, de degré $\leq N$, coûte $O(\log^2 N)$ en parallèle et $N^{O(1)}$ en séquentiel [26])

iv) Calcul final des complexités:

Pour compléter l'algorithme "élimination de quantificateurs" il faut évaluer le signe que prennent les polynômes de $\mathbb{P}_\Phi$ sur le système de représentants (donné par $I(\nu_1) \times \ldots \times I(\nu_r) \times I(B_1) \times \ldots \times I(B_s)$, où $r+s=n$ et $I(P)$ désigne l'ensemble des racines réelles de $P \in \mathbb{R}[X]$, qui est constitué d'au plus $(\sigma(\Phi)^{2^{cn^2}})^n$ points, c'est-à-dire $\sigma(\Phi)^{2^{cn^2}}$ points.

Comme $\sigma(\mathbb{P}_\Phi) \leq \sigma(\Phi)^{2^{cn^2}}$, et les mêmes bornes valent aussi pour $\sigma(\nu_i)$, $(1 \leq i \leq r)$, et $\sigma(B_i)$, $1 \leq i \leq s$, on applique ces données a l'algorithme SIGNE (pour les au plus $\sigma(\Phi)^{2^{cn^2}}$ polynômes qui apparaissent dans $\mathbb{P}_\Phi$)

On obtient par conséquent:

$$D(\text{"élimination de quantificateurs"}) \leq D(\mathbb{P}_\Phi) + D(B_s) + D(\text{SIGNE}(n,\sigma(\Phi)^{2^{cn^2}})) \leq$$
$$\leq 2^{cn}\log^2\sigma(\Phi) + 2^{cn^2}\log^2\sigma(\Phi) + 2^{cn^2}\log^3\sigma(\Phi)^{2^{cn^2}} \leq$$
$$\leq 2^{cn^2}\log^3\sigma(\Phi)$$

Et similairement:

$$L(\text{"élimination de quantificateurs"}) < L(\mathbb{P}_\Phi) + L(\{\nu_1,\ldots,\nu_s,B_1,\ldots,B_s\}) +$$
$$+ \sigma(\Phi)^{2^{cn^2}} L(\text{SIGNE}(n,\sigma(\Phi)^{2^{cn^2}}) \leq$$
$$\leq \sigma(\Phi)^{2^{cn^2}}.$$

2) Bornes supérieures pour l'élimination de quantificateurs dans la théorie élémentaire des corps algébraiquement clos:

La démonstration suit les lignes générales des processus d'élimination de quantificateurs [29] et [11] ; mais comme ces algorithmes ne donnent pas les résultats désirés en parallèle, on est obligé d'en changer des points essentiels. Comme résultat immédiat, on obtient un nouvel algorithme rapide en séquentiel pour les corps algébriquement clos

de caractéristique arbitraire.

Soit $\Phi \in L$ une formule arbitraire, prénexe, contenant les variables $X_1,\ldots,X_n$ où $X_1,\ldots,X_{n-m}$ sont libres et $X_{n-m+1},\ldots,X_n$ sont liées. Φ est de la forme:

$$(Q_{n-m+1}\, X_{n-m+1})\ldots(Q_n X_n)\, \Psi(X_1,\ldots,X_n)$$

où $Q_{n-m+1},\ldots,Q_n \in \{\forall,\exists\}$ et $\Psi(X_1,\ldots,X_n)$ est une formule libre de quantificateurs, qui est une combinaison booléenne des formules atomiques contenant des polynômes, disons $F_1,\ldots,F_s \in k[X_1,\ldots,X_n]$ avec $\sigma := \sigma(\Phi) = \sum_{1\leq i\leq s}(2 + \deg(F_i))$

Comme dans [29], nous dirons que $Z \subseteq k^n$ est une $F_1,\ldots,F_s$-cellule si Z est non-vide et s'il existe $\mathcal{M} \subseteq \{1,\ldots,s\}$ tel que

$$Z = \{x \in k^n / \; F_i(x) = 0 \;\; \forall\, i \in \mathcal{M} \text{ et } F_j(x) \neq 0 \;\; \forall j \in \{1,\ldots,s\} - \mathcal{M}\}$$

Considérant que le quantificateur $\forall$ peut être reécrit comme $\neg\exists\neg$, nous pouvons supposer que le dernier bloc de quantificateurs (qui est le premier à éliminer) est existentiel.

Le premier pas de notre algorithme consiste à reécrire la formule $\Psi(X_1,\ldots,X_n)$ de la manière suivante:

$$\bigvee_{\mathcal{M} \subset \{1,\ldots,s\}} \; \bigwedge_{i \in \mathcal{M}} F_i = 0 \;\wedge\; \bigwedge_{j \in \{1,\ldots,s\}-\mathcal{M}} F_j \neq 0$$

définit une

$F_1,\ldots,F_s$-cellule.

Ceci est possible parce que les $F_1,\ldots,F_s$-cellules sont les atomes de l'algèbre de Boole des sous-ensembles de k^n définis par des formules sans quantificateurs composées des polynômes $F_1,\ldots,F_s \in k[X_1,\ldots,X_n]$.

A cette fin, nous construisons un réseau de profondeur $O(n^{O(n)}\log^3\sigma)$ avec $O(\sigma^{n^{O(n)}})$ noeuds, qui énumère les $F_1,\ldots,F_s$-cellules. Ceci est possible en utilisant [29] et [31]. Dans le cas de char(k) = 0, on peut remplacer [31] par [10], et on obtient un réseau de profondeur $O(n^2\log^3\sigma)$ avec $O(\sigma^{O(n^2)})$ noeuds. La construction du réseau suit les lignes générales de [6]. La différence la plus importante est que nous travaillons ici avec des polynômes en plusieurs variables, et non avec des polynômes en une seule variable. Nous utilisons la stratégie de "diviser et régner" de [6], en vérifiant à chaque étape si les sous-ensembles de k^n qui vérifient les conjonctions construites sont vides ou non.

Nous formons un arbre binaire de profondeur log s : dans l'étape 0 nous déterminons lesquels des sous-ensembles de k^n, qui correspondent à $F_i = 0$ ou $F_i \neq 0$ $(1 \leq i \leq s)$ sont non-vides; dans l'étape suivante nous construisons les s/2 ensembles de conjonctions consistantes du type:
$\{F_1=0 \wedge F_2=0,\ F_1=0 \wedge F_2\neq 0,\ F_1\neq 0 \wedge F_2=0,\ F_1\neq 0 \wedge F_2\neq 0\}, \ldots,$
$\{F_{s-1}=0 \wedge F_s=0,\ F_{s-1}=0 \wedge F_s\neq 0,\ F_{s-1}\neq 0 \wedge F_s=0,\ F_{s-1}\neq 0 \wedge F_s\neq 0\}$;
dans l'étape j, $0 \leq j \leq \log s$, nous construisons les $s/2^j$ ensembles adjacents de l'étape j-1.

De cette manière, nous obtenons un arbre du type suivant:

étape 0: $\{F_1=0,\ F_1\neq 0\}$ $\{F_2=0,\ F_2\neq 0\}$ $\cdots$ $\{F_s=0,\ F_s\neq 0\}$

étape 1: $\{F_1=0 \wedge F_2=0, \ldots,$ $F_1\neq 0 \wedge F_2\neq 0\}$

étape 2:

étape log s: $\{\bigwedge_{i\in\mathcal{M}} F_i=0 \wedge \bigwedge_{j\in\{1,\ldots,s\}-\mathcal{M}} F_j\neq 0$; définit une $F_1,\ldots,F_s$-cellule$\}$

Dans l'étape j, on construit $\leq s/2^j$ ensembles; chacun d'eux consiste en différentes conjonctions qui sont composeés de $\leq 2^j$ polynômes dont la somme des degrés est controlée par σ.

Ces conjonctions sont consistantes et, comme nous avons déjà mentionné, formées à partir de conjonctions consistantes adjacentes de l'étape j-1. Cela implique qu'on a affaire à seulement σ^n conjonctions à l'étape j (voir [29], Corollary 1), ce qui conduit à $(s/2^j).\sigma^{2n}$ tests de consistance à l'étape j. Au total, on a créé un arbre de profondeur log s avec 2.s noeuds, en utilisant à chaque étape $0 \leq j \leq \log s$, $(s/2^j).\sigma^{2n}$ tests de consistance qu'on peut exécuter simultanément (cela nous ramène en somme à $2.s\ \sigma^{2n}$ tests) l'algorithme est complet si nous expliquons maintenant comment on effectue un test de consistance pour une conjonction, disons $F_1=0 \wedge \ldots \wedge F_r=0 \wedge F_{r+1}\neq 0 \wedge \ldots \wedge \ldots \wedge F_s \neq 0$.

Nous utilisons le "truc de Rabinowitsch", qui est bien connu: posons $F := F_{r+1}\cdot F_{r+2}\cdots F_s$. Soit T une nouvelle variable; selon le Théorème des Zéros de Hilbert, $F_1=0 \wedge \ldots \wedge F_r=0 \wedge F_{r+1}\neq 0 \wedge \ldots \wedge F_s\neq 0$ est inconsistant si et

seulement si l'idéal engendré par $F_1,\ldots,F_r$, 1-T.F. dans $k[X_1,\ldots,X_n,T]$ est trivial, c'est à dire si $1 \in (F_1,\ldots,F_r,\ 1\text{-T.F})$.

Dans le cas où char(k) est arbitraire, nous nous servons de la version effective du Théoreme des Zéros [31], dans le cas où char(k)=0, nous avons des meilleures bornes [10]. Considérons par exemple ce dernier cas, on a:

$$1 \in (F_1,\ldots,F_r,\ 1\text{-T.F}) \Leftrightarrow \exists P_1,\ldots,P_r,\ P \in k[X_1,\ldots,X_n,\ T]\ /$$

$$\deg(P_i) \leq 3n\sigma^n (1 \leq i \leq r),\ \deg(P) \leq 3n\sigma^{n+1} \text{ et } 1 = P_1F_1+\ldots+P_rF_r+P(1-T.F)$$

Le problème se réduit donc a résoudre un système linéaire non-homogène d'équations, d'ordre $\sigma^{cn^2} \times \sigma^{cn^2}$ ($c>0$, constante) dont les coefficients proviennent des coefficients de $F_1,\ldots,F_r$ et 1-T.F.

C'est à dire on a à comparer le rang de deux matrices d'ordre controlé par σ^{cn^2} sur k : cela nous ramène au problème de calculer le rang d'une matrice avec un algorithme rapide en parallèle et en séquentiel, nous suivons le traitement de [38], on pourrait aussi suivre [12].

En introduisant une nouvelle variable Z, on transforme la matrice donnée en une matrice carrée, et nous calculons son polynôme charactéristique (les coefficients du polynôme charactéristique dans $k[Z]$ s'obtiennent en temps parallèle $O(n^2 \log^2\sigma)$ et en temps séquentiel $O(\sigma^{O(n^2)})$ grâce à [7]). La multiplicité de la racine 0 dans le polynôme charactéristique donne le rang de la matrice du départ. On élimine la variable Z artificiellement introduite en évaluant les coefficients du polynôme charactéristique qui sont des polynômes de degré σ^{cn^2} en Z en σ^{cn^2} points de k (ce qui est possible car k est infini).

Il est évident que la profondeur de l'algorithme donné ne dépend essentiellement que de log(s) et de la profondeur des algorithmes qui calcu-

lent le rang d'une matrice (si char(k) = 0, d'ordre $\sigma^{cn^2} \times \sigma^{cn^2}$).

Le nombre de processeurs utilisé est essentiellement controlé par le nombre de $F_1,\ldots,F_s$-cellules ($\leq \sigma^n$), indépendemment des coefficients de $F_1,\ldots,F_s$.

Par conséquent, une fois les $F_1,\ldots,F_s$-cellules énumérées, $\Psi(X_1,\ldots X_n)$ peut être réécrit de la manière désirée.

Puisque les quantificateurs existentiels et les disjonctions peuvent s'interchanger, nous sommes ramenés à caractériser des ensembles du type:

$$(\exists X_\ell)\ldots(\exists X_n)\ (F_1=0 \wedge \ldots \wedge F_r=0 \wedge F_{r+1}\neq 0 \wedge \ldots \wedge F_s\neq 0)$$

(où $\ell \geq n-m+1$ indique la longueur du dernier bloc de quantificateurs, qui peut être supposé existentiel, par l'observation faite précédemment).

Nous cherchons donc à déterminer, par des formules sans quantificateurs, des projections d'ensembles localement fermés, dans la topologie de Zariski de k^n.

Soit $D:= \{x\in k^{\ell-1};\ k\models(\exists X_\ell)\ldots(\exists X_n)\ F_1(x, X_\ell,\ldots,X_n)=0 \wedge \ldots$

$\ldots\wedge F_r(x, X_\ell,\ldots,X_n)=0 \wedge F_{r+1}(x, X_\ell,\ldots,X_n)\neq 0 \wedge \ldots \wedge F_s(x, X_\ell,\ldots,X_n)\neq 0\}$

On a à trouver des polynômes $G_1,\ldots,G_t\in k[X_1,\ldots,X_{\ell-1}]$ qui décrivent D par une formule sans quantificateurs.

Soit $E:= k^{\ell-1} - D$, $F:= F_{r+1}\cdot F_{r+2}\ldots F_s$ et T une nouvelle variable. Par le Théoreme des Zéros, on a:

$$E = \{x\in k^{\ell-1} / 1\in (F_1(x,X_\ell,\ldots,X_n),\ldots,F_r(x,X_\ell,\ldots,X_n),\ 1-T.F(x,X_\ell,\ldots,X_n))\}$$

Considérons $F_1,\ldots,F_r$, 1-T.F comme polynômes en $X_\ell,\ldots,X_n,T$, à coefficients dans $k[X_1,\ldots,X_{\ell-1}]$, et supposons comme avant que char(k)=0 afin de pouvoir utiliser les bornes de [10]. Pour un instant, remplaçons $(X_1,\ldots,X_{\ell-1})$ par $x\in k^{\ell-1}$, on a alors:

$$1\in (F_1(x,X_\ell,\ldots,X_n),\ldots,F_r(x,X_\ell,\ldots,X_n),\ 1-T.F(x,X_\ell,\ldots,X_n)) \Leftrightarrow$$

$$\exists P_1,\ldots,P_r,P\in k[X_\ell,\ldots,X_n,T] \ /\ \deg(P_i)\leq 3(n-\ell+2)\sigma^{(n-\ell+2)+1}\ (1\leq i\leq r),$$

$$\deg P< 3(n-\ell+2)\sigma^{(n-\ell+2)+1} \text{ et } 1 = P_1F_1(x,X_\ell,\ldots,X_n)+\ldots+P_rF_r(x,X_\ell,\ldots,X_n)+$$

$$+ P(1-T.F(x,X_\ell,\ldots,X_n))$$

Comparons les coefficients en $X_\ell,\ldots,X_n,T$ en tenant compte des bornes des degrés de $P_1,\ldots,P_r,P$ et aussi du fait que $F_1,\ldots,F_r,1-T.F$ sont considérés comme polynômes en $X_\ell,\ldots,X_n,T$ à coefficients dans $k[X_1,\ldots,X_{\ell-1}]$: on est ramené à résoudre un certain système linéaire non-homogène d'équations, c'est à dire a décrire un ensemble du type:

$$\{x\in k^{\ell-1};\ \sum_{1\leq j\leq p} F_{kj}(x)\ T_\ell = F_{k,p+1}(x)\ (1\leq k\leq q) \text{ a une solution dans } k^p\}$$

par une expression sans quantificateurs en polynômes $G_1,\ldots,G_t\in k[X_1,\ldots,X_{\ell-1}]$ (où les $T_1,\ldots,T_p$ sont des nouvelles variables décrivant les inconnues du système, et, toujours en supposant char(k)=0 et grâce à [10], $q,p\leq \sigma^{c(n-\ell+2)^2}$, ($c > 0$, constante)).

Dans [29], Lemma 9, un nombre suffisemment grand d'algorithmes de Gauss (dans le sens de [3] ou [23]) est énuméré afin d'épuiser toutes les possibilités indépendantes de résoudre ce système non-homogène d'équations linéaires, après substitution de points "typiques" de $k^{\ell-1}$ par des variables dans les polynômes F_{kj}. Ce processus, intrinsèquement séquentiel, ne peut être appliqué ici. Nous utilisons à nouveau l'algorithme de [38], essentiellement de la même manière qu'avant, qui permet d'exhiber des conditions polynômiales nécessaires et suffisantes sur $x\in k^{\ell-1}$ pour l'égalité des rangs de $(F_{kj}(x))_{\substack{1\leq k\leq q\\ 1\leq j\leq p}}$ et de $(F_{kj}(x))_{\substack{1\leq k\leq q\\ 1\leq j\leq p+1}}$

Dans ce but, nous considérons les matrices (génériques):

$$(F_{kj}(X_1,\ldots,X_{\ell-1}))_{\substack{1\leq k\leq q\\ 1\leq j\leq p}} \quad \text{et} \quad (F_{kj}(X_1,\ldots,X_{\ell-1}))_{\substack{1\leq k\leq q\\ 1\leq j\leq p+1}}$$

et comme avant, il faut obtenir la multiplicité de la racine 0 dans les polynômes caractéristiques des matrices obtenues par le processus de [38] (en ajoutant à nouveau une variable auxiliaire Z qu'on élimine ensuite). Les coefficients des polynômes obtenus sont les G_i cherchés. Décrire les conditions pour la multiplicité de 0 (c'est-à-dire les conditions pour la résolubilité du système en question) se fait simultanément en imposant des conditions booléennes sur les G_i.

En tenant compte du fait que $\ell\geq n-m+1$, calculer $G_1,\ldots,G_t$ coûte $O(m^2\log^2\sigma)$ en parallèle et $O(\sigma^{cm^2(n-m)})$ en séquentiel. De plus, on a:

$$\sum_{1\leq i\leq t} \deg(G_i)\leq \sigma^{cm^2}.$$

Comme il faut énumérer toutes les conditions sur les G_i, la complexité séquentielle de ce processus est $O(\sigma^{cm^2})$. Cela veut dire qu'on peut éliminer un bloc de quantificateurs existentiels devant une conjonction en temps parallèle $O(m^2\log^2\sigma)$ et en temps séquentiel $O(\sigma^{cm^2(n-m)})$ en charactéristique 0; si char(k) est arbitraire, on obtient les bornes: $O(n^{cm}\log^2\sigma)$ en parallèle et $O(\sigma^{n^{cm}})$ en séquentiel ($\sum_{1\leq i\leq t} \deg(G_i) \leq \sigma^{2cm}$)

Les bornes générales annoncées dans les théorèmes 2 et 3 pour l'élimination de quantificateurs dans la théorie élémentaire des corps algébriquement clos suivent en répétant ce processus bloc de quantificateurs par bloc de quantificateurs (r au total).

3) Bornes inférieures pour l'élimination des quantificateurs dans la théorie élémentaire des corps réel et algébriquement clos.

La démonstration du Théorème 4 diffère selon le cas $k = \mathbb{R}$ où k algébriquement clos de charactéristique arbitraire. Elle est basée sur les formules données en [19] et [29] qui impliquent d'une manière assez directe les bornes inférieures mentionnées pour le cas de la complexité séquentielle. Nous traitons ici seulement les bornes inférieures pour la complexité parallèle.

Commençons par le cas $k = \mathbb{R}$.

Dans [19], Proposition 2 on construit une succession de formules $\Psi_k(X,Y) \in L$, $k = 0,1,\ldots$ dans les variables libres X,Y avec les propriétés suivantes:

i) Ψ_k ne contient que des polynômes à coefficients dans $\mathbb{Q}$.
ii) $|\Psi_k| = O(k)$
iii) Ψ_k contient 6k quantificateurs
iv) Ψ_k définit l'ensemble fini $M_k := \{(\cos \frac{2\pi j}{2^{2^{k+1}}}, \sin \frac{2\pi j}{2^{2^{k+1}}});$ $j=0,\ldots,2^{2^{k+1}}-1\}$

Notons que M_k est un sous-ensemble semialgébrique de $\mathbb{R}^2$ composé de $2^{2^{k+1}}$ points isolés a coordonnées réelles et algébriques.

Soit $\Theta \in L$ une formule sans quantificateurs équivalente à Ψ_k. Par (i), Θ est composée de polynômes $F_1,\ldots,F_s \in \mathbb{Q}[X,Y]$. En particulier Θ définit M_k (comparer (iv)). Nous verrons qu'il existe j, $1 \leq j \leq s$ tel que deg $F_j \geq 2^{2^{k+1}-3}$. Cela implique que n'importe quelle imprimante qui travaille au parallèle et qui écrit Θ contient un reséau arithmétique de profondeur $2^{k+1}-3$ parce qu'elle doit évaluer F_j [25]

En appliquant a Θ des transformations booléennes sans changer $F_1,\ldots,F_s$ nous pouvons supposer que Θ est une disjonction d'expressions consistantes du type

$$(*) F_{i_1} = 0 \wedge \ldots F_{i_m} = 0 \wedge F_{i_{m+1}} > 0 \wedge \ldots F_{i_r} > 0 \wedge F_{i_{r+1}} \neq 0 \wedge \ldots \wedge F_{i_s} \neq 0$$

où, en principe, m = 0 n'est pas exclu (voir [19]).

Soit $(x_0,y_0) := (\cos \frac{2\pi}{2^{2^{k+1}}}, \sin \frac{2\pi}{2^{2^{k+1}}})$. Comme $(x_0,y_0) \in M_k$, il existe une conjonction (*) qui est satisfaite par (x_0,y_0). Puisque (x_0,y_0) est un point isolé de M_k on a $m \geq 1$ et en particulier $F_{i_1}(x_0,y_0) = \ldots = F_{i_m}(x_0,y_0) = 0$.

Pour le moment soit $F \in \mathbb{Q}[X,Y]$ n'importe quel polynôme avec $F(x_0,y_0)=0$. Nous allons démontrer que F s'annulle sur le cercle unité $S^1(\mathbb{R}) := \{(x,y) \in R^2; x^2+y^2-1 = 0\}$ ou, sinon, deg $(F) \geq 2^{2^{k+1}-3}$. Cela impliquera qu'il existe un $j \in \{i_1,\ldots,i_m\}$ tel que $\deg(F_j) \geq 2^{2^{k+1}-3}$. Autrement $F_{i_1},\ldots,F_{i_m}$ s'annullent tous sur $S^1(\mathbb{R})$ ce qui contredit le fait que (*) est consistant et que (x_0,y_0) est un point isolé de M_k.

Nous écrivons F sous la forme $F = \sum_{i,j} \alpha_{ij} X^i Y^{2j} + Y \sum_{k,\ell} \beta_{k\ell} X^k Y^{2\ell}$ avec $\alpha_{ij}, \beta_{k\ell} \in \mathbb{Q}$. Soit $\bar{F} := \sum_{i,j} \alpha_{ij} X^i Y^{2j} - Y \sum_{k,\ell} \beta_{k\ell} X^k Y^{2\ell}$.

On a $F\bar{F} = (\sum_{i,j} \alpha_{ij} X^i Y^{2j})^2 - Y^2 (\sum_{k,\ell} \beta_{k\ell} X^k Y^{2\ell})^2$.

Substituant dans cette expression pour $F\bar{F}$, le monôme Y^2 par $1-X^2$ nous obtenons le polynôme

$$G := (\sum_{i,j} \alpha_{ij} X^i (1-X^2)^j)^2 - (1-X^2)(\sum_{k,\ell} \beta_{k\ell} X^k (1-X^2)^\ell)^2 \in \mathbb{Q}[X]$$

Nous avons G = 0 ou $G \neq 0$.

Supposons $G = 0$. Alors on a $F(x,y)\,\bar{F}(x,y) = 0$ pour tout $(x,y) \in S^1(\mathbb{C}) := \{(x,y)\in\mathbb{C}^2;\ x^2+y^2-1=0\}$.

Comme $S^1(\mathbb{C})$ est une hypersurface algébrique irréductible de $\mathbb{C}^2$ avec polynôme minimal X^2+Y^2-1, X^2+Y^2-1 divise F ou $\bar{F}$. Dans le premier cas F s'annulle sur tout $S^1(\mathbb{R}) \subseteq S^1(\mathbb{C})$. Dans le second cas on a $0 = \bar{F}(x,y) = F(x,-y)$ pour tout $(x,y)\in S^1(\mathbb{C})$. Cela implique aussi que F s'annulle sur tout $S^1(\mathbb{R})$.

Supposons maintenant $G \neq 0$. Nous allons prouver $\deg(F) \geq 2^{2^{k+1}-3}$ ce qui conclut notre démonstration.

Rappelons: $(x_0,y_0) = (\cos 2\pi/2^{2^{k+1}}, \sin 2\pi/2^{2^{k+1}})$.

En particulier $e^{2\pi i/2^{2^{k+1}}} = \cos 2\pi/2^{2^{k+1}} + i \sin 2\pi/2^{2^{k+1}} = x_0 + iy_0 \in \mathbb{C}$

et $\cos 2\pi/2^{2^{k+1}} = \dfrac{e^{2\pi i/2^{2^{k+1}}} + e^{-2\pi i/2^{2^{k+1}}}}{2}$.

Par hypothèse $0 = F(x_0,y_0) = F(\cos 2\pi/2^{2^{k+1}}, \sin 2\pi/2^{2^{k+1}})$, donc $G(\cos 2\pi/2^{2^{k+1}}) = F(\cos 2\pi/2^{2^{k+1}}, \sin 2\pi/2^{2^{k+1}})\cdot \bar{F}(\cos 2\pi/2^{2^{k+1}}, \sin 2\pi/2^{2^{k+1}}) = 0$.

Considérons les extensions de corps:

$$\mathbb{Q} \subseteq \mathbb{Q}(\cos 2\pi/2^{2^{k+1}}) \subseteq \mathbb{Q}(e^{2\pi i/2^{2^{k+1}}})$$

$$T^2 + (e^{2\pi i/2^{2^{k+1}}} + e^{-2\pi i/2^{2^{k+1}}})\,T + e^{2\pi i/2^{2^{k+1}}} \cdot e^{-2\pi i/2^{2^{k+1}}} =$$

$$T^2 + 2\cos 2\pi/2^{2^{k+1}}\,T + 1 \in \mathbb{Q}(\cos 2\pi/2^{2^{k+1}})[T],$$ (où T est une nouvelle indéterminée) est le polynôme minimal de $e^{2\pi i/2^{2^{k+1}}}$ sur $\mathbb{Q}(\cos 2\pi i/2^{2^{k+1}})$

On a donc $2^{2^{k+1}-1} = \left[\mathbb{Q}(e^{2\pi i/2^{2^{k+1}}}) : \mathbb{Q}\right] = \left[\mathbb{Q}(e^{2\pi i/2^{2^{k+1}}}) : \mathbb{Q}(\cos 2\pi/2^{2^{k+1}})\right] \cdot \left[\mathbb{Q}(\cos 2\pi/2^{2^{k+1}}) : \mathbb{Q}\right] = 2\left[\mathbb{Q}(\cos 2\pi/2^{2^{k+1}}) : \mathbb{Q}\right]$, ce qui implique :

$$\left[\mathbb{Q}(\cos 2\pi/2^{2^{k+1}}) : \mathbb{Q}\right] = 2^{2^{k+1}-2}$$

Comme par hypothèse $G \neq 0$ et $G(\cos 2\pi/2^{2^{k+1}}) = 0$ on obtient $\deg(G) \geq 2^{2^{k+1}-2}$

Finalement on a $2^{2^{k+1}-2} \leq \deg G \leq \deg F + \deg \bar{F} = 2 \deg F$, ce qui implique: $\deg F \geq 2^{2^{k+1}-3}$.

Maintenant soit k algébriquement clos. Soit Ω le corps premier de k.

Dans [29] on construit une sucession de formules $\Phi_k(X,Y) \in L, k=0,1\ldots$ dans les deux variables libres X et Y avec les propriétés suivantes:

(i) $|\Phi_k| = O(k)$

(ii) Φ_k définit le graphe de l'application $k \to k$ qui applique $x \in k$ sur $x^{2^{2^k}}$, c'est-à-dire l'ensemble:

$$M_k := \{X^{2^{2^k}} - Y = 0\} := \{(x,y) \in k^2 / x^{2^{2^k}} = y\}$$

Soit $\Theta \in L$ une formule sans quantificateurs contenant les polynômes $F_1,\ldots,F_s \in \Omega[X,Y]$, et soient $G_1,\ldots,G_t$ les facteurs premiers de $F_1,\ldots,F_s$ dans $k[X,Y]$: on a $\max\{\deg F_j;\ 1 \leq j \leq s\} \geq \max\{\deg G_i;\ 1 \leq i \leq t\}$. Il suffit alors de démontrer qu'il existe un i, $1 \leq i \leq t$ tel que $\deg G_i \geq 2^{2^k}$. Ensuite, on conclut comme dans le cas réel clos, en utilisant [25].

On transforme $\Theta \in L$ en une formule $\tilde{\Theta}$ du langage $\tilde{L}$ avec les symboles non logiques $\{a;\ a \in k\} \cup \{+, -, ., =\}$, en remplaçant chaque formule atomique $F_j = 0$, où $F_j = G_{i_1}^{r_1} \ldots G_{i_m}^{r_m}$, $(i_1,\ldots,i_m \in \{1,\ldots,t\}$, $r_1,\ldots,r_m \in \mathbb{N})$, par l'expression $G_{i_1} = 0 \vee \ldots \vee G_{i_n} = 0$.

Par conséquent, $\tilde{\Theta}$ est composée de polynômes <u>premiers</u> sur k: $G_1,\ldots, G_t$.

De plus, nous supposons que $\tilde{\Theta}$ est une disjonction d'expressions <u>consistantes</u>:

$$(*)\quad G_{i_1} = 0 \wedge \ldots \wedge G_{i_\ell} = 0 \wedge G_{i_{\ell+1}} \neq 0 \wedge \ldots \wedge G_{i_t} \neq 0$$

(où apparaissent tous les G_i $(1 \leq i \leq t)$. (En principe, on ne peut pas exclure $\ell = 0$).

$\tilde{\Theta}$ est une formule sans quantificateurs dans les deux variables libres, X,Y, équivalente à Θ, et, par conséquent, a Φ_k.

Alors $\tilde{\Theta}$ définit le sous-ensemble $M_k = \{X^{2^{2^k}} - Y = 0\}$ de k^2, fermé dans la topologie de Zariski.

M_k est une union d'ensembles définis par des conjonctions (*). Comme $\bar{M}_k = M_k \neq k^2$ et les ouverts sont denses dans k^2, on a $\ell \geq 1$ dans chacune des conjonctions consistantes (*).

En tenant compte du fait que dans (*), $G_{i_1}, \ldots, G_{i_\ell}$ sont des polynômes premiers et différents, on a, par le théorème de la dimension ([32], II, 7, Th.11), que (*) définit un ensemble fini dans le cas $\ell \geq 2$. Alors M_k s'écrit comme union d'ensembles définis par des conjonctions (*), avec $\ell = 1$ et des ensembles finis.

Considérons une conjonction (*) avec $\ell = 1$, qui apparait dans $\tilde{\Theta}$.

Comme G_{i_1} est premier et (*) est consistant, la fermeture de l'ensemble défini par (*) est $\{G_{i_1} = 0\}$. Puisque d'autre part $\bar{M}_k = M_k$, M_k peut s'écrire comme union d'ensembles de la forme $\{G_{i_1} = 0\}$ et d'ensembles finis.

Mais M_k est le graphe de $\{X^{2^{2^k}} - Y = 0\}$, donc un ensemble irréductible, et $X^{2^{2^k}} - Y$ est un polynôme premier dans $k[X,Y]$. C'est-à-dire que $X^{2^{2^k}} - Y$ est l'équation minimale de l'hypersurface irréductible M_k de k^2.

Nous savons donc que M_k est irréductible et infini, et que les ensembles $\{G_i = 0\}$ et les ensembles finis apparaissant dans la décomposition de M_k sont fermés. Il existe alors un $i_1 \in \{1,\ldots,t\}$ tel que $\{X^{2^{2^k}} - Y = 0\} = M_k = \{G_{i_1} = 0\}$. Comme $X^{2^{2^k}} - Y$ est l'équation minimale de M_k, $X^{2^{2^k}} - Y$ divise G_{i_1}, par conséquent $\deg G_{i_1} \geq 2^{2^{2^k}}$.

Il faut dire encore un mot sur la démonstration du théorème 5: en principe, ce théorème s'obtient des bornes inférieures pour l'élimination de quantificateurs sur $\mathbb{R}$, car l'élimination de quantificateurs est une conséquence facile (sans croissance de complexité) de la décomposition algébrique cylindrique (voir[19]). On peut aussi procéder directement: la décomposition algébrique cylindrique de $\mathbb{R}^{6k+2}$ induite par $\psi_k \in L$ contient au moins 2^{2k+1} régions de dimension zéro dans $\mathbb{R}^2$ et en particulier la région formée par le point isolé $(\cos 2\pi/2^{2k+1}, \sin 2\pi/2^{2k+1}) \in \mathbb{R}^2$. Un

algorithme séquentiel pour la décomposition algébrique cylindrique de de $\mathbb{R}^{6k+2}$, où sont donnés les 8 k + 2 polynômes de degré ≤ 4 (qui apparaissent dans Ψ_k) doit imprimer les $2^{2^{k+1}}$ régions de dimension zéro de $\mathbb{R}^2$ du résultat. Il utilise donc un temps 2^{2k+1} pour ce processus, ce qui correspond a un temps $2^{2(n+4)/6}$, en termes de la dimension n:= 6 k + 2 de l'espace ambiant. Un algorithme qui fonctionne en parallèle doit imprimer une définition algébrique sur $\mathbb{Q}$ de la région de $\mathbb{R}^2$ formée par le point isolé $(\cos 2\pi/2^{2k+1}, \sin 2\pi/2^{2k+1})$ qui apparait dans la décomposition. Comme nous avons déja vu, cela implique nécessairement un polynôme de degre $\geq 2^{2k+1-3}$ sur $\mathbb{Q}$, qui s'évalue avec un réseau arithmétique de profondeur au moins $2^{k+1} - 3$, ou bien $2^{(n+4)/6} - 3$, en termes de la dimension n de l'espace ambiant ([25]).

Remerciements :

Une partie de ce travail a été réalisée pendant le séjour du co-auteur J. Heintz (Noaï Fitchas) à l'Université de Nice, au printemps 1987.

Celui-ci remercie chaleureusement l'Institut de Mathématique et Sciences Physiques de cette université pour l'appui reçu pendant cette période. Il aimerait aussi exprimer sa gratitude à l'Université de Strasbourg où il a séjourné au printemps 1986, et en particulier à M. Mignotte, qui, à travers son Séminaire sur les structures semi-algébriques, l'a fortement enthousiasmé sur le sujet, point de départ pour la réalisation de ce travail. D'autre part, les discussions extensives sur le parallélisme en géométrie avec Amparo López, de l'Université Autonome de Barcelone, J.H. Davenport, de l'Université de Bath, Angleterre, et M. Karpinski de l'Université de Bonn, ont été de grande importance pour clarifier les concepts concernant la complexité.

REFERENCES

[1] D.S. Arnon, On mechanical quantifier elimination for elementary algebra and geometry: Solution of a nontrivial problem; Proc. EUROCAL 85, Vol.2, Springer LN Comput. Sci. 204 (1985) 270-271.

[2] D.S. Arnon, S.F. Smith, Towards mechanical solutions of the Kahan ellipse problem I; Proc. EUROCAL 83, Springer LN Comput Sci. 162 (1983) 36-44.

[3] E.H. Bareiss, Sylvester's identity and multistep integer preserving Gaussian Elimination; Math. Comput. 22 (103) (1968) 565-578.

[4] P. Bayer and M. Stillman, On the complexity of computing syzygies; Preprint (1985).

[5] M. Ben-Or, D. Kozen, J. Reif, The complexity of elementary algebra and geometry. Proc. 16th. Ann. ACM Symp. Theory of Computing (1984) 457-464.

[6] M. Ben-Or, D. Kozen, J. Reif, The complexity of elementary algebra and geometry; J. of Comput. and System Sci. 32 (1986) 251-264.

[7] S. J. Berkowitz, On computing the determinant in small parallel time using a small number of processors; Information Processing Letters 18, 147-150, (1984).

[8] J. Bochnak, M. Coste, M.F. Roy, Géométrie algébrique réelle. A apparaitre dans"Ergebnisse der Mathematik und ihrer Grenzgebiete"; Springer Verlag, Berlin-Heidelberg (1987).

[9] W.S. Brown and J.F. Traub, On Euclid's algorithm and the theory of subresultants; J. Assoc. Comput. Mach. 18 (1971), 505-514.

[10] D. Brownawell, Bounds for the degrees in the Nullstellensatz; Preprint Princeton Univ. (1986).

[11] A.L. Chistov, D. Ju. Grigor'ev, Complexity of quantifier elimination in the theory of algebraically closed fields; Proc. 11th. Symp. Mathematical Foundations of Computer Science 1984, Springer LN in Comp. Sci. 176 (1984), 17-31.

[12] A.L. Chistov, Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic; Proc. Int. Conf. Foundat. of Comp. Theory 1985, Springer LN in Comp. Sci. 199 (1985) 63-69.

[13] A.L. Chistov, D.Ju. Grigor'ev, Subexponential-time solving systems of algebraic equations I, II; LOMI preprints E-9-83, E-10-83, Leningrad (1983)

[14] G.E. Collins, Quantifier elimination for real closed fields by cylindrical algebraical decomposition; Proc. 2nd. G.I. Conference Automata Theory and Formal Languages. Springer LN in Comp. Sci. 35 (1975) 134-183.

[15] G.E. Collins, Subresultants and reduced polynomial sequences. J. ACM 14 (1967), 128-142.

[16] M. Coste, M.F. Roy, Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets (Preprint Université de Rennes, 1986).

[17] M. Coste, M.F. Roy, La topologie du spectre réel; Contemporary Math., Ordered fields and Real Alg. Geom., AMS Vol 8 (1981) 27-60.

[18] L.Csanky, Fast parallel matrix inversion algorithms; SIAM J. Comp. 5, (1976) 618-623.

[19] J.H. Davenport, J. Heintz, Real quantifier elimination is doubly exponential. A apparaitre dans J. on Symbolic Comp., special issue 3/1 (1987).

[20] M. Demazure, Notes informelles de calcul formel, 3. Le monoïde de Mayr-Meyer, 4. Le théoreme de complexité de Mayr-Meyer; Prépublications Centre de Mathématiques de l'Ecole Polytechnique (1985).

[21] M. Demazure, Communication in "Journée sur aspects algorithmiques de la géométrie algébrique", Université Paris VII, U.E.R. de Mathématique et Informatique, 2-2-1987.

[22] M. Dickmann, Applications of model theory to real algebraic geometry. A survey; Springer LN Math. 1130 (1985) 76-150.

[23] J. Edmonds, Systems of distinct representatives and linear algebra; J. Res. Nat. Bur. Standards 71 B(4) (1967) 241-245.

[24] M.J. Fischer, M.O. Rabin, Super-exponential complexity of Presburger arithmetic; Complexity of Comp. ed. R.M. Karp., AMS (1974) 27-41.

[25] J. Von zur Gathen, Parallel arithmetic computations: a survey; Mathematical Foundations of Computer Science, 1986 13th. Proc. MFCS (1986).

[26] J. von zur Gathen, Parallel algorithms for algebraic problems; SIAM J. Comp. 13 (1984), 802-824.

[27] D.Ju Grigoriev, Complexity of deciding Tarski algebra; a apparaitre dans Journal on Symbolic Comp. Special issue 3/1 (1987).

[28] D.Ju Grigoriev, N.N. Vorobjov (Jr.), Solving Systems of polynomial inequalities in subexponential time; a apparaitre dans Journal of Symbolic Comput.

[29] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields; Theoret. Comput. Sci. 24 (1983), 239-277.

[30] J. Heintz, R. Wüthrich, An efficient quantifier elimination algorithm for algebraically closed fields, SIGSAM Bull. 9 (4) (1975) 11.

[31] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale; Math, Ann. 95 (1926) 736-788.

[32] S. Lang, Introduction to algebraic geometry; Interscience tracts in pure and applied mathematics (1958).

[33] S. Lang, Algebra; Addison-Wesley, Reading, MA. (1969).

[34] D. Lazard, Quantifier elimination: optimal solution for 2 classical examples; a apparaitre dans Journal on Symbolic Comp.

[35] E. Mayr, A. Meyer, The complexity of the word problem for commutative semigroups amd polynomial ideals; Advances in Math. 46 (1982) 305-329.

[36] M. Mignotte, Computer versus paper and pencil CALSYF 4 (1986) 63-69.

[37] L. Monk, Elementary recursive decision procedures; Ph. D. Thesis, Univ. of California, Berkeley (1974).

[38] K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field; Proc. 18th. Ann. ACM Symp. Theory of Computing (1986).

[39] J. Schwartz, M. Sharir, On the "piano movers" Problem I, The case of two-dimensional rigid polygonal body moving admist polygonal barriers; Comm. Pure Appl. Math. 36 (1983) 345-398.

[40] J. Schwartz, M. Sharir, On the "piano movers" Problem II, General techniques for computing topological properties of real algebraic manifolds; Adv. Appl. Math. 36 (1983) 298-351.

[41] R. Solovay, Communication personnelle, 1975.

[42] A. Tarski, A decision method for elementary algebra and geometry, 2nd. ed.; Univ. California Press, Berkeley (1951)

[43] V. Weispfenning, The complexity of linear problems in fields; a apparaitre dans Journal of Symbolic Comp.,Special issue 3/1 (1987)

[44] H.R. Wüthrich, Ein Entscheidungsverfahren für die Theorie der reell-abgeschlossenen Körper; Komplexität von Entscheidungsproblemen;Ein Seminar ed. E. Specker, V. Strassen. LN Comput. Sci. 43 (1976) 138-162.

CORPS ORDONNES DIFFERENTIELS

C. MICHAUX

A. Robinson fut le premier à introduire la notion de corps ordonné différentiel dans [1], en liaison avec l'étude des corps de Hardy. La théorie des modèles des corps ordonnés différentiels, qui sera le sujet de cet exposé, a été développée par M.F. Singer (voir [2] et [3]).

Un corps ordonné différentiel est un corps ordonné muni d'une dérivation. Dans le langage $L = < +,.,-,^{-1},0,1,<,' >$, la théorie des corps ordonnés différentiels (notée ODF) est universelle.

THEOREME (voir [2], p. 85). ODF a une modèle complétion. La preuve est semblable à celles de Blum et Wood pour les corps différentiels différentiellement parfaits (voir [4]). Plus précisément, M. Singer montre que la modèle complétion de ODF est axiomatisée dans L par ODF + RCF (= théorie des corps réels clos) + le schéma d'axiomes $A_{f,\overline{g}}$ suivants : pour tous $f(X,\ldots X^{(n)})$, $g_1(X,\ldots,X^{(n)})$, ..., $g_k(X,\ldots,X^{(n)})$ des polynômes différentiels tels que ordre de $f \geqslant$ ordre de g_j, $j = 1, \ldots, k$

$$A_{f,g} : [(\exists X_o,\ldots,X_n)(f(X_o,\ldots,X_n) = 0 \wedge \frac{\partial f}{\partial X^{(n)}}(X_o,\ldots,X_n) \neq 0$$

$$\wedge \bigwedge_{j=1}^{k} g_j(X_o,\ldots,X_n) > 0)) \rightarrow (\exists X)(f(X,\ldots,X^{(n)}) = 0$$

$$\wedge \bigwedge_{j=1}^{k} g_j(X,\ldots,X^{(n)}) > 0))]$$

où $g(X_o,\ldots,X_n)$ est le <u>polynôme ordinaire</u> obtenu en remplaçant $X,\ldots,X^{(n)}$ par des indéterminées $X_o,\ldots,X_n$.

La modèle complétion de ODF est appelée la théorie des corps ordonnés différentiellement clos et notée CODF.

COROLLAIRE 1 – CODF admet l'élimination des quantificateurs dans L et cette élimination est effective.

PREUVE : CODF a l'élimination des quantificateurs puisque CODF est la modèle complétion d'une théorie universelle. Cette élimination est effective car CODF $\cup$ $\mathcal{D}\mathbb{Q}$ (où $\mathcal{D}\mathbb{Q}$ est le diagramme du corps des rationnels) est complète et admet une axiomatisation récursive.

COROLLAIRE 2 – CODF est complète.

REMARQUE – En fait, l'axiomatisation de CODF montre que la procédure d'élimination des quantificateurs pour CODF dans L se ramène à celle de RCF dans $< +,.,-,0,1,< >$.

THEOREME 2 – CODF n'a pas de modèle premier au-dessus de $\mathbb{Q}$.

PREUVE : Voir [2], p. 87.

THEOREME 3 – Si K est un modèle de CODF, alors K(i) (où $i^2 = -1$) est un corps différentiellement clos.

PREUVE : Voir [3].

THEOREME 4 – a) Il existe un algorithme qui étant donné $p_1(X_1,\ldots,X_n)$, ..., $p_m(X_1,\ldots,X_n)$, $h(X_1,\ldots,X_n)$ des polynômes différentiels en n variables et à coefficients dans $\mathbb{Q}$, décide s'il existe un voisinage de 0 et des fonctions réelles analytiques $u_1,\ldots,u_n$ définies dans ce voisinage telles que :

$$p_1(u_1,\ldots,u_n) = 0, \ldots, p_m(u_1,\ldots,u_n) = 0 \text{ et } h(u_1,\ldots,u_m) \neq 0.$$

b) Il existe un algorithme qui étant donné $p_1(X_1,\ldots,X_n)$, ..., $p_m(X_1,\ldots,X_n)$, $h(X,\ldots,X_n)$ des polynômes différentiels en n variables et à coefficients dans

$\mathbb{Q}(X)$ (le corps des fonctions rationnelles sur $\mathbb{Q}$), décide s'il existe un voisinage dans $\mathbb{R}$ et des fonctions réelles analytiques $u_1,\ldots,u_n$ définies dans ce voisinage telles que $p_1(u_1,\ldots,u_n) = 0, \ldots, p_m(u_1,\ldots,u_n) = 0$ et $h(u_1,\ldots,u_m) \neq 0$.

PREUVE : Voir [2], p. 90.

THEOREME 5 — Il n'existe pas d'algorithme qui étant donné $p_1(X_1,\ldots,X_n), \ldots, p_m(X_1,\ldots,X_n), h(X_1,\ldots,X_m)$ des polynômes différentiels en n variables et à coefficients dans $\mathbb{Q}(X)$ décide s'il existe un voisinage de 0 et des fonctions réelles analytiques $u_1,\ldots,u_n$ définies dans ce voisiange telles que

$p(u_1,\ldots,u_n) = 0,\ldots,p_m(u_1,\ldots,u_n) = 0$ et $h(u_1,\ldots,u_n) \neq 0$.

PREUVE : Voir [2], p. 90,91.

Les preuves des théorèmes 3, 4, 5 sont en fait basées sur le résultat suivant :

THEOREME 6 — Soit $K = \mathbb{Q}\langle u_1,\ldots,u_n\rangle$ une extension différentielle de $\mathbb{Q}$, formellement réelle. Alors K est isomorphe (en tant que corps différentiel) à $\mathbb{Q}\langle \bar{u}_1,\ldots,\bar{u}_n\rangle$ où chaque $\bar{u}_i$ est une fonction de $\mathbb{R}$ dans $\mathbb{R}$ analytique dans un voisinage de 0 et où la dérivation sur $\mathbb{Q}\langle \bar{u}_1,\ldots,\bar{u}_n\rangle$ est $\frac{d}{dx}$.

PREUVE : Voir [2], p. 88-89

REFERENCES

[1] ROBINSON A., Ordered differential fields, Journal of Comb. Th. (A) 14 (1973), p. 324-333.

[2] SINGER M., The model theory of ordered differential fields, J.S.L. 43 (1978), p. 82-91.

[3] SINGER M., A class of differential fields with minimal differential closures, Proc. of the A.M.S., 69 (1978), p. 319-322.

[4] WOOD C., The model theory of differential fields revisited, Israël J. Math., 25 (1976), p. 331-352.

C. MICHAUX
Univ. de l'Etat à Mons
Fac. des Sciences
Av. Maistriau, 15
B-7000 Mons (Belgique).

Quelques constructions sur les groupes abéliens ordonnés (g.a.o.)

Françoise Delon

François Lucas

Depuis les travaux de Peter Schmitt [S1,S2], on contrôle bien équivalence et inclusion élémentaires entre g.a.o.. Les propriétés logiques d'un g.a.o. G sont ramenées à celles d'une infinité de "chaînes colorées", c'est-à-dire d'ordres totaux portant des prédicats unaires en nombre infini. Ces chaînes sont appelées les spectres de G et sont indexées par $\mathbb{N}$. Elles sont interprétables dans G. P. Schmitt a montré que deux g.a.o. sont élémentairement équivalents ssi, pour tout $n \in \mathbb{N}$, leurs spectres d'ordre d'ordre n le sont, et il a donné un critère d'inclusion élémentaire (pour tout n il y a un plongement naturel élémentaire du spectre d'ordre n, plus d'autres conditions).

Quelques notations

$Sp_n(G)$ désigne le spectre d'ordre n;

$H \lhd G$ exprime que H est un sous-groupe convexe de G (G/H est alors ordonné par l'ordre quotient de celui de G);

$\mathcal{C}(G) = \{ H;\ H \lhd \neq G \}$.

Clôture convexe et quotient

Chaque spectre de G est un sous ensemble de $\mathcal{C}(G)$, l'ordre est l'inclusion. On sait que pour $H \lhd G$, $\mathcal{C}(H)$ s'identifie à un segment initial de

$\mathfrak{C}(G)$, et $\mathfrak{C}(G/H)$ à un segment final. Cela reste presque vrai pour les spectres de Schmitt: pour chaque $n \in \mathbb{N}$, $Sp_n(H)$ s'identifie à $\{ C \in Sp_n(G) ; C \not\lhd H \}$ et $Sp_n(G/H) - \{0\}$ à $\{ C \in Sp_n(G) ; H \not\lhd C \}$ (selon les cas, $\{0\}$ est ou n'est pas dans $Sp_n(G/H)$).

Ces propriétés nous permettent de transférer dans les g.a.o. des résultats de Rubin sur les chaînes colorées, à savoir: si C_1 et C_2 sont des chaînes colorées et C la clôture convexe initiale $\{ x \in C_2 ; \exists y \in C_1, y > x \}$, ou finale $\{ x \in C_2 ; \exists y \in C_1, y < x \}$ de C_1 dans C_2, alors $C_1 \prec C_2$ implique $C_1 \prec C \prec C_2$. On obtient ainsi les deux théorèmes suivants.

Théorème 1.

Soient des g.a.o. $H \prec G$ et E la clôture convexe de H dans G. Alors $H \prec E \prec G$.

Théorème 2.

Soient des g.a.o. $H \prec G$ et H_o le plus gros sous groupe-convexe de G coupant H en $\{0\}$ (donc H se plonge dans G/H_o). Si on suppose que, pour chaque entier n, ni $\{0\}$ ni H_o n'est dans $Sp_n(G)$, alors $H \prec G/H_o$ (les hypothèses sur $\{0\}$ et H_o sont nécessaires et indépendantes).

Le Théorème 1 est agréable en ce qu'il permet de faire avec un g.a.o. arbitraire ce qui est devenu classique avec les entiers, c'est-à-dire utiliser les modèles non standard. Donnons un exemple dans les corps valués.

Van den Dries a montré que le théorème de Greenberg se généralise à des anneaux de valuation quelconques. Enonçons ce résultat sous la forme (faible) suivante: soit un anneau de valuation henselien D de caractéristique 0 et un système équationnel fini f à coefficients dans D; si pour tout $g \in vD$ il existe $\bar{x} \in D$ vérifiant $v(f(\bar{x})) \geq g$, alors f admet un zéro dans D. Lorsque la caractéristique de D/v est nulle, donnons de ce résultat une preuve dans un esprit non-standard.

La propriété à prouver est du premier ordre, c'est la conjonction sur m, d et n, des énoncés suivants

pour tout système f de m polynômes de degré$\leq$d en n variables

$$[\forall g\ \exists \bar{x}\ v(\bar{x})\geq 0 \wedge v(f(\bar{x}))\geq g] \longrightarrow \exists \bar{x}\ [f(\bar{x})=0].$$

Grâce au principe d'Ax-Kochen-Eršov, il suffit de prouver qu'elle est vraie dans les anneaux maximaux, c'est-à-dire les anneaux de séries formelles $k[[G]]$. Considérons une extension G^* ω-saturée de G et la clôture convexe C de G dans G^*; d'après ce qui précède et Ax-Kochen-Eršov, on a $k((G)) \prec k((C)) \prec k((G^*))$; considérons sur $k((G^*))$ la valuation naturelle v à valeurs dans G^* et la valuation w composée de v avec la projection $G \longrightarrow\!\!\!\!\!\rightarrow G^*/C$; on a $k((G^*))/w \simeq k((C))$ et sur ce corps est définie la valuation quotient v/w induite par v; $w\restriction k((C))$ est la valuation triviale et $(k((G^*))/w, v/w)$ est isomorphe à $(k((C)),v)$. Soit maintenant un système f à coefficients dans $k[[G]]$ admettant des zéros approchés à n'importe quel ordre, $g\in G^*$ vérifiant $g>G$ et $\bar{x}\in k[[G^*]]$ tel que $v(f(\bar{x}))\geq g$; on a donc $w(f(\bar{x}))>0$ et $f(\bar{x})/w \simeq f/w(\bar{x}/w) = 0$; donc $k[[C]]$ satisfait la formule $\exists \bar{x}\ f(\bar{x})=0$, et $k[[G]]$ aussi.

Produits de g.a.o.

Pour des g.a.o. H et G, G×H est le produit lexicographique; H s'identifie au sous groupe convexe O×H de G×H, et G au quotient G×H/H; d'où $\mathfrak{C}(G\times H) = \mathfrak{C}(H)+\mathfrak{C}(G)$. La situation peut ne pas être tout-à-fait aussi simple pour les spectres de Schmitt: pour chaque entier n,

- ou bien $Sp_n(G\times H) = Sp_n(H) + Sp_n(G)$,
- ou bien $Sp_n(H)$ a un élément maximal et $Sp_n(G)$ un élément minimal qui se confondent, c'est à dire (g et h sont des chaînes colorées) $Sp_n(H) = h + *$, $Sp_n(G) = * + g$ et $Sp_n(G\times H) = h + * + g$, avec une règle de coloration du *

restant.

Cela peut se généraliser. Si I est un ordre total et G^I le produit de Hahn de I copies de G, $Sp_n(G^I)$ est à peu près égal à $Sp_n(G).I$ (il peut y avoir contraction comme dans le cas GxH) et en tout état de cause parfaitement déterminé par $Sp_n(G)$ et I. Là encore on transporte alors un résultat sur les ordres (si $I \equiv J$ sont des ordres totaux et C une chaîne colorée, alors $C.I \equiv C.J$) en un résultat sur les g.a.o. :

Théorème 3.

Pour des ordres totaux élémentairement équivalents I et J, et un g.a.o. G, on a $G^I \equiv G^J$.

Il est intéressant de rapprocher ce résultat des travaux de Feferman et Vaught. Ces derniers ont défini une notion très générale de produit, qui inclut les produits de Hahn de structures ordonnées. Leur analyse de ces produits généralisés leur a permis de ramener les formules d'un produit aux formules de la structure commune des composantes et à celles de l'ensemble d'indices. En particulier, pour ce qui est des g.a.o. ils obtiennent les résultats suivants:

- pour I fixé, si pour chaque $i \in I$, $G_i \equiv H_i$, alors $(G_i)^I \equiv (H_i)^I$;
- si $G_i = G$ est fixé, $< I, \mathcal{P}(I), \in, < > \equiv < J, \mathcal{P}(J), \in, < > \implies G^I \equiv G^J$ (où $\mathcal{P}(I)$ est l'ensemble des parties de I et $<$ l'ordre entre éléments de I).

Ce deuxième résultat est strictement plus faible que le théorème 3 car $< I, < > \equiv < J, < > \not\Leftrightarrow < I, \mathcal{P}(I), \in, < > \equiv < J, \mathcal{P}(J), \in, < >$. Le théorème 3 ne pourrait pas être obtenu par une étude générale des produits car il est faux lorsque les G_i sont seulement des semi-g.a.o. (i.e. modèles de la théorie universelle des g.a.o.). De la même façon, le théorème suivant est faux pour les semi g.a.o..

Théorème 4.

Si G est un g.a.o. et I un ordre total, on a $G^I \searrow G^{(I)}$, où $G^{(I)}$ est la somme lexicographique.

On a vu que les résultats de Feferman et Vaught impliquent que, pour des g.a.o. G et H, $G \equiv H \Longrightarrow G^m \equiv H^m$. Notre étude des spectres d'un produit (i.e. $Sp_n(G^m)$ à peu près égal à $Sp_n(G).m$) permet de montrer une réciproque:

Théorème 5.

Si G et H sont des g.a.o., $G^m \equiv H^m$ inplique $G \equiv H$.

Démonstration. Si $G^m \equiv H^m$ alors, pour tout n, $Sp_n(G^m) \equiv Sp_n(H^m)$, d'où (avec un peu de travail) $Sp_n(G).m \equiv Sp_n(H).m$; donc (d'après un résultat déjà connu sur les chaînes colorées) $Sp_n(G) \equiv Sp_n(H)$ et $G \equiv H$. □

Le théorème 5 a été prouvé simultanément par d'autres techniques par M. Giraudet (voir son exposé dans ce volume); il est d'autant plus intéressant que l'énoncé obtenu en remplaçant équivalence élémentaire par isomorphisme est faux, ainsi que le montrent les contre-exemples de F. Oger (ce volume).

Bibliographie

[DL] F. Delon et F. Lucas, Inclusions et produits de groupes abéliens ordonnés étudiés au premier ordre, manuscrit.

[FV] S. Feferman et R. Vaught, The first order properties of products of algebraic systems, Fund. Math. XLVII (1959), pp. 57-103.

[G] M. Giraudet, Cancellation and absorption of lexicographic powers of

totally ordered abelian groups, ce volume.

[O] F. Oger, An example of two nonisomorphic countable ordered abelian groups with isomorphic lexicographical squares, ce volume.

[S1] P. Schmitt, Model theory of ordered abelian groups, Habilitationsschrift, Heidelberg 1982.

[S2] Model- and substructure complete theories of ordered abelian groups, in Models and Sets, Proceedings Logic Colloquium (Aachen 1983), G. Müller et M. Richter éd., Springer-Verlag LNM 1103, Berlin 1984.

SPECTRE p-ADIQUE:
ASPECTS TOPOLOGIQUES & GEOMETRIQUES

L. Bélair

§.0. PRELIMINAIRES

Soit p un nombre premier fixé. Cet exposé a comme toile de fond le corps des nombres p-adiques (voir [Am]). Ax-Kochen et Ershov ont montré que, en tant que corps muni de la valuation p-adique, v_p, la théorie élémentaire de $\mathbb{Q}_p$ est axiomatisée par les propriétés de corps valué hensélien, dont le groupe de valuation est un $\mathbb{Z}$-groupe où le plus petit élément positif est donné par la valuation de p, et dont le corps des restes est canoniquement isomorphe au corps premier F_p. Ils ont aussi montré que cette théorie est modèle-complète. La structure valuée de $(\mathbb{Q}_p, v_p)$ est définissable algébriquement: $v_p(x) \leq v_p(y) \Leftrightarrow \exists z(x^\varepsilon + py^\varepsilon = z^\varepsilon)$, où $\varepsilon=3$ si $p=2$, et $\varepsilon=2$ sinon. La théorie $Th(\mathbb{Q}_p)$ est aussi modèle-complète dans le langage des anneaux, L. Pour chaque entier $n\geq 2$, soit P_n, P_n^* des prédicats unaires interprétés comme suit: $Th(\mathbb{Q}_p) \models P_n(x) \leftrightarrow \exists y(x=y^n)$ et $Th(\mathbb{Q}_p) \models P_n^*(x) \leftrightarrow x\neq 0 \wedge P_n(x)$. Macintyre a montré que $Th(\mathbb{Q}_p)$ élimine les quantificateurs dans le langage des anneaux muni des prédicats P_n, que nous noterons $L(P_\omega)$. Notons qu'on a $v_p(x) \leq v_p(y) \leftrightarrow P_\varepsilon(x^\varepsilon + py^\varepsilon)$; la topologie

p-adique est donc décrite dans $L(P_\omega)$ par des formules atomiques.

Le spectre p-adique a été introduit par E. Robinson [Ro1], motivé par le spectre réel de Coste et Coste-Roy [CR]. Comme on le verra ci-dessous, cet objet est davantage lié à $Th(\mathbb{Q}_p)$ qu'à $\mathbb{Q}_p$ en soi. Cette construction a été généralisée aux extensions finies de $\mathbb{Q}_p$ par Bröcker-Schinke [BS], et indépendamment dans [Bé1]. Les démonstrations ci-dessous s'adaptent naturellement à ce contexte.

Dans cet exposé, on qualifie un espace topologique de <u>compact</u> si il possède <u>la propriété de sous-recouvrement fini</u>. <u>Un espace compact ne sera donc pas nécessairement séparé</u>. On note CAC la théorie élémentaires des corps algébriquement clos, et X^c le complémentaire du sous-ensemble X d'un ensemble donné. Soit K un corps, on note K^* son groupe multiplicatif et P_n^* le sous-groupe multiplicatif des puissances n-ièmes. Une formule $\varphi(x_1,\ldots x_n)$ de L désignera tout aussi bien le sous-ensemble de K^n qu'elle définit. Soit A un anneau et $L(A)$ le langage L muni de nouvelles constantes pour les éléments de A, on note $\Delta^+(A)$ le diagramme positif de A dans L, i.e. l'ensemble des énoncés atomiques de $L(A)$ vrais dans A. On note $\underline{x}$ le n-uplet $(x_1,\ldots,x_n)$. Soit $f_1,\ldots,f_m \in K[\underline{X}]$, I l'idéal engendré par les f_i dans $K[\underline{X}]$, et V la variété affine définie par les f_i, alors on pose $V(K) = \{\underline{x} \in K^n: f_i(\underline{x})=0 \ ,i=1,\ldots,m\}$, et $K[V] = K[\underline{X}]/I$. L'anneau $K[V]$ est appelé anneau des coordonnées de V au-dessus K. Soit $X \subseteq K^n$ et f une fonction de X dans K alors on pose $Z(f) = \{\underline{x} \in X: f(\underline{x})=0\}$. Nous utiliserons le fait suivant, conséquence du lemme de Hensel : si $x \in \mathbb{Q}_p^*$ est tel que $v_p(x-1) > v_p(n^2)$, alors $x \in P_n^*$. Soit $\underline{x} \in \mathbb{Q}_p^n$, $a \in \mathbb{Q}_p$ on pose $B(\underline{x},a) = \{\underline{y} \in \mathbb{Q}_p^n: v_p(x_i-y_i) \geq v(a) \ , 1\leq i<n\}$.

§.1. SPECTRE p-ADIQUE ?

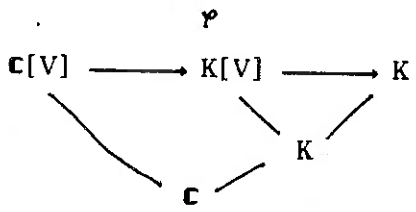
Le rapport entre le spectre réel et la géométrie algébrique réelle est

maintenant bien connu. Le spectre p-adique relève un peu du même genre de procédé. Plaçons nous momentanément dans un contexte général pour situer ce type de construction. Soit (K,τ) un corps topologique de base. On s'intéresse aux variétés algébriques affines munies de la topologie induite par celle de K. Il s'agit d'introduire un objet qui jouerait un rôle analogue à celui du spectre premier d'un anneau en géométrie algébrique.

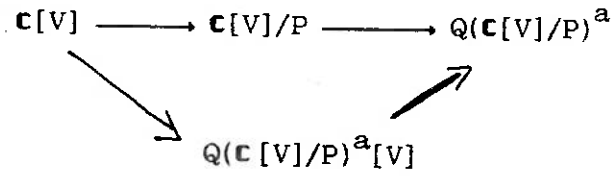
Exemple (1) Les nombres réels avec la topologie de l'ordre $(\mathbb{R},<)$: les variétés héritent alors de la topologie euclidienne.

(2) Les nombres p-adiques avec la topologie de la valuation p-adique $(\mathbb{Q}_p,v_p)$: les variétés héritent de la topologie p-adique.

Notons que, dans cette optique, si on considère les nombres complexes avec la topologie de Zariski $(\mathbb{C},\tau)$, la topologie induite n'est pas la topologie de Zariski puisque cette dernière est plus fine que la topologie produit de $(\mathbb{C},\tau)$. Rappelons brièvement le rapport entre le spectre premier et la géométrie algébrique (voir [DG], Introduction). Soit $f_1,\ldots,f_m \in \mathbb{C}[\underline{X}]$, $I=(f_1,\ldots f_m)$, V la variété affine définie par les f_i. Alors il y a correspondance biunivoque entre Spec $\mathbb{C}[V]$ et les points de V dans les extensions algébriquement closes de $\mathbb{C}$, au sens suivant: $V(\mathbb{C})$ (les points de V dans $\mathbb{C}$) se plonge dans Spec $\mathbb{C}[V]$ en envoyant $\underline{x}$ sur l'idéal maximal $M_{\underline{x}}=(X_1-x_1,\ldots,X_n-x_n)+I$, qui correspond au noyau de l'homomorphisme de $\mathbb{C}$-algèbre $\text{év}(\underline{x}):\mathbb{C}[V] \longrightarrow \mathbb{C}$ qui envoie $g+I$ sur $g(\underline{x})$. Soit $K/\mathbb{C}$ une extension algébriquement close de $\mathbb{C}$. Considérons les points de V rationnels sur K, i.e. $V(K)$, qui correspondent donc aux K-homomorphismes $K[V] \longrightarrow K$. Par rapport à l'anneau des coordonnées de V au-dessus de $\mathbb{C}$,

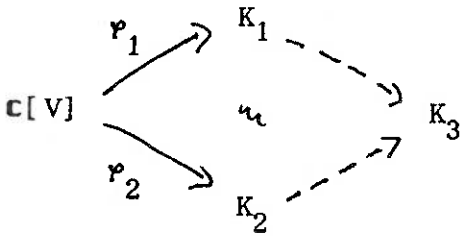


on n'obtient plus en général des idéaux maximaux mais des idéaux premiers: $\ker \varphi \in \mathrm{Spec}\ \mathbf{C}[V]$. Réciproquement, si $P \in \mathrm{Spec}\ \mathbf{C}[V]$ alors P correspond à un point de V rationnel sur la clôture algébrique du corps des fractions de $\mathbf{C}[V]/P$.



Définissons la relation $\sim$ sur les $\mathbf{C}$-homomorphismes $\mathbf{C}[V] \longrightarrow K$, où K est une extension algébriquement close de $\mathbf{C}$. Soit $\varphi_i : \mathbf{C}[V] \longrightarrow K_i$, $i=1,2$ deux tels morphismes, alors $\varphi_1 \sim \varphi_2$ ssi il existe $K_3/\mathbf{C}$ algébriquement clos et des $\mathbf{C}$-homomorphismes $K_i \longrightarrow K_3$ tel que le carré ci-dessous commute.

$\varphi_1 \sim \varphi_2$ ssi



La relation $\sim$ est une relation d'équivalence: elle est clairement réflexive et symétrique, et la transitivité découle de la propriété d'amalgamation des corps algébriquement clos. Remarquons que cette dernière propriété peut être déduite de la modèle-complétude de CAC . D'autre part on vérifie sans peine que $\varphi_1 \sim \varphi_2$ ssi $\ker \varphi_1 = \ker \varphi_2$. Cette discussion se transpose directement: pour tout anneau A , il y a correspondance biunivoque entre

Spec A et les classes d'équivalence d'homomorphismes $A \longrightarrow K$, où $K \models CAC$, pour la relation $\sim$. Nous laissons le soin au lecteur de faire une discussion analogue pour le spectre réel. Rappelons que la topologie de Spec A est donnée par la base $\{D(a) : a \in A\}$, où $D(a) = \{P : a \notin P\} = \{P : A/P \models (a \neq 0)\}$, ce qui correspond à $\{A \longrightarrow K/\sim : K \models (a \neq 0)\}$. Si $A = \mathbb{C}[V]$ alors la topologie induite par Spec $\mathbb{C}[V]$ à travers le plongement $V(\mathbb{C}) \longrightarrow$ Spec $\mathbb{C}[V]$ n'est nulle autre que la topologie de Zariski sur $V(\mathbb{C})$.

Une façon d'introduire le spectre p-adique est donc comme suit. Soit A un anneau, et considérons les homomorphismes de A dans les modèles de $Th(\mathbb{Q}_p)$. Puisque $Th(\mathbb{Q}_p)$ est modèle-complète, la relation analogue $\sim$ est aussi une relation d'équivalence et le spectre p-adique de A est alors l'ensemble des classes d'équivalences pour cette relation. Rappelons que la topologie p-adique peut être définie directement avec le prédicat P^*_ε .

Définition. Le spectre p-adique de A , $\mathrm{Spec}_p A$, est l'espace topologique suivant : $\mathrm{Spec}_p A = \{A \longrightarrow K : K \models Th(\mathbb{Q}_p)\} / \sim$, et la topologie est celle engendrée par la base $\{D_{\underline{n}}(\underline{a}) : n_i \in \omega , a_i \in A , 1 \leq i \leq k , k \in \omega\}$, où $D_{\underline{n}}(\underline{a}) = \{A \longrightarrow K/\sim : K \models \wedge P^*_{n_i}(a_i)\}$. Cet ensemble est bien défini grâce à l'E.Q. de $Th(\mathbb{Q}_p)$ dans le langage $L(P_\omega)$.

§.2. PROPRIETES ELEMENTAIRES.

Le spectre p-adique possède des propriétés analogues à celles du spectre premier. Nous vérifierons d'abord ces propriétés pour le spectre premier et nous verrons que les démonstrations se transposent au spectre p-adique (cf.[CR]). Dans ce qui suit, soit A un anneau.

Proposition. L'espace Spec A est compact.

Démonstration. Notons d'abord que pour $a,b \in A$, on a:

$$D(1) = \text{Spec } A$$

$$D(0) = \emptyset$$

$$D(a) \cap D(b) = D(ab)$$

$$D(a+b) \subset D(a) \cup D(b) .$$

Introduisons la théorie propositionnelle T, dont les variables propositionnelles sont $\{D(a) : a \in A\}$, et les axiomes sont:

$$1) \quad D(1) = \top$$

$$2) \quad D(0) = \bot$$

$$3) \quad D(a) \wedge D(b) \longleftrightarrow D(ab)$$

$$4) \quad D(a+b) \longrightarrow D(a) \vee D(b) .$$

Il y a correspondance biunivoque entre Spec A et les modèles de cette théorie: à $M \models T$ on associe $P_M = \{a \in A : M(D(a)) = \bot\}$, et à $P \in \text{Spec } A$ on associe M_p où $M_p(D(a)) = \top$ ssi $a \notin P$. Il est clair que $M_p \models T$, et $P_M \in \text{Spec } A$ découle des axiomes : 1),2),3)$\rightarrow$ et 4) impliquent que c'est un idéal propre, et 3)$\rightarrow$ qu'il est premier. On est ramené au lemme suivant.

Lemme. Pour tout $a \in A$, $D(a)$ est un sous-ensemble compact de Spec A.

Démonstration. Montrons que toute famille de fermés de base ayant la propriété d'intersection finie possède une intersection non vide. Soit $\{D(a_i) : a_i \in \Lambda\}$ tel que pour tout $a_1,\ldots,a_n \in \Lambda$ on ait $D(a_1)^c \cap \ldots \cap D(a_n)^c \cap D(a) \neq \emptyset$. En termes de notre langage propositionnel ceci nous dit que tout sous-ensemble fini de $\{\neg D(a_i), D(a) : a_i \in \Lambda\}$ a un modèle. Par compacité cet ensemble d'énoncés a aussi un modèle, i.e. $\bigcap_i D(a_i)^c \cap D(a) \neq \emptyset$. □

Autre démonstration de la Proposition (voir [vdD], Definition 5.5). Considérons la topologie plus fine engendrée par les $D(a)$, $D(a)^c$, dite

topologie constructible, et remplaçons T par $\Delta^+(A)$ + CAC . Alors il y a correspondance biunivoque entre Spec A et les complétions de $\Delta^+(A)$ + CAC dans $L(A)$, et comme ci-dessus on montre que tout $D(a)$ est compact dans cette topologie et donc, a fortiori, dans la topologie de départ qui est moins fine. □

Proposition. Pour tout $\underline{a} \in A^k$, $\underline{n} \in \omega^k$ $D_{\underline{n}}(\underline{a})$ est compact et en particulier $\mathrm{Spec}_p A = D_n(1)$ est compact.

Démonstration. On peut utiliser la topologie plus fine (constructible) comme ci-dessus et la correspondance entre $\mathrm{Spec}_p A$ et les complétions de $\Delta^+(A) + \mathrm{Th}(\mathbb{Q}_p)$ dans $L(A)$. Ou encore on peut procéder comme dans la première preuve en axiomatisant la théorie universelle $(\mathrm{Th}(\mathbb{Q}_p))_\forall$ dans $L(P_\omega)$ et en notant qu'il y a une correspondance entre $\mathrm{Spec}_p A$ et l'ensemble des couples $(P, (P^\cdot_{P,n})_{n\in\omega})$, où $P \in \mathrm{Spec}\ A$, et $(A/P, P^\cdot_{P,n}; n\in\omega) \models (\mathrm{Th}(\mathbb{Q}_p))_\forall$. A la classe de $\varphi: A \longrightarrow K$ on fait correspondre $(\ker \varphi, (P^\cdot_{\varphi,n})_{n\in\omega})$, où $P^\cdot_{\varphi,n} = \{a \in A : K \models P^\cdot_n(\varphi(a))\}$, qui est bien défini par E.Q.; et à $(P,(P^\cdot_{P,n}))$ on fait correspondre la classe de $A \longrightarrow K$, où $(A/P,(P^\cdot_{P,n})) \longrightarrow K$, $K \models \mathrm{Th}(\mathbb{Q}_p)$, qui est aussi bien définie par E.Q. . Une telle axiomatisation a été donnée dans [Ro2] et (indépendamment) [Bé2] . □

Proposition. Tout fermé irréductible de Spec A,$\mathrm{Spec}_p A$ est l'adhérence d'un seul et unique point.

Démonstration. Par exemple pour Spec A . Soit F un fermé irréductible non vide (i.e. $F = F_1 \cup F_2$, F_i fermés, $\Longrightarrow$ $F = F_1$ ou $F = F_2$). Définissons un modèle de T : posons $M(D(a)) = T$ ssi il existe $A \longrightarrow K/\sim \in F$ tel que $K \models (a \neq 0)$. Alors $M \models T$ et $F = \overline{\{P_M\}}$. Pour montrer que $M \models T$, seul l'axiome 3)→ mérite qu'on s'y arrête. Si $M(D(ab)) = \bot$, alors pour tout $A \longrightarrow K/\sim \in F$ on a $K \models (ab = 0)$, et donc $K \models (a = 0)$ ou $K \models (b = 0)$. Ainsi

$F \subset D(a)^C \cup D(b)^C$, d'où $F \subseteq D(a)^C$ ou $F \subseteq D(b)^C$, i.e. $M(D(a)) = \perp$ ou $M(D(b)) = \perp$. Que $F = \overline{\{P_M\}}$ et l'unicité de ce point générique sont immédiats puisqu'un point x appartient à l'adhérence d'un point y ssi tous les ouverts qui contiennent x contiennent aussi y . Pour une démonstration analogue dans l'esprit de la topologie constructible et un contexte légèrement différent voir [Pi]. □

Proposition. Soit $K = \mathbb{C},\mathbb{Q}_p$, $Spec_* = Spec, Spec_p$, $f_1,\ldots,f_m \in K[\underline{X}]$, $I = (f_1,\ldots,f_m)$, V la variété affine définie par les f_i , $V(K)$ muni de la topologie de Zariski, p-adique respectivement. Alors l'injection $\iota: V(K) \longrightarrow Spec_* K[V]$ est un plongement topologique dense.

Démonstration. Pour Spec $\mathbb{C}[V]$. On a $\iota(\underline{x}) = (X_1-x_1,\ldots,X_n-x_n) + I$ et Spec $\mathbb{C}[V] \cong \{P \in \text{Spec } \mathbb{C}[\underline{X}] : I \subseteq P\}$, et donc pour $g \in \mathbb{C}[\underline{X}]$, $D(g+I) \cong \{P \in \text{Spec } \mathbb{C}[\underline{X}] : g \notin P\}$. Voyons que ι et ι^{-1} sont continues: $\iota^{-1}D(g+I) = \{\underline{x} : g(\underline{x}) \neq \emptyset\}$ est ouvert et $\iota\{\underline{x} : g(\underline{x}) \neq \emptyset\} = im(\iota) \cap D(g+I)$ est ouvert. Pour la densité de $im(\iota)$ dans Spec $\mathbb{C}[V]$ il faut montrer que si $D(g+I) \neq \emptyset$ alors il existe $\underline{x} \in V(\mathbb{C})$ tel que $g(\underline{x}) \neq 0$. Soit $P \in D(g+I)$ et E la clôture algébrique du corps des fractions de $\mathbb{C}[V]/P$, alors $\mathbb{C} \subseteq E$ et $E \models \exists \underline{x}(\underline{x} \in V(E) \wedge g(\underline{x}) \neq 0)$, et par modèle-complétude il existe $\underline{x} \in V(\mathbb{C})$ tel que $g(\underline{x}) \neq 0$. Un argument similaire s'applique à $Spec_p$ en ayant à l'esprit que les $\{\underline{x} : P_n^*(f(\underline{x}))\}$, $f \in \mathbb{Q}_p[\underline{X}]\}$, engendrent la topologie p-adique sur la variété. □

§.3. FONCTIONS CONTINUES DEFINISSABLES.

Un espace topologique est dit spectral si il est compact, possède une base d'ouverts compacts close par intersection finie, et si tout fermé irréductible est l'adhérence d'un unique point (voir [Ho]). Hochster (ibid.) a montré que les espaces spectraux sont exactement les espaces homéomorphes au

spectre premier d'un anneau. On a vu que $\mathrm{Spec}_{p}\mathbb{Q}_p[V]$ est un espace spectral. On peut se demander si il y a un anneau ayant un rapport significatif avec la variété V dont le spectre premier est homéomorphe à $\mathrm{Spec}_{p}\mathbb{Q}_p[V]$. On connaît une réponse dans le cas du spectre réel.

Proposition ([CC]). Soit $f_1,\ldots,f_m \in \mathbb{R}[\underline{X}]$, V la variété affine définie par les f_i , et $\mathcal{C}(V(\mathbb{R}))$ l'ensemble des fonctions continues définissables (avec paramètres) de $V(\mathbb{R})$ dans $\mathbb{R}$. Alors le spectre réel de $\mathbb{R}[V]$ est homéomorphe au spectre premier de $\mathcal{C}(V(\mathbb{R}))$ par un isomorphisme naturel au niveau de leur treillis d'ouverts compacts.

Nous allons montrer un résultat analogue dans le cas p-adique. Dans ce qui suit, définissable sera synonyme de définissable avec paramètres, et la topologie p-adique sera sous-entendue.

Définition. Soit $n \in \omega$, et $S \subseteq \mathbb{Q}_p^n$ un sous-ensemble définissable, on note $\mathcal{C}(S)$ l'ensemble des fonctions $S \longrightarrow \mathbb{Q}_p$ continues et définissables.

La proposition suivante fournit la clé du résultat.

Proposition 1. Soit $n \in \omega$, $S \subseteq \mathbb{Q}_p^n$ définissable et localement fermé (en particulier pour $S = V(\mathbb{Q}_p)$), $f \in \mathcal{C}(S)$ et $g \in \mathcal{C}(S\text{-}Z(f))$. Alors il existe un entier $N \geq 1$ tel que pour tout $\underline{x}_0 \in \overline{S\text{-}Z(f)}$ il existe $c(\underline{x}_0)$, $d(\underline{x}_0) \in \mathbb{Q}_p$ tel que $(*)$ $v_p(f^N g) \geq v_p(c(\underline{x}_0))$, sur l'ensemble $\overline{B}(\underline{x}_0, d(\underline{x}_0)) \cap S\text{-}Z(f)$.

En termes de norme p-adique on a $|f^N g|_p \leq |c(\underline{x}_0)|_p$, c'est donc dire que $f^N g$ est localement bornée sur $\overline{S\text{-}Z(f)}$. Il s'agit d'analyser la croissance de g sur la frontière de $Z(f)$: g,f sont localement les zéros d'une équation polynomiale et a fortiori de croissance polynomiale; d'autre part par E.Q. leur comportement est décrit par les restes de polynômes à deux variables $h(g(\underline{x}),f(\underline{x}))$ modulo des P_m^* , et le fait que ceux-ci soient "relativement

explicitement ouverts" nous dit qu'on peut prédire le comportement de $h(y,z)$ à partir de celui de $h(0,z)$, dans un voisinage relatif de $(0,0)$. Nous allons d'abord voir comment le résultat principal découle de cette proposition.

Corollaire 2. Soit $f,g \in \mathcal{C}(S)$ tel que $Z(g) \subseteq Z(f)$, alors il existe un entier $N \geq 1$ tel que g divise f^N dans $\mathcal{C}(S)$, i.e. $f \in \sqrt{(g)}$.

Démonstration. On a alors $g^{-1} \in \mathcal{C}(S-Z(f))$. Il existe N tel que $f^N g^{-1}$ est localement bornée sur $\overline{S-Z(f)}$. Ainsi $ff^N g^{-1}$ prolongée par 0 sur $Z(f)$ appartient à $\mathcal{C}(S)$ et $gf^{N+1}g^{-1} = f^{N+1}$. □

Voici un autre fait-clef.

Proposition 3 ([Ro2]). Soit $n \in \omega$, $U \subseteq \mathbb{Q}_p^n$ un ouvert définissable, alors il existe des polynômes $f_{ij} \in \mathbb{Q}_p[\underline{X}]$ et des entiers n_{ij} tel que $U = \bigcup_i \bigcap_j P'_{n_{ij}}(f_{ij}(\underline{x}))$.

Corollaire 4 . Soit $\iota : V(\mathbb{Q}_p) \longrightarrow \mathrm{Spec}_p\mathbb{Q}_p[V]$ le plongement canonique. Alors la correspondance $\mathcal{P}(\underline{x}) \longmapsto \{\mathbb{Q}_p[V] \longrightarrow K/\sim : K \models \mathcal{P}(\underline{x})\}$ entre les sous-ensembles définissables de $V(\mathbb{Q}_p)$ et les sous-ensembles constructibles de $\mathrm{Spec}_p\mathbb{Q}_p[V]$ (par E.Q.) induit une bijection entre les ouverts définissables de $V(\mathbb{Q}_p)$ et les ouverts compacts de $\mathrm{Spec}_p\mathbb{Q}_p[V]$.

On vérifie que la bijection en question induit un isomorphisme de treillis entre le treillis des ouverts définissables de $V(\mathbb{Q}_p)$ et le treillis des ouverts compacts de $\mathrm{Spec}_p\mathbb{Q}_p[V]$, qui est engendré par les $D_n(g+I)$, $g \in \mathbb{Q}_p[\underline{X}]$.

Proposition 5. Il y a un homéomorphisme entre $\mathrm{Spec}_{\mathbb{Q}_p}\mathbb{Q}_p[V]$ et $\mathrm{Spec}\ \mathcal{C}(V(\mathbb{Q}_p))$ induit par un isomorphisme naturel au niveau des treillis d'ouverts compacts.

Démonstration. (1) Ces deux espaces étant spectraux, il suffit de montrer que leurs treillis d'ouverts compacts sont isomorphes: cet isomorphisme induit alors une bijection entre les ultrafiltres de ces treillis qui s'identifient avec les points de chacun des espaces (dualité espaces spectraux $\longleftrightarrow$ treillis distributifs). Cette bijection est alors clairement un homéomorphisme.

(2) Comme on l'a vu, le treillis des ouverts compacts de $\mathrm{Spec}_{\mathbb{Q}_p}\mathbb{Q}_p[V]$ peut être identifié au treillis des ouverts définissables de $V(\mathbb{Q}_p)$. Notons-le $\tau(V)$.

(3) Soit $\tau(\mathcal{C})$ le treillis des ouverts compacts de $\mathrm{Spec}\ \mathcal{C}(V(\mathbb{Q}_p))$; alors $\tau(\mathcal{C})$ coïncide avec $\{D(f) : f \in \mathcal{C}(V(\mathbb{Q}_p))\}$. En effet, $\tau(\mathcal{C})$ est le treillis engendré par les $D(f)$, $f \in \mathcal{C}(V(\mathbb{Q}_p))$. On sait déjà que $D(f) \cap D(g) = D(fg)$. Soit $\Psi(x,y) = x^2 + py^2$, on vérifie aisément que $\mathbb{Q}_p \models (\Psi(x,y)=0 \longleftrightarrow (x=0 \wedge y=0))$ et alors $D(f) \cup D(g) = D(\Psi(f,g))$: l'inclusion $\supseteq$ est claire, d'autre part $Z(\Psi(f,g)) \subseteq Z(f) \cap Z(g)$ et par le corollaire 2 on a $f,g \in \sqrt{(\Psi(f,g))}$ et l'inclusion $\subseteq$ s'ensuit aussitôt.

(4) Soit $\Phi : \tau(\mathcal{C}) \longrightarrow \tau(V)$ l'application qui envoie $D(f)$ sur $\{\underline{x} \in V(\mathbb{Q}_p) : f(\underline{x}) \neq 0\}$. L'application Φ est bien définie puisque si $D(f) = D(g)$ alors $\sqrt{(f)} = \sqrt{(g)}$ et $Z(f) = Z(g)$, et donc $\Phi(D(f)) = \Phi(D(g))$. On vérifie immédiatement que Φ est un homomorphisme de treillis. Si $\Phi(D(f)) = \Phi(D(g))$ alors $Z(f) = Z(g)$, et par le corollaire 2 $\sqrt{(f)} = \sqrt{(g)}$ d'où $D(f) = D(g)$ et Φ est injective. La surjectivité de Φ découle du lemme suivant.

Lemme 6. Pour tout fermé définissable $F \subseteq \mathbb{Q}_p^n$, il existe une fonction continue définissable qui s'annule exactement sur F.

Démonstration. Notons que dans le cas réel on peut utiliser

$\mathrm{dist}(\underline{x},F) = \inf\{|\underline{x} - \underline{y}| : \underline{y} \in F\}$, mais dans notre cas on ne dispose pas de la section $p^{-v_p(x)}$ pour définir la norme p-adique . Pour tout m il existe $e_i \in \mathbb{N}$ tel que , $\mathbb{Q}_p = \{0\} \dot\cup P_m^* \dot\cup e_1 P_m^* \dot\cup \ldots \dot\cup e_{k(m)} P_m^*$. Alors par la proposition 3 il existe $m(i,j) \in \mathbb{N}$ et $f_{ij} \in \mathbb{Q}_p[\underline{X}]$ tel que

$$F = \bigcup_{i=1}^{q} \bigcap_{j=1}^{r(i)} P_{m(i,j)}(f_{ij}(\underline{x}))$$. Pour m fixé et pour $x \in \mathbb{Q}_p^*$ posons $\rho_m(x) = e_i$ ssi $x \in e_i P_m^*$. Ainsi $x \in P_m^*$ ssi $\rho_m(x) = 1$. Notons que ρ_m est continue sur $\mathbb{Q}_p^*$ puisque les $e_i P_m^*$ sont ouverts. Soit $\varphi_m : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ défini par

$$\varphi_m(x) = \begin{cases} 0 & \text{si } x = 0 \\ x(\rho_m(x)-1) & \text{si } x \neq 0 \end{cases} .$$

On vérifie aisément que φ_m est continue sur $\mathbb{Q}_p$ et que $\varphi_m(x) = 0$ ssi $x \in P_m$. Soit

$$\psi_i(X_1,\ldots,X_{r(i)}) = X_1^{r(i)} + pX_2^{r(i)} + \ldots + p^{r(i)-1}X_{r(i)}^{r(i)}$$

alors comme précédemment $\mathbb{Q}_p \models (\psi_i(\underline{x}) = 0 \leftrightarrow \wedge x_j = 0)$, et

$$\psi_F(\underline{x}) = \prod_{i=1}^{q} \psi_i(\varphi_{m(i,1)}(f_{i1}(\underline{x})),\ldots,\varphi_{m(i,r(i))}(f_{ir(i)}(\underline{x})))$$

est la fonction cherchée. □

Notons comme corollaire que la dimension de Krull de $\varphi(V(\mathbb{Q}_p))$ est égale à la dimension combinatoire de $\mathrm{Spec}_p\mathbb{Q}_p[V]$ comme espace spectral, qui coïncide avec la dimension p-adique au sens de [SvdD], qui elle-même coïncide avec la dimension au sens de la géométrie algébrique.

Démonstration de la proposition 1 (cf. [CC] et la preuve de l'inégalité de Lojasiewicz p-adique (thm. 2.5) dans [BS])

Soit $v = v_p$. Si $\underline{x}_0 \in S\text{-}Z(f)$ alors par continuité de fg l'inégalité (*) est vérifiée avec $N=1$. On peut donc supposer que $\underline{x}_0 \in Z(f) \cap \overline{S\text{-}Z(f)}$.

Considérons la formule

$$H(\underline{x},t,y,z) := \exists \underline{u}(\underline{u}\in S \wedge \underline{u}\in B(\underline{x},t) \wedge [(y=0 \wedge z=0) \vee (f(\underline{u})\neq 0 \wedge g(\underline{u})\neq 0 \wedge z=f(\underline{u}) \wedge y=g(\underline{u})^{-1})] .$$

Par E.Q. cette formule est équivalente dans $Th(\mathbb{Q}_p)$ à une formule de la forme

$$\bigvee_i \bigwedge_j \{P^{\cdot}_{m_{ij}}(h_{ij}(\underline{x},t,y,z)) , P_{n_{ij}}(k_{ij}(\underline{x},t,y,z)) : h_{ij},k_{ij} \in \mathbb{Q}_p[\underline{X},T,Y,Z]\}$$

Soit t_0 tel que $\overline{B}(\underline{x}_0,t_0) \cap S$ est fermé, et soit $S_0 := H(\underline{x}_0,t_0,y,z)$. Notons que $S_0 \cap OZ = \{O\}$, où $OZ = \{(y,z) : y=0\}$ et $O = (0,0)$. Pour $a \neq 0$ quelconque, g est bornée sur le compact $\overline{B}(\underline{x}_0,t_0) \cap S \cap \{\underline{x} \in S : v(f(\underline{x})) \leq v(a)\}$ et $(*)$ est vérifiée sur cet ensemble pour $N=1$. Il suffit donc de considérer $\overline{B}(\underline{x}_0,t_0) \cap S \cap \{\underline{x} \in S : v(f(\underline{x})) \geq v(a)\}$ pour un $a\neq 0$ approprié, i.e. montrer que dans un voisinage pointé de O on a $v(z^N y^{-1}) \geq v(c)$ pour tout $(y,z) \in S_0$ et des c,N appropriés. Dans l'expression de S_0 sans quantificateur, il suffit de considérer chacune des intersections $\cap_j$, et on peut supposer que O appartient à cette intersection sinon zy^{-1} est sûrement borné sur un voisinage pointé de O . On peut donc supposer

$$O \in S_0 = \bigcap_i P^{\cdot}_{m_i}(h_i(y,z)) \cap P_{n_i}(k_i(y,z))$$

et en outre $h_i,k_i \in \mathbb{Z}_p[Y,Z]$. Rappelons que $S_0 \cap OZ = \{O\}$, et donc l'un au moins des $h_i(0,z),k_i(0,z)$ ne s'annule pas partout sur OZ . Soit $r(Y,Z)$ l'un de ces polynômes et P_m le prédicat correspondant. Pour $a \in \mathbb{Q}_p$ soit $U(a) = \{(y,z) : v(y),v(z) \geq v(a)\}$. Soit ε_1 tel que $r(0,Z)$ n'a pas de zéro différent de O sur $U(\varepsilon_1) \cap OZ$. D'autre part soit $r(0,Z) = Z^N s(Z)$, où $s(0)\neq 0$. Pour un ε_2 approprié on a

$$v(r(0,z)) < v(\alpha z^N) \quad , \text{ pour } v(z) > v(\varepsilon_2) \ , \ z \neq 0$$

où $\alpha = \max \{v(s(z))+v(p) : v(z) \geq v(\varepsilon_2) \ , \ z \neq 0\}$ et $v(\alpha) \geq 0$. Soit $\varepsilon \in \mathbb{Q}_p^*$ tel que $v(\varepsilon) > \max \{v(\varepsilon_1), v(\varepsilon_2), 0\}$, et exprimons r comme polynôme en Y :

$$r(Y,Z) = \sum_{j \geq 1} \gamma_j(Z) \, Y^j + r(0,Z) \ .$$

Alors pour $z \neq 0$ tel que $v(z) \geq v(\varepsilon)$, on a $r(0,z) \neq 0$ et donc

$$r(Y,z)r(0,z)^{-1} = \sum \gamma_j(z) r(0,z)^{-1} \, Y^j + 1 \ .$$

Si $v(y) \geq v(m^2 \alpha z^N) > v(m^2 r(0,z))$, alors pour $j \geq 1$, $v(\gamma_j(z) r(0,z)^{-1} y^j) > v(\gamma_j(z) m^2) \geq v(m^2)$, $(v(\gamma_j(z)) \geq 0)$, ce qui implique que $r(y,z)r(0,z)^{-1} \in P_m^*$. Nous pouvons choisir ε, α, N tel que pour chacun des $r(Y,Z)$ et P_m comme ci-dessus on ait $r(y,z)r(0,z)^{-1} \in P_m^*$ pour $y,z \in \mathbb{Q}_p^*$ tel que $v(z) \geq v(\varepsilon)$ et $v(y) \geq v(m^2 \alpha z^N)$. Posons $c_0 = q^2 \alpha$, où q est le produit de tous les m nécessaires. Alors $(y,z) \notin S_0$ pour (y,z) tel que $z \neq 0$, $v(z) \geq v(\varepsilon)$ et $v(y) > v(c_0 z^N)$, sinon, par ce qui précède, on aurait aussi $(0,z) \in S_0$, ce qui est impossible. Ainsi $v(y) \leq v(c_0 z^N)$ pour $(y,z) \in U(\varepsilon) \cap S_0$, et on obtient l'inégalité voulue pour le voisinage pointé $U(\varepsilon)-O$. Il est clair que ce N ne dépend que du degré en Z des polynômes $r(0,Z)$ et donc a fortiori que de la description sans quantificateur de $H(\underline{x},t,y,z)$. On en conclut l'existence d'un N uniforme pour tous les x_0 . □

Notons que cette démonstration fonctionne dans tout modèle de $Th(\mathbb{Q}_p)$ et dans les corps p-adiquement clos de rang supérieur à 1 , en ajoutant les constantes nécessaires.

REFERENCES BIBLIOGRAPHIQUES

[Am] Y. Amice, Les nombres p-adiques, Presses Univ. de France, 1975.

[Bél] L. Bélair, Spectres p-adiques en rang fini, C. R. ACAD. SCI. PARIS , (à paraître).

[Bé2] , Substructures and Uniform Elimination for p-Adic Fields, ANN. PURE APPL. LOGIC, (à paraître).

[BS] L. Bröcker et J.H. Schinke, On the L-Adic Spectrum, SCHRIFTEN MATH. UNIV. MUNSTER, 2 SER. 40, 1986.

[CC] M. Carral et M. Coste, Normal Spectral Spaces and Their Dimensions, J. PURE APPL. ALG. 30 (1983),p. 227-235.

[CR] M. Coste et M.-F. Coste-Roy, La topologie du spectre réel, in Ordered Fields and Real Algebraic Geometry, A.M.S., (Cont. Mat.,8), 1982.

[DG] J. Dieudonné et A. Grothendieck, Eléments de géométrie algébrique I , Springer-Verlag, 1971.

[Ho] M. Hochster, Prime Ideal Structure in Commutative Rings, TRANS. A.M.S. 142 (1969), p. 43-60.

[Pi] A. Pillay, Sheaves of Continuous Definable Functions, pré-publication.

[Ro1] E. Robinson, The P-Adic Spectrum, J. PURE APPL. ALG. 40 (1986), p. 281-297.

[Ro2] , The Geometric Theory of P-Adic Fields, pré-publication.

[SvdD] P. Scowcroft et L. van den Dries, On the Structure of Semi-Algebraic Sets over p-Adic Fields, pré-publication.

[vdD] L. van den Dries, Artin-Schreier Theory for Commutative Regular Rings, ANN. MATH. LOGIC 12 (1977), p. 113-150.

L. Bélair
Université de Paris VII - C.N.R.S.
Equipe de logique mathématique, U.A. 753
2, place Jussieu
Paris, 5ième

XVII^{ème} PROBLEME DE HILBERT AU NIVEAU n DANS LES CORPS CHAINE-CLOS

Françoise Delon, C.N.R.S., Université Paris 7

Danielle Gondard, Université Paris 6

Le XVII^{ème} problème de Hilbert classique concerne la caractérisation des polynômes $f \in \mathbb{R}[\overline{X}]$ qui ne prennent sur $\mathbb{R}^n$ que des valeurs positives ou nulles. Artin a montré que, si K est réel clos et $f \in K(\overline{X})$, alors

$$(\forall \overline{x} \in K \quad f(\overline{x}) \geq 0) \Leftrightarrow f(\overline{X}) \in \Sigma\, K(\overline{X})^2 \quad ,$$

équivalence qu'on peut aussi écrire, pour souligner l'analogie entre ses deux membres,

$$(\forall \overline{x} \in K \quad f(\overline{x}) \in \Sigma\, K^2) \Leftrightarrow f(\overline{X}) \in \Sigma\, K(\overline{X})^2 \ .$$

Il ne peut y avoir une équivalence de même nature pour les puissances 2^n car, dans un corps réel clos K, $\Sigma K^2 = K^2 = K^{2^n} = \Sigma K^{2^n}$. Par contre, sur un corps K vérifiant $\Sigma K^{2^{n+1}} \subsetneq \Sigma K^{2^n}$ pour tout entier n, on peut espérer une équivalence

$$(\forall \overline{x} \in K \quad f(\overline{x}) \in \Sigma\, K^{2^n}) \Leftrightarrow f(\overline{X}) \in \Sigma\, K(\overline{X})^{2^n} \ .$$

Becker [B] a montré que les corps ordonnables K vérifiant $\Sigma K^{2^{n+1}} \subsetneq \Sigma K^{2^n}$ sont ceux qui portent un ordre de niveau supérieur non trivial. Ce sont aussi les corps chaînables de Harman [H]. A l'intérieur de cette famille, les corps chaîne-clos sont l'analogue des réels clos parmi les ordonnables ; on peut ici les définir par la

caractérisation algébrique suivante : K *est chaîne-clos ssi il porte une valuation* v *hensélienne, avec* K/v *réel clos,* vK *impair-divisible et* $|vk/2vk| = 2$. Pour préciser la description, considérons sur K chaîne-clos l'ensemble V(K) des valuations ayant les propriétés ci-dessus, et choisissons un ordre de K. Les valuations de V(K) sont convexes (par définition une valuation v est convexe lorsque son anneau de valuation A_v l'est, au sens habituel ; une valuation hensélienne sur un corps ordonné est nécessairement convexe) et donc comparables pour l'ordre habituel sur les valuations : $v \geq w$ (v plus fine que w) lorsque $A_v \subset A_w$. Il est facile de vérifier que V(K) admet un élément minimal v_0, défini par $A_{v_0} = \cup\{A_v ; v \in V(K)\}$, et pour lequel $2v_0K$ est dense dans v_0K, et un élément maximal v_1, défini par $A_{v_1} = \cap\{A_v ; v \in V(K)\}$ et pour lequel K/v_1 est archimédien. Autrement dit on a les équivalences plus fines que la caractérisation donnée précédemment :

K chaîne-clos ssi il existe $v \in V(K)$ avec 2 vK dense dans vK

ssi il existe $v \in V(K)$ avec K/v archimédien.

Cela n'est évidemment pas équivalent en général à la propriété "il existe $v \in V(K)$ avec 2vK dense dans vK et K/v archimédien", mais le sera lorsque $v_0 = v_1$, c'est-à-dire lorsque V(K) est réduit à un unique élément.

On peut maintenant énoncer le résultat

Définition - $f \in K(\overline{X})$ *a la propriété* (★) *sur le corps* K *lorsqu'on a :* $\forall \overline{x} \in K \quad f(\overline{x}) \in \Sigma K^{2^n}$.

Théorème - *Soit un corps* K *chaîne-clos tel que* V(K) *n'a qu'un élément et* $f \in K(X)$. *Alors* $f \in \Sigma K(X)^{2^n}$ *ssi* f *a la propriété* (★) *sur toute extension algébrique ordonnable de* K.

(Rappelons que dans un corps chaîne-clos $K^{2^n} = \Sigma K^{2^n}$ et soulignons le fait que, dans cet énoncé, f est une fraction rationnelle à une seule variable).

Il est clair que pour tout corps K et $f \in K(\overline{X})$, $f \in \Sigma K(\overline{X})^{2^n}$ ssi f satisfait $(\star)$ sur toute extension L de K. Le théorème dit que, sous certaines hypothèses, il suffit de considérer les cas où L est algébrique sur K et ordonnable, donc bien sûr, les cas où L est de degré fini sur K et ordonnable (en fait les cas $[L : K]$ au plus égal au degré de f suffisent). On verra qu'il y a peu de telles extensions (2^n extensions de degré 2^n pour tout n) et qu'elles ressemblent beaucoup à K ; elles sont chaîne-closes.

Les faits suivants montrent que, sauf une extension possible au cas où f a plusieurs variables, l'énoncé du théorème ne peut être radicalement amélioré (K est maintenant chaîne-clos) :

1) f satisfait $(\star)$ sur $K \not\Rightarrow f \in \Sigma K(\overline{X})^{2^n}$;

2) pour $n = 1$ le théorème est vrai sans autre hypothèse sur K que le fait d'être ordonnable, c'est ce que dit la proposition 15 ; par contre, pour tout entier $n \geq 2$ et K avec plus d'un élément dans $V(K)$, il y a des contre-exemples.

Pour une autre généralisation du $17^{\text{ème}}$ problème de Hilbert sur les corps chaîne-clos, consulter [B-J].

I - DESCRIPTION DES EXTENSIONS ALGEBRIQUES D'UN CORPS CHAINE-CLOS

Lemme 1 - *Soit un corps valué* (K,v) *hensélien, de caractéristique résiduelle nulle et vérifiant* $K/v = (K/v)^2 \cup [-(K/v)^2]$.

Supposons de plus K *ordonnable. On a alors l'équivalence*

$$\forall x \in K \qquad x \in K^{2^n} \Leftrightarrow 2^n | v(x) \quad \text{et} \quad x > 0$$

(Démonstration sans problème).

Ce lemme s'applique en particulier lorsque K est chaîne-clos avec $v \in V(K)$. Plus précisément :

Lemme 2 - *Si* K *est chaîne-clos et* $x \in K$:

a) $\forall v \in V(K)$, $x \in K^{2^n} \cup (-K^{2^n})$ *ssi* $2^n | v(x)$

b) $x \in K^{2^n} \cup (-K^{2^n})$ *ssi* $\exists\, v \in V(K)$, $2^n | v(x)$.

Corollaire 3 - *Soit* K *chaîne-clos ; alors pour tout* $k \in K - (\pm K^2)$, *on a* $K = K^2 \cup (-K^2) \cup kK^2 \cup (-kK^2)$.

Démonstration - Pour $v \in V(K)$, on a $vK = (2vK)(g_0)$ pour tout $g_0 \notin 2vK$, ou encore $vK = 2vK \cup \{2g + g_0 \ ; \ g \in vK\}$; donc pour $x \in K$, ou bien $2 | v(x)$ et $x \in \pm K^2$, ou bien $2 | v(k^{-1}x)$ si $v(k) = g_0$, et $x \in \pm kK^2$. □

Lemme 4 - *Les extensions algébriques de degré 2 de* K *chaîne-clos sont :*

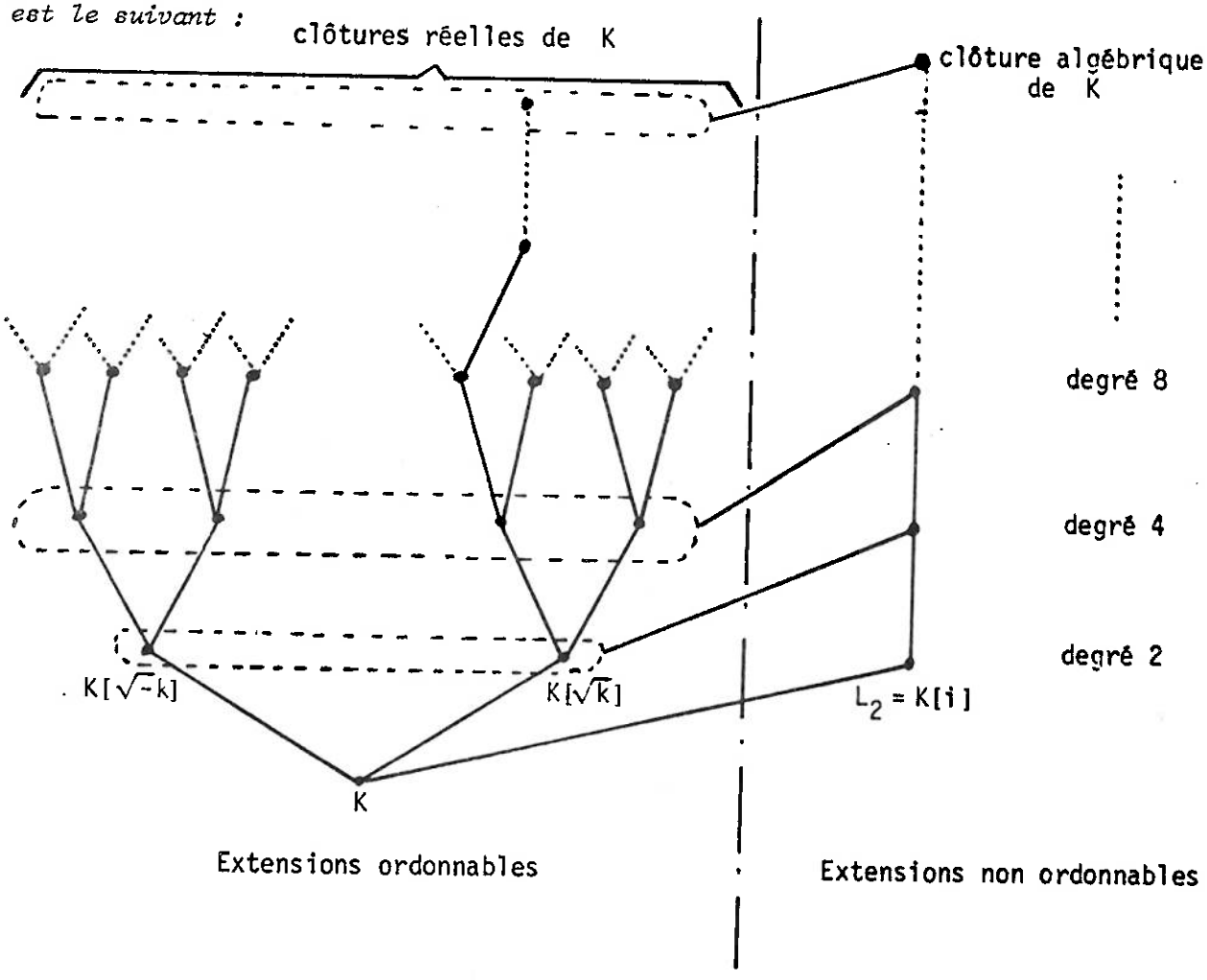
$K[i]$ *non ordonnable (où* $i^2 = -1$)

$K[\sqrt{k}]$ *et* $K[\sqrt{-k}]$ *pour un* k *fixé* $\notin \pm K^2$.

Ces 2 dernières extensions sont chaîne-closes.

Démonstration - Soit $v \in V(K)$. Si M est une extension algébrique de K, v se prolonge de façon unique à M et reste hensélienne, l'extension $K/v \subset M/v$ est algébrique et $vK \subset vM$ rationnelle (c'est-à-dire que vM se plonge dans la clôture divisible de vK). Le théorème d'Ostrowski nous dit, pour $[M:K]$ fini, $[M:K] = [M/v : K/v]\,(vM ; vK)$. Si $[M:K] = 2$, ou bien $[M/v : K/v] = 2$ et M/v est algébriquement clos, donc M non ordonnable, et $vM = vK$; ou bien $M/v = K/v$ et $(vM ; vK) = 2$; Dans ce cas là, M reste chaîne-clos car v est hensélienne sur M, $M/v = K/v$ et vM conserve les propriétés demandées à vK à cause de la relation $(vM ; vK) = 2$. De plus $M = K[k]$ pour un $k \in K - (\pm K^2)$; en effet $M = K[m]$ avec $v(m) \in vK/2$; il existe k et $k' \in K$ vérifiant $v(m^2k) = 0$ et $m^2k/v = (k'/v)^2$; donc $M = K[\sqrt{k}]$. A cause du corollaire 3 il n'y a que deux telles extensions distinctes, et elles sont de la forme indiquée. □

Proposition 5 - *Le treillis des extensions algébriques d'un corps K chaîne-clos est le suivant :*



Démonstration - Une extension finie de K engendre une extension galoisienne M qui doit être de degré 2^n d'après le théorème d'Ostrowski, donc résoluble ; en conséquence il existe L' , $K \subset L' \subset M$, de degré 2 sur K . Le résultat s'obtient alors par induction en remarquant que :

- aucun corps ordonnable ne contient simultanément $\sqrt{x}$ et $\sqrt{-x}$, donc tous les corps décrits dans la partie gauche de l'arbre sont bien distincts ;
- le corps $L_2\,[\sqrt{k}] = L_2\,[\sqrt{-k}]$ est l'unique extension de degré 2 de L_2 . □

Corollaire 6 - *Les extensions algébriques ordonnables d'un corps chaîne-clos sont de deux types :*

- *les extensions finies qui sont chaîne-closes ;*
- *les extensions infinies qui sont réelles closes.*

Démonstration - Une extension infinie est de la forme $M = \cup K_n$ pour une suite croissante de K_n , avec $K_o = K$; si M est ordonnable, les K_n vérifient $K_n/v = K/v$ et, par exemple, $(vK_{n+1} ; vK_n) = 2$; vK_{n+1} est la seule extension de dimension 2 de vK_n , donc $vM = \cup vK_n$ est 2-divisible. □

II - GROUPES ABELIENS ORDONNES n-REGULIERS

Les groupes abéliens ordonnés (ou "g.a.o.") n-régulier ont été introduits par Robinson et Zakon [R-Z] . Les équivalences des lemmes 7 et 8 sont faciles à vérifier (sauf peut-être $1 \Rightarrow 7$ dans le lemme 7 ; on en trouvera la preuve dans [S] pages 8 et 9). Le lemme 9 a été montré, dans un contexte beaucoup plus général, par Robinson et Zakon ; il a motivé la définition des n-réguliers.

Définition - *Un g.a.o.* G *tel que* $2G$ *soit dense dans* G *est dit dense 2-régulier*

Lemme 7 - *Sont équivalents*

1. G *est dense 2-régulier* ;
2. $2^n G$ *est dense dans* G *pour tout entier* $n > 0$;
3. " *un* " ;
4. $G \models \forall g_1 < g_2 \quad \forall g \quad \exists h \ [h \equiv g \ (2^n) \wedge g_1 < h < g_2]$ *pour tout* $n > 0$;
5. " " " *pour un* $n > 0$;
6. G *est dense dans sa clôture 2-divisible* $\hat{G}$;
7. $\forall g_1 < g_2 \in \hat{G} \quad \forall g \in G \quad \exists h \in G$
$g_1 < h < g_2 \wedge g \equiv h \ (2^n)$ *dans* G .

Lemme 8 - Si G *est dense,* G *est dense 2-régulier ssi pour tout sous-groupe convexe* H *de* G *(ce qu'on note* $H \lhd G$*),* $H \neq 0$ *entraîne* G/H *est 2-divisible.*

Lemme 9 - *Soient* $H \subset G$ *deux g.a.o. denses 2-réguliers impair-divisibles et vérifiant* $(H ; 2H) = (G ; 2G)$. *Alors* $H \prec G$ *ssi* H *est pur* (i.e. ***divisiblement clos***) *dans* G .

Lemme 10 - *Soit* G *un g.a.o. dense 2-régulier et* $H \lhd G$. *Alors* $H = 0$ *ou* $(H ; 2H) = (G ; 2G)$.

Démonstration - Découle du lemme 8 . □

III - INCLUSIONS DE CORPS CHAINE-CLOS

Si $v \geqslant w$ sont deux valuations sur un corps K on en déduit une valuation v/w sur K/w : si $p_v : A_v \to K/v$ est le passage au quotient modulo v, v/w est définie par $A_{v/w} = p_w(A_v)$; $(v/w)(K/w)$ s'identifie alors à un sous-groupe convexe de vK, par l'égalité (si $w(x) = 0$) $(v/w)(x/w) = v(x)$, et les corps de restes $(K/w)/(v/w)$ et K/v sont canoniquement isomorphes. Cette construction admet un genre de réciproque : si w est une valuation sur K et $\overline{v}$ une valuation sur K/w, on définit la valuation "composée de w et $\overline{v}$", qu'on notera $w \times \overline{v}$, définie par $A_{w \times \overline{v}} = p_w^{-1}(A_{\overline{v}})$. Pour toutes ces constructions, nous renvoyons à [Rib] partie C. On a $w \times \overline{v} \geqslant w$, $w \times \overline{v}/w = \overline{v}$ et $w \times (v/w) = v$; enfin $w \times \overline{v}$ est hensélienne ssi w et $\overline{v}$ le sont.

L'ensemble $W(K)$ des valuations convexes sur un corps K ordonné est totalement ordonné ; il admet un premier élément, la valuation triviale, et un dernier élément, la valuation archimédienne v_1, dont l'anneau est la clôture convexe de $\mathbb{Q}$ dans K. Pour des valuations $v \geqslant w$ sur K ordonné, v est convexe ssi w et v/w le sont.

Si K est chaîne-clos, il porte exactement deux ordres qui sont échangeables dans un automorphisme de K laissant v_1 invariante. En conséquence, une valuation est convexe pour un ordre de K ssi elle l'est pour l'autre ; cela permet de parler de $W(K)$ sans préciser l'ordre sur K. On notera désormais $v_K = \min V(K)$ (c'est-à-dire la plus grossière notée v_0 dans l'introduction).

Proposition 11 - *Soit K chaîne-clos ; alors $V(K)$ est le segment final de $W(K)$ de 1er élément v_K et on a les équivalences, pour $v \in W(K)$:*

- $v \in V(K)$ *ssi* K/v *est réel clos ssi* $(vK ; 2vK) = 2$
- $v \notin V(K)$ *ssi* K/v *est chaîne-clos ssi* vK *est divisible.*

Démonstration

1. Si $v \geq v_K$, v est la composée de v_K et v/v_K ; K/v_K étant réel clos, $(v/v_K)(K/v_K)$ est divisible et vK est une extension de $(v/v_K)(K/v_K)$, qui est divisible, par $v_K K$, qui vérifie $(v_K K ; 2v_K K) = 2$; donc $(vK ; 2vK) = 2$.

2. Si $v < v_K$, $(v_K/v)(K/v)$ est un sous-groupe convexe non nul de $v_K K$, donc $((v_K/v)(K/v) ; 2(v_K/v)(K/v)) = 2$ d'après le lemme 10. Par ailleurs $(K/v)/(v_K/v) \simeq K/v_K$ est réel clos et v_K/v reste hensélienne, donc $v_K/v \in V(K/v)$, ce qui prouve que K/v est chaîne-clos. Enfin $(vK ; 2vK) = 2$ parce que $v_K K$ est une extension de $(v_K/v)(K/v)$ par vK . □

Proposition 12 - *Soient deux corps chaîne-clos* $K \subset L$ *avec un seul élément dans* $V(K)$. *Alors sont équivalents :*

1. $K \cap L^2 = K^2$
2. K *relativement algébriquement clos dans* L
3. $K \prec L$.

Démonstration

$1 \Rightarrow 2$ - Clair d'après la proposition 5 .

$2 \Rightarrow 3$ - Soit $k \in K - (K^2 \cup -K^2)$; d'après 2, $k \notin L^2 \cup -L^2$ donc $v_L(k)$ n'est pas divisible par 2 dans $v_L L$, a fortiori dans $v_L K$; alors, d'après la proposition 11, K/v_L est réel clos, donc $v_L \restriction K = v_K$ d'après l'hypothèse sur $V(K)$, c'est-à-dire $(K, v_K) \subset (L, v_L)$. On a $K/v_K \prec L/v_L$ puisque ces 2 corps sont réels clos. D'après Ax- Kochen - Eršov il suffit de $v_K K \prec v_L L$ pour avoir $(K, v_K) \prec (L, v_L)$; d'après le lemme 9, il suffit de montrer que $v_K K$ est pur dans $v_L L$; or, pour $k \in K$ et $g = v_K(k)$, on a $2|g$ dans $v_K K$ ssi (lemme 2) $k \in \pm K^2$ ssi (hypothèse 2) $k \in \pm L^2$ ssi $2|g$ dans $v_L L$. □

Le modèle complétude de la théorie des corps chaîne-clos ne peut être obtenue que dans un langage enrichi. On trouvera deux résultats de cette nature dans [Di] et [J] .

Nous allons utiliser une autre caractérisation des corps chaîne-clos (voir [G]).

Proposition 13 - *Un corps ordonnable* K *est chaîne-clos ssi il a les propriétés suivantes :*

1. K *n'admet aucune extension finie de degré impair*
2. $(K^* ; K^{*4}) = 4$
3. $K^2 = K^2 + K^2$
4. $K^4 = K^4 + K^4$.

Proposition 14 - *Soit* K *relativement algébriquement clos dans* L *chaîne-clos. Alors* K *est ou chaîne-clos ou réel clos.*

Démonstration - Les propriétés 1, 3 et 4 de la caractérisation précédente passent de L à K ; selon que $(K^*; K^{*4}) = 4$ ou 1 , K est chaîne-clos ou réel clos. □

IV - QUELQUES CONSEQUENCES DE LA PROPRIETE (★)

Définition - *On appelle* (★★) *la propriété* (★) *au niveau* 1 *c'est-à-dire*, $f \in K(\overline{X})$ a (★★) *sur* K *si* : $\forall \overline{x} \in K \quad f(\overline{x}) \in \Sigma K^2$.

Proposition 15 - *Soit un corps ordonné* K *et* $f \in K(\overline{X})$. *Si* f *a la propriété* (★★) *sur toute extension algébrique ordonnable de* K, *alors* $f \in \Sigma K(\overline{X})^2$.

Démonstration - Il faut montrer que f est positif pour tout ordre sur $K(\overline{X})$, ou encore positif dans toute clôture réelle L de $K(\overline{X})$. Si K' est la clôture algébrique relative de K dans L, on a $K' \prec L$. Par hypothèse f conserve (★★) sur K', donc aussi sur L ; mais alors on trouve $f \in \Sigma L^2$ en faisant $\overline{x} = \overline{X}$ dans (★★), donc f positif ou nul dans L . □

Dans la suite K est chaîne-clos, v_K est notée v, et $x \sim y$ est la relation d'équivalence $v(x) = v(y) < v(x-y)$; si $x \sim y$ on a, pour tout entier $n > 0$, $x \in K^m$ ssi $y \in K^m$ (lemme 1).

Lemme 16 - *Soit* K *chaîne-clos et* $f \in K[X]$ *satisfaisant* (★) *sur* K . *Alors le terme de plus bas degré de* f *est une puissance* 2^n .

Démonstration - On peut écrire $f(X) = aX^m(1+g(X))$ avec $a \in K$, $g \in K(X)$ $v_X(g) > 0$. Si on prend $x \in K$ de (v_K)-valuation assez grande pour absorber les valuations éventuellement négatives des coefficients de g, on a $v(g(x)) > 0$ donc $1+g(x) \in K^{2^n}$ pour tout n . En conséquence (★) implique

(E) $\forall x \in K$ avec $v(x)$ assez grand, $ax^m \in K^{2^n}$.

Si on prend $x_1 \in K$ de valuation grande et divisible par 2^n, on a $ax_1^m \in K^{2^n}$, donc $2^n | v(ax_1^m)$, donc $2^n | v(a)$. On prend maintenant $x_2 \in K$ avec $v(x_2)$ grand mais non 2-divisible ; alors $2^n | v(ax_2^m)$ implique $2^n | m$. Enfin (E) permet maintenant de conclure $a \in K^{2^n}$. □

Lemme 17 - *Mêmes hypothèses. Alors toute racine de* f *dans* K *est d'ordre divisible par* 2^n .

Démonstration - Le lemme précédent donne le résultat pour la racine nulle. Par ailleurs si f satisfait (*), $f(X-a)$ aussi pour tout $a \in K$, d'où le résultat. □

Lemme 18 - *Mêmes hypothèses. Alors le terme de plus haut degré de* f *est une puissance* 2^n .

Démonstration - Si f satisfait (*) il en va de même de $f(X^{-1})$. Si $f = \sum_0^m a_i X^i$ avec $a_m \neq 0$, alors

$$f(X^{-1}) = X^{-2^{sn}} \underbrace{\sum_0^m a_i X^{2^{sn-i}}}_{g(x)} .$$

Pour s assez grand $g(X)$ est un polynôme, et il satisfait (*). Son terme de plus bas degré est donc une puissance 2^n , c'est-à-dire

$$a_m X^{2^{sn}-m} \in K(X)^{2n} \Rightarrow 2^n | m \text{ et } a_m \in K^{2^n} . \square$$

Lemme 19 - *Mêmes hypothèses. Alors le nombre de racines de* f *(dans la clôture algébrique de* K*) ayant une valuation donnée est divisible par* 2^n .

Démonstration - Décomposons

$$f(X) = \Pi(X-b_i) \prod_{i=1}^{A} (X-a_i) \quad \text{où} \quad v(a_i) = v(a_j) > v(b_i)$$

et prenons $g \in vK$, vérifiant $v(b_j) < g < v(a_i)$ et

- si $v(a_i) \in vK$, alors $g \not\equiv v(a_i) \pmod 2$;
- sinon (alors $a_i \in vK/2^s$ pour un certain $s \leq n$), $2 | g$; (cela se fait grâce au lemme 7).

Alors, si $x \in K$ avec $v(x) = g$,

$2^n | v(f(x)) = \Sigma\, v(b_i) + Ag$. Par ailleurs

$2^n | v(f(0)) = \Sigma\, v(b_i) + Av(a_i)$. Donc

$2^n | A(g - v(a_i))$, et $2^n | A$.

Puis on raisonne par induction ; si on sait que

$f(x) = \prod_C (x-g_i) \prod_F (x-f_i) \prod_E (x-e_i) \ldots \prod_A (x-a_i)$ avec

$$v(g_j) < v(f_i) = v(f_j) < v(e_i) = v(e_j) < \ldots < v(a_i) = v(a_j)$$

et $2^n | E, \ldots, A$, on choisit x_1 et $x_2 \in K$ vérifiant

$$v(f_i) < v(x_1) < v(e_j) \quad , \quad v(g_i) < v(x_2) < v(f_j)$$

et $v(x_2) \not\equiv v(f_i) \pmod{2vK}$; alors

$2^n | v(f(x_1)) = \Sigma\, v(g_i) + Fv(f_i) + 2^n . A_1$

$2^n | v(f(x_2)) = \Sigma\, v(g_i) + Fv(x_2) + 2^n . A_2$,

donc $2^n | F$. □

V - DEMONSTRATION DU THEOREME

L'implication $\Rightarrow$ est claire. Supposons donc que $f \in K(X)$ a la propriété (*) sur toute extension algébrique ordonnable de K, il nous faut montrer $f \in \Sigma K(X)^{2^n}$. Nous allons utiliser la caractérisation suivante :

Proposition [B] et [H] - *Soit un corps ordonnable* C *et* $a \in C$. *Alors* $a \in \Sigma C^{2^n}$ *ssi* $a \in \Sigma C^2$ *et* a *est dans tout ordre de niveau exact* 2^n *sur* C.

Nous allons appliquer ce théorème à f dans le corps $C = K(X)$. Il est clair qu'on peut se réduire à $f \in K[X]$. Nous savons déjà grâce à la proposition 15 que f est dans $\Sigma K(X)^2$, il reste à montrer qu'il est dans tout ordre de niveau exact 2^n sur $K(X)$. Soit P un tel ordre, par lequel on fait passer une chaîne [voir [H], cor. 1.4] de $K(X)$, soit L la clôture pour cette chaîne, soit $\overline{P}$ le prolongement de P à L et K' la clôture algébrique relative de K dans L ; K' est ordonnable et f conserve donc la propriété (*) sur K'. Grâce à la proposition 14, K' est réel clos ou chaîne-clos.

1. Si K' est chaîne-clos, alors $K' \prec L$ donc f a la propriété (*) sur L et $f(X) \in L^{2^n} \subset \overline{P}$ donc $f \in \overline{P} \cap K(X) = P$.

2. Supposons K' réel clos. Soit $v = v_K$ et $w = v_L$; wK' est divisible ; par contre $wK'(X)$ ne l'est pas, sinon wL le serait (car L est une extension algébrique de $K(X)$) ; donc $wK' \subsetneq wK'(X)$. Puisque $K'(X)$ est ordonnable, il est plongeable dans une extension élémentaire de K', et même il existe $(M,w) \succ (K',w)$ avec $X \in M$ (prendre pour M la clôture réelle de L pour un de ses ordres et l'unique prolongement de w de L à M). La situation est alors bien connue ([D], th. 2.20 p. 54) : il existe $c \in K'$ tel que $w(X-c) \notin wK'$ et même $w(X-c)$ irrationnel sur wK'. Par ailleurs $K[c]$ est chaîne-clos et f y satisfait (*), donc (lemme 19) se décompose

$$f = \prod_A (X-c+a_i) \cdot \prod_B (X-c+b_i) \ldots$$

avec $v(a_i) = v(a_j) < v(b_i) = v(b_j) < \ldots$ et $2^n | A, B, \ldots$

Puisque w est convexe sur L, $w|K$ l'est sur K et donc est plus grossière que la valuation archimédienne sur K, dont on a supposé qu'elle coïncidait avec $v = v_K$; donc $w|K \leq v_K$ et $w(a_i) = w(a_j) < w(b_i) = w(b_j) < \ldots$. On sait que $w(X-c)$ est distinct de $w(a_i), w(b_i), \ldots$ et donc se place entre deux d'entre eux, c'est-à-dire $w(a_i), w(b_i), \ldots, w(e_i) < w(X-c) < w(f_i), \ldots$

Mais alors $f(X)$ est équivalent pour w à

$$\underbrace{\Pi a_i \cdot \Pi b_i \ldots \Pi e_i}\ \Pi(X-c)^{F+G} \cdots ;$$

or $2^n | A,B,\ldots,F,G,\ldots \Rightarrow 2^n | w(f(X))$. Donc $f(X) \in \overline{P}$ puisque $f(X)$ est positif pour tout ordre. □

BIBLIOGRAPHIE

[B] E. Becker : "Hereditarily pythagorean fields and orderings of higher types", I.M.P.A., Lectures notes n° 29 (1978), Rio de Janeiro.

[B-J] E. Becker et B. Jacob : "Rational points on algebraic varieties over a generalized real closed field : a model theoretic approach"
J. fur die reine und ang. Mathematik, 357, 1985.

[D] F. Delon : "Quelques propriétés des corps valués en Théorie des modèles"
Thèse de Doctorat d'Etat, Université de Paris 7, 1982.

[Di] M. Dickmann : "The Model Theory of chain closed fields"
à paraître : J.S.L.

[G] D. Gondard : "Théorie du premier ordre des corps chaînables et des corps chaîne-clos"
C.R. Acad. Sc. Paris, t. 304, Série I, n° 16, 1987, pp. 463-465.

[H] J. Harman : "Chains of higher level orderings"
Contemporary Mathematics, Vol 8 (1982), pp. 141-174.

[J] B. Jacob : "The model theory of generalized real closed fields"
J. fur die reine und ang. Mathematik, 323, 1981.

[Rib] P. Ribenboim : "Théorie des Valuations"
Les presses de l'Université de Montréal, 1964.

[R-Z] A. Robinson et E. Zakon : "Elementary properties of ordered abelian groups"
Trans. A.M.S., 96 (1960), pp. 222-236.

[S] P. Schmitt : "Model Theory of ordered abelian groups"
Habilitationsschrift, Heidelberg, 1982.

MAXIMALITY PROPERTIES OF VALUED FIELDS: SOME NEW RESULTS

Franz–Viktor Kuhlmann, Heidelberg

In this paper we want to present the (partial) solution of a problem stated in [5]. We called it the problem of separating immediate from anti-immediate extensions. We considered that problem mainly for model theoretical reasons, but the solution involves some valuation theoretical results that might be of independent interest. On the other hand, in the following presentation we want to examplify our general approach by proving a result of ERSHOV and ZIEGLER about finitely ramified fields in a different and somewhat more algebraic way.

For the general framework of our investigations, we refer to the article [5]. Let us explicitly recall here the two properties (M5) and (M6). A field (K,v) is said to have the property (M5) if it is existentially closed in every immediate extension. (K,v) has property (M6) if it is an AX – KOCHEN – ERSHOV – field, i.e. for any extension $(L,v) \mid (K,v)$ with $v(K) \prec_\exists v(L)$ and $\overline{K} \prec_\exists \overline{L}$ it follows that $(K,v) \prec_\exists (L,v)$ ("$\prec_\exists$" denotes "existentially closed in"). The central question of our work is whether every algebraically complete valued field has property (M6). Many elementary classes of valued fields are known for which this is true, but the general problem is still unsolved. A first step towards a general solution might be the following theorem:

Theorem 1: *Let (K,v) be algebraically complete and $(L,v) \mid (K,v)$ an anti-immediate extension. If $v(K) \prec_\exists v(L)$ and $\overline{K} \prec_\exists \overline{L}$, then $(K,v) \prec_\exists (L,v)$.*

Here $(L,v) \mid (K,v)$ is called anti-immediate, if for every subextension $(L_0,v) \mid (K,v)$ such that L_0 is finitely generated over K, the following equality holds:

$$\mathrm{trdeg}(L_0 \mid K) = \mathrm{trdeg}(\overline{L_0} \mid \overline{K}) + \mathrm{rr}(v(L_0)/v(K))$$

where $\mathrm{rr}(\Gamma)$ denotes the rational rank of the ordered abelian group Γ (= the $\mathbb{Q}$-dimension of the vector space $\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma$).

For this definition and a description of the proof of Theorem 1, see [5].

Clearly, the question arises whether Theorem 1 can serve us to reduce our general problem to the problem whether any algebraically complete field has property (M5). Indeed, suppose that for a given extension $(L,v) \mid (K,v)$ with (K,v) algebraically complete, $v(K) \prec_\exists v(L)$ and $\overline{K} \prec_\exists \overline{L}$, we would find a subextension $(K_1,v) \mid (K,v)$ such that

1) $(K_1,v) \mid (K,v)$ is anti-immediate,
2) $(L,v) \mid (K_1,v)$ is immediate,
3) (K_1,v) is algebraically complete,

then we could conclude $(K,v) \prec_\exists (K_1,v)$ by Theorem 1, and if we would know that every algebraically complete field is existentially closed in every immediate extension then we would get $(K_1,v) \prec_\exists (L,v)$ and thus $(K,v) \prec_\exists (L,v)$. This shows that the existence of such intermediate fields would immediately yield the desired reduction of our general problem. Unfortunately, we can't expect the existence of such fields for any extension $(L,v) \mid (K,v)$ with the above properties. We have to introduce additional conditions for the extension $(L,v) \mid (K,v)$.

Firstly, it is natural to work in an elementary class K of algebraically complete fields. Now our general problem, relative to K, is whether every $(K,v) \in K$ has property (M6) restricted to extensions $(L,v) \mid (K,v)$ with $(L,v) \in K$ (we call this property $(\mathrm{M6})_K$). We want to reduce this to the problem, whether every $(K,v) \in K$ has property (M5) restricted to immediate extensions $(L,v) \mid (K,v)$ with $(L,v) \in K$ (i.e. $(\mathrm{M5})_K$). Every class K which contains an intermediate field with the described properties for every extension $(L,v) \mid (K,v)$ where both fields are in K is immediately seen to satisfy the equivalence $(\mathrm{M5})_K \Leftrightarrow (\mathrm{M6})_K$.

Secondly, since not every class will have these intermediate fields for every extension, we should make use of saturation. We want to show that it is enough to find these intermediate fields for extensions with nice saturation properties. But before doing this, we want to draw the reader's attention to the meaning of the property $(\mathrm{M6})_K$.

If an elementary class of algebraically complete fields satisfies $(\mathrm{M6})_K$, it will follow from general model theory that K is model complete if $v(K) := \{v(K) \mid (K,v) \in K\}$ and $\overline{K} := \{\overline{K} \mid (K,v) \in K\}$ are model complete elementary classes. Take for instance the class K_1 given by the axioms

1) (K,v) is an algebraically complete valued field
2) $\mathrm{char}(K) = p > 0$
3) $v(K)$ is a $\mathbb{Z}$-group with smallest positive element $v(\tau)$
4) $\overline{K} = \mathbb{F}_q$ with $q = p^r$

where τ is a constant that we add to the language of valued fields. If in K_1 every field has the property $(\mathrm{M6})_{K_1}$, then K_1 is model complete. Now K_1 has the prime model $(\mathbb{F}_q(t),v)^h$ which is the henselization of the field $(\mathbb{F}_q(t),v)$ with $v(t) = 1$ and residue field $\mathbb{F}_q$. Hence model completeness of K_1 implies completeness of K_1 and this in turn implies the decidability of K_1 because the given axiom system is expressable by a recursive scheme of elementary sentences (cf. e.g. [2] for "algebraically complete" and [9] for "$\mathbb{Z}$-group"). Since the power series field $\mathbb{F}_q((t))$ with its natural valuation is a member of K_1 we conclude that it will have a decidable theory if every field in K_1 has the property $(\mathrm{M6})_{K_1}$.

The restriction of the properties (M5) and (M6) to elementary classes is no severe restriction, since for wellbehaving classes they are equivalent to their restrictions:

Lemma 1: *If K is axiomatized only by the axioms*

a) *"(K,v) is a valued field"*
b) *"$\mathrm{char}(K) = 0$" or "$\mathrm{char}(K) = p > 0$"*
c) *"(K,v) is henselian" or "(K,v) is algebraically maximal" or "(K,v) is algebraically complete"*
d) *axioms about the value groups and residue fields*

then for every $(K,v) \in K$ we have the equivalences:

$$(M5) \Longleftrightarrow (M5)_K\,, \quad (M6) \Longleftrightarrow (M6)_K\,,$$

and $v(K)$ and $\overline{K}$ are elementary classes.

Proof: Assume $(L,v) \mid (K,v)$ is an extension with $(K,v) \in K$ and $v(K) \prec_\exists v(L)$, $\overline{K} \prec_\exists \overline{L}$. Then $v(L)$ is embeddable over $v(K)$ into a $|v(L)|$-saturated elementary extension $v(K)^*$ of $v(K)$ and $\overline{L}$ is embeddable over $\overline{K}$ into a $|\overline{L}|$-saturated elementary extension $\overline{K}^*$ of $\overline{K}$. Take (L'',v) to be an extension of (L,v) with $\overline{L''} \cong \overline{K}^*$ and $v(L'') \cong v(K)^*$; (L'',v) can be found by

a straightforward construction. Take (L',v) to be a maximal immediate extension of (L'',v). Then (L',v) is algebraically complete (cf. [8], Theorem 1, p. 230), hence algebraically maximal and henselian. Moreover, it satisfies the axioms of d) since its residue field is an elementary extension of $\overline{K}$ and its value group is an elementary extension of $v(K)$. Consequently, $(L',v) \in \mathcal{K}$ with $\overline{K} \prec_\exists \overline{L'}$ and $v(K) \prec_\exists v(L')$. If (K,v) satisfies $(\mathrm{M6})_{\mathcal{K}}$ then $(K,v) \prec_\exists (L',v)$ and, a forteriori, $(K,v) \prec_\exists (L,v)$. This shows that (K,v) satisfies (M6) if it satisfies $(\mathrm{M6})_{\mathcal{K}}$.
If the extension $(L,v) \mid (K,v)$ is immediate, take (L',v) to be a maximal immediate extension of (L,v) so that the extension $(L',v) \mid (K,v)$ will be immediate too and $(L',v) \in \mathcal{K}$. If (K,v) satisfies $(\mathrm{M5})_{\mathcal{K}}$ then $(K,v) \prec_\exists (L',v)$ and thus $(K,v) \prec_\exists (L,v)$ showing that (K,v) satisfies (M5) if it satisfies $(\mathrm{M5})_{\mathcal{K}}$.
Given a field k and an ordered abelian group Γ satisfying the axioms of d), choose any valued field (N,v) of characteristic indicated by b) with $\overline{N} \cong k$ and $v(N) \cong \Gamma$. Take a maximal immediate extension (M,v) of (N,v). Then (M,v) is algebraically complete and thus satisfies all axioms of c). Consequently, $(M,v) \in \mathcal{K}$. This shows that $\overline{\mathcal{K}}$ and $v(\mathcal{K})$ are exactly the elementary classes given by the axioms of d).

Now we want to examine which elementary classes $\mathcal{K}$ of algebraically complete fields have the following reduction property:

(R) If every field in $\mathcal{K}$ has the property $(\mathrm{M5})_{\mathcal{K}}$, then every field in $\mathcal{K}$ has property $(\mathrm{M6})_{\mathcal{K}}$.

We have seen already that if a class $\mathcal{K}$ contains an intermediate field as described in the beginning for every extension of fields in $\mathcal{K}$, then $\mathcal{K}$ has the reduction property (R). This helps us to find a name for those intermediate fields, and we use the occasion to replace the condition "anti-immediate" by a condition that is slightly stronger but equivalent to "anti-immediate" in case of extensions of finite transcendence degree.

Definition: An intermediate field (K_1,v) of the extension $(L,v) \mid (K,v)$ is called a reduction field, if
1) $(K_1,v) \mid (K,v)$ admits a valuation transcendence basis,
2) $(L,v) \mid (K_1,v)$ is immediate,
3) (K_1,v) is algebraically complete.

A valuation transcendence basis of $(K_1,v) \mid (K,v)$ is a transcendence basis $(x_i, y_j \mid i \in I, j \in J)$ such that $(\overline{x_i} \mid i \in I)$ forms a transcendence basis of the extension $\overline{K_1} \mid \overline{K}$ and $(v(y_j) \mid j \in J)$ forms a maximal system of elements in $v(K_1)$ that are rationally independent over $v(K)$.

It can be shown that every extension admitting a valuation transcendence basis is anti-immediate. — Some elementary classes of algebraically complete fields contain reduction fields for every extension:
a) henselian fields with residue fields of characteristic 0,
b) henselian $\wp$–adic fields,
c) algebraically maximal perfect fields of characteristic $p > 0$.

The proof for a) is straightforward and just uses Hensel's Lemma. For b) see [7], Lemma 3.4 and Lemma 3.5. The proof for c) uses the following lemma (cf. [6]):

Lemma 2: *Let (L,v) be an algebraically maximal perfect field of characteristic $p > 0$ and (K_1,v) a relatively algebraically closed subfield such that $\overline{L} \mid \overline{K_1}$ is algebraic. Then (K_1,v) is algebraically maximal and perfect with $\overline{L} = \overline{K_1}$ and $v(K_1)$ pure in $v(L)$.*

In all these three cases the reduction fields can be found by choosing elements $x_i \in L$, $i \in I$ such that $(\overline{x_i} \mid i \in I)$ is a transcendence basis of $\overline{L} \mid \overline{K}$, and elements y_j, $j \in J$ such that $(v(y_j) \mid j \in J)$ is a maximal system of elements in $v(L)$ rationally independent over $v(K)$. The relative algebraic closure (K_1, v) of $(K(x_i, y_j \mid i \in I, j \in J), v)$ in (L, v) is a reduction field: By construction $(K_1, v) \mid (K, v)$ is anti-immediate and by Hensel's Lemma resp. Lemma 2 we know that $\overline{L} = \overline{K_1}$ and $v(L) = v(K_1)$. Being a relatively algebraically closed subfield of a henselian field, (K_1, v) is itself henselian and this is equivalent to "algebraically complete" in cases a) and b); in case c) we know by Lemma 2 that (K_1, v) is algebraically maximal, and for perfect fields of characteristic $p > 0$ this is equivalent to "algebraically complete" (cf. [5]).

To find reduction fields in more general cases, we need saturation properties. This is comparable to the use that model theorists made of saturated models to find cross–sections, and indeed the notion of a reduction field is in some way a generalization covering the value group extension as well as the residue field extension. Note that in all cases described above, if $(L, v) \mid (K, v)$ is an extension with $\overline{K} = \overline{L}$, from a cross–section π of (L, v) whose restriction to $v(K)$ is a cross–section of (K, v) we get a reduction field by taking the relative algebraic closure of $(K(\pi \circ v(L)), v)$ in (L, v) .

The saturation properties that we need are properties of a field extension rather than properties of one single field. So we will pass from one extension to a nicer one which is an elementary extension of the first one in the following sense: Given an extension $(L, v) \mid (K, v)$ of fields in the elementary class $\mathcal{K}$ we will add a new predicate to the language of valued fields whose range on L is just the subfield K. In this new language, we take an elementary extension (L', v) of (L, v) with the required saturation properties. Taking K' to be the range of the new predicate on L', $(L', v) \mid (K', v)$ is again an extension of fields in $\mathcal{K}$, (L', v) and (K', v) are elementary extensions of (L, v) and (K, v) resp., and (L', v) and (K', v) will have corresponding saturation properties. The proof of the next lemma shows that w.l.o.g. we may replace the old extension by the new one:

Lemma 3: *Let $\mathcal{K}$ be an elementary class of algebraically complete fields. If every special model in $\mathcal{K}$ of cardinality κ a limit cardinal satisfies $(M6)_{\mathcal{K}}$ [or $(M5)_{\mathcal{K}}$] then <u>every</u> field in $\mathcal{K}$ satisfies $(M6)_{\mathcal{K}}$ [or $(M5)_{\mathcal{K}}$ resp.].*

For the definition, existence and properties of special models see [1], chapter 5. The employment of special models was suggested to the author by M. ZIEGLER.

Proof: Let $(L, v) \mid (K, v)$ be an extension of fields in $\mathcal{K}$ with $\overline{K} \prec_\exists \overline{L}$ and $v(K) \prec_\exists v(L)$. The properties "$\overline{K} \prec_\exists \overline{L}$" and "$v(K) \prec_\exists v(L)$" can be expressed by a scheme of elementary sentences in the language of valued fields together with the predicate for the subfield K which are true in (L, v). This shows that for every elementary extension $(L', v) \mid (K', v)$ of $(L, v) \mid (K, v)$ we will have $\overline{K'} \prec_\exists \overline{L'}$ and $v(K') \prec_\exists v(L')$. Assume $(K', v) \prec_\exists (L', v)$. Given an existential formula with parameters from K that holds in (L, v), it holds in (L', v) too since (L', v) is an overfield of (L, v), and it holds in (K', v) because of $(K', v) \prec_\exists (L', v)$. In view of $(K, v) \prec (K', v)$, it holds in (K, v) too, showing that $(K, v) \prec_\exists (L, v)$ if $(K', v) \prec_\exists (L', v)$. Now choose $(L', v) \mid (K', v)$ to be a special elementary extension of $(L, v) \mid (K, v)$ of cardinality κ a limit cardinal $> \kappa_0$. Then (K', v) will be a special elementary extension of (K, v) of cardinality κ. If it satisfies $(\mathrm{M6})_{\mathcal{K}}$ then $(K', v) \prec_\exists (L', v)$ and thus $(K, v) \prec_\exists (L, v)$. This shows our proposition for $(\mathrm{M6})_{\mathcal{K}}$. Now if $(L, v) \mid (K, v)$ is immediate this is an elementary property of the extension $(L, v) \mid (K, v)$ which will be inherited by the extension $(L', v) \mid (K', v)$. Hence

if (K',v) satisfies $(\mathrm{M5})_{\mathcal{K}}$ then again $(K',v) \prec_\exists (L',v)$, which yields $(K,v) \prec_\exists (L,v)$. This proves the proposition for $(\mathrm{M5})_{\mathcal{K}}$.

If we want to show that a given valued field (K,v) in a given elementary class $\mathcal{K}$ satisfies $(\mathrm{M5})_{\mathcal{K}}$ or $(\mathrm{M6})_{\mathcal{K}}$, we may replace it in view of the preceeding lemma by a special model of cardinality κ a limit cardinal. In addition, given an extension field (L,v) for which we want to prove $(K,v) \prec_\exists (L,v)$, we may assume by the following lemma that (L,v) is a special model of cardinality λ a limit cardinal with cofinality bigger than κ.

Lemma 4: *Let $(L,v) \mid (K,v)$ be an extension with $\overline{K} \prec_\exists \overline{L}$ and $v(K) \prec_\exists v(L)$ and (L',v) an elementary extension of (L,v). Then $\overline{K} \prec_\exists \overline{L'}$, $v(K) \prec_\exists v(L')$, and if $(K,v) \prec_\exists (L',v)$ then $(K,v) \prec_\exists (L,v)$.*

The proof of this lemma is straightforward. – Putting Lemma 3 and Lemma 4 together we get:

Reduction Lemma: *Let $\mathcal{K}$ be an elementary class of algebraically complete fields. If $\mathcal{K}$ admits a reduction field for every extension $(L,v) \mid (K,v)$ with (L,v), $(K,v) \in \mathcal{K}$, $\overline{K} \prec_\exists \overline{L}$, $v(K) \prec_\exists v(L)$, (K,v) a special model of cardinality κ a limit cardinal and (L,v) a special model of cardinality λ a limit cardinality of cofinality bigger than κ, then $\mathcal{K}$ has the reduction property* (R).

Proof: Assume that $(\mathrm{M5})_{\mathcal{K}}$ holds for every field in $\mathcal{K}$. Given an arbitrary field $(K,v) \in \mathcal{K}$, we have to prove that (K,v) satisfies $(\mathrm{M6})_{\mathcal{K}}$. By Lemma 3, we may assume w.l.o.g. that (K,v) is a special model of cardinality κ a limit cardinal. Given an arbitrary extension field (L,v) of (K,v) such that $\overline{K} \prec_\exists \overline{L}$ and $v(K) \prec_\exists v(L)$, we have to show that $(K,v) \prec_\exists (L,v)$. By Lemma 4 we may assume w.l.o.g. that (L,v) is a special model of cardinality λ a limit cardinal of cofinality bigger than κ (since we can replace every such extension field by an elementary extension of it having the required properties). By hypothesis, the extension $(L,v) \mid (K,v)$ will now admit a reduction field $(K_1,v) \in \mathcal{K}$. From Theorem 1 we infer $(K,v) \prec_\exists (K_1,v)$. Since by hypothesis every field in $\mathcal{K}$ has property $(\mathrm{M5})_{\mathcal{K}}$ we know that $(K_1,v) \prec_\exists (L,v)$. From this we conclude $(K,v) \prec_\exists (L,v)$, as desired.

The next elementary class we will investigate is the class of henselian finitely ramified fields.

Definition: (K,v) is called finitely ramified, if there exist only finitely many elements in the value group between 0 and $v(p \cdot 1_K)$, where $p = \mathrm{char}(\overline{K})$ and 1_K is the 1 of the field K.

Consequently, a finitely ramified field is of characteristic 0 with residue field of characteristic $p > 0$ since otherwise between 0 and $v(p \cdot 1_K) = v(0) = \infty$ there are infinitely many elements.

Lemma 5: *Any extension $(L,v) \mid (K,v)$ of henselian finitely ramified fields with $\overline{K} \prec_\exists \overline{L}$, $v(K) \prec_\exists v(L)$ and (L,v) a special model of cardinality λ a limit cardinal with cofinality bigger than the cardinality of K admits a finitely ramified reduction field.*

For the proof we need the following embedding lemma which at the same time represents the valuation theoretical basis for Theorem 1.

Embedding Lemma 1: *Let (k,v) be algebraically complete, $(k_1,v_1) \mid (k,v)$ an anti-immediate extension and (k_2,v_2) a $|k_1|^+$- saturated extension of (k,v). Assume*

(†) $v_1(k_1)/v(k)$ *has no torsion element of order* p *and* $\overline{k_1} \mid \overline{k}$ *is separable.*

If $\sigma: k_1/v_1 \longrightarrow k_2/v_2$ *is an embedding over* k/v *and* $\tau: v_1(k_1) \longrightarrow v_2(k_2)$ *is an embedding over* $v(k)$ *then there exists an analytic embedding* $\iota: (k_1, v_1) \longrightarrow (k_2, v_2)$ *over* (k, v) *that respects* σ *and* τ, *i.e.* $\iota(a)/v_2 = \sigma(a/v_1)$ *and* $v_2(\iota(a)) = \tau(v_1(a))$ *for all* $a \in k_1$. *Here "*$/v$*", "*$/v_1$*", "*$/v_2$*" denote the residue maps of* (k, v), (k_1, v_1) *and* (k_2, v_2).

Note that (†) *is always satisfied if* $k/v \prec_\exists k_1/v_1$ *and* $v(k) \prec_\exists v_1(k_1)$.

The proof is given in [6]. Furthermore, we need the following lemma:

Lemma 6: *Any henselian finitely ramified field is algebraically complete.*

Proof: (Short sketch.) The valuation v of a finitely ramified field (K, v) admits a decomposition $v = v_0\overline{v}$ with $\mathrm{char}(K/v_0) = 0$ and $\overline{v}(K/v_0) = \mathbb{Z}$. If (K, v) is henselian, both (K, v_0) and $(K/v_0, \overline{v})$ are henselian too. Since the residue characteristic of (K, v_0) is 0, "henselian" and "algebraically complete" are equivalent for this field. The same is true for $(K/v_0, \overline{v})$ since it is of characteristic 0 and its value group is $\mathbb{Z}$. The composition of two algebraically complete valuations is algebraically complete, thus every henselian finitely ramified field is algebraically complete. The details of the proof are given in [6].

Proof of Lemma 5: The idea of the proof is to construct a henselian extension (K', w) of (K, v) admitting a valuation transcendence basis over (K, v) such that $K'/w = L/v$ and $w(K') = v(L)$, and to show with the help of Embedding Lemma 1 and the saturation property of (L, v) that (K', w) allows an embedding ι into (L, v) over (K, v) that respects both id: $K'/w \longrightarrow L/v$ and id: $w(K') \longrightarrow v(L)$. Then we are done since $\iota(K', w)$ is henselian like (K', w), hence algebraically complete by Lemma 6 and consequently a reduction field since by construction it admits like (K', w) a valuation transcendence basis over (K, v) and it has the same value group and residue field as (L, v).

The special model (L, v) is the union of an elementary chain of μ^+-saturated submodels (L_μ, v) of power $\leq 2^\mu < \lambda$, $\mu_0 < \mu < \lambda$ (for large enough $\mu_0 < \lambda$). Since the cofinality of λ is bigger than the cardinality of K we can choose μ_0 so large that L_{μ_0} and hence every L_μ, $\mu_0 < \mu$ will contain K. Now we choose henselian extension fields (K'_μ, w) of (K, v) for $\mu_0 < \mu < \lambda$ in the following way:

1) Choose (K''_{μ_0}, w) to be an extension of (K, v) admitting a valuation transcendence basis over (K, v) with $K''_{\mu_0}/w = L_{\mu_0}/v$ and $w(K''_{\mu_0}) = v(L_{\mu_0})$; let (K'_{μ_0}, w) be a henselization of (K''_{μ_0}, w).

2) If (K'_μ, w) is already constructed, choose (K''_{μ^+}, w) to be an extension of (K'_μ, w) admitting a valuation transcendence basis over (K'_μ, w), having the same residue field and value group as (L_{μ^+}, v). By induction hypothesis (K'_μ, w) has a valuation transcendence basis over (K, v). The union of both bases is a valuation transcendence basis of (K''_{μ^+}, w) over (K, v). Let (K'_{μ^+}, w) be a henselization of (K''_{μ^+}, w).

3) If for a limit cardinal $\nu < \lambda$ all (K'_μ, w) with $\mu < \nu$ are constructed, then take (K''_ν, w) to be an extension of the field $(\bigcup_{\mu<\nu} K'_\mu, w)$ having the same residue field and value group as (L_ν, v) such that (K''_ν, w) admits a valuation transcendence basis over $(\bigcup_{\mu<\nu} K'_\mu, w)$ (whose valuation transcendence basis over (K, v) is the union of all the valuation transcendence bases constructed earlier); the union of both bases is a valuation transcendence basis of (K''_ν, w) over (K, v). Take (K'_ν, w) to be a henselization of (K''_ν, w).

Now we observe that

1) $K/v \prec_\exists L_{\mu_0}/v = K'_{\mu_0}/w$ and $v(K) \prec_\exists v(L_{\mu_0}) = w(K'_{\mu_0})$ since, by assumption, $K/v \prec_\exists L/v$ and $v(K) \prec_\exists v(L)$;
2) $K'_\mu/w = L_\mu/v \prec_\exists L_{\mu^+}/v = K'_{\mu^+}/w$ and $w(K'_\mu) = v(L_\mu) \prec_\exists v(L_{\mu^+}) = w(K'_{\mu^+})$ since $(L_\mu, v) \prec (L_{\mu^+}, v)$ and thus $L_\mu/v \prec L_{\mu^+}/v$, $v(L_\mu) \prec v(L_{\mu^+})$ for all μ, $\mu_0 \leq \mu < \lambda$;
3) $(\bigcup_{\mu<\nu} K'_\mu)/w = \bigcup_{\mu<\nu}(K'_\mu/w) = \bigcup_{\mu<\nu}(L_\mu/v) \prec_\exists L_\nu/v = K'_\nu/w$ and $w(\bigcup_{\mu<\nu} K'_\mu) = \bigcup_{\mu<\nu} w(K'_\mu) = \bigcup_{\mu<\nu} v(L_\mu) \prec_\exists v(L_\nu) = w(K'_\nu)$ since for every $\mu < \nu$ we know that $(L_\mu, v) \prec (L_\nu, v)$.
Using 1), we are able to embed (K'_{μ_0}, w) over (K, v) into $(L_{2^{\mu_0}}, v)$ by Embedding Lemma 1 since $(L_{2^{\mu_0}}, v)$ is $(2^{\mu_0})^+$–saturated and hence $|K'_{\mu_0}|^+$–saturated (an easy argument shows that $|K'_{\mu_0}|^+ \leq |L_{\mu_0}|^+ \leq (2^{\mu_0})^+$). At every step of the induction, we will identify the embedded field with its image in (L, v). Assume that (K'_μ, w) is already embedded and identified with its image in (L, v). Then using 2) we can embed (K'_{μ^+}, w) over the algebraically complete field (K'_μ, w) into $(L_{2^{\mu^+}}, v)$. If all fields (K'_μ, w), $\mu < \nu$ are already embedded into (L, v), then the henselian and thus algebraically complete field $(\bigcup_{\mu<\nu} K'_\mu, w)$ is embedded over (K, v) into (L, v) . Using 3), we can embed (K'_ν, w) over this field into (L_{2^ν}, v). All the constructed embeddings are understood as to respect the corresponding restrictions of the identity maps id: $K/w \longrightarrow L/v$ and id: $w(K) \longrightarrow v(L)$. Hence by induction we get the desired embedding of (K', w) over (K, v) into (L, v).

From the Reduction Lemma and Lemma 5 we get

Corollary 1: *The elementary class K_2 of henselian finitely ramified fields has the reduction property* (R).

In the next step we want to prove that every field in K_2 has property $(\text{M5})_{K_2}$ which in view of Corollary 1 and Lemma 1 will yield

Theorem 2: *Every henselian finitely ramified field is an AX – KOCHEN – ERSHOV – field.*

This result is an immediate consequence of ERSHOV's and ZIEGLER's results on henselian finitely ramified fields (without cross–section), but in turn the model–completeness results can be directly derived from it by purely model–theoretical means. The completeness results can also be proved using our approach. We leave it as an exercise to the reader to change the construction of the reduction field such as to show that Theorem 2 remains true in the language of valued fields enriched by a cross–section.

To show that every henselian finitely ramified field has property $(\text{M5})_{K_2}$ we use the following

Embedding Lemma 2: *Let (k, v) be an algebraically maximal field and $(k(x), v) \mid (k, v)$ a nontrivial immediate extension. Then x is transcendent over k and $(k(x), v)$ can be embedded analytically over (k, v) into every $|k|^+$–saturated extension $(k, v)^*$ of (k, v).*

Proof: Clearly, x is transcendent over k. Since $(k(x), v) \mid (k, v)$ is immediate, x is a limit of a pseudo Cauchy sequence $\{x_\rho\}$ in (k, v). This pseudo Cauchy sequence can't be of algebraic type in (k, v) since by [4], Theorem 3, for any pseudo Cauchy sequence of algebraic type there exists an immediate algebraic extension of (k, v) contradicting our assumption that (k, v) is algebraically maximal. It is an easy exercise to show that if $k(x) \mid k$ were immediate and algebraic, then $\{x_\rho\}$ had to be of algebraic type. Since $(k, v)^*$ is $|k|^+$–saturated, $\{x_\rho\}$ has a

limit x' in $(k,v)^*$. By [4], Theorem 2, the homomorphism induced by $x \mapsto x'$ is an analytic embedding of $(k(x),v)$ over (k,v) into $(k,v)^*$ since $\{x_\rho\}$ is of transcendent type.

Corollary 2: *Every henselian finitely ramified field has property* $(M5)_{\mathcal{K}_2}$.

Proof: Let $(L,v) \mid (K,v)$ be an immediate extension, (K,v), $(L,v) \in \mathcal{K}_2$. We have to show that any finitely generated subextension (L',v) of $(L,v) \mid (K,v)$ is analytically embeddable over (K,v) into a fixed $|L|^+$–saturated elementary extension $(K,v)^*$ of (K,v). (K,v) is algebraically complete by Lemma 6, hence algebraically maximal. By Embedding Lemma 2, given $x \in L' \setminus K$, x is transcendent over K and we can embed $(K(x),v)$ analytically over (K,v) into $(K,v)^*$. We choose a henselization $(L',v)^h$ within the henselian field (L,v) and a henselization $(K(x),v)^h$ within $(L',v)^h$. Then the embedding of $(K(x),v)$ into $(K,v)^*$ can be prolongated to an embedding of $(K(x),v)^h$ into the henselian field $(K,v)^*$ due to the minimality property of a henselization. We may identify $(K(x),v)^h$ with its isomorphic image in $(K,v)^*$; by Lemma 6, it is algebraically complete and hence algebraically maximal. If $(K(x),v)^h$ is a proper subfield of $(L',v)^h$ there exists $x' \in L'^h \setminus K(x)^h$, hence x' is transcendent over $K(x)^h$, and we can repeat the above described procedure. Since $(L',v)^h$ is an algebraic extension of the finitely generated extension field (L',v) of (K,v), its transcendence degree over K is finite. This shows that after a finite repetition of the embedding procedure we will arrive at an analytic embedding of $(L',v)^h$ and a forteriori at the desired embedding of (L',v).

This completes the proof of Theorem 2.

Now we turn to algebraically complete fields in equal characteristic.

Theorem 3: *The class* $\mathcal{K}_3$ *of all algebraically complete fields* (K,v) *with* $char(K) = char(\overline{K})$ *has the reduction property* (R).

Since every extension $(L,v) \mid (K,v)$ of henselian fields with residue fields of characteristiv 0 admits a reduction field (as we pointed out already), we only have to consider algebraically complete fields of characteristic $p > 0$ for the proof of Theorem 3.

Lemma 7: *Let* $(L,v) \mid (K,v)$ *be an extension of algebraically complete fields of characteristic* $p > 0$ *such that* (K,v) *is a special model of cardinality* κ *a limit cardinal and* (L,v) *is a special model of cardinality* λ *a limit cardinal of cofinality bigger than* κ. *Assume that* $\overline{K} \prec_\exists \overline{L}$ *and* $v(K) \prec_\exists v(L)$. *Then* $(L,v) \mid (K,v)$ *admits a reduction field.*

Theorem 3 now follows from Lemma 7 and the reduction lemma.

The proof of Lemma 7 follows the same idea as the proof of Lemma 5, but in this case something like Lemma 6 is not available. In the construction of the fields (K'_μ, w) we will not be done by just taking henselizations, because these may not be algebraically complete. We will replace "taking a henselization" by "taking a maximal immediate algebraic extension" such that the fields (K'_μ, w) will be algebraically maximal, but even this doesn't guarantee without any further argument that they are also algebraically complete. The consequence is to ask for a further property which may be realized by construction and which in union with "algebraically maximal" will imply "algebraically complete". For fields of finite p–degree one may choose the property "excellent" in the sense of [2], but this would only be a special case of the following more general fact:

Lemma 8: *An algebraically maximal field (K,v) of characteristic $p>0$ is algebraically complete iff every finite purely inseparable extension $(L,v) \mid (K,v)$ is defectless, i.e. $[L:K] = [\overline{L}:\overline{K}]\cdot(v(L):v(K))$.*

The proof is given in [6]. Using Lemma 8, one can show

Lemma 9: *Let (K,v) be an algebraically complete field of characteristic $p>0$ and (N,v) an algebraically maximal extension of (K,v). Let ξ_i, $i\in I$, η_j, $j\in J$ be a system of elements in N such that $(\overline{\xi_i} \mid i\in I)$ forms a basis of $\overline{N} \mid \overline{N^p.K}$ and $(v(\eta_j) \mid j\in J)$ forms a system of representatives for $v(N)/v(N^p.K)$. If the system $(\xi_i\cdot\eta_j \mid i\in I, j\in J)$ forms a basis of the algebraic extension $N \mid N^p.K$, then (N,v) is algebraically complete.*

The realization of the hypothesis of Lemma 9 in the course of the construction of the fields (K'_μ,w) is not very difficult if one uses in addition the fact that (K,v), being a special model of limit cardinality, admits an embedding of its residue field such that the residue map is inverse to this embedding. The details are given in [6], as well as the proof of Lemma 9.

The undecidability results for valued fields of characteristic $p>0$ with cross-section are here reflected by the fact that it is not possible in general to find reduction fields that respect the cross–section. To make this more precise, let us consider an extension $(L,v) \mid (K,v)$ such that (L,v) has a cross–section π whose restriction to $v(K)$ is a cross–section of (K,v). For a reduction field (K_1,v) in the language of valued fields enriched with a cross–section it would be required that the cross–section of (L,v) is at the same time a cross–section of (K_1,v). If we assume in addition that $\overline{L}=\overline{K}$, then this would imply that K_1 is algebraic over the field $K(\pi\circ v(L))$ generated over K by the image elements of the cross–section of L (this is an immediate consequence of the condition that (K_1,v) should admit a valuation transcendence basis over (K,v)). Furthermore, this would imply that the relative algebraic closure of $(K(\pi\circ v(L)),v)$ in (L,v) is an algebraically complete field. But on the other hand it is possible to construct examples for which this is not true.

Unfortunately we don't know a criterion for "algebraically complete" similar to Lemma 8 for valued fields of mixed characteristic.

Problem: Does the class of all algebraically complete fields (K,v) of characteristic 0 with $\mathrm{char}(\overline{K}) = p > 0$ have the reduction property (R)? Is there an analogue to Lemma 8 or Lemma 9 for these fields? Which extensions of these fields play the role of the purely inseparable extension of valued fields of characteristic $p>0$? Is there an analogue to "excellent" in mixed characteristic?

[1] Chang, C. C. — Keisler, H. J.: Model Theory, Amsterdam–London (1973)

[2] Delon, F.: Quelques propriétés des corps valués en théories des modèles, *Thèse Paris VII* (1981)

[3] Ershov, Yu. L.: On the elementary theory of maximal valued fields III (in Russian), *Algebra i Logika* **6**:3 (1967), 31–38

[4] Kaplansky, I.: Maximal fields with valuations I, *Duke Math. Journ.* **9** (1942), 303–321

[5] Kuhlmann, F.–V.: Some valuation theoretical concepts for the examination of the model theory of valued fields, in: Structures Algébriques Ordonnées, Séminaire 1985–1986, Paris VII (1987)

[6] Kuhlmann, F.–V.: *Manuscript*, (1987)

[7] Prestel, A. – Roquette, P.: Formally p–adic fields, Lecture Notes in Math. **1050**, Berlin–Heidelberg–New York–Tokyo (1984)

[8] Ribenboim, P.: Théorie des valuations, *Les Presses de l'Université de Montréal*, Montréal (1968^2)

[9] Robinson, A. – Zakon, E.: Elementary properties of ordered abelian groups, *Transactions AMS* **96** (1960), 222–236

[10] Ziegler, M.: Die elementare Theorie der henselschen Körper, *Inaugural Dissertation*, Köln (1972)

Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
D-6900 Heidelberg

On the absolute Galois group of formally real fields

by

Eberhard Becker

1. Generalities

Let K be a field and $\overline{K}$ its separable closure. We set $G(K) := G(\overline{K}/K)$ for the absolute Galois group of K. One is interested in the following questions (among others).

i) Which profinite groups occur as G(K), K a field?

ii) Is there a relation between field theoretic properties of K and properties of G(K) as a topological group?

The class of formally real fields (f. r. - for short) is a distinguished one, in view of the second question. This already follows from the following fundamental result of Artin and Schreier [A-S], cf. also [L].

Theorem 1: i) K is f. r. $\Leftrightarrow$ G(K) contains an element $\sigma \neq 1$ of finite order.

ii) If K is f. r. and $\sigma \in G(K)$, $\sigma \neq i$, σ of finite order then $\sigma^2 = 1$.

In the sequel we concentrate on f. r. fields. We set

$$I(K) = \{\sigma \in G(K) \mid \sigma^2 = 1 \neq \sigma\},\quad X(K) = \{P \subset K \mid P \text{ ordering}\},$$

$$N := G(K(\sqrt{-1})).$$

In the Krull topology of G(K), I(K) turns out to be a compact Hausdorff space. G(K), and hence N, operates on I(K) by conjugation. By Artin-Schreier theory, cf. [P] one has a surjective map

$$I(K) \to X(K),\ \sigma \mapsto (\overline{K}^{\sigma})^2 \cap K =: P_{\sigma},$$

where $\overline{K}^{\sigma}$ denotes the fix field under σ. $\overline{K}^{\sigma}$ is real closed, thus $(\overline{K}^{\sigma})^2$ and P_{σ} are orderings of $\overline{K}^{\sigma}$ and K respectively. We impose on

$X(K)$ the quotient topology. Again by Artin-Schreier theory one sees that the fibers of the map

$$I(K) \to X(K)$$

are isomorphic with the compact space N, i. e. fixing $\sigma \in I(K)$ then the assignment

$$\omega \mapsto \omega\sigma\omega^{-1}, \quad \omega \in N$$

constitutes a homeomorphism between N and the fiber over P_σ. The quotient topology on $X(K)$ coincides with the Harrison topology on $X(K)$ as defined in [P$_1$] e. g.

The map $I(K) \to X(K)$ is a trivial N-fibration as was first observed by Ershov [E], cf. also [F-J].

Theorem 2: The above map $I(K) \to X(K)$ admits a continuous section, i. e. there is a homeomorphism

$$I(K) \tilde{\to} X(K) \times N.$$

From what has been said so far it seems clear that a study of $G(K)$, K a formally real field, should give special attention to the following two questions:

i) structure of the involutions in $G(K)$, influence of the 2-Sylow group of $G(K)$,

ii) importance of $X(K)$, N for the structure of $G(K)$.

Note that $G(K) = \langle\sigma\rangle \leftthreetimes N$, σ any involution, operating on the normal subgroup N by conjugation.

2. Sovable groups

In this section, sovable means solvable as an abstract group, not to be mixed up with the notion pro-solvable. A field K is called solvable if G(K) is solvable in the above sense. Solvable number fields were first studied by Neukirch, subsequently by Geyer [G]. The basic examples are the following ones, pick $\sigma,\tau \in I(\mathbb{Q})$, set

$$F_{\sigma,\tau} = \overline{\mathbb{Q}}^{\sigma} \cap \overline{\mathbb{Q}}^{\tau}.$$

Then $G(F_{\sigma,\tau}) = \langle\sigma,\tau\rangle = \langle\sigma\rangle \rtimes \langle\sigma\tau\rangle$ where $N = \langle\sigma\tau\rangle$ is pro-cyclic, torsionfree and $\sigma(\sigma\tau)\sigma = (\sigma\tau)^{-1}$. Hence $F_{\sigma,\tau}$ is solvable. Geyer proved that every f. r. solvable number field is of type $F_{\sigma,\tau}$. In the case of general f. r. solvable fields on has the following

Theorem 3 ([B2, B3]): Let K be f. r. Then the following statement are equivalent

i) K solvable, ii) $G(K(\sqrt{-1}))$ abelian,

iii) a 2-Sylowgroup of G(K) is solvable,

iv) $\sigma\tau\omega \in I(K)$ for all $\sigma,\tau,\omega \in I(K)$,

v) (L. Bröcker) the Haar-measure of I(K) is > 0 ($= \frac{1}{2}$ if measure is normalized),

vi) every f. r. algebraic extension of K is pythagorean (i. e. $K^2 + K^2 = K^2$).

If K is solvable then, given $\sigma \in I(K)$, $\tau \in N$, one has:

$\sigma\tau\sigma = \tau^{-1}$, $G(K) \cong \langle\sigma\rangle \rtimes \prod_p \mathbb{Z}_p^{\alpha_p}$, σ operates by taking the inverse,

and $\alpha_p = -\delta_{2,p} + \dim_{\mathbb{F}_p} K^{\times}/K^{\times p}$.

A typical example is the following one: I a well-ordered set, $\Gamma = \mathbb{Z}^{(I)}$ the lexicographically ordered direct sum, $K = \mathbb{R}((\Gamma))$, then K is solvable and $G(K) = \langle\sigma\rangle \ltimes \prod_p \mathbb{Z}_p^I$. A solvable f. r. field is also called hereditarily-pythagorean (h. p. - for short), in view of 3, vi).

3. The examples of Engler/Viswanathan [E-V]

They studied the following situation: R|k, R real closure of K, $\alpha \in R\backslash k$, let $k \subset K \subset R$ be maximal with $\alpha \notin K$; denote this by $K = k_{\alpha,R} = k_\alpha$. By $F_2(I)$, we denote the free pro-2-group with I as a set of free generators; G' is the (topological) commutator subgroup.

Theorem 4: There are 3 possibilities for G(K) for such $K = k_\alpha$; they all occur; a field K is of type k_α iff G(K) is one of the following groups:

1) $G = \langle\sigma\rangle \ltimes \mathbb{Z}_p$, $\sigma u \sigma = u^{-1}$ ($\Rightarrow$ K h. p.)

2) $G = \langle\sigma\rangle \ltimes F_2(\tau,\Phi)$, $\sigma\tau\sigma = \Phi$, $\sigma\Phi\sigma = \tau$ ($G' = F_2(\aleph_0)$)

3) $G = \langle\sigma\rangle \ltimes (\mathbb{Z}_p \ltimes F_2(\aleph_0))$, action only depends on p, $G' = F_2(\aleph_0)$, $p > 2$.

Remarks:

i) There are algebraic characterizations of such fields, cf. [E-V].

ii) Examples: 2) $k = \mathbb{Q}$, $\alpha = \sqrt{2} \Rightarrow \mathbb{Q}_{\sqrt{2}}$ of type 2)

3) $h = \mathbb{Q}$, $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois-ext. of degree $p > 2 \Rightarrow \mathbb{Q}_\alpha$ of type 3)

iii) in cases 2) 3) consider

$$\begin{array}{c} \overline{K} \\ \uparrow \\ F_1 = \overline{K}^{G'} = K_{ab} \\ \uparrow \\ K \end{array}$$

(= max. abelian extension);

pick $\sigma \in I(K)$, then $F = F_1^\sigma$ is f. r. and $G(F) = \langle\sigma\rangle \ltimes F_2(\aleph_0)$.

Corollary: k h. p. $\Leftrightarrow$ all $k_{\alpha,R}$ are of type 1).

The above results lead to the following consequences:

i) Let K be not h. p., then the 2-Sylow-field k is not h. p. by theorem 3, hence there is $k_{\alpha,R}$ of type 2) or 3), so by the above remark there is $K \subset k_{\alpha,R} \subset F$ with $G(F(\sqrt{-1})) = F_2(\aleph_0)$.

ii) The structure of $N = G(K(\sqrt{-1}))$ shows big jumps in complexity:
- N finite $\Rightarrow N = 1$,
- N not finite, but no free pro-2 subgroups of rank ≥ 2 $\Rightarrow$ N abelian,
- $N \supset F_2(\aleph_0) \Rightarrow N \supset F_2(\aleph_0)$.

4. The maximal 2-extension and quadratic form theory

In this section we study the extension K_2/K, K still a f. r. field, where K_2 is the maximal 2-extension of K. Being the union of iterated quadratic extensions, K_2/K is a Galois extension with Galois group a pro-2-group. Here, we set

$$G = G(K) := G(K_2/K),\ I(K) = \{\sigma \in G(K) \mid \sigma^2 = 1 \neq \sigma\}.$$

Using [B1] and Ershov's proof one still has

$$I(K) \simeq X(K) \times G(K_2/K(\sqrt{-1})).$$

Because of this fact and many other observations the extension K_2/K can be thought of as the relative version of $\overline{K}/K$.

In the sequel we summarize several facts about pro-2-groups and Galois cohomology, cf. [S].

i) Facts from the theory of pro-2-group

G a pro-2-group, $H^k(G) := H^k(G, \mathbb{Z}/2\mathbb{Z})$

α) $H^1(G) \simeq (G/G^2[G,G])^*$; $\dim H^1(G) = \#$ generators of G

β) $\dim_{F_2} H^2(G) = \#$ relations of G

ii) Interpretation in Galois theory

Kummer-theory: $G/_{G^2[G,G]}$ = Galoisgroup of $K(\sqrt{K})$

$$H^1(G) \simeq K^x/_{K^{x2}}$$

$$H^1(G) \times H^1(G) \xrightarrow{\cup} H^2(G) = Br(K)_2 \qquad (\cup \text{ cup product})$$

$$K^x/_{K^{x2}} \times K^x/_{K^{x2}} \xrightarrow{(\ ,\ )} Br(K)_2$$

where (,) is the usual quaternion pairing.

Now, by Satz 7 of Witt [Wi], the Witt ring W(K) of K has the following presentations:

$$W(K) \simeq Z[K^x/_{K^{x2}}]/(\overline{1} + (-\overline{1}), \overline{\alpha} + \overline{\beta} - \overline{\gamma} - \overline{\delta} \text{ where } \overline{\alpha\beta} = \overline{\gamma\delta} \text{ and } (\alpha,\beta) \simeq (\gamma,\delta)).$$

Hence, W(K) is determined by $H^1(G(K))$ and $H^1 \times H^1 \xrightarrow{\cup} H^2$.

In particular

Theorem 5 (Delzant, Scharlau, R. Ware [Sch, Wa]. Let K, F be formally real, then

$$W(K) \simeq W(F) \Leftrightarrow G(K) \simeq G(F).$$

We have the following decomposition of K_2/K, cf. [B1]

$$\begin{array}{ccc} & & K_2 \\ & & | \\ \bigcap_{\sigma \in I(K)} & & K_2^{\sigma} \\ & & | \\ & & K \end{array} = K_{pyth}$$

where K_{pyth} is the smallest pythagorean extension of K in $\overline{K}$ = the pythagorean closure of K.

One has i) $G(K_2/K_{pyth}) = \langle \mathfrak{T}(K) \rangle$,

ii) $G(K_{pyth}/K)$ torsionfree.

Therefore the study of $G(K_2/K)$ splits into two parts:

i) the special case where K is pythagorean,

ii) in the general case one has to consider the exact sequence

$$1 \to G(K_2/K_{pyth}) \to G(K_2/K) \to G(K_{pyth}/K) \to 1.$$

In the case of K being pythagorean and having finite square class number $q_k := [K^x : K^{x2}] < \infty$ the structure of G(K) is completely solved by B. Jacob [J] in the following way.

Theorem 6: The G(K) for K as above are just those pro-2-groups which can be obtained from $\mathbf{Z}/_{2\mathbf{Z}}$ by taking finitely often the following two operations:

i) finite free products in the category of pro-2-groups,

ii) semi-direct products with $\mathbf{Z}_2^k$, $k < \infty$ and a certain action.

The proof depends on the Merkurjev-Suslin result that

(*) k_2K, $IK^2/_{IK^3}$ and $Br(K)_2$

are naturally isomorphic where IK denotes the fundamental ideal of W(K), cf. [M]. The paper [J] was written before [M] appeared. However, Jacob pointed out in [J] that the completion of his classification only depends on (*), a result now available. In a quite recent paper, Jacob and Ware [J-W] dropped the hypothesis "K pythagorean" and succeeded in a recursive construction of all possible Galois groups $G(K_2/K)$ with $q_k < \infty$.

References

[A-S] Artin, E. and Schreier, O.: Eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Univ. Hamburg 5 (1927), 225-231.

[B1] Becker, E.: Euklidische Körper und euklidische Hüllen von Körpern, J. reine angew. Math. 268-269 (1974), 41-52.

[B2] Becker, E.: Hereditarily-pythagorean fields and orderings of higher level, Monografias de Matemática 29 (1978), IMPA, Rio de Janeiro.

[B3] Becker, E.: Formal-relle Körper mit streng-auflösbarer absoluter Galoisgruppe, Math. Ann. 238 (1978), 203-206.

[E] Eršov, Ju. L.: Über die Galoissche Gruppe der maximalen 2-Erweiterung, Manuskript 1983.

[E-V] Engler, A. J. and Viswanathan, T. M.: Formally real fields with a simple description of the absolute Galois group, manuscripta math. 56 (1986), 71-87.

[G] Geyer, W.-D.: Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist, J. Number Theory 1 (1969), 346-374.

[J] Jacob, B.: On the structure of pythagorean fields, J. Algebra 68 (1981), 247-267.

[F-J] Fried,M. and Jarden,M.: Field arithmetic, Berlin Heidelberg New York 1986.

[J-W] Jacob, B. and Ware, R.: Elementary Witt Rings and pro-2-groups, 1986, submitted.

[L] Leicht, J. B.: Zur Charakterisierung reell abgeschlossener Körper, Monatsh. Math. 70 (1966), 452-453.

[P] Prieß-Crampe, S.: Angeordnete Strukturen: Gruppen, Körper, projektive Ebenen, Berlin Heidelberg New York Tokyo 1983.

[Pr] Prestel, A.: Lectures on formally real fields, Lecture Notes Math. 1093

[S] Serre, J.-P.: Cohomologie Galoisienne, Lecture Notes Math. 5 (1956).

[Sch] Scharlau, W.: Quadratische Formen und Galois-Cohomologie, Invent. Math. 4 (1967), 238-264.

[Wa] Ware, R.: Quadratic forms and profinite 2-groups, J. Algebra 58 (1979), 227-237.

[Wi] Witt, E.: Theorie der quadratischen Formen in beliebigen Körpern, J. reine angew. Math. 176 (1937), 31-44.

GENERALISATION DU THEOREME DE HOLLAND AUX GROUPES A MOITIE RETICULES

M. Giraudet

Ce texte fait suite à [G] dans le volume précédent de ce séminaire et reprend donc les mêmes notations et définitions.

Nous considérons ici les groupes réticulés et à moitié réticulés comme des modèles d'un langage L constitué du langage des groupes et de celui des treillis (L={.,sup,inf} par exemple), les notions de sous-structure et d'homomorphisme se réfèrent donc à ce langage.

Rappelons d'abord le célèbre théorème de plongement, établi par W.C. Holland dans [H], que nous nous proposons de généraliser:

Le théorème de Holland:
Soit G un groupe réticulé. Il existe une chaîne T telle que G soit isomorphe à une sous structure de AutT.

Proposition :
Si G est un groupe à moitié réticulé tel que G↓ soit non vide, alors E(G) est non vide.

Démonstration: Si $x \in G\downarrow$, où G est un groupe à moitié réticulé, d'après la Proposition 3-b-ii:
$(\sup(x,x^{-1}))^{-1}=\sup(x,x^{-1})$, donc $\sup(x,x^{-1}) \in E$.

Théorème : Théorème de Holland généralisé
Soit G un groupe à moitié réticulé. Il existe une chaîne S telle que G soit isomorphe à une sous-structure de M(T).

Démonstration: Nous supposerons G↓ non vide, l'autre cas n'étant qu'une application du Théorème de Holland. D'après la proposition, nous pouvons considérer un $a \in E=E(G)$ fixé.

D'après le Théorème de Holland, il existe une chaîne T telle que $G\uparrow$ soit isomorphe à une sous-structure de AutT. Nous considèrerons sans inconvénients que G est égal à cette sous-structure de AutT.

Notons T^* la chaîne duale de T et s un anti-isomorphisme de T sur T^*. La concaténation $\sigma=s\hat{}s^{-1}$ de s et s^{-1} est un anti-automorphisme d'ordre de la chaîne $T+T^*$, notée S.

Définissons une application F de AutT dans M(S) par:

$F(f)=safas^{-1}\hat{}f$, concaténation de $safas^{-1}$ et f, pour tout $f\in AutT$.

Il est facile de vérifier que F induit un isomorphisme (également noté F) de $G\uparrow$ sur une sous-structure de $M(S)\uparrow$.

Vérifier que cet automorphisme s'étend en un automorphisme de G sur une sous-structure de M(T) en posant:

$F(a)=\sigma$

est également de pure routine; à titre d'exemple, vérifions ci-dessous que $F(fg)=F(f)F(g)$ pour $f\in G\uparrow$ et $g\in G\downarrow$:

La definition de F impose, en notant $g'=ag\in G\uparrow$:

$F(g)=F(a)F(g')=\sigma(sag'as^{-1}\hat{}g'=ag'as^{-1}\hat{}sg'$

et:

$F(fg)=F(a(afag'))=\sigma F(afag')$, où $afag'\in G\uparrow$, donc:

$F(fg)=\sigma(saafag'as^{-1}\hat{}afag')=fag'as^{-1}\hat{}safag'$

$F(f)F(g)=(safas^{-1}\hat{}f)(ag'as^{-1}\hat{}sg')=F(f)F(g)$.

Le reste de la démonstration est laissé au lecteur.

Bibliographie:

[B] A.Bigard, K. Keimel et S. Wolfenstein. Groupes et Anneaux Réticulés. Springer l.n. 608. 1977.

[F] L. Fuchs Partially Ordered Algebraic Systems. Pergamonn Press 1963.

[G] Groupes à moitié ordonnés. Ce séminaire 1985-86.

[G.1] M. Jambu-Giraudet. Bi-interpretable groups and lattices. Trans A.M.S. 278. Vol. 1 p. 253-269. (1983).

[G.2] M Jambu-Giraudet. Interprétations d'arithmétiques dans des groupes et des treillis. Dans Model Theory and Arithmetic. Proceedings, Paris, 1979/80. Springer L.N. 890. P. 143-153.

[H] W.C. Holland. The lattice-ordered group of automorphisms of an ordered set. Michigan Math. J. 10. p. 399-408. (1963).

K_o AF C^* ℓ Γ MV : a brief outline

Daniele Mundici
Dipartimento Scienze Informazione
Università di Milano
via Moretto da Brescia 9
20133 Milano
Italy

1. Partially ordered groups with strong unit [1] , [10]

A p.o. abelian group is an abelian group G equipped with a translation invariant partial order relation $\leq$. We let $G^+ = \{x \in G \mid x \geq 0\}$ be the positive cone of G. An element $u \geq 0$ is a strong unit in G iff for each $x \in G$ there is an integer $n > 0$ such that $x \leq nu$. We write $\psi: (G,u) \to (G',u')$ to mean that ψ is a morphism in the category of p.o. abelian groups with strong unit, i.e., ψ is an order preserving group homomorphism, and ψ is unital, viz., $\psi(u) = u'$. G is directed iff any two elements of G have a common majorant; this is always the case if G has a strong unit. G is unperforated (alias isolated, alias semiclosed) iff for every $x \in G$ the existence of $n > 0$ such that $nx \geq 0$ implies $x \geq 0$. Weinberg's theorem [1,Appendix 2.6] states that unperforatedness is a (necessary and) sufficient condition for the existence of the free ℓ-group over the p.o. abelian group G. G has the Riesz property iff whenever $x_1, x_2, y_1, y_2 \in G$ satisfy $x_i \leq y_j$ for all i,j there is $z \in G$ such that $x_i \leq z \leq y_j$ for all i, j. Of course, every lattice-ordered group (for short, ℓ-group) has the Riesz property. Given a directed set I and a direct system of abelian groups $\{(G_\alpha ; \psi_{\alpha\beta}) \mid \alpha \leq \beta, \alpha, \beta \in I\}$ let G be the direct limit group, and for each $\alpha \in I$ let $\psi_{\alpha\infty}: G_\alpha \to G$ be the direct limit homomorphism. If each G_α is a p.o. abelian group, and the $\psi_{\alpha\beta}$ are order preserving, G is naturally equipped with the partial

order given by $x \leq y$ iff $y-x \in \bigcup \psi_{\alpha\infty}(G_\alpha^+)$, for all $x,y \in G$. Then G is a p.o. abelian group. If in addition each G_α has a distinguished strong unit u_α and the $\psi_{\alpha\beta}$ are unital, then the element $u = \psi_{\alpha\infty} u_\alpha$ (does not depend on α, and) is a strong unit of G. Unless otherwise specified, $\mathbb{Z}^n$ will denote the p.o. abelian group $\mathbb{Z}^n$ with product order: $(z_1,\ldots,z_n) \geq 0$ iff $z_i \geq 0$ for all i. A countable dimension group is a p.o. abelian group G which is isomorphic to the direct limit of a sequence

$$\mathbb{Z}^{n_1} \xrightarrow{\psi_1} \mathbb{Z}^{n_2} \xrightarrow{\psi_2} \ldots ,$$

where each ψ_i is an order preserving group homomorphism.

1.1 Theorem. (Effros, Handelman, Shen) G is a countable dimension group iff G is a countable directed unperforated p.o. abelian group with the Riesz property.

Proof. The $\rightarrow$-direction is an easy exercise. The converse direction is the main result of [10]. □

2. K_0 of rings [23 §1], [12], [14]

All rings considered in this paper have a unit, and all ring homomorphisms are unit-preserving. For any ring R we let $\mathcal{P}(R)$ be the family of finitely generated projective right R-modules. Equivalently, $P \in \mathcal{P}(R)$ iff P is a direct summand of a free R-module with a finite base [19,II,p.152]. Two modules $P,Q \in \mathcal{P}(R)$ are stably isomorphic, in symbols $P \sim Q$, iff $P \oplus S \cong Q \oplus S$ for some $S \in \mathcal{P}(R)$. Since the equivalence relation $\sim$ is preserved under $\oplus$, letting $+$ be the induced operation on $\mathcal{P}(R)/\sim$, we obtain a cancellative abelian monoid. By formally adding inverses, we finally obtain an abelian group, called the Grothendieck group of R, and denoted $K_0(R)$.

Thus, letting P,Q,S,T range over elements of $\mathcal{P}(R)$, and denoting by $[P]$ the stable isomorphism class of P, we can write:

$K_0(R) = \{[P] - [Q] \mid P,Q \in \mathcal{P}(R)\}$;

$[P] - [Q] = [S] - [T]$ iff $P \oplus T \sim Q \oplus S$ iff $P \oplus T \oplus R^r \cong Q \oplus S \oplus R^r$ for some $r \in \omega$;

$([P] - [Q]) + ([S] - [T]) = [P \oplus S] - [Q \oplus T]$;

$[O] - [O]$ is the zero element in $K_0(R)$;

$-([P] - [Q]) = [Q] - [P]$.

Identifying $\mathcal{P}(R)/\sim$ with a subset $\mathcal{C}$ of $K_0(R)$, for all p,q in $K_0(R)$ we can write $p \leq q$ iff $q-p \in \mathcal{C}$. Then $\leq$ is reflexive ($O \in \mathcal{C}$) and transitive ($\mathcal{C} + \mathcal{C} \subset \mathcal{C}$). Further, $\leq$ is translation invariant: $p \leq q$ implies $p+s \leq q+s$ for all $s \in K_0(R)$. The image $[R]$ of the R-module $R \in \mathcal{P}(R)$ is a strong unit in $K_0(R)$, because for all $p \in K_0(R)$ we have $p = [S] - [T] \leq [S] \leq [S \oplus Q] = [R^n] = n[R]$, for suitable $Q \in \mathcal{P}(R)$ and $n \in \omega$.

Let R,R' be rings, and $f: R \to R'$ be a homomorphism. The maps

$$(a,z) \mapsto f(a)z \quad , \quad a \in R, \ z \in R' \quad , \text{ and}$$
$$(z,b) \mapsto zb \quad , \quad z,b \in R'$$

naturally make R' into an (R,R')-bimodule, also denoted R'. Hence every $P \in \mathcal{P}(R)$ is mapped into $P \otimes_R R' \in \mathcal{P}(R')$. Since this mapping preserves stable isomorphism and direct sums, we can define the function $K_0(f): K_0(R) \to K_0(R')$ by

$$[P] - [Q] \xrightarrow{K_0(f)} [P \otimes_R R'] - [Q \otimes_R R'] \quad ,$$

thus obtaining a $\leq$-preserving group homomorphism sending $[R]$ into $[R']$. Since $K_0(-)$ preserves identities and compositions of ring homomorphisms, we have

2.1 Proposition. K_o is a functor from rings into abelian groups. For every ring homomorphism $f:R\to R'$, $K_o(f)$ also preserves the pre-order relation $\leq$, and maps the strong unit $[R]$ of $K_o(R)$ into the strong unit $[R']$ of $K_o(R')$. □

2.2 Examples. (i) For F a fixed field, let $R = M_n(F)$ be the F-algebra of $n\times n$ matrices over F. The F-vector space F^n can be considered as a right R-module V (letting vectors be acted by matrices by right multiplication), which is finitely generated, projective ($V^n \cong R$), and has no proper submodules. Hence every submodule of R^m ($\cong V^{nm}$) is isomorphic to some V^k. Since $R^m \cong R^{m'}$ implies $m=m'$, it follows that $K_o(R)$ can be identified with $\mathbb{Z}$ with the natural order, $[V] = 1$, $[R] = [V^n] = n$. For short,

$$(K_o(R),[R]) = (\mathbb{Z},n).$$

(ii) If R is a direct product $M_{n_1}(F) \times \ldots \times M_{n_k}(F)$, then since R-modules are in 1-1 correspondence with k-tuplas $(P_1,\ldots,P_k)$ where each P_i is an $M_{n_i}(F)$ module, we can identify $K_o(R)$ with $\mathbb{Z}^k$ (with product order), and $[R]$ with the strong unit $(n_1,\ldots,n_k)$. For short

$$(*) \qquad (K_o(R),[R]) = (\mathbb{Z}^k, (n_1,\ldots,n_k)).$$

(iii) An F-algebra R is called ultramatricial iff R is the union of a sequence $R_1 \subset R_2 \subset \ldots$ of F-algebras, where each R_i is an F-subalgebra of R_{i+1} (with the same unit), and R_i is a finite direct product of k_i matrix algebras as in Example (ii). By (*) together with Proposition 2.1, K_o yields a direct system

$$(**) \qquad (\mathbb{Z}^{k_i}, (n_1,\ldots,n_{k_i})) \xrightarrow{\psi_i} (\mathbb{Z}^{k_{i+1}}, (m_1,\ldots,m_{k_{i+1}})),$$

where each ψ_i is the order preserving unital group homomorphism given by $\psi_i = K_o(f_i)$, f_i the inclusion function of R_i into R_{i+1}. In general, ψ_i is not 1-1, and is not an ℓ-homomorphism.

2.3 Theorem. (Elliott) (i) For every ultramatricial F-algebra R, $(K_o(R),[R])$ is the direct limit of the associated direct system (**), whence by Theorem 1.1, it is a countable unperforated p.o. abelian group with strong unit and with the Riesz property.

(ii) If R' is another ultramatricial F-algebra, then $(K_o(R'),[R'])$ is isomorphic to $(K_o(R),[R])$ as a p.o. abelian group with strong unit, iff R' and R are isomorphic as F-algebras.

(iii) Every countable unperforated p.o. abelian group G with strong unit u and with the Riesz property is isomorphic to $(K_o(R),[R])$ for some ultramatricial F-algebra R.

Proof. This follows from the classification of [12]. Similar proofs are given in [17] and [9]. □

3. K_o of AF C^*-algebras [17]

As all algebras in this paper have a unit, subalgebras will always be unital subalgebras, and algebra homomorphisms will be unit preserving.

A complex $*$-algebra is an algebra A over the field $\mathbb{C}$ of complex numbers, equipped with a map $*$ of A into itself such that

$x^{**}=x$, $(x+y)^*=x^*+y^*$, $(\mu x)^*=\bar{\mu}x^*$, $(xy)^*=y^*x^*$ for all $x,y\in A$, $\mu\in\mathbb{C}$.

The adjective "complex" shall be omitted whenever possible.
A C^*-algebra is a $*$-algebra A equipped with a norm making it a Banach space, such that $\|1\| = 1$, $\|xy\|\leq\|x\|\cdot\|y\|$ and $\|xx^*\|=\|x\|^2$ for all $x,y\in A$.

Examples of C^*-algebras. (a) For every compact Hausdorff space X, let $C(X)$ be the set of complex-valued continuous functions on X with pointwise operations and sup norm. Then $C(X)$ is a C^*-algebra.

(b) Let $B(H)$ be the set of bounded linear operators on a Hilbert space H, equipped with addition, subtraction, multiplication, scalar multiplication, adjoint and norm. Then every norm closed $*$-subalgebra of $B(H)$ is a C^*-algebra.

(c) Let $M_n(\mathbb{C})$ be the $*$-algebra of $n \times n$ complex matrices, where $*$ is conjugate transpose, and $\|\cdot\|$ is the operator norm obtained by identifying $M_n(\mathbb{C})$ with $B(\mathbb{C}^n)$. Then every product

$$M_{n_1}(\mathbb{C}) \times \ldots \times M_{n_k}(\mathbb{C})$$

with componentwise operations and sup norm, is a C^*-algebra.

3.1 Theorem. (i) (Gelfand) Every commutative C^*-algebra is isomorphic to $C(X)$ for some compact Hausdorff space X. Further, $C(X)$ is isomorphic to $C(Y)$ iff X is homeomorphic to Y.

(ii) (Gelfand, Naimark) Every C^*-algebra is isomorphic to a norm closed $*$-subalgebra of some $B(H)$.

(iii) Every finite dimensional C^*-algebra is isomorphic to a C^*-algebra of the form

$$M_{n_1}(\mathbb{C}) \times \ldots \times M_{n_k}(\mathbb{C}) \ .$$

Proof. [17], or any other textbook on C^*-algebras . □

Definition [3]. An AF C^*-algebra $\mathfrak{A}$ is the norm closure of a union of a sequence $R_1 \subset R_2 \subset \ldots$ of finite dimensional C^*-algebras, each R_i a $*$-subalgebra of R_{i+1} . In symbols, $\mathfrak{A} = \overline{\cup R_i}$.

Thus, every AF C^*-algebra $\mathfrak{A}$ has at least one $*$-subalgebra $\cup R_i$ which is norm dense in $\mathfrak{A}$, and which is the union of an

ascending sequence of finite dimensional C^*-algebras, all with the same unit. By Theorem 3.1(iii), $\cup R_i$ can be identified with a ultramatricial ($*$-) algebra R over $\mathbb{C}$. We call R a dense ultramatricial $*$-subalgebra of $\mathfrak{A}$.

The following lemma shows that K_o is invariant under the completion process $\cup R_i \hookrightarrow \overline{\cup R_i}$:

3.2 Lemma. Let $j:R \to \mathfrak{A}$ be the inclusion map of a dense ultramatricial $*$-subalgebra R into an AF C^*-algebra $\mathfrak{A}$. Let $\psi = K_o(j)$. Then ψ is a group isomorphism of $K_o(R)$ onto $K_o(\mathfrak{A})$, and both ψ and ψ^{-1} preserve the pre-order relation $\leq$ on K_o defined in § 2. Thus in particular, by 2.3(i), $(K_o(\mathfrak{A}),[\mathfrak{A}])$ is a p.o. abelian group with strong unit.

Proof. The preservation properties of ψ are ensured by Proposition 2.1. As for the remaining properties of ψ and ψ^{-1}, see, e.g., [17, 19.10] . □

3.3 Theorem. For each $i=1,2$ let $\mathfrak{A}_i$ be an AF C^*-algebra, and R_i a dense ultramatricial $*$-subalgebra of $\mathfrak{A}_i$. Then the following are equivalent:

(i) $\mathfrak{A}_1 \cong \mathfrak{A}_2$ as C^*-algebras ;

(ii) $\mathfrak{A}_1 \cong \mathfrak{A}_2$ as rings ;

(iii) $(K_o(\mathfrak{A}_1), [\mathfrak{A}_1]) \cong (K_o(\mathfrak{A}_2),[\mathfrak{A}_2])$ as p.o. abelian groups with strong unit ;

(iv) $(K_o(R_1),[R_1]) \cong (K_o(R_2),[R_2])$ as p.o. abelian groups with strong unit ;

(v) $R_1 \cong R_2$ as algebras over $\mathbb{C}$;

(vi) $R_1 \cong R_2$ as $*$-algebras ;

(vii) $R_1 \cong R_2$ as rings.

Proof. (i)→(ii)→(iii) are trivial. (v)→(vii)→(iv) are trivial. There remains to be proved (iii)→(iv)→(v)→(vi)→(i).

(iii)→(iv) follows from Lemma 3.2. (iv)→(v) follows from Theorem 2.3(ii). (v)→(vi)→(i) follows from the analysis of [12, Appendix], and [3, 2.7]. See Goodearl's book for a self-contained proof of this theorem, culminating in [17, 20.7]. □

3.4 Corollary. The map $\mathfrak{A} \mapsto (K_0(\mathfrak{A}), [\mathfrak{A}])$ is a 1-1 correspondence, in the sense of isomorphism, between AF C^*-algebras and countable unperforated p.o. abelian groups with strong unit and with the Riesz property. □

3.5 Examples. We present some examples of AF C^*-algebras by specifying their associated complete invariant, in conformity with Corollary 3.4. We let $\mathbb{Q}$ be the p.o. group of rationals with the natural order, $\mathbb{Q}'$ an arbitrary subgroup of $\mathbb{Q}$ with the induced order, $\mathbb{Z}[1/2]$ the subgroup of $\mathbb{Q}$ generated by $\{2^{-i} \mid i \in \omega\}$, $\mathcal{A}$ the group of real algebraic numbers, $\mathbb{Z} \oplus_{lex} \mathbb{Z}$ the group $\mathbb{Z}^2$ equipped with the lexicographic order from the left: $(a,b) \geq (a',b')$ iff $a > a'$, or ($a=a'$ and $b \geq b'$).

the complete invariant	the corresponding AF C^*-algebra
$(\mathbb{Q},1)$	Glimm's universal UHF algebra [8]
$(\mathbb{Z}[1/2],1)$	the CAR algebra [4],[13] of the Fermi gas
$(\mathbb{Q}',1)$	every UHF algebra [16],[9],[14]
$(\mathbb{Z}+\mathbb{Z}\rho,1)$, $\rho \in [0,1]\setminus\mathbb{Q}$	the Effros-Shen $\mathfrak{F}_\rho$, [11],[32]
$(\mathcal{A},1)$	Blackadar's algebra B [2,p.504]
$(\mathbb{Z} \oplus_{lex} \mathbb{Z}, (1,0))$	the AF C^*-algebra of [26, 6.5].

Remarks. An equivalent approach to K_0 of AF C^*-algebras in terms of self-adjoint idempotents is given, e.g., in [14], [9], [17]. For the role of C^*-algebras, including AF C^*-algebras, in quantum mathematical physics, see, e.g., [14] and [13]. For further information on C^*-algebras see, e.g., [20].

4. MV ℓ Γ [5],[6],[26]

Let us equip the unit real interval [0,1] with the operations $z^*=1-z$, $y \oplus z=\min(1,y+z)$, $y \cdot z=\max(0,y+z-1)$. Algebras in the variety generated by $([0,1], 0,1,*,\oplus,\cdot)$ are precisely (Chang's) MV algebras [6, Lemma 8]. A boolean algebra is an MV algebra A such that $x \oplus x=x$ for all $x \in A$ [5, 1.16 and 1.17].

Following [25], for every abelian ℓ-group G with strong unit 1 we let $\Gamma(G,1)$ be the unit interval $\{g \in G \mid 0 \leq g \leq 1\}$ equipped with the operations $g^*=1-g$, $g \oplus h=1 \wedge (g+h)$, $g \cdot h=0 \vee (g+h-1)$. Further, for every ℓ-homomorphism $\psi: G \to G'$ such that $\psi(1)=(1')$ we let $\Gamma(\psi)$ be the restriction of ψ to the unit interval of G.

4.1 Theorem [26,3.9]. Γ is a categorical equivalence between abelian ℓ-groups with strong unit,and MV algebras. □

Recalling Corollary 3.4 we then have

4.2 Corollary. The map $\tilde{\Gamma}$ given by $\mathfrak{A} \overset{\tilde{\Gamma}}{\longmapsto} \Gamma(K_0(\mathfrak{A}),[\mathfrak{A}])$ is a 1-1 correspondence, in the sense of isomorphism, between AF C^*-algebras with lattice-ordered K_0, and countable MV algebras. □

4.3 Theorem. For every AF C^*-algebra $\mathfrak{A}$ the following are equivalent:

(i) $\mathfrak{A}$ is commutative

(ii) $K_0(\mathfrak{A})$ is lattice-ordered and $\tilde{\Gamma}(\mathfrak{A})$ is a boolean algebra.

Proof. (i)→(ii) By Gelfand's theorem 3.1(i) we can identify $\mathfrak{A}$ with $C(X)$ for a (unique) compact Hausdorff space X. The basic properties of AF C^*-algebras ensure that X has a countable base of clopens [17, 16A] . By direct computation, we have that $(K_0(\mathfrak{A}), [\mathfrak{A}])$ is the ℓ-group $C(X,\mathbb{Z})$ of continuous integer-valued functions on X ($\mathbb{Z}$ with the discrete topology) with pointwise operations and with the constant function 1 as the

strong unit [17, 19F] . Then $\tilde{\Gamma}(\mathfrak{A})$ is the boolean algebra of $\{0,1\}$-valued continuous functions on X.

(ii)$\rightarrow$(i) Using Stone's duality, and recalling that $|\tilde{\Gamma}(\mathfrak{A})| \leq \omega$, we can identify $\tilde{\Gamma}(\mathfrak{A})$ with the boolean algebra B of $\{0,1\}$-valued continuous functions over some compact Hausdorff space Y with a countable base of clopens. Arguing as in the first part, we have that the AF C^*-algebra $\mathfrak{B} = C(Y)$ satisfies $\tilde{\Gamma}(\mathfrak{B}) \cong B$, whence by Corollary 4.2, $\mathfrak{A} \cong \mathfrak{B}$, and $\mathfrak{A}$ is commutative. □

Given an AF C^*-algebra $\mathfrak{A}$, since by Corollary 3.4 $K_0(\mathfrak{A})$ is unperforated, there exists the free ℓ-group $K_0(\mathfrak{A})_\ell$ over $K_0(\mathfrak{A})$. Let $\eta: K_0(\mathfrak{A}) \rightarrow K_0(\mathfrak{A})_\ell$ be the natural embedding, and $[\mathfrak{A}]_\ell = \eta[\mathfrak{A}]$. Then $[\mathfrak{A}]_\ell$ is a strong unit in the countable abelian ℓ-group $K_0(\mathfrak{A})_\ell$.

4.4 Theorem [26, 1.3]. Define the AF C^*-algebra $\mathfrak{A}_\ell$ by

$$(K_0(\mathfrak{A}_\ell), [\mathfrak{A}_\ell]) \cong (K_0(\mathfrak{A})_\ell, [\mathfrak{A}]_\ell) .$$

Then $\mathfrak{A}$ is embeddable into $\mathfrak{A}_\ell$, and $\mathfrak{A}_\ell$ has lattice-ordered K_0. □

Identifying $\mathfrak{A}$ with a subalgebra of $\mathfrak{A}_\ell$ we are then able to completely classify arbitrary AF C^*-algebras in terms of MV algebras, as follows

4.5 Theorem [26, 3.14]. For any two AF C^*-algebras $\mathfrak{A}$ and $\mathfrak{B}$ we have $\mathfrak{A} \cong \mathfrak{B}$ iff there is an MV isomorphism of $\tilde{\Gamma}(\mathfrak{A}_\ell)$ onto $\tilde{\Gamma}(\mathfrak{B}_\ell)$ carrying the image of the unit interval of $K_0(\mathfrak{A})$ in $\tilde{\Gamma}(\mathfrak{A}_\ell)$ onto the image of the unit interval of $K_0(\mathfrak{B})$ in $\tilde{\Gamma}(\mathfrak{B}_\ell)$. □

Remark. Since boolean algebras are to 2-valued logic as MV algebras are to infinite-valued logic, the results of this

section suggest that each stable isomorphism class [P] , with $P \in \mathcal{P}(\mathfrak{A})$ and $[P] \leq [\mathfrak{A}]$ is faithfully transformed by Γ into an equivalence class of sentences in infinite-valued logic, the two-valued case occurring precisely when $\mathfrak{A}$ is commutative. This suggestion is taken seriously in the next section, where for simplicity we restrict attention to AF C^*-algebras with lattice-ordered K_o. By Theorem 4.4, this class is universal, in a strong sense, for the class of all AF C^*-algebras.

Further, the class of AF C^*-algebras with lattice-ordered K_o encompasses all commutative AF C^*-algebras (Theorem 4.3), all finite dimensional C^*-algebras (Theorem 3.1(iii) together with Example 2.2(iii)), as well as all AF C^*-algebras with comparability in the sense of Murray,von Neumann (this is equivalent to their K_o being totally ordered), including all the examples of 3.5 . Other examples will also be presented in the next section.

5. Projective $\mathfrak{A}$-modules as sentences in Łukasiewicz logic [33],[22]

The set S of sentences in the infinite-valued calculus of Łukasiewicz is the smallest set of words over the alphabet $\Sigma = \{X,|,N,C\}$ containing all the variables $X, X|, X||, \ldots$, and containing the words Nq and Cqr, whenever $q,r \in S$. Every point $\xi = (\xi_0, \xi_1, \ldots)$ in the Hilbert cube $[0,1]^\omega$ assigns to each $p \in S$ the (truth) value $p(\xi) \in [0,1]$ via the following definition

$$p(\xi) = \xi_i \quad \text{if } p \text{ is } X|\ldots| \quad (i \text{ strokes})$$
$$p(\xi) = 1-q(\xi) \quad \text{if } p \text{ is } Nq$$
$$p(\xi) = \min(1, 1-q(\xi)+r(\xi)) \quad \text{if } p \text{ is } Cqr.$$

Accordingly, N is called the negation connective, and C the implication connective. The McNaughton function $f_p : [0,1]^\omega \to [0,1]$ is defined by $f_p(\xi) = p(\xi)$ for all $\xi \in [0,1]^\omega$. A sentence p is a tautology, $p \in TAUT_\infty$, iff $f_p = 1$. A theory Θ is a subset of S. The set $\tilde{\Theta} \subset S$ of syntactic consequences of Θ is given by

$$\tilde{\Theta} = TAUT_\infty \cup \{p \in S \mid Cq_1 \ldots Cq_n p \in TAUT_\infty \text{, for some } q_1, \ldots, q_n \in \Theta\}.$$

Θ is deductively closed iff $\Theta = \tilde{\Theta}$. The family $L = \{f_p \mid p \in S\}$ is closed under pointwise MV operations on $[0,1]$, contains the constant functions 0 and 1, as well as the canonical projections $\pi_0, \pi_1, \ldots$, where $\pi_i(\xi) = \xi_i$. A basic construction of universal algebra shows that $L = (L, 0, 1, {}^*, \oplus, \cdot)$ is the free MV algebra over the free generating set $\{\pi_i \mid i \in \omega\}$. Corollary 4.2 then states that $\tilde{\Gamma}$ is a 1-1 correspondence between AF C^*-algebras with lattice-ordered K_0, and quotient MV algebras L/I, where I ranges over ideals (=kernels of MV homomorphisms) in L. On the other hand, the map

$$\Theta \mapsto I_\Theta = \{1-f_p \mid p \in \Theta\}$$

is a 1-1 correspondence between deductively closed theories and

ideals in L. Thus every such theory Θ uniquely determines, up to isomorphism, an AF C*-algebra $\mathfrak{A}_\Theta$ such that

$$\tilde{\Gamma}(\mathfrak{A}_\Theta) \cong L/I_\Theta = \text{the Lindenbaum algebra of } \Theta.$$

$K_0(\mathfrak{A}_\Theta)$ is lattice-ordered. Conversely, every AF C*-algebra with lattice-ordered K_0 is isomorphic to an $\mathfrak{A}_\Theta$, for some deductively closed theory Θ. Since Θ is a set of words over the alphabet Σ, the Turing complexity of Θ is a well-defined mathematical notion [15].

5.1 Theorem [26]. If $\Theta = \tilde{\Theta}$ is undecidable and recursively enumerable, then $\mathfrak{A}_\Theta$ has some nontrivial ideal. □

5.2 Theorem [26],[28]. The AF C*-algebra $\mathfrak{M}$ defined by $\tilde{\Gamma}(\mathfrak{M}) \cong$ L has the following properties:

(i) Every AF C*-algebra is embeddable in a quotient of $\mathfrak{M}$;
(ii) An AF C*-algebra $\mathfrak{A}$ has comparability in the sense of Murray, von Neumann iff $\mathfrak{A} \cong \mathfrak{M}/\mathfrak{J}$ for some primitive ideal $\mathfrak{J}$ of $\mathfrak{M}$;
(iii) $\mathfrak{M} \cong \mathfrak{A}_\Theta$ for some coNP-complete deductively closed theory Θ (namely, $\Theta = \text{TAUT}_\infty$). □

5.3 Theorem [31],[28]. The AF C*-algebra $\mathfrak{M}_1$ defined by

$$\tilde{\Gamma}(\mathfrak{M}_1) \cong \text{the MV algebra of one-variable McNaughton functions,}$$

has the following properties:

(i) Every Effros-Shen algebra (3.5) is a simple quotient of $\mathfrak{M}_1$, whence [32] every irrational rotation C*-algebra is embeddable in a simple quotient of $\mathfrak{M}_1$;

(ii) $(K_0(\mathfrak{M}), [\mathfrak{M}]) \cong (K_0(\mathfrak{M}_1), [\mathfrak{M}_1]) \amalg (K_0(\mathfrak{M}_1), [\mathfrak{M}_1]) \amalg \ldots$ (ω times), where $\amalg$ is coproduct in the category of abelian ℓ-groups with strong unit;

(iii) $\mathfrak{M}_1 \cong \mathfrak{A}_\Theta$ for some $\Theta = \tilde{\Theta}$ which is recognized in deterministic polynomial time. □

5.4 Theorem [28]. The following AF C^*-algebras are isomorphic to $\mathfrak{A}_\Theta$ for some $\Theta = \tilde{\Theta}$ which is recognized in deterministic polynomial time:

(i) Glimm's universal UHF algebra (3.5);

(ii) Every finite dimensional C^*-algebra ;

(iii) The Effros-Shen algebra $\mathfrak{F}_\rho$ for each quadratic irrational $\rho \in [0,1]$, or for $\rho = 1/e$, (3.5) □

5.5 Theorem [26],[28]. Let Θ be the following set of sentences:

CNXX		CXNX	
CXCNX| X|	CCNX| X| X	CNX| CXX|	CCXX| NX|
CX| CNX| | X| |	CCNX| | X| | X|	CNX| | CX| X| |	CCX| X| | NX| |
...	...	...	...

Then we have:

(i) $\mathfrak{A}_{\tilde{\Theta}}$ is the CAR algebra (3.5) ;

(ii) Theory $\tilde{\Theta}$ is recognized in deterministic polynomial time. □

Remarks. Since Θ characterizes $\mathfrak{A}_\Theta$ and Γ maps stable isomorphism classes of finitely generated projective $\mathfrak{A}_\Theta$-modules $\leq [\mathfrak{A}_\Theta]$ one-one onto logical equivalence classes of sentences in the Lindenbaum algebra of Θ, Theorems 5.4 and 5.5 are a contribution to a general problem [24, 5.4(iv)] on the complexity of (the underlying combinatorial structure of) actual examples of AF C^*-algebras existing in the literature.

Theorems 5.1-5.3 , too, are meant as a contribution to a general problem [18,p.852], [21,p.468], [7, p.85] on the role of nonsimple C^*-algebras in mathematical physics. See also [26, 6.4].

For further applications, see [27]-[31].

References.

[1] A.Bigard, K.Keimel, S.Wolfenstein, Groupes et anneaux réticulés, Springer Lecture Notes in Mathematics, vol. 608 (1977).

[2] B.B.Blackadar, A simple C^*-algebra with no nontrivial projection, Proc.Amer.Math.Soc. 78 (1980) 504-508.

[3] O.Bratteli, Inductive limits of finite dimensional C^*-algebras, Trans.Amer.Math.Soc. 171 (1972) 195-234.

[4] O.Bratteli, D.W.Robinson, Operator algebras and Quantum Statistical Mechanics, I,II, Springer, Berlin (1979).

[5] C.C.Chang, Algebraic analysis of many valued logics, Trans. Amer.Math.Soc., 88 (1958) 467-490.

[6] C.C.Chang, A new proof of the completeness of the Łukasiewicz axioms, Trans.Amer.Math.Soc. 93 (1959) 74-80.

[7] J.Cunz, The internal structure of simple C^*-algebras, AMS Proc.Symp. Pure Math. vol. 38 I (1982) 85-115.

[8] J.Dixmier, On some C^*-algebras considered by Glimm, J.Functional Analysis 1 (1967) 182-203.

[9] E.G.Effros, Dimensions and C^*-algebras, CBMS Regional Conference Series in Math., AMS, Providence, RI, vol.46 (1981).

[10] E.G.Effros, D.E.Handelman, C.L.Shen, Dimension groups and their affine representation, Amer.J.Math. 102 (1980) 385-407.

[11] E.G.Effros, C.L.Shen, Approximately finite C^*-algebras and continued fractions, Indiana J.Math. 29 (1980) 191-204.

[12] G.A.Elliott, On the classification of inductive limits of sequences of semisimple finite-dimensional algebras, J.Algebra 38 (1976) 29-44.

[13] G.G.Emch, Mathematical and conceptual Foundations of 20th Century Physics, North-Holland Math.Studies vol.100, North-Holland, Amsterdam (1984).

[14] T.Fack, O.Maréchal, Applications de la K-théorie algèbrique aux C^*-algèbres, Springer Lecture Notes in Math., vol.725 (1979) 144-169.

[15] M.R.Garey, D.S.Johnson, Computers and Intractability: a guide to the theory of NP-completeness, W.H.Freeman, San Francisco (1979).

[16] J.G.Glimm, On a certain class of operator algebras, Trans. Amer.Math.Soc. 95 (1960) 318-340.

[17] K.R.Goodearl, Notes on real and complex C^*-algebras, Shiva Math.Series 5, Birkhäuser, Boston (1982).

[18] R.Haag, D.Kastler, An algebraic approach to quantum field theory, J.Math.Physics 5 (1964) 848-861.

[19] N.Jacobson, Basic Algebra I,II, W.H.Freeman and Co., New York (1985).

[20] R.V.Kadison, J.R.Ringrose, Fundamentals of the theory of operator algebras I,II, Academic Press, New York (1983).

[21] D.Kastler, Does ergodicity plus locality imply the Gibbs structure ?, AMS Proc.Symp.Pure Math., vol.38 II (1982) 467-489.

[22] R.McNaughton, A theorem about infinite-valued sentential logic, J.Symbolic Logic 16 (1951) 1-13.

[23] J.Milnor, Introduction to algebraic K-theory, Annals of Math.Studies, vol.72, Princeton NJ (1972).

[24] D.Mundici, Abstract model theory and nets of C^*-algebras: noncommutative interpolation and preservation properties, In: Proc.Logic Coll. '83, Aachen FRG, Springer Lecture Notes in Math., vol. 1103 (1984) 351-377.

[25] D.Mundici, Mapping abelian ℓ-groups with strong unit one-one into MV algebras, J.Algebra 98 (1986) 76-81.

[26] D.Mundici, Interpretation of AF C^*-algebras in Łukasiewicz sentential calculus, J.Functional Analysis 65 (1986) 15-63.

[27] D.Mundici, Every abelian ℓ-group with two positive generators is ultrasimplicial, J.Algebra 105 (1987) 236-241.

[28] D.Mundici, The Turing complexity of AF C^*-algebras with lattice-ordered K_0, In: D.Rödding memorial volume "Logic and Computation Theory", Springer Lecture Notes in Computer Science (1987).

[29] D.Mundici, The derivative of truth in Łukasiewicz sentential calculus, In:"Methods and Applications of Math.Logic", Proc. VII Latin Amer.Symp. on Math.Logic, Contemporary Mathematics, AMS (1987).

[30] D.Mundici, Free products in the category of abelian ℓ-groups with strong unit, J.Algebra 111 (1987).

[31] D.Mundici, Farey stellar subdivisions, ultrasimplicial groups, and K_0 of AF C^*-algebras, Advances in Math. 66 (1987).

[32] M.Pimsner, D.Voiculescu, Imbedding the irrational rotation algebra into an AF algebra, J.Operator Theory 4 (1980) 201-210.

[33] A.Tarski, J.Łukasiewicz, Investigations into the sentential calculus, In: Logic, Semantics, Metamathematics, Chapter IV, Oxford University Press (1956) pp. 38-59.

~

Model theoretic versions of Weil's theorem on pregroups

Elisabeth Bouscaren

In 1955, A.Weil published a paper ["On algebraic groups of transformations", Am.J.of Math., vol.77 (1955), p:355-391] where, starting from a variety V over some algebraically closed field K, together with a binary operation on V which has "good" properties (associativity, rationality) on a large piece of V (generic points), he constructs an algebraic group G over K, whose multiplication is an extension of the given one on generic points and which is birationaly equivalent to V.

More precisely :

Let K be an algebraically closed field and let V be an irreducible variety over K such that there is a mapping f: $V \times V \longrightarrow V$ with the following properties:

(i) if a,b are independent generic points of V over K and c = f(a,b), then

$$K(a,b) = K(a,c) = K(b,c)$$

(ii) if a,b,c are independent generic points of V over K, then

$$f(f(a,b),c) = f(a,f(b,c)).$$

Then there is an algebraic group G over K which is birationaly equivalent to V, such that this birational equivalence takes f(a,b), for a,b independent generics of V, to the product of the images of a and b.

Model-theorists working on stable groups got interested in this theorem in the following context: first, recall that, by a stable (ω-stable) group, we

mean a group $(G,.)$ definable in M^n for M a model of a stable (ω-stable) theory or interpretable, i.e. definable on some quotient of M^n by some definable equivalence relation.

Amongst the first natural examples of ω-stable groups are the algebraic groups over some algebraically closed field K (they are definable in the theory of K in the language of fields).

Some years ago arose the conjecture that in fact all simple ω-stable groups with finite Morley Rank "were" algebraic groups. Now, if one hopes to be able to define a topology and a variety structure on any such abstract group, one should certainly first try to do it (and the construction should hopefully be rather canonical) in the particular case of a group interpretable in some algebraically closed field but which has a priori no variety struture which makes it into an algebraic group.

This question was asked by B.Poizat and a first positive answer was given at the time by L.van den Dries (unpublished notes, characteristic 0 case): in order to simplify, let us say that the idea is to find a good $V \subseteq G$ with a variety structure satisfying the assumptions of Weil's theorem and then, to get the algebraic group by applying the theorem.

This was unsatisfying, even in the characteristic 0 case, on two aspects: first, if one does not know the proof of Weil's theorem, then one does not really know much about this structure of algebraic group and the way it relates to the original group; secondly, using the fact that we start with a real group, there should be a more direct proof, avoiding some of the difficulties encountered when starting with an operation defined only on generic points.

This indeed turned out to be the case: a direct proof was given by E.Hrushovski (1986), in all characteristic.

This is the proof we want to present here.

Theorem 1 :

Let K be an algebraically closed field, let (G,.) be a group interpretable in K, then G is definably isomorphic to an algebraic group over K.

More precisely this is decomposed in two parts:

Theorem 1-A : Let (G,.,inv) (inv denotes the inverse on G) $\subseteq K^n$ be a group definable with parameters in some countable $k_o < K$, such that for a,b generic independent,

$a.b \in k_o(a,b)$

$inv(a) \in k_o(a)$.

Then there is a structure of variety on G (over K) which makes(G,.,inv) into an algebraic group.

Theorem 1-B : Let H be interpretable in K, then there is $G \subseteq K^n$ satisfying the assumptions of 1-A, such that H and G are definably isomorphic.

The theorem above certainly qualifies as a model-theoretic version of Weil's theorem, but it does not deal with the part of the theorem which constructs a group from an operation on the generic points. Now, the following result can certainly be considered as the model-theoretic version of this aspect of Weil's theorem. It was in fact proved by E.Hrushovski prior to the other one, and is purely model-theoretic.

Theorem *2* (Hrushovski, Ph.D.,Berkeley, 1986):

Let T be an ω-stable theory, let $p \in S(\emptyset)$ be a stationary type and let * be a partial definable operation such that:

(i) for a,b realizing p, independent,

a*b realizes $p_{|a}$ and $p_{|b}$ (where $p_{|a}$ denotes the unique non forking extension of p over a)

(ii) for a,b,c realizing p, independent,

$$(a*b)*c = a*(b*c).$$

Then there is a definable set G, a definable operation . on G and a definable embedding g of p into G, such that

(G,.) is a group

for $a,b \models p$, independent, $g(a*b) = g(a).g(b)$

g(p) is the generic of G.

(In fact this theorem with the weaker conclusion that G be infinitely definable is proved for all stable theories).

We will not say more about this aspect, but one should note that, from these two theorems, one recovers the full statement of Weil's theorem: let V be an irreducible variety satisfying the assumptions in Weil's theorem and consider p the generic type of V. Then p satisfies the assumptions in Theorem 2, and by applying first Theorem 2 and then Theorem 1, one gets the algebraic group.

Remark: The same kind of result was also more recently proved in a different (and unstable) setting by A.Pillay ["On groups and fields definable in O-minimal structures", preprint]. In particular he shows that if a group G is definable in the reals, then G is a Lie group.

Before we begin the proof of Theorem 1, we need to recall, as briefly as possible, a few basic facts we will be using all the time and also, to clarify some definitions.

0 - Preliminaries

0.1 - ω-stable groups

Let T be an ω-stable theory and let (G,.) be a definable group in T, with

parameters $\bar{a}$. We recall some basic definitions and facts; we will state them in the context of an ω-stable theory but most of them are valid in the more general context of a group definable in a stable theory.

Definition: A type $p \in S(\bar{a})$, $p \vdash G$, is said to be **generic** if, for all model M of T, $\bar{a} \subseteq M$, for all b realizing over M a non forking extension of p, and for all $g \in G \cap M$, $t(g.b/M)$ does not fork over $\bar{a}$.

If T is ω-stable, then the generic types of G are exactly the (finitely many) types of maximal Morley Rank in G.

The following are direct consequences of the above definition:

Facts : - for all $g \in G$, there are b_1 and b_2 , realizing generic types of G such that $g = b_1.b_2$

- if $X \subseteq G$ is definable, X containing one generic type of G, then there are $a_1,\ldots,a_n \in G$ such that $G = a_1X \cup \ldots \cup a_nX$.

Definition: we say that G is **connected** if G has no proper definable subgroup of finite index.

Fact: G is connected if and only if G has only one generic type; in this case, this generic is stationary, i.e. has a unique non forking extension over any $B \supseteq \bar{a}$.

0.2 - Algebraically closed fields and varieties

Let K be an algebraically closed field. Recall that, by elimination of quantifiers, there is a one-to-one correspondance between the space of n-types over K and the prime ideals of $K[X_1,\ldots,X_n]$, the Krull dimension of the ideal being equal to the Morley Rank of the type. If X is a definable subset of K^n, then $X = \bigcup_{i<m} (O_i \cap F_i)$, where the F_i's are Zariski closed subsets of K^n and the O_i's are Zariski open subsets of K^n (the O_i's can be chosen to be principal open sets).

Let f be a definable map from K^n to K. If K has characteristic 0, then f is locally rational: by compactness, there are $O_1,\ldots,O_k$, open in K^n, such that $K^n = \bigcup_{j\leq k} O_j$ and $f|O_j$ is a rational function. If K has characteristic p>0, then $K^n = \bigcup_{j\leq k} O_j$, where $f|O_j$ is a p^m-th root of a rational function.

The following theorem will enable us to consider only definable groups instead of interpretable ones:

Theorem [B.Poizat, "Une théorie de Galois imaginaire", J.S.L. vol.48 (1983)]: The theory of algebraically closed fields admits elimination of imaginaries, i.e., every definable equivalence relation $E(\bar{x},\bar{y})$ on K^n is of the form $f(\bar{x}) = f(\bar{y})$, where f is a definable map from K^n in K^m for some m.

Let A,B be two Zariski closed sets and let f be a map from A to B. We say that f is a **morphism** if there is a finite covering of A by open sets O_i's such that $f|O_i$ is rational.

We will use the following definition of a **prevariety**:

V is a prevariety if $V = V_1 \cup \ldots \cup V_n$, and there are bijective maps f_i from V_i into U_i, where each U_i is an open subset of a Zariski closed set, such that

- if U_{ij} is the image by f_i of $V_i \cap V_j$, then U_{ij} is open in U_i
- the map $f_{ij} = f_j \circ f_i^{-1}$ from U_{ij} into U_{ji} is a morphism.

The topology on V is given by the following: $X \subseteq V$ is open if, for all i, $f_i(X \cap V_i)$ is open in U_i.

A prevariety V is a **variety** if the diagonal is closed in V×V (for the prevariety structure on V×V given by the $U_i \times U_j$'s).

We will consider a prevariety as living on a definable set, by identifying V with the union of the U_i's, modulo the relation that identifies U_{ij} and U_{ji}.

In order to simplify definitions, we will consider only irreducible varieties, i.e. varieties which are not the union of two proper closed

subsets.

If V is irreducible, there is a unique prime ideal contained in every open subset of V, which is called the generic point of V. The corresponding type is the unique type of maximal Morley Rank in V.

Note that if V is irreducible, with generic type p, then VxV is irreducible, with generic type pxp, that is the type of any pair (a,b), a and b realizing p, and independent.

It now remains only to recall the definition of an **algebraic group** : (G,.,inv) is an algebraic group if G is a prevariety and multiplication and inverse are morphisms. Note that it follows that G is a variety. It is clear from the above remarks that an algebraic group is connected (as defined above) if and only if, as a variety, it is irreducible.

1- Proof of Theorem 1

We are going to assume that the group G is connected but this is no loss of generality as the general case follows from the connected case.

Theorem 1-A:

Let $(G,.,inv) \subseteq K^n$ be a connected definable group with parameters in $k_o \prec K$ such that, for a,b generic independent

$$a.b \in k_o(a,b)$$

$$inv(a) \in k_o(a),$$

then there is a structure of variety on G which makes (G,.,inv) into an algebraic group.

We are going to need the following easy lemma:

Lemma 0:

a) - Let V be an irreducible variety and let $X \subseteq V$ be a definable set, X

containing the generic of V. Then X contains an open subset O of V (and of course O contains the generic).

b) - Let V and V' be two irreducible varieties, and let f be a definable map from V to V' such that, on the generic of V, f is rational. Then there is $O \subseteq V$, open, such that $f|O$ is a morphism.

Proof:

a) - The set X is definable, therefore it is a finite union of sets of the form $O \cap F$, where O is open in V and F is closed in V.
Choose one such $O \cap F$ that contains the generic, so F contains the generic, but the complement of F in V is open and, as V is irreducible, must also contain the generic, so F = V.

b) - Choose a definable $X \subseteq V$, containing the generic, such that f(a) is a given rational function of a, for all a in X. By a) X contains an open set of V.

Proof of Theorem 1-A:

The group G is definable, so $G = \bigcup_{i<} (O_i \cap F_i)$, where we can assume the O_i's to be principal open sets in K^n and where the F_i's are closed in K^n. Let V_o be one of these intersections, containing the generic of G, p.
Then on V_o we have the structure of an irreducible prevariety, with generic p; we also have the usual structure of prevariety on $V_o \times V_o$, with generic pxp.
Let X be a definable subset of $V_o \times V_o$ containing pxp, such that if $(x,y) \in X$, then x.y is rational over x,y.
Let $X' = \{ (x,y) \in X \ ; \ x.y \in V_o \}$, X' is definable. By the lemma above, there is $M_o \subseteq X'$, open in $V_o \times V_o$, such that multiplication, from M_o in V_o, is a morphism. For the same reasons, there is $V_1 \subseteq V_o$, open such that inv is a morphism from V_1 in V_o.

Now let

$$Y = \{x \in V_1 \ ; \text{ for all } y \text{ generic independent from } x,\ (y,x) \in M_o \text{ and } (inv(y),y.x) \in M_o \ \}.$$

By definability of the type p, Y is a definable set, and Y contains the generic p.

By the lemma again, there is $V_2 \subseteq Y \subseteq V_1$, open, and of course, inv is still a morphism from V_2 in V_o. Now let $V = V_2 \cap inv(V_2)$, then V is open, because V is the inverse image (in V_2) by a morphism, of an open set, and $V = inv(V)$.

Let $M = \{(x,y) \in M_o \cap VxV \ ; \ x.y \in V\}$, again, because multiplication is a morphism, M is open.

So, by taking smaller and smaller open sets we have come to the following situation:

we have V, open in V_o, therefore with the induced variety structure, and M, open in VxV, such that:

(i) multiplication is a morphism from M into V

(ii) inv is a morphism from V into V and $inv(V) = V$

(iii) for all x in V, for all y generic independent from x, (y,x) and (inv(y),y.x) are both in M.

The structure of variety on G is obtained by covering G by translates of V (i.e. of the form a.V). As G is an ω-stable group and V contains the generic of G, we know that a finite number of translates of V will be sufficient to cover G.

In order to see that this indeed gives G the structure of a variety and in fact of an algebraic group, we need the following lemma:

Lemma:

Let $a,b \in G$, let $H = \{ (x,y) \in VxV;\ a.x.b.y \in V\}$. Then

- H is open
- the map f_{ab} from H into V, which takes (x,y) to a.x.b.y is a morphism.

Proof of the lemma:

Let $(x_o,y_o) \in H$, we want to find H_o, $(x_o,y_o) \in H_o \subseteq H$, open, such that f_{ab} restricted to H_o is a morphism.

We know that b = c.d, where c and d both realize the generic p; let e also realize p, independent from $\{a,c,d,x_o,y_o\}$.

Let $H_o = \{ (x,y) \in VxV ;\ (e.a,x) \in M ,\ (e.a.x,c) \in M ,\ (e.a.x.c,d) \in M$

$(e.a.x.c.d,y) \in M ,(inv(e),e.a.x.c.d.y) \in M\}$.

First, by the choice of e, and by applying condition (iii) on V each time, $(x_o,y_o) \in H_o$.

We see that H_o is open in VxV by applying successively the following classical facts: if O is open in VxV, if h is a morphism from O in V, if $z \in V$, then the set

$$\{ (x,y);\ (x,z) \in O \text{ and } (h(x,z),y) \in O \}$$

is open, and also,

$$O_z = \{ x \in V;\ (z,x) \in O \}$$

is open and h_z, from O_z in V, is a morphism.

Now a.x.b.y = inv(e).e.a.x.c.d.y ; so $H_o \subseteq H$, and over H_o, f_{ab} becomes a composition of morphisms because at each step the elements one wants to multiply are in M, and hence it is a morphism.

We can now go back to the proof of the theorem. Choose $a_1,\ldots,a_n$ in G such that $G = a_1V \cup \ldots \cup a_nV$ (where aV denotes the set { a.x; $x \in V$ }).

In order to check that this, together with the left translations f_i from V into a_iV, is a prevariety on G, we need that for all i,j

- $V_{ij} = \{x \in V;\ a_i.x \in a_jV\} = \{x \in V;\ inv(a_j).a_i.x \in V\}$ is open
- the map f_{ij} from V_{ij} into V which takes x to $inv(a_j).a_i.x$ is a morphism.

But, it is a direct consequence of the lemma that, for all a in G, the set $V_a = \{x \in V;\ a.x \in V\}$ is open and the left translation by a is a morphism.

It remains to check that multiplication and inverse are morphisms.

Multiplication:

GxG, as a variety is covered by products of the form aVxbV, which get their variety structure from VxV. To say that multiplication is a morphism means exactly that the set

$$A_{abc} = \{(x,y) \in VxV;\ a.x.b.y \in cV\} = \{(x,y) \in VxV;\ inv(c).a.x.b.y \in V\}$$

is open in VxV and that the map from A into V which takes (x,y) to inv(c).a.x.b.y is a morphism. This is exactly the lemma.

Inverse:

it is a morphism if the set

$$A_{ab} = \{x \in V;\ inv(a.x) \in bV\} = \{x \in V;\ inv(a.x.b) \in V\}$$

is open and the map from A_{ab} into V which takes x to inv(a.x.b) is a morphism. But (condition (ii)), inv(V) = V so $A_{ab} = \{x \in V;\ a.x.b \in V\}$, and again it is open, as a direct consequence of the lemma, and the map taking x to a.x.b is a morphism. We also have that, on V, inv is a morphism, so inv(a.x.b) is the composition of two morphisms. □

Theorem 1-B:

Let (H,.,inv) be a connected group interpretable in K. Then there is a definable group $(G,*,inv') \subseteq K^n$ and some countable $k_o \leq K$, k_o containing the defining parameters of H and G, such that H and G are definably isomorphic and, for a,b generic independent in G, $a*b \in k_o(a,b)$ and $inv'(a) \in k_o(a)$.

Proof:

Note first that, by elimination of imaginaries in algebraically closed fields, any interpretable group is definably isomorphic to some definable group in some K^n, so we can assume that $(H,.,inv) \subseteq K^n$.

Without loss of generality, assume K is very saturated.

Now if K has characteristic 0, then there is nothing left to prove, as any

definable function is locally rational, so we assume that K has characteristic p>0.

Let $k \subseteq K$ be an uncountable algebraically closed field, containing all the defining parameters of H. There is some $q = 1/p^m$ such that, for all $\bar{a},\bar{b} \in H$, $\bar{a}.\bar{b} \in k(\bar{a}^q,\bar{b}^q)^n$ and $inv(\bar{a}) \in k(\bar{a}^q)^n$ (where if $\bar{a} = (a_1,\ldots,a_n)$, $k(\bar{a}^q)$ denotes $k(a_1^q,\ldots,a_n^q)$).

Let $\bar{a}$ realize the generic of H over k. We define:

$$k^*(\bar{a}) = k(\bar{a}^q,\ inv(\bar{a})^q,\ \bar{b}_1.\bar{a}.\bar{b}_2,\ \bar{b}_1.inv(\bar{a}).\bar{b}_2;\ \bar{b}_1,\bar{b}_2 \in H \cap k^n).$$

We have that $k^*(\bar{a}) \subseteq k(\bar{a}^{q'})$, with $q' = q^2$.

Now $k(\bar{a}^{q'})$ is a finite extension of $k(\bar{a})$ hence so is $k^*(\bar{a})$, so there are $c_1,\ldots,c_k$ in $k(\bar{a}^{q'})$, such that $k^*(\bar{a}) = k(\bar{a},c_1,\ldots,c_k)$, and of course, each c_i is definable over $k \cup \bar{a}$.

Consider $f: H \longrightarrow K^{n+k}$, definable injection such that for $\bar{a}$ generic, $f(\bar{a}) = (\bar{a},c_1,\ldots,c_k)$.

Trivially, $k^*(\bar{a}) = k^*(inv(\bar{a}))$, so $k(f(\bar{a})) = k(f(inv(\bar{a}))$, so if G is the image of H by f, with the obvious group law, it is true that, on a generic of G, the inverse is rational.

Now it is also trivial that, if $\bar{b} \in k^n \cap H$, then

$$k^*(\bar{a}.\bar{b}) = k^*(\bar{a}),\ \text{so}\ k(f(\bar{a}.\bar{b})) = k(f(\bar{a}))$$

$$k^*(\bar{b}.\bar{a}) = k^*(\bar{a}),\ \text{so}\ k(f(\bar{b}.\bar{a})) = k(f(\bar{a})). \qquad (*)$$

We also have that, as f is a definable bijection, for $\bar{a},\bar{b}$ generic, $f(\bar{a}.\bar{b}) \in k(f(\bar{a})^r,f(\bar{b})^r)^{n+k}$ for $r = 1/p^l$, for some l.

Let k_o, countable , $k_o < k$, contain all the necessary parameters.

Let $\bar{b} \in H \cap k^n$ realize the generic of H over k_o, and let $\bar{a}$ realize the generic of H over k. By (*), $f(\bar{a}.\bar{b}) \in k(f(\bar{a}))^{n+k}$, and we also have that

$$f(\bar{a}.\bar{b}) \in k_o(f(\bar{a})^r,f(\bar{b})^r)^{n+k}.$$

But, $k(f(\bar{a})) \cap k_o(f(\bar{a})^r,f(\bar{b})^r) = k_o(f(\bar{a}),f(\bar{b})^r)$: because $f(\bar{a})^r$ remains over $k(f(\bar{a}))$ of the same degree as over $k_o(f(\bar{a}),f(\bar{b})^r)$, since $\bar{a}$ is independent from

k, which contains $f(\bar{b})^r$, over k_o.

Symetrically, because $\bar{a}^\frown\bar{b}$ and $\bar{b}^\frown\bar{a}$ have the same type over k_o, we have that $f(\bar{a}.\bar{b}) \in (k_o(f(\bar{a}),f(\bar{b})^r) \cap k_o(f(\bar{a})^r,f(\bar{b})))^{n+k}$.

But these two fields are linearly disjoint over $k_o(f(\bar{a}),f(\bar{b}))$: more generally, it is classical algebra that if K_1, K_2 are linearly disjoint over k_o, if $x \in K_1$, $y \in K_2$, then $K_1(y)$ and $K_2(x)$ are linearly disjoint over $k_o(x,y)$. As $\bar{a}$ and $\bar{b}$ are independent over k_o, $k_o(f(\bar{a})^r) = K_1$ and $k_o(f(\bar{b})^r) = K_2$ are linearly disjoint over k_o, then we get the result by letting $f(\bar{a}) = x$ and $f(\bar{b}) = y$. It follows that $f(\bar{a}.\bar{b}) \in k_o(f(\bar{a}),f(\bar{b}))^{n+k}$, that is, that in G, the multiplication of two independent generics is rational.□

UA 753 - CNRS

Université Paris 7.

Simplification pour les produits lexicographiques d'ordres totaux

Gauthier Henri

1 Notations et rappels

En ce qui concerne les ordres totaux, leurs sommes et leurs produits lexicographiques, nous utilisons les notations de [1].

. ω, ξ, η représentent respectivement les types d'ordres de $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$.

.A et B désignent deux ensembles totalement ordonnés

.On rappelle certains résultats concernant les ordinaux: distributivité à droite du produit lexicographique par rapport à la somme; non distributivité à gauche ($2\omega=(1+1)\omega=\omega$); division euclidienne.

.δ désigne un ordinal successeur inférieur à ω^{ω},et nous l'écrivons sous la forme $\omega^n a_n+\ldots.+\omega^2 a_2+\omega a_1+k$ où $k, a_1, \ldots, a_n$ sont des entiers; $k\neq 0$.

.δ' désigne un ensemble totalement ordonné élémentairement équivalent à δ.

. Il résulte immédiatement de [1], p 258, que l'on peut écrire δ' sous la forme $\sum_{j\in J}(\omega+\xi\gamma_j)+k$ où J et γ_j sont des ensembles totalement ordonnés.

.On définit par récurence la notion d'<u>ordinaux m-limites:</u>

les ordinaux 1-limites sont les ordinaux limites;

les ordinaux m-limites sont les ordinaux limites d'ordinaux (m-1)-limites.

.Si W est un bon-ordre, $x\in W$ est un <u>point m-limite</u> si et seulement si l'isomorphisme entre W et son ordinal envoie x sur un ordinal m-limite.

.On montre par exemple que les points 1-limites de $\omega^n a_n+\ldots+\omega^2 a_2+\omega a_1+k$ ont pour type d'ordre $\omega^{n-1} a_n+\ldots+\omega a_2+a_1+1$, et que les points m-limites de $\omega^n a_n+\ldots+\omega^2 a_2+\omega a_1+k$ ont pour type d'ordre $\omega^{n-m} a_n+\ldots+\omega a_{m+1}+a_m+1$.

.c[A] désigne la <u>condensation finie</u> de A, c'est à dire l'ensemble totalement ordonné obtenu en quotientant A par la relation d'équivalence: $x\sim y$ si et

seulement si chacun des intervalles [x,y], [y,x] est fini.

.Pour $x \in A$, $c(x)=\{y \in A | x \sim y\}$. Lorsqu'il y a ambiguïté, on le note $c_A(x)$

.Si λ est un ordinal, on définit par induction $c_A^\lambda(x)$ et $c^\lambda[A]$ comme dans [1], p 80.

Le rang de A,noté rg(A),est le plus petit ordinal λ tel que $c^\lambda[A]$ est dense ou égal à 1.

.A est dispersé s'il existe λ tel que $c^\lambda[A]=1$.

.On donne alors des propriétés évidentes des condensations:

a $c^\lambda(x)$ est un intervalle de A.

b Les $c^\lambda(x)$ forment une partition de A; $(c^\lambda(x) \cap c^\lambda(y) \neq \emptyset \Rightarrow c^\lambda(x) = c^\lambda(y))$.

c Si A est un intervalle de B: $c_A^\lambda(x) = c_B^\lambda(x) \cap A$. ([1],p 82)

d Si A est un intervalle de B: $rg(A) \leq rg(B)$.

e $rg(A\omega) \leq rg(A)+1$.

2 Résultats préliminaires;

LEMME 1:

(i) Si A est dispersé et a un rang limite λ, alors $rg(A+A)=rg(A\omega)=\lambda+1$

(ii) Si A est dispersé et si le rang λ de A n'est pas limite, alors $\lambda=\mu+1$, et

(α) Si $c^\mu[A]$ est fini, alors $rg(A+A)=rg(A\omega)=rg(A)$, et $c^\mu[A\omega]=\omega$.

(β) Si $c^\mu[A]$ est infini, alors $rg(A+A)=rg(A\omega)=rg(A)+1$.

Démonstration:

On montre tout d'abord le lemme 0:

Si A a un rang limite λ, alors tout segment initial ou tout segment final de A a le même rang λ.

Sinon, il existe I_0, segment initial de A, et I_1, segment final de A tels que $A=I_0+A'+I_1$ et $rg(I_0)=\beta_0<\lambda$; $rg(I_1)=\beta_1<\lambda$.

On note $r=Sup(\beta_0,\beta_1)$.

On utilise la propriété ensembliste b pour montrer que si $x \in I_0$, $y \in I_1$ et $\beta<\lambda$, alors $c^\beta(x) \cap c^\beta(y)=\emptyset$.

Sinon, $c^\beta(x)=c^\beta(y)$. Si $\beta \geq r$, $c^\beta(x) \supseteq I_0$ et $c^\beta(y) \supseteq I_1$. Comme $c^\beta(x)$ est un intervalle: $c^\beta(x)=A$, et donc, $rg(A) \leq \beta$. Contradiction.

D'autre part, si $\beta<r$, $c^r(x)=c^r(y)$. Idem.

Ainsi, pour tout $\beta<\lambda$, $c^\beta(x) \cap c^\beta(y)=\emptyset$, et donc, $\bigcup_{\beta<\lambda} c^\beta(x) \cap \bigcup_{\beta<\lambda} c^\beta(y)=\emptyset$.

Donc, $c^\lambda(x) \cap c^\lambda(y)=\emptyset$, et donc $rg(A)>\lambda$. Contradiction. CQFD

(i) On écrit alors A sous la forme $A=I_0+I_1=I_0'+I_1'$, où I_0 a un plus grand élément et I_1' un plus petit.

Alors $rg(A+A)=rg(I_0'+I_1'+I_0+I_1) \geq rg(I_1'+I_0) \geq Sup(rg(I_1'),rg(I_0))=\lambda$.

Comme $I_1'+I_0$ a un premier et un dernier élément, son rang ne peut pas être limite (lemme 0). Donc $rg(A+A)>\lambda$. Ainsi, $rg(A+A)=\lambda+1$.

(ii)(α) $c^\mu[A]$ est fini (de cardinal k).

$A\omega=A_0+A_1+A_2+\ldots$ où $A_i=A$ pour tout $i \geq 0$.

Si $x,y \in A\omega$, et si $y \in c^\mu_{A_i}(x)$, alors $y \in c^\mu_{A\omega}(x)$ (clair).

Les $c^\mu_{A_i}(x)$ partitionnent A_i en k ensembles, donc les $c^\mu_{A\omega}(x)$ partitionnent $A\omega$ en au plus $k\omega=\omega$ ensembles.

Comme $rg(A)=\mu+1$, si $x \in A_i$, $c^\mu_{A\omega}(x)$ ne recouvre aucun des A_i; et comme c'est un intervalle, $c^\mu_{A\omega}(x)$ intersecte au plus deux des A_i.

Donc, les $c^\mu_{A\omega}(x)$ partitionnent $A\omega$ en exactement ω ensembles.

Ainsi, $c^\mu[A\omega]=\omega$, et $rg(A\omega)=\mu+1=rg(A)$.

(β) Si $c^\mu[A]$ est infini, $c^\mu[A]=\omega$ ou ω^* ou ξ. On suppose par exemple que $c^\mu[A]=\omega$.

On écrit encore A sous la forme $A=\sum_{i \in \omega} A_i$, où $A_i=A$ pour tout $i \geq 0$.

Soit $x \in A_i$, $c^\mu_{A\omega}(x)$ intersecte au plus deux A_j et ne contient aucun A_j.

Si $c^\mu_{A\omega}(x)$ intersecte A_i et A_i+1: on prend $y \in A_{i+1}$ tel que $c^\mu_{A\omega}(x)=c^\mu_{A\omega}(y)$.

$c^\mu[A_i]=\omega$, donc $A_i=A_i^0+A_i^1+A_i^2+\ldots$, où $A_i^n=c^\mu_{A_i}(x_n)$ avec $x_{n_0}=x$.

$c^\mu_{A_i}(x)=c^\mu_{A_i}(x_{n_0})=A_i^{n_0}=c^\mu_{A\omega}(x) \cap A_i$.

$c^{\mu}_{A\omega}(x)$ contient $x\in A^{n}_{i}0$ et $y\in A_{i+1}$. Comme c'est un intervalle, $c^{\mu}_{A\omega}(x)$contient tous les A^{n}_{i} pour $n>n_0$.

Par exemple, $A^{n_0+1}_{i}\subseteq c^{\mu}_{A\omega}(x)\cap A_i=c^{\mu}_{A_i}(x)=A^{n}_{i}0$. Contradiction.

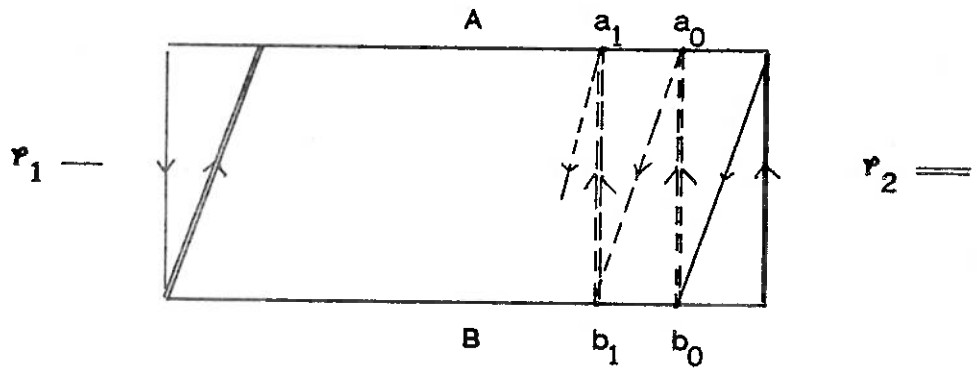
Donc, $c^{\mu}_{A\omega}(x)$ intersecte un seul A_j.

$c^{\mu}_{A\omega}(x)\subseteq A^{n}_{i}0$, donc, les $c^{\mu}_{A\omega}(x)$ partitionnent $A\omega$ en $\omega\omega$ ensembles. Ainsi, $rg(A\omega)=\lambda+1$. CQFD

Proposition 1: (Théorème de Lindenbaum)

Si A est un segment initial de B, et B un segment final de A, alors $A\simeq B$.

Démonstration:



On se place dans les complétés de Dedekind de A et B. La suite définie par $a_0=\varphi_2(b_0)$; $a_1=\varphi_2(\varphi_1(a_0))$; ...; $a_{n+1}=\varphi_2(\varphi_1(a_n))$;... est décroissante et converge vers a. La suite (b_n) correspondante converge vers b.

$\varphi_1(a)=b$ et $\varphi_2(b)=a$.

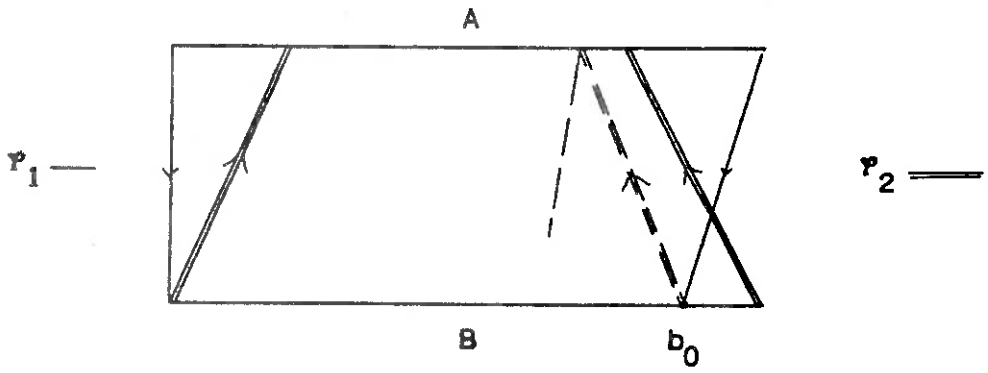
On construit alors l'isomorphisme φ en posant: $\varphi=\varphi_1$ sur $A^{<a}$, et $\varphi=\varphi_2^{-1}$ sur $A^{>a}$.

CQFD.

Proposition 2:

Si A est un segment initial et final de B, et si B est un intervalle de A, alors $A\simeq B$.

Démonstration:



On construit de la même façon un isomorphisme φ_3 qui fait de B un segment initial de A.

On utilise alors le théorème de Lindenbaum. CQFD.

Conformément aux notations précédentes, nous allons démontrer le théorème suivant:

THEOREME: Si $A\delta' \simeq B\delta'$, et si A est dispersé, alors $A \simeq B$.

Nous démontrerons ce théorème par l'absurde. Les propositions 1 et 2 permettent alors de se placer sous l'hypothèse suivante:

(H)
- $A\delta' \simeq B\delta'$; φ désigne l'isomorphisme de $A\delta'$ dans $B\delta'$.
- A est un segment initial et final de B.
- $A \neq B$, et donc, B n'est pas un intervalle de A.

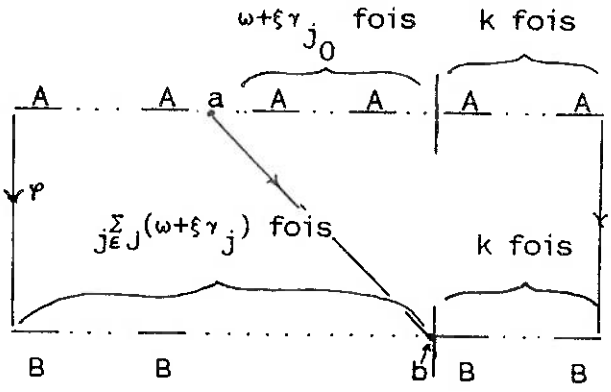
LEMME 2: (sous l'hypothèse (H))

$A\omega$ est un intervalle de B.

Démonstration:

B n'est pas un intervalle de A, donc Bk n'est pas un intervalle de Ak. On se place dans les complétés de Dedekind de $A\delta'$ et $B\delta'$. L'isomorphisme φ plonge Ak (segment final de $A\delta'$) dans Bk (segment final de $B\delta'$). On utilise alors l'écriture de δ' sous la forme $\sum_{j\in J}(\omega+\xi_{\gamma_j})+k$. On appelle b le premier élément de Bk (segment final de $B\delta'$), et $a=\varphi^{-1}(b)$

1° cas: J n'a pas de plus grand élément.

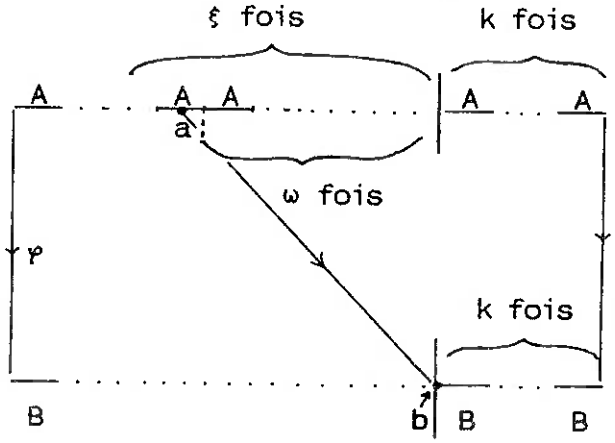


Il existe j_0 tel que,
pour tout $x\in A(\omega+\xi\gamma_{j_0})$ dans $A\delta'$,
$a<x$.
Alors, $A(\omega+\xi\gamma_{j_0})$ est un intervalle de Bk.
Donc, $A\omega$ est un intervalle de B.

2° cas: J a un plus grand élément j_∞.

Si a est plus petit que la portion $A\xi\gamma_{j_\infty}$, on est ramené au cas précédent.

Sinon, si γ_{j_∞} n'a pas de dernier élément, on peut plonger $A\xi$ dans Bk, et donc $A\omega$ dans B.



Si γ_{j_∞} a un dernier élément,
$A\omega$ est un intervalle de Bk,
donc $A\omega$ est un intervalle de B.
CQFD.

LEMME 3: (sous l'hypothèse (H))

A et B n'ont pas de premier élément.

Démonstration:

On montre que, pour $1\leq m\leq n$, les points limites de δ ont pour type d'ordre $\omega^{n-m}a_n+\ldots+\omega a_{m+1}+a_m+1$, et que leur ensemble est définissable.
On peut ainsi définir $L_m(\delta')$, l'ensemble des points "m-limites" de δ', pour tout $\delta'\equiv\delta$. On sait alors que $L_m(\delta')\equiv L_m(\delta)$.

On suppose que A et B ont des premiers éléments, notés respectivement a_0 et b_0, et on note, pour $1\leq m\leq n$, $A_m=\{(a_0,x)\,|\,x\in L_m(\delta')\}$ et $B_m=\{(b_0,x)\,|\,x\in L_m(\delta')\}$. $A_m\subseteq A\delta'$, $B_m\subseteq B\delta'$ et $A_m\simeq B_m\simeq L_m(\delta')$.

On démontre par récurrence que $\mathcal{P}^{-1}(B_m)\leq A_m$, et que le dernier élément de B_m n'est pas l'image par $\mathcal{P}$ du dernier élément de A_m. La contradiction provient du fait que A_n et B_n ont exactement a_n+1 éléments.

1° $\mathcal{P}^{-1}(B_1)\leq(A_1)$:

Soit $(b_0,y)\in B_1$ et $(a,x)=\mathcal{P}^{-1}((b_0,y))$. On veut montrer que $a=a_0$ et que $x\in L_1(\delta')$.

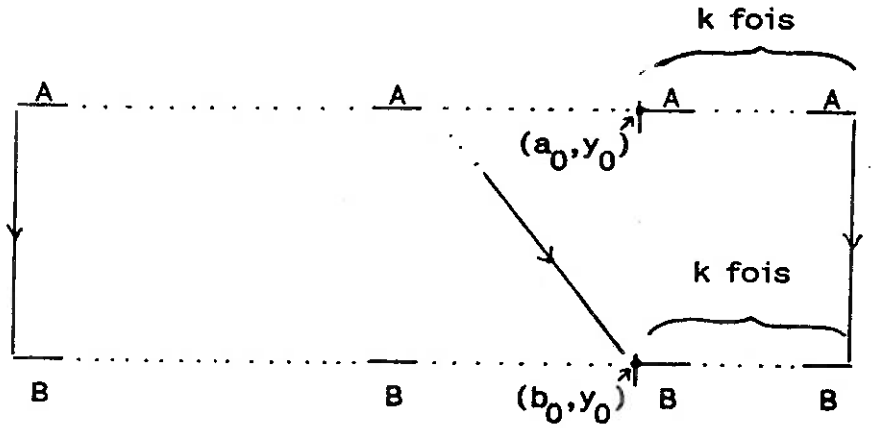
Si $a>a_0$: $\mathcal{P}((a_0,x))=(b,z)<(b_0,y)\Rightarrow z<y$. Comme $(b_0,y)\in B_1$, y n'a pas d'antécédent dans δ', et donc, il existe $z_1\in\delta'$ tel que $z<z_1<y$.

Alors, pour tout $q\in B$, $(b,z)<(q,z_1)<(b_0,y)\Rightarrow\forall q\in B$, $(a_0,x)<\mathcal{P}^{-1}((q,z_1))<(a,x)$. Donc, B est un intervalle de A, ce qui contredit l'hypothèse (H). Donc, $a=a_0$.

Si $x\notin L_1(\delta')$, alors x a un antécédent x'. Soit $(b,z)=\mathcal{P}(a_0,x')$, $(a_0,x')<(a_0,x)\Rightarrow(b,z)<(b_0,y)\Rightarrow z<y$. On choisit, comme précédemment z_1 tel que $z<z_1<y$ ... Contradiction.

Donc, $x\in L_1(\delta')$.

2° Le dernier élément de B_1 n'est pas l'image par $\mathcal{P}$ du dernier élément de A_1:



Ces deux points sont les points (a_0,y_0) et (b_0,y_0) du dessin.

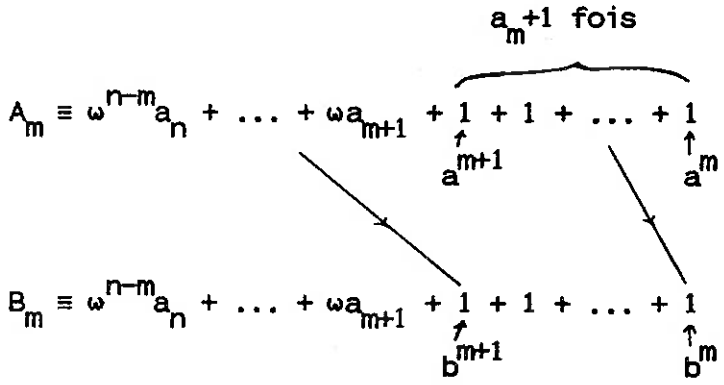
Le résultat est clair, car si $(b_0,y_0)=\mathcal{P}(a_0,y_0)$, $Ak\simeq Bk$.

3° On suppose que $\varphi^{-1}(B_m)\subseteq A_m$ et que le dernier élément b^m de B_m n'est pas l'image par φ du dernier élément a^m de A_m.

$B_{m+1}\subseteq B_m$, donc $\varphi^{-1}(B_{m+1})\subseteq A_m$. Si $(b_0,y)\in B_{m+1}$, $\varphi^{-1}((b_0,y))=(a_0,x)$, où $x\in L_m(\delta')$. Si $x\notin A_{m+1}$, x a un antécédent x' dans A_m, donc $\varphi((a_0,x'))=(b,z)<(b_0,y)$. Donc $z<y$, et comme $y\in L_{m+1}(\delta')$, il existe $z_1\in L_m(\delta')$ tel que $z<z_1<y$. Alors $(b,z)<(b_0,z_1)<(b_0,y)$ dans B_m. Donc $(a_0,x')<\varphi^{-1}((b_0,z_1))<(a_0,x)$ dans A_m, ce qui contredit le fait que x' est l'antécédent de x dans $L_m(\delta')$.

Donc $\varphi^{-1}(B_{m+1})\subseteq A_{m+1}$.

Le type d'ordre de A_m et B_m est élémentairement équivalent à $\omega^{n-m}a_n+\ldots+\omega a_{m+1}+a_m+1$. Il suffit de reconnaître b^m et b^{m+1} dans B_m, ainsi que a^m et a^{m+1} dans A_m:



Comme $\varphi^{-1}(b^m)<a^m$:

$\varphi^{-1}(b^{m+1})<a^{m+1}$

CQFD.

3 Démonstration du théorème:

THEOREME: A, B, et δ' sont des ensembles totalement ordonnés. $\delta'\equiv\delta$ ordinal successeur, $\delta<\omega^\omega$. Si A est dispersé, alors

$$A\delta'\simeq B\delta' \Rightarrow A\simeq B.$$

Démonstration: On se place sous l'hypothèse (H), et l'on suppose de plus que A est dispersé.

Si $c^{rg(A)}[B]\neq 1$, alors $c^{rg(A)}[B]\neq c^{rg(A)}[A]$.

Donc, pour tout $\lambda<rg(A)$, $c^{\lambda}[A]\neq c^{\lambda}[B]$

On montre par induction, et en utilisant le lemme 3, que pour tout $\lambda<rg(A)$:

(i) $c^{\lambda}[A]\delta'\simeq c^{\lambda}[B]\delta'$

(ii) $c^{\lambda}[A\delta']\simeq c^{\lambda}[A]\delta'$

(iii) $c^{\lambda}[B\delta']\simeq c^{\lambda}[B]\delta'$

D'après le lemme 3, A et B n'ont pas de premier élément, donc,

$c[A\delta']=c[A]\delta'$ et $c[B\delta']=c[B]\delta'$ (clair).

Comme $A\delta'\simeq B\delta'$, en condensant une fois, il vient: $c[A]\delta'\simeq c[B]\delta'$.

Si on a (i), (ii) et (iii) pour $\lambda<rg(A)$, comme $c^{\lambda}[B]\neq c^{\lambda}[A]$:

$c^{\lambda}[A]$ et $c^{\lambda}[B]$ vérifient l'hypothèse (H).

D'après le lemme 3, ils n'ont pas de premier élément, et donc, en condensant une fois de plus, il vient:

$c[c^{\lambda}[A]\delta']\simeq c[c^{\lambda}[B]\delta'] \Rightarrow c^{\lambda+1}[A]\delta'\simeq c^{\lambda+1}[B]\delta'$.

Si on a (i), (ii) et(iii) pour tout $\mu<\lambda$ limite:

$A\delta'\simeq B\delta' \Rightarrow c^{\lambda}[A\delta']\simeq c^{\lambda}[B\delta']$.

Pour tout $\mu<\lambda$, pour tout $(x,y)\in A\delta'$, $c^{\mu}((x,y))$ appartient toujours au même A

$c^{\lambda}((x,y))=\bigcup_{\mu<\lambda} c^{\mu}((x,y))$, donc, $c^{\lambda}[A\delta']=c^{\lambda}[A]\delta'$. CQFD.

Ainsi, pour $\lambda=rg(A)$, il vient: $c^{rg(A)}[A]\delta'\simeq c^{rg(A)}[B]\delta'$ et $c^{rg(A)}[A]\neq c^{rg(A)}[B]$

Donc, $c^{rg(A)}[A]$ et $c^{rg(A)}[B]$ vérifient l'hypothèse (H).

D'après le lemme 3, ils n'ont pas de premier élément, or $c^{rg(A)}[A]=1$.

Contradiction. Donc, $c^{rg(A)}[B]=1$; B est dispersé, et $rg(B)\leq rg(A)$.

Ainsi, $rg(B)=rg(A)$.

D'après le lemme 2, $A\omega$ est un intervalle de B, donc: $rg(A)\leq rg(A\omega)\leq rg(B)=rg(A)$

D'après le lemme 1, rg(A) est un ordinal successeur $\mu+1$, et $c^{\mu}[A]$ est fini.

Si $c^{\mu}[A]\neq c^{\mu}[B]$, alors $c^{\mu}[A]$ et $c^{\mu}[B]$ vérifient l'hypothèse (H), et donc, $c^{\mu}[A]$ et $c^{\mu}[B]$ n'ont pas de premier élément, ce qui contredit la finitude de $c^{\mu}[A]$.

Donc, $c^{\mu}[A]\simeq c^{\mu}[B]$. Or, $c^{\mu}[A\omega]\simeq\omega\leq c^{\mu}[B]$, ce qui contredit la finitude de $c^{\mu}[B]$. CQFD.

4 Remarques:

Des exemples simples montrent qu'il n'y a pas d'amélioration grossière du théorème:

(i)lorsque δ est un ordinal limite:

$2\delta \simeq 1\delta$ et $2 \not\simeq 1$.

(ii)lorsque δ est un ordinal successeur supérieur à ω^ω:

$\delta = \omega^\omega \delta_1 + \delta_2$; $1\delta \equiv (\omega^\omega + \delta_2)\delta$. Donc, il existe un ensemble I, et $\mathcal{U}$ un ultrafiltre sur I tels que: si $A = 1^I/_{\mathcal{U}} = 1$, si $B = (\omega^\omega + \delta_2)^I/_{\mathcal{U}}$, et si $\delta' = \delta^I/_{\mathcal{U}}$, alors $A\delta' \simeq B\delta'$, A est dispersé, et $A \not\simeq B$.

(iii)supposons A et B non dispersés.

En supposant l'hypothèse du continu, on montre que si $\mathcal{U}$ est un ultrafiltre non principal sur $\mathbb{N}$, $\omega^{\mathbb{N}}/_{\mathcal{U}} + 1 = \omega + \xi\eta^{\mathbb{N}}/_{\mathcal{U}} + 1$. (Il est clair qu'il existe τ tel que $\omega^{\mathbb{N}}/_{\mathcal{U}} = \omega + \xi\tau$, et que τ est saturé. Sous l'hypothèse du continu, il n'y a qu'un seul ensemble saturé de cardinal $\aleph_1$, donc $\tau = \eta^{\mathbb{N}}/_{\mathcal{U}}$; voir [2])

On note $\tau = \eta^{\mathbb{N}}/_{\mathcal{U}}$.

On montre successivement que: (a) $(1+\eta)(\omega+1) = 1+\eta$

(b) $(1+\tau)(\omega+\xi\tau+1) = 1+\tau$

(c) $\eta(1+\tau+1)\omega = \eta(1+\tau)\omega$

(d) $\eta(1+\tau+1)\xi = \eta(1+\tau)\xi$

(e) $[\eta(1+\tau+1)](\omega+\xi\tau+1) = [\eta](\omega+\xi\tau+1) = \eta(1+\tau+1)$

(a): Dans $\mathbb{Q}$,

$[1,1+1/2[+ [1+1/2,1+1/2+1/4[+ [1+1/2+1/4,1+1/2+1/4+1/8[+ \ldots + [2,3[$ est isomorphe à $1+\eta$, ainsi que chacun des intervalles considérés.

(b) s'obtient en passant aux ultrapuissances.

(c): $\eta(1+\tau+1)\omega = (\eta+\eta\tau+\eta)\omega = (\eta+\eta\tau+\eta)+(\eta+\eta\tau+\eta)+ \ldots$

$= (\eta+\eta\tau)+(\eta+\eta+\eta\tau)+(\eta+\eta+\eta\tau)+ \ldots$

$= (\eta+\eta\tau)+(\eta+\eta\tau)+(\eta+\eta\tau)+ \ldots = (\eta+\eta\tau)\omega = \eta(1+\tau)\omega$

(d) se démontre de la même façon.

(e): $\eta(\omega+\xi\gamma+1)=\eta\omega+(\eta\xi)\gamma+\eta=\eta+\eta\gamma+\eta=\eta(1+\gamma+1)$

$\eta(1+\gamma+1)(\omega+\xi\gamma+1)=\eta(1+\gamma+1)\omega+\eta(1+\gamma+1)\xi\gamma+\eta(1+\gamma+1)$

$=\eta(1+\gamma)\omega+\eta(1+\gamma)\xi\gamma+\eta(1+\gamma+1)$ (d'après (c) et (d))

$=\eta[(1+\gamma)(\omega+\xi\gamma+1)]+\eta=\eta(1+\gamma)+\eta$ (d'après (b))

$=\eta(1+\gamma+1)$

Ainsi, si l'on note $A=\eta(1+\gamma+1)$; $B=\eta$ et $\delta'=\omega+\xi\gamma+1$:

$A\delta'\simeq B\delta'$ et $A\not\equiv B$ car Card(A)>Card(B).

Nous concluons par une question:

CONJECTURE: Si A et B sont des ensembles totalement ordonnés, et si δ est un ordinal successeur inférieur à ω^{ω}, alors $A\delta\equiv B\delta \Rightarrow A\equiv B$.

En passant aux ultrapuissances, il suffirait de montrer que si $\delta'\equiv\delta$,

$A\delta'\simeq B\delta' \Rightarrow A\equiv B$.

Dans l'exemple (iii), $A\not\equiv B$, mais $A\equiv B$.

Références bibliographiques:

[1] J.G.Rosenstein, Linear orderings, Acad Press, 1982

[2] C.C.Chang et H.J.Keisler, Model Theory, North-Holland, 1973

BETWEEN GROUPS AND RINGS*

ABSTRACT

Anand Pillay, University of Notre Dame
Philip Scowcroft, Stanford University
Charles Steinhorn, Vassar College**

In [1], van den Dries asked if new operations or relations could be added to the ordered group $(\mathbf{R}, +, 0, <)$ so that the collection of definable sets in the resulting structure lies strictly between the semilinear and semialgebraic sets. We show that an obvious candidate serves as such an example.

Theorem 1. *Let $B \subseteq \mathbf{R}$ be the restriction of the graph of multiplication to $[-1, 1]$. Then multiplication cannot be defined in the proper o-minimal expansion $(\mathbf{R}, +, 0, <, B)$ of $(\mathbf{R}, +, 0, <)$.*

Our original proof of Theorem 1 actually proceeds through a more general "two-cardinal" result for o-minimal structures:

Theorem 2. *Suppose that $\mathcal{M}$ is an ω-saturated, o-minimal L-structure, $\varphi(x)$ is a formula over $\mathcal{M}$, and $\mathcal{N} \succ \mathcal{M}$ is an ω-saturated L-structure satisfying $\varphi(\mathcal{M}) = \varphi(\mathcal{N})$. If $R \subseteq \varphi(\mathcal{M})^n$ is a new relation, then $(\mathcal{M}, R) \prec (\mathcal{N}, R)$.*

We remark that we also prove a stable version of Theorem 2.

After proving Theorem 1, we found the following refinement of that result:

Theorem 3. *Let $g: \mathbf{R} \to \mathbf{R}$ be given by*

$$g(x) = \begin{cases} x & \text{if } |x| \leq 1 \\ \text{the sign of } x & \text{if } |x| > 1 \end{cases}$$

and let $*: \mathbf{R}^2 \to \mathbf{R}$ be given by $x * y = g(x)g(y)$. Then, $Th(\mathbf{R}, +, *, 0, 1, <)$ admits elimination of quantifiers.

We finally note that although for simplicity, we have stated our results for $(\mathbf{R}, +, 0, <)$, they hold for $(\mathbf{R}, +, 0, <, f_a)_{a \in \mathbf{R}}$, where $f_a: \mathbf{R} \to \mathbf{R}$ is multiplication by a. This last structure is, properly speaking, the structure about which van den Dries raised his question.

REFERENCE

[D] L. van den Dries, *A generalization of the Tarski-Seidenberg theorem, and some nondefinability results*, Bull. Amer. Math. Soc. 15(1986), 189-193.

* To appear in the Rocky Mountain Journal of Mathematics as part of the proceedings of the 1986 Corvallis Conference on Quadratic Forms and Real Algebraic Geometry
** Authors partially supported by the N.S.F.

TOPOI AND (MULTISORTED) HIGHER ORDER INTUITIONISTIC LOGIC

Eduardo J. Dubuc
Universidad de Buenos Aires
Matematicas - 1428 BS.AS

I will present here a summary of some constructions and ideas due to F.W. Lawvere, and which are, by now, well known among category theorycists.

§1 LOGIC IN A CATEGORY

Given an object R in a category $\mathcal{E}$, and two monomorphisms $A \rightarrowtail R$, $B \rightarrowtail R$, we say that $A \subset B$ if there is a factorization $(A \rightarrowtail B \rightarrowtail R) = (A \rightarrowtail R)$. If $A \subset B$ and $B \subset A$, $A \rightarrowtail R$ and $B \rightarrowtail R$ define the same subobject, and A and B are isomorphic in $\mathcal{E}$. We shall very often write $A \subset R$ instead of $A \rightarrowtail R$, and say (by abuse of language) that A is a subobject of R.

1.1 Propositional Logic.

The relation "$\subset$" in the set of subobjects of R is reflexive and transitive (C1 and C2 below), and we can define by the usual universal properties the notions of infimun, supremun, implication, negation, zero and one. (C3 to C7 below).

C1) $A \subset A$

C2) $A \subset B$, $B \subset D$ $\Longrightarrow$ $A \subset D$

C3) $0_R \subset X$

C4) $X \subset 1_R$

C5)
$$\frac{A \subset X \ , \ B \subset X}{A \vee B \subset X}$$

C6) $$\frac{X \subset A \ , \ X \subset B}{X \subset A \wedge B}$$

C7) $$\frac{X \wedge A \subset B}{X \subset A \longrightarrow B} \ , \quad \frac{X \cap A = 0_R}{X \subset \neg A}$$

thus, $\neg A$ is the same that $A \longrightarrow 0_R$.

Here, A, B, C are arbritrary (but fixed) subojects of R , and X ranges over all the subobjects of R . The horizontal lines mean "if and only if".

1.2 First order logic.

Given any two arrows in a category, $R \xrightarrow{f} S$, $H \xrightarrow{g} S$, the pull back of f and g :

$$\begin{array}{ccc} P & \xrightarrow{\pi_H} & H \\ \downarrow{\scriptstyle \pi_R} & & \downarrow{\scriptstyle g} \\ R & \xrightarrow{f} & S \end{array}$$

is defined by the following universal propertie :

$$\frac{X \xrightarrow{r} R \ , \ X \xrightarrow{h} H \ \mid \ gh = fr}{X \xrightarrow{u} P \ \mid \ \pi_H u = h \ , \ \pi_R u = r}$$

Here X ranges over all the objects in $\mathcal{C}$, and the horizontal line means that there is a bijection, natural in X , between pairs of arrows (r,h) and arrows u as indicated. Given an arrow $R \xrightarrow{f} S$, and a subobject $A \rightarrowtail S$, the inverse image of A along f is defined as a pull-back :

$$\begin{array}{ccc} f^{-1}A & \longrightarrow & A \\ \downarrow & & \downarrow \\ R & \xrightarrow{f} & S \end{array}$$

It follows that inverse image preserves the relation "$\subset$" (C8 below). We can define existential and universal quantification by means of the universal properties of the left and the right adjoints to inverse image (C9 and C10 below)

C8) $$A \subset B \implies f^{-1}A \subset f^{-1}B$$

C9) $$\frac{D \subset f^{-1}X}{\exists_f D \subset X}$$

C10) $$\frac{f^{-1}X \subset D}{X \subset \forall_f D}$$

Here, f is an arrow $R \xrightarrow{f} S$ in $\mathcal{E}$, A, B and D are arbritrary (but fixed) subobjects, $A \subset S$, $B \subset S$ and $D \subset R$, and X ranges over all the subobjects of S.

The subobject $\exists_f D \subset S$ is the (direct) image by f of the subobject $D \subset R$. In order to have an adequate interpretation of intuitionistic logic, it is necessary that in $\mathcal{E}$, (direct) images be stable under pull-back. This means that given any subobject $D \subset R$ and any pull-back diagram :

$$\begin{array}{ccc} P & \xrightarrow{h} & H \\ \downarrow e & & \downarrow g \\ R & \xrightarrow{f} & S \end{array}$$

the following equation holds :

$$g^{-1}(\exists_f D) = \exists_h(e^{-1}D) \ .$$

The corresponding equation for universal quantification follows :

$$g^{-1}(\forall_f D) = \forall_h(e^{-1}D) \ .$$

These equations are known as "Beck conditions".

Remark In any category $\mathcal{E}$ such that it has an structure such as C1) to C10), and the Beck condition holds, all of the intuitionistic first order

logic can be interpreted in an adequate way. As we shall do in section §3.

The terminal object, denoted 1, is defined by the universal property :

$$X \xrightarrow{\text{singleton}} 1 \ .$$

This means that for all objects X in $\mathcal{E}$, there exists a unique arrow into 1.

Given two objects R, H in $\mathcal{E}$, their product and the projections are defined as a pull-back :

$$\begin{array}{ccc} R\times H & \xrightarrow{\pi_H} & H \\ \downarrow{\scriptstyle \pi_R} & & \downarrow \\ R & \xrightarrow{f} & 1 \end{array}$$

Given two arrows $X \xrightarrow{r} R$, $X \xrightarrow{h} H$, the arrow into $R \times H$ determined by the universal property is usually denoted $X \xrightarrow{(r,h)} R \times H$. When $R = H$ there is a <u>diagonal</u> $\Delta H = (id_H , id_H) : H \rightarrowtail H \times H$.

It is clear how to define finite products. The empty product turns out to be the terminal object 1.

Quantification along the projections correspond to the usual quantification of variables. The reader can verify the following :

<u>Remark</u> Assume R, H are sets, and let $A \subset H$, $D \subset R \times H$ be any subsets. Write $\pi_H = \pi$. Then :

$$\pi^{-1}A = \{(r,h) \mid h \in A\} ,$$

$$\forall_\pi D = \{h \mid \forall r\ (r,h) \in D\} ,$$

$$\exists_\pi D = \{h \mid \exists r\ (r,h) \in D\} .$$

<u>1.3 Higer order Logic</u>.

Given an arbritrary (but fixed) object R in $\mathcal{E}$, the generic (or membership) relation in R is an object $\Omega(R)$ together with a subobject $\in_R$

as indicated below

$$\in_R \rightarrowtail R \times \Omega(R)$$

characterized by the following universal property :

C11) $$\frac{Z \rightarrowtail R \times X}{X \xrightarrow{\varphi} \Omega(R)}$$

such that the following diagram is pull-back

$$\begin{array}{ccc} Z & \longrightarrow & \in_R \\ \downarrow & & \downarrow \\ R\times X & \xrightarrow{R\times\varphi} & R\times\Omega(R) \end{array}$$

where X ranges over all the objects of $\mathcal{E}$, Z over all the subobjects of $R \times X$, and the horizontal line means that there is a bijection <u>natural in X</u> .

We say that φ "classifies" the subobject Z .

The reader can verify the following :

<u>Remark</u> Assume $\mathcal{E}$ is the category of sets. Then $\Omega(R)$ is the power set of R , $\in_R$ the usual membership relation, and for x in X :

$$\varphi : x \longmapsto \{r \mid (r,x) \in Z\} .$$

Usually, the generic relation for every object R in $\mathcal{E}$ is constructed in two stepts.

<u>First</u> . A subobject classifier.

<u>Second</u>. Exponentials.

Subobject classifier : it is the generic relation in 1 . That is ; it is an object Ω in $\mathcal{E}$ together with $1 \xrightarrow{t} \Omega$ such that :

$$\frac{Z \rightarrowtail X}{X \xrightarrow{\varphi} \Omega} \quad \Big| \quad \begin{array}{ccc} Z & \longrightarrow & 1 \\ \downarrow & & \downarrow t \\ X & \xrightarrow{\varphi} & \Omega \end{array} \text{ pull-back}$$

where X an Z are as above C11. Thus, subobjects of X are "classified" by "characteristic functions" $X \longrightarrow \Omega$.

Exponentials : given any two objects R , S in $\mathcal{E}$, the exponential R^S

is defined by the following universal property :

$$\frac{X \longrightarrow R^S}{S \times X \longrightarrow R}$$

where X ranges over all the objects in $\mathcal{E}$, and the horizontal line, as usual, means that there is a bijection natural in X. It follows that there is an arrow "evaluation" $S \times R^S \xrightarrow{ev} R$ such that every $S \times X \xrightarrow{f} R$ is of the form $f(s) = ev(s, \hat{f})$ for a unique $S \xrightarrow{\hat{f}} R^S$, (here s stands for an arbritrary arrow $Z \xrightarrow{s} S$, and the parenthesis indicate composition).

Then, the generic relation is defined as pull-back :

$$\begin{array}{ccc} \in_R & \longrightarrow & 1 \\ \downarrow & & \downarrow t \\ \Omega \times \Omega & \xrightarrow{ev} & \Omega \end{array}$$

That is, $\Omega(R) = \Omega^R$, and $\in_R$ is the subobject classified by ev.

1.4 Elementary Topoi.

Definition (Lawvere-Tierney). An elementary topos is a category such that :

1) It has pull-backs and a terminal object.

2) It has exponentials.

3) It has a subobject classifier.

Theorem 1 (Lawvere-Tierney).

An elementary topos has all the (logical) structure C1 to C11 described above (and the Beck condition holds).

For a beautiful and intuitive but rigorous proof of this Theorem see [2].

As we have seen above, any topos has generic relations. The idea that "functions" are "functional relations" leads to a proof that generic relations can be used to construct exponentials.

Proposition 1 (A. Kock).

A categorie is an elementary topos if and only if :

1) It has pull-backs and a terminal object.

2) It has generic (or membership) relations.

§2 MULTISORTED HIGER ORDER INTUITIONISTIC LOGIC.

We will define the language and the axioms and rules.

2.1 Data.

Basic Data :

L1) i) There are symbols called types. In order to simplify the notation, we shall denote a finite sequence of types with a single letter, and call it an stype. There is an special symbol Ω . The basic (and only) construction is :

if R is an stype, then $\Omega(R)$ is a type.

The empty sequence is an stype. In this case, the type $\Omega(R)$ is denoted Ω . Types are identified with stypes of length 1. But stypes in general are not types.

ii) There are (a dennumerable set of) variables associated to each type. A finite sequence of variables associated to the types (of an stype) will be denoted with a single letter and refered to as an svariable.

L2) For each stype R there are predicate symbols of domain R .

L3) For each stype R and each type S , there are functional symbols of domain R and type S .

As usual, the terms and the formulae of the language are defined inductively. There are special symbols "TRUE", "FALSE", "=", "$\in$" and "{ | }" . Terms will have an associated type. A finite sequence of terms associated to

the types (of an stype) will be denoted with a single letter, and refered to as an sterm.

Terms :

L4) For each type S , each variable of type S is a term of type S .

L5) If t is an sterm of stype R , and f is a functional symbol of domain R and type S , then $f(t)$ is a term of type S .

L6) If Φ is a formula, and x is an svariable of stype R , then $\{x \mid \Phi\}_R$ is a term of type $\Omega(R)$ (we assume that all the variables in x are different).

Formulae

L7) If t is an sterm of stype R , and A a predicate symbol of domainn R , then $A(t)$ is a formula.

L8) If t and e are terms of the same type, then $t = e$ is a formula.

L9) If t is an sterm of stype R , and P is a term of type $\Omega(R)$, then $t \in P$ is a formula.

L10) TRUE and FALSE are formulae. If Φ and Ψ are formulae, then $\Phi \vee \Psi$, $\Phi \wedge \Psi$, and $\Phi \longrightarrow \Psi$ are formulae. $\neg \Phi$ is shorthand for $\Phi \longrightarrow$ FALSE.

L11) If x is a variable of type R , and Φ is a formula, then $(\exists x)_R \Phi$ and $(\forall x)_R \Phi$ are formulae.

Of course the recursion to construct terms and formulae is carried simultaneously. The stept L6 binds all the variables in the svariable x , and the stept L11 binds the variable x . A variable in a term or formula is free

if it is not bounded.

Definition 2.1. A domain of a term t is an stype R which contains a distinguished copy of the type of each different free variable in t. In particular, distinct variables of the same type correspond to different copies of that type in R. R may contain other types or more (non distinguished) copies of the same types.

A domain of a formula Φ is defined in the same way.

2.2 Deduction Rules.

A sequent is a pair of formulae Φ, Ψ and an stype R which is simultaneously a domain for both formulae.

We write :

$$\Phi \Longrightarrow_R \Psi$$

The axioms and deduction rules of intuitionistic logic are obtained directly from the universal properties C1 to C11 described in section §1.

We shall write them now explicitely. Each A1 to A11 corresponding to the respective C1 to C11

A1) $\Phi \Longrightarrow_R \Phi$

A2) $\Phi \Longrightarrow_R \Psi$, $\Psi \Longrightarrow_R \Gamma$, then $\Phi \Longrightarrow_R \Gamma$

A3) FALSE $\Longrightarrow_R \Phi$

A4) $\Phi \Longrightarrow_R$ TRUE

A5) $$\frac{\Phi \Longrightarrow_R \Gamma \ , \ \Psi \Longrightarrow_R \Gamma}{\Phi \vee \Psi \Longrightarrow_R \Gamma}$$

A6) $$\frac{\Gamma \Longrightarrow_R \Phi \ , \ \Gamma \Longrightarrow_R \Psi}{\Gamma \Longrightarrow_R \Phi \wedge \Psi}$$

A7) $$\frac{\Gamma \wedge \Phi \Longrightarrow_R \Psi}{\Gamma \Longrightarrow_R \Phi \rightarrow \Psi} \ , \ \frac{\Gamma \wedge \Phi \Longrightarrow_R \text{FALSE}}{\Gamma \Longrightarrow_R \neg \Phi}$$

A8) $$\Phi \Longrightarrow_S \Psi \ , \text{ then } \Phi(t|x) \Longrightarrow_R \Psi(t|x) \ .$$

Where : x is a variable and t a term of the same type, and $\Phi(t|x)$, $\Psi(t|x)$ indicate the substitution of t in all the free occurrences of x (we assume that t does not have any free variable that becomes bounded after substitution).

Notice that usually R will have the types of a domain of t in place of the type of the variable x .

Notice that this rule has as a particular case the following :

$$\Phi \Longrightarrow_S \Psi \ , \text{ then } \Phi \Longrightarrow_R \Psi$$

each time that R contains all the types in S .

A9) $$\frac{\Phi \Longrightarrow_{(R,H)} \Gamma}{(\exists x)_R \Phi \Longrightarrow_H \Gamma}$$

A10) $$\frac{\Gamma \Longrightarrow_{(R,H)} \Phi}{\Gamma \Longrightarrow_H (\forall x)_R \Phi}$$

Where x is not free in Γ and R is the type of x .
Notice that this corresponds to the particular case in C9 and C10 where the arrow $R \xrightarrow{f} H$ is the projection $R \times H \xrightarrow{\pi} H$ of the product.

A11) $\Phi \Longrightarrow_S x \in \{x \mid \Phi\}_R$

Where x is a svariable of stype R.

Finally, there are three rules atached to the "=" symbol between variables.

A12) $\text{TRUE} \Longrightarrow_R x = x$

A13) $\Phi \wedge (x = y) \Longrightarrow_R \Phi(y|x)$

A14) $(\forall x)_R(x \in P \longleftrightarrow x \in Q) \Longrightarrow_S P = Q$

Here x is a variable of type R, P and Q are variables of type $\Omega(R)$ (and, of course, S contains $\Omega(R)$).

§3 INTERPRETATIONS IN TOPOI.

3.1 Let $\mathcal{E}$ be an elementary topos (cf. §1) and $\mathcal{L}$ be a language (cf. §2). The notion of an interpretation of $\mathcal{L}$ dans $\mathcal{E}$ follows the same stepts that the concept of a language $\mathcal{L}$. Each I1 to I11 below corresponding to the respective L1 to L11.

Basic Data :

I1) i) To each type R it is associated an object R in $\mathcal{E}$. Notice that we abuse the notation and write the same letter for a type and its associated object. In order to simplify the notation, we make the following convention :

if $R = (R_1, R_2, \ldots, R_n)$ is an stype, then we write R for the product$R_1 \times R_2 \times \ldots R_n$ in $\mathcal{E}$.

In this way, we have also an object of the topos associated to each stype. Notice that the terminal object 1 is associated to the empty stype.

ii) The assignment in i) is such that for any stype R, the object

associated to the type $\Omega(R)$ is the exponential $\Omega(R) = \Omega^R$ in $\mathcal{E}$. (see C11 in §1.3).

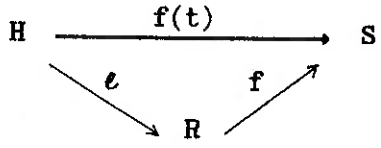
I2) To each predicate symbol A of domain R, it is associated a subobject $A \rightarrowtail R$ of R in $\mathcal{E}$.

I3) To each functional symbol f of domain R and type S, it is associated an arrow $R \xrightarrow{f} S$ in $\mathcal{E}$.

Terms : To the terms of $\mathcal{L}$ they will correspond arrows in $\mathcal{E}$. More precisely, to each term t of type S, and each domain H of t (cf. Définition 2.1), it is associated an arrow $H \xrightarrow{t} S$ in $\mathcal{E}$, denoted with the same letter. Recursively :

I4) If t is a variable of type S, we associate the corresponding projection (notice that a domain of a variable is any stype that contains a distinguished copy of its type).

I5) If f is a functional symbol of domain R and type S, and ℓ is an sterm of stype R, we associate the composite :



(notice that since H is a domain of t, it is simultaneously a domain of each term in the sterm ℓ. Then, the arrow ℓ in the diagram is determined by the universal property of the product and the arrows associated to each term in ℓ).

I6) If Φ is a formula and x is an svariable of stype R, we

ssociate the arrow that classifies the extension of Φ associated to the stype (R,H) (cf. C11 in §1.3)

$$\frac{[(x,y) \mid \Phi]_{(R,H)} \longrightarrow R \times H}{\{x|\Phi\}_R : H \longrightarrow \Omega(R)}$$

Here y is any appropriate svariable of stype H , for the meaning of [|] see below. (notice that since H is a domain of $\{x|\Phi\}_R$, (R,H) is a domain of Φ).

Formulae To the formulae of $\mathscr{L}$ they will correspond objects in $\mathcal{E}$. More precisely, to each formula Φ and each domain H of Φ (cf. Definition 2.1), it is associated a subobject of H , denoted $[x|\Phi]_H$, (here x is any svariable of stype H such that all its variables are different). This subobject is called the "extension" of Φ associated to H . Recursively :

I7) If t is an sterm of stype R and A is a predicate symbol of domain R , we associate the pull-back (inverse image) (cf. §1.2)

$$\begin{array}{ccc} [x|A(t)]_H & \longrightarrow & A \\ \downarrow & & \downarrow \\ H & \xrightarrow{t} & R \end{array}$$

(notice that since H is a domain of A(t) , it is a domain of t).

I8) If t and ℓ are terms of type S , we associate the pull-back (inverse image) :

$$\begin{array}{ccc} [x|t=\ell)]_H & \longrightarrow & S \\ \downarrow & & \downarrow \Delta S \\ H & \xrightarrow{(t,\ell)} & S\times S \end{array}$$

Where ΔS indicates the diagonal of SxS (notice that since H is a domain of Φ , it is simultaneously a domain of t and of ℓ).

I9) If P is a term of type $\Omega(R)$ and t is an sterm of stype R, we associate the pull-back (inverse image) :

$$\begin{array}{ccc} [x|t\in P]_H & \longrightarrow & \in_R \\ \downarrow & & \downarrow \\ H & \xrightarrow{(t,P)} & R\times\Omega(R) \end{array}$$

Where $\in_R$ is the generic (or membership relation in R (cf. C11 in §1.3). (notice that since H is a domain of Φ, it is simultaneously a domain of t and of P).

I10) This is clear. See L10 in §2.1 and C3 to C7 in §1.1. We associate :

$$[x|\mathrm{FALSE}]_H = 0_H$$

$$[x|\mathrm{TRUE}]_H = 1_H$$

$$[x|\Phi \vee \Psi]_H = [x|\Phi]_H \vee [x|\Psi]_H \ .$$

$$[x|\Phi \wedge \Psi]_H = [x|\Phi]_H \wedge [x|\Psi]_H \ .$$

$$[x|\Phi \longrightarrow \Psi]_H = [x|\Phi]_H \longrightarrow [x|\Psi]_H \ .$$

$$[x|\ \Phi]_H = \ [x|\Phi]_H \ .$$

(notice that H is simultaneously a domain of Φ and of Ψ).

I11) See C9, C10 and the definition of product in §1.1. If x is a variable of type R and Φ is a formula, we associate :

$$[y|(\exists x)_R\ \Phi]_H = \exists_\pi [(x,y)|\Phi]_{(R,H)}$$

$$[y|(\forall x)_R\ \Phi]_H = \forall_\pi [(x,y)|\Phi]_{(R,H)}$$

Where y is any appropirate svariable of stype H, and π is the projection $R \times H \xrightarrow{\pi} H$ in $\mathcal{E}$. (notice that since H is a domain of the quantified formula, (R,H) is a domain of the unquantified formula).

This finishes the description of the semantics of the language $\mathcal{L}$ in a topos $\mathcal{E}$.

Theorem 2. A sequent $\Phi \Longrightarrow_R \Psi$ of the language $\mathcal{L}$ follows from the axioms and rules A1 to A14 if and only if given any interpretation in any topos $\mathcal{E}$, $[x|\Phi]_R \subset [x|\Psi]_R$ as subobjects of R in $\mathcal{E}$.

The adequacy of the axioms and rules A1 to A14 is not a big surprise. As for the completness, a logician will notice that the methods of section §3 will provide a construction of the free topos on the language $\mathcal{L}$, automatically furnished with an interpretation. (notice Proposition 1 in §1.4). For a proof of all this see [1].

Conclusion. We see that Lawvere solved the contradiction between syntax and semantics. Conceptualizing the first, he made out of the two only one.

As a final comment, we mention that Lawvere also defined a natural number object $\mathbb{N}$ by means of a universal propety C). This property governs the beahavior of an intuitionistic type for natural number variables, which can then be added to the language $\mathcal{L}$, together whith the corresponding L) stepts in the formation of terms and the corresponding A) rules or axioms. A language $\mathcal{L}$ enriched in this way corresponds to the mathematical concept of "Elementary Topos with Natural Number Object".

Also, it is clear that any Topos $\mathcal{E}$ has an associated language $\mathcal{L}$ which interprets in itself. In this way we do "internal mathematics" in $\mathcal{E}$ as if $\mathcal{E}$ where the category of Sets. But using naive intuitionistic reasoning.

A word about Kripky-Joyal Semantics. Given an object R in a topos $\mathcal{E}$, a subobject $A \rightarrowtail R$ is characterized if we know which "sections" $X \xrightarrow{r} R$

factorize $(X \longrightarrow A \rightarrowtail R) = (X \longrightarrow R)$, where X ranges over the objects of $\mathcal{E}$. The rules that charaterize the extensions :

$$\text{Given } X \xrightarrow{r} R \text{ , } \frac{X \xrightarrow{r} [x|\Phi]_R}{\text{such and such happens}}$$

for the eight formulae in I10 and I11 are called "Kripky-Joyal Semantics. This was discovered by A. Joyal, which generalized Kripky Semantics to general Topoi.

Je veux remercier Mme Orieux, de l'UA 753, CNRS, avec qui ce fut un grand plaisir de travailler pour la mise en page de ce manuscrit.

REFERENCES

[1] A. Boileau, A. Joyal ; "La logique des topos" ; J. Symb. Log., vol. 46, nr.1, (1981).

[2] O. Bruno "Internal Mathematics in Toposes". Trabajos de Matematica 70, I.A.M., c.c. 1727, 1000 Buenos Aires (1984).

Additional REFERENCES (among many)

M. Coste : Langage interne d'un topos (1972).

Logique du premier ordre dans les topos élémentaires (1973).

Logique d'ordre supérieur dans les topos élémentaires (1974).

dans Séminaire Bénabou - Université Paris Nord.

On trace forms of algebraic function fields

Alexander Prestel *)

1. Introduction and results

Let L/K be a finite separable field extension. The trace form of L/K is the following symmetric bilinear form over K

$$L \times L \to K \quad , \quad (x,y) \to Tr_{L/K}(x \cdot y) \quad .$$

This form will be denoted by $T_K(L,1)$. If P is an ordering of K, it is well-known that

$$sgn_P T_K(L,1) = \#\{\text{extensions of } P \text{ to } L\} \quad .$$

Thus every trace form has totally positive signature over K, i.e.

$$sgn_P T_K(L,1) \geq 0 \quad \text{for all} \quad P \in X_K \quad .$$

As usual X_K denotes the set of all orderings of K. Therefore every (regular) quadratic form ρ over K which is Witt equivalent to some trace form over K has totally positive signature.

In [C-P] the question has been raised whether for algebraic number fields K the converse also holds, i.e. whether in this case every regular quadratic form ρ which has totally positive signature over K is Witt equivalent to a trace form $T_K(L,1)$ for some finite extension L/K. Conner and Perlis succeeded in proving this in case $K = \mathbb{Q}$. In a recent paper W. Scharlau [Sch$_1$]

*) The result of this paper has been announced at the Conference on Quadratic Forms and Real Algebraic Geometry, Corvallis, July 1986, and will appear in "Rocky Mountain Journal".

gave a positive answer for all number fields, reducing the general case to the 1-dimensional case already solved in [E-H-P]. In the 1-dimensional case $\rho = \langle\beta\rangle$, the condition of totally positive signature just means that β is a sum of squares in K.

The main result of this paper is

MAIN THEOREM Let K be an algebraic function field in one variable over a real closed field R. Then every regular quadratic form ρ which has totally positive signature over K is Witt equivalent to some trace form $T_K(L,1)$.

The strategy of the proof is the same as in [Sch$_1$]: reducing first the general case to the 1-dimensional case, and then proving the 1-dimensional case.

Scharlau's reduction step used the two facts that algebraic number fields are hilbertian (i.e. satisfy Hilbert's Irreducibility Theorem) and have only a finite number of orderings. While the first fact is still true for algebraic function fields, the second no longer holds (except for the case $X_K = \emptyset$). A substitute for this second fact will be that every algebraic function field in one variable over a real closed field R (as well as every algebraic number field) allows Effective Diagonalization (ED) of quadratic forms (see [W] and [P-W]), i.e. for every quadratic form ρ over K there is a diagonalization

$$\rho \simeq \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

such that for each $P \in X_K$ we have

$$d_{i+1} \in P \Rightarrow d_i \in P .$$

This means that - independent of P - the positive elements d_i always are on top of the negative ones.

The fist theorem we prove corresponds to Scharlau's reduction step.

THEOREM 1 Let K be a hilbertian field of characteristic zero*) satisfying ED . Then every regular quadratic form ρ having totally positive signature over K is isometric to a scaled trace form $T_K(L,\beta)$ for some finite extension L/K with β being a sum of squares in $L^\times$.

A scaled trace form $T_K(L,\beta)$ is given by the symmetric bilinear form over K

$$L\times L \to K \ , \ (x,y) \to Tr_{L/K}(\beta xy)$$

where L/K is a finite (separable) extension and $\beta \in L$.
It is easy to prove (see e.g. [Sch_2],Ch.3, Theorem 4.5) that for every $P \in X_K$

$$\begin{aligned} sgn_P T_K(L,\beta) = &\ \{\text{extensions } P' \text{ of } P \text{ to } L \text{ s.t. } \beta \in P'\} \\ - &\ \{\text{extensions } P' \text{ of } P \text{ to } L \text{ s.t. } -\beta \in P'\} \end{aligned}$$

Thus as a consequence we have

PROPOSITION Let $T_K(L,\beta)$ be a scaled trace form with $\beta \in L$. Then β is a sum of squares in L if and only if for all $P \in X_K$

$$sgn_P T_K(L,\beta) = \#\{\text{extensions of } P \text{ to } L\}.$$

*) Since the fields in the Main Theorem are of characteristic zero, we will restrict ourselves to this case.

The second theorem we prove will correspond to Corollary 1 of [E-H-P]. We will say that a field L satisfies the Norm Theorem (NT) of [E-H-P] if for every sum of squares $\beta \in L$ which is not a square in L, there is a natural number m such that $-m$ is a Norm of $L(\sqrt{\beta})$ over L, i.e. the form $\langle 1,-\beta,m\rangle$ is isotropic over L. By a theorem of Witt (see [Wi] and [E-L-P]) every totally indefinite quadratic form of dimension ≥ 3 over an algebraic function field L in one variable over a real closed field is isotropic. Thus by taking e.g. $m = 1$, every such function field L satisfies the Norm Theorem.

THEOREM 2 Let L be a hilbertian field of characteristic 0 satisfying NT. Then for every sum of squares $\beta \in L^{\times}$ the 1-dimensional form $\langle\beta\rangle$ is Witt equivalent to a trace form $T_L(F,1)$ over L for some extension F/L obtained by an irreducible linear trinomial $X^{m+1}+aX+b \in L[X]$ of odd degree.

From these two theorems the Main Theorem follows at once:

Let K be an algebraic function field in one variable over a real closed field R and let ρ be a regular quadratic form which has totally positive signature over K. Since K is hilbertian and satisfies ED, by Theorem 1 we find a finite extension L/K and a sum of squares $\beta \in L^{\times}$ such that

$$\rho \simeq T_K(L,\beta) .$$

Since L is again an algebraic function field in one variable over R, it is hilbertian and satisfies NT. Thus applying Theorem 2 to L and β, we obtain a finite extension F/L such that

$$\langle\beta\rangle \sim T_L(F,1) \text{ in } W(L) .$$

Using the transitivity of the trace and Corollary VII.1.5 of [L], we finally get

$$\rho \sim T_K(F,1) \text{ in } W(K) .$$

At the end of the paper we will investigate the property NT for function fields a little closer.

Concerning notations and basic results about quadratic forms we refer the reader to [L].

2. Proof of Theorem 1

Since the case $X_K = \emptyset$ is already covered by Scharlau's paper, we concentrate on the case $X_K \neq \emptyset$.

Let K be hilbertian and satisfy ED . Given a regular quadratic form ρ of dimension n over K , we can then assume that ρ is represented by a diagonal matrix

$$D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \quad \text{with } d_i \in K^*$$

such that for all $P \in X_K$

$$d_{i+1} \in P \Rightarrow d_i \in P .$$

If we assume $\operatorname{sgn}_P \rho \geq 0$ for all $P \in X_K$, we know that each d_i with $i \leq \left[\frac{n+1}{2}\right]$ is a sum of squares in K . As usual $[\frac{m}{2}]$ denotes the integral part of $\frac{m}{2}$. Thus after rearranging the

elements of the diagonal, we can assume that all d_i with odd index

$$d_1, d_3, d_5, \ldots\ldots$$

are sums of squares in K. Multiplying by suitable squares, we may in addition assume that

$$d_{2i-1}\, d_{2i} * d_{2j-1}\, d_{2j}$$

for all $1 \leq i < j \leq \left[\frac{n+1}{2}\right]$. We require this condition also for the case $j = \left[\frac{n+1}{2}\right]$ and n odd after setting $d_{n+1} := d_n$.

Using now Scharlau's argument (see [Sch_1]) it suffices to find a symmetric matrix $B \in K^{(n,n)}$ such that

(i) the characteristic polynomial $f(X)$ of DB is irreducible over K,

(ii) $f(X)$ has exactly $\operatorname{sgn}_P \rho$ roots in the real closure $(\overline{K,P})$ of K with respect to P.

As it is explained in [Sch_1], by (i) there exists a β in

$$L = K[X]/(f)$$

such that

$$\rho = T_K(L, \beta) .$$

By (ii) the number of extensions of P to L is

$$\operatorname{sgn}_P T_K(L, \beta) .$$

Thus by Proposition, β is a sum of squares in L.

In order to find such a matrix B, let us start with the symmetric matrix

$$B_o = \begin{pmatrix} 01 & & & \\ 10 & & & \\ & 01 & & \\ & 10 & & 0 \\ & & \ddots & \\ 0 & & & \ddots \end{pmatrix} = (b_{ij})$$

The last square in the diagonal of B_o is the 2-by-2 matrix $\left(\begin{smallmatrix} 01 \\ 10 \end{smallmatrix}\right)$ if n is even, and the 1-by-1 matrix (1) if n is odd.

Forming the characteristic polynomial

$$f_o(X) = \det_n(DB_o - XI_n)$$

we find that

$$f_o(X) = \prod_{1 \le i \le [\frac{n}{2}]} (d_{2i-1}d_{2i} - X^2) \cdot l(X)$$

where $l(X) = 1$ if n is even and $l(X) = d_n - X$ if n is odd. By our choice of the $d_i \in K$ we see immediately that

$$\operatorname{sgn}_P \rho = \#\{\text{zeros of } f_o \text{ in } (\overline{K,P})\}$$

for each $P \in X_K$. Thus f_o satisfies (ii).

Since for a fixed ordering P all the zeros of f_o in $(\overline{K,P})$ are simple, any matrix B_P which has its elements very close to that of B_o in $(\overline{K,P})$ yields a polynomial

$$f_P = \det_n (DB_P - XI_n)$$

which has the same number of zeros in $(\overline{K,P})$ as f_o. Actually, for a fixed $P \in X_K$ we find some $a_P \in P^\times$ such that for all $\varepsilon_{ij} \in (\overline{K,P})$ with

$$0 \le_P \varepsilon_{ij} \le_P \frac{1}{a_P^2} \quad \text{and} \quad \varepsilon_{ij} = \varepsilon_{ji}$$

the symmetric matrix

$$B_{P,\varepsilon} = B_o + \varepsilon = (b_{ij} + \varepsilon_{ij})$$

yields a polynomial

$$f_{P,\varepsilon} = \det_n(DB_{P,\varepsilon} - XI_n)$$

having the same number of zeros in $(\overline{K,P})$ as f_o. Thus in particular

$$\operatorname{sgn}_P \rho = \#\{\text{zeros of } f_{P,\varepsilon} \text{ in } (\overline{K,P})\}.$$

As we will see there are always choices of $\varepsilon_{ij} \in K$ which make $f_{P,\varepsilon}$ irreducible over K. This gives a positive solution to (i). But now (ii) can be guaranteed only for the ordering P which we fixed. Thus our problem is to find some $\varepsilon_{ij} \in K$ which do the job simultaneously for all $P \in X_K$. This can be achieved in the following way.

For every $P \in X_K$ we choose $a_P \in K^x$ as above and consider the subset U_P of X_K consisting of those $Q \in X_K$ such that

$$\operatorname{sgn}_Q \rho = \#\{\text{zeros of } f_{Q,\varepsilon} \text{ in } (\overline{K,Q})\}$$

for all $\varepsilon_{ij} \in (\overline{K,Q})$ satisfying

$$0 <_Q \varepsilon_{ij} <_Q \frac{1}{a_P^2} \quad \text{and} \quad \varepsilon_{ij} = \varepsilon_{ji}.$$

Clearly $P \in U_P$. As it is well-known X_K is a compact space with respect to the topology generated by the subsets

$$H(c) = \{P \in X_K \mid c \in P\} \quad , \quad c \in K.$$

The sets U_P are open in this topology. This is a consequence of Tarski's Theorem on the Elimination of Quantifiers over real closed fields. In fact, it is not difficult to write down a formula $\varphi(x_1,\ldots,x_n,y)$ in the language of ordered fields such that

$$U_P = \{Q \in X_K \mid (\overline{K,Q}) \text{ satisfies } \varphi(d_1,\ldots,d_n,a_P)\}.$$

By Tarski's Theorem there are polynomials

$$p_{ij},q_i \in \mathbb{Z}[X_1,\ldots,X_n,Y]$$

such that $\varphi(d_1,\ldots,d_n,a_P)$ is equivalent to

$$\bigvee_{i=1}^{r} (q_i(\bar{d},a_P) = 0 \wedge \bigwedge_{j=1}^{s} p_{ij}(\bar{d},a_P) > 0)$$

in all real closures $(\overline{K,Q})$. Assuming w.l.o.g. that $q_i(\bar{d},a_P) = 0$ for all i, we thus have

$$U_P = \bigcup_{i=1}^{r} \bigcap_{j=1}^{s} H(p_{ij}(\bar{d},a_P)) .$$

Hence U_P is open in X_K. By compactness we can therefore find a finite cover

$$U_{P_1} \cup \ldots \cup U_{P_m}$$

of X_K. If we now let

$$a = a_{P_1}^2 + \ldots + a_{P_m}^2$$

then the choice

$$\varepsilon_{ij} = \frac{1}{a+y_{ij}^2} \quad \text{with} \quad y_{ij} = y_{ji} \in K$$

obviously satisfies

$$0 \leq_Q \varepsilon_{ij} \leq_Q \frac{1}{a_{P_\nu}^2} \quad \text{and} \quad \varepsilon_{ij} = \varepsilon_{ji}$$

for all $Q \in U_P$ and all $1 \leq \nu \leq m$. Thus, if we set

$$B_Y = B_o + \left(\frac{1}{a+Y_{ij}^2}\right) \quad \text{with} \quad Y_{ij} = Y_{ji}$$

and

$$f_Y = \det_n (DB_Y - XI_n) ,$$

by the definition of U_P we obtain

$$\operatorname{sgn}_Q P = \#\{\text{zeros of } f_y \text{ in } (\overline{K,Q})\}$$

for all substitutions $y_{ij} \in K$ and all $Q \in X_K$. Thus f_y satisfies (ii). In addition we can choose $y_{ij} \in K$ such that f_y is also irreducible, thus also satisfying (i). In fact,

$$f_Y = \frac{g(X,\bar{Y}_{ij})}{\prod\limits_{1\leq i,j\leq n} (a+Y_{ij}^2)} \quad \text{with} \quad g \in K[X,\bar{Y}_{ij}]$$

As we will show in the next section, g is irreducible over K. Thus by the assumption on K being hilbertian we find $y_{ij} \in K$ such that $g(X,\bar{y}_{ij}) \in K[X]$ is irreducible. This finishes the proof of Theorem 1.

Looking carefully at the proof of Theorem 1 we can see that after having used ED the rest of the proof actually yields the following

ADDITION LEMMA Let K be a hilbertian field of characteristic zero. If $\rho_i \simeq T_K(L_i,\beta_i)$ for some extensions L_i/K and some sums of squares β_i of L_i (for $i=1,2$), then $\rho_1 \perp \rho_2 \simeq T_K(L,\beta)$ for some extension L/K and some sum of squares β of L.

In fact, by Scharlau's argument we find symmetric matrices B_i such that (i) and (ii) holds for D_iB_i where D_i are symmetric matrices representing ρ_i (for $i=1,2$). Considering now the matrix

$$B_o = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}$$

we can follow the proof of Theorem 1 in order to obtain the Addition Lemma.

As a consequence we get

COROLLARY Every closed and open subset of the order space X_K of a hilbertian field K is the image under the restriction map of some finite extension L/K.

Proof: Let $A \subset X_K$ be open and closed. Then

$$A = \bigcup_{i=1}^{n} \bigcap_{j=1}^{m_i} H(a_{ij}) \quad , \quad a_{ij} \in K^x .$$

Clearly, the sets $B_i = \bigcap_{j=1}^{m_i} H(a_{ij})$ are the images under the restriction map for the fields

$$L_i = K(\sqrt{a_{i1}},\ldots,\sqrt{a_{im_i}})$$

for $1 \leq i \leq n$. Since the trace forms $\rho_i = T_K(L_i,1)$ have non-vanishing signature exactly on B_i, the corollary follows from the Addition Lemma.

QED

This corollary generalizes the corresponding result of Andradas and Gamboa for real function fields ([A-G], Theorem 4.1).

3. An irreducibility result

The aim of this section is to prove the following

LEMMA *Assume that* K *is a formally real field. For* $1 \le i, j \le n$ *let* $a_{ij} \in K$ *and* $c_{ij} \in K^\times$. *Then for any sum of squares* $a \in K^\times$ *the characteristic polynomial* f_n *of the matrix*

$$A_n = \left(a_{ij} + \frac{c_{ij}}{a+Y_{ij}^2}\right) \quad \text{with} \quad Y_{ij} = Y_{ji}$$

is a quotient of an irreducible polynomial $g_n \in K[X, \bar{Y}_{ij}]$ *and* $\prod_{1 \le i,j \le n} (a+Y_{ij}^2)$.

This lemma applied to the case

$$a_{ij} = d_i b_{ij} \quad \text{and} \quad c_{ij} = d_i$$

yields the result used in the proof of Theorem 1 .

Proof: We proceed by induction on n . For the use $n = 1$ one obtains

$$g_1 = a_{11}(a+Y_{11}^2) + c_{11} - X(a+Y_{11}^2) .$$

As a polynomial in X this is clearly irreducible over $K[Y_{11}]$ since $c_{11} \neq 0$.

Now let us assume by induction that $n \ge 2$ and for all $m < n$ the polynomial g_m is irreducible and of degree m in X .

Writing for a moment Z_{ij} for $(a+Y_{ij}^2)^{-1}$, we obtain

$$f_n = \det_n \begin{pmatrix} a_{11}+c_{11}Z_{11}-X & a_{12}+c_{12}Z_{12} & \cdots \\ a_{21}+c_{21}Z_{12} & & \\ \vdots & & \end{pmatrix}$$

$$= (a_{11}+c_{11}Z_{11}-X) f_{n-1} + \sum_{1 \neq i,j} (a_{1i}+c_{1i}Z_{1i})(a_{j1}+c_{j1}Z_{1j}) f_{n-2}^{(i,j)}$$

where $f_{n-2}^{(i,j)}$ is (up to sign) the $\det_{n-2}$ of the matrix obtained by cancelling 1^{st} and i^{th} column and 1^{st} and j^{th} row of $A_n - XI_n$. By induction hypothesis we have:

$$f_{n-1} = \frac{g_{n-1}}{\prod_{1<i,j\leq n} (a+Y_{ij}^2)}$$

with g_{n-1} irreducible and of degree $n-1$ in X,

$$f_{n-2}^{(\nu,\nu)} = \frac{g_{n-2}^{(\nu)}}{\prod_{i,j\neq 1,\nu} (a+Y_{ij}^2)}$$

with $g_{n-2}^{(\nu)}$ irreducible and of degree $n-2$ in X.
Clearly, in the case $n=2$ we let $f_o^{(2,2)} = g_o^{(2,2)} = -1$.
Thus we obtain

$$g_n = (c_{11}+(a_{11}-X)(a+Y_{11}^2))\delta + (a+Y_{11}^2)\gamma$$

with

$$\delta = g_{n-1}(a+Y_{12}^2)^2 \cdot \ldots \cdot (a+Y_{1n}^2)^2$$

$$\gamma = \sum_{1\neq i,j} h^{(i,j)} \prod_{\nu\neq 1,i} (a+Y_{1\nu}^2) \prod_{\mu\neq 1,j} (a+Y_{1\mu}^2)$$

for suitable polynomials $h^{(i,j)} \in K[X, \bar{Y}_{ij}]_{i,j\neq 1}$.
In particular we find

$$h^{(i,i)} = (c_{1i}+a_{1i}(a+Y_{1i}^2))(c_{i1}+a_{i1}(a+Y_{1i}^2))g_{n-2}^{(i)}(a+Y_{ii}^2) \cdot \prod_{j\neq 1,i} (a+Y_{ij}^2)^2$$

As a polynomial in Y_{11} we have

$$g_n = \alpha Y_{11}^2 + \beta \quad \text{with}$$

$\alpha = \gamma + a_{11}\delta - X\delta$ and $\beta = a\gamma + c_{11}\delta + aa_{11}\delta - aX\delta$.

If α and β would have a common divisor, also δ and γ would have one. If $(a+Y_{1i}^2)$ for some $1 < i$ would divide γ, then it would also divide $h^{(i,i)}$ and hence c_{1i} or c_{i1} which is impossible. Since g_{n-1} is irreducible and

$$\deg_X g_{n-1} = n-1 > \deg_X \gamma$$

there could only be a common divisor of δ and γ, if $\gamma = 0$. But this would yield

$$0 = \sum_{1 \neq i,j} (a_{1i}+c_{1i}Z_{1i})(a_{j1}+c_{j1}Z_{1j}) f_{n-2}^{(i,j)}$$

Observing that

$$\deg_X f_{n-2}^{(i,j)} < \deg_X f_{n-2}^{(\nu,\nu)} = n-2$$

for $i \neq j$ one easily sees that the highest coefficients of X cannot cancel.

If g_n would be reducible in Y_{11}, then the highest coefficients of α and β in X would differ by a negative square from the field

$$\mathrm{Quot}(K[\bar{Y}_{ij}]_{(i,j)\neq(1,1)}) .$$

This is impossible since they differ by a which is a non-zero sum of squares in K. Thus g_n is irreducible.

4. Proof of Theorem 2

Let $f \in L[X]$ be an irreducible linear trinomial

$$f(X) = X^{m+1} + aX + b$$

of odd degree. The trace form $T_L(F,1)$ of the extension $F = L[X]/(f)$ turns out to be (for a computation see [C-P] or [S]):

$$T_L(F,1) \sim \langle 1, m, -md \rangle \text{ in } W(L)$$

where

$$d \equiv m^m a^{m+1} + (m+1)^{m+1} b^m \bmod L^2 .$$

If we would know in addition that

$$d \equiv \beta \bmod L^2$$

and that $-m$ is a norm from $L(\sqrt{\beta})$ over L (assuming that β is not a square in L), then the form $\langle 1, -\beta, m \rangle$ would be isotropic. Hence the 2-fold Pfister form $\langle 1, -\beta, m, -\beta m \rangle$ would be zero in $W(L)$. Thus we would get

$$T_L(F,1) \sim \langle \beta \rangle \text{ in } W(L).$$

We are therefore looking for such a trinomial.

Let us first assume that β is not a square in L, since otherwise we may take $F = L$. Next let us assume w.l.o.g. that $-m$ is a norm from $L(\sqrt{\beta})$ and m is even. Now let

$$r = \frac{(m+1)^{m+1}}{m^m} \quad , \quad \beta_1 = \frac{\beta}{m^m} .$$

The polynomial

$$f(X,Y) = X^{m+1} + (\beta_1 Y^2 - r)X + (\beta_1 Y^2 - r)$$

is irreducible in $K[X,Y]$. This follows at once by Eisenstein's Criterion if we consider f as a polynomial in X over $L[Y]$. Since L is hilbertian, we find $y \in L^*$ such that

$$f(X) = X^{m+1} + (\beta_1 y^2 - r)X + (\beta_1 y^2 - r)$$

is irreducible in $K[X]$.

If we now set

$$a = b = \beta_1 y^2 - r$$

we have found the desired linear trinomial of odd degree. In fact, we have (observing that m is even) mod L^2:

$$\begin{aligned} d &\equiv m^m a^{m+1} + (m+1)^{m+1} b^m \\ &\equiv m^m a + (m+1)^{m+1} \\ &\equiv \beta y^2 \\ &\equiv \beta \end{aligned}$$

This finishes the proof of Theorem 2 .

It may be interesting to observe that the converse of Theorem 2 also holds, i.e. assuming that in L every sum of squares β is Witt equivalent to a trace form $T_L(F,1)$ for some F obtained by a linear trinomial $X^{m+1} + aX + b$ with m even, then L satisfies NT .

In fact, by this assumption we have

$$\langle \beta \rangle \sim \langle 1, m, -md \rangle \quad \text{in } W(L)$$

with d as above. From this Witt equivalence we obtain the isometry

$$\langle \beta,1,-1\rangle \simeq \langle 1,m,-md\rangle$$

which clearly implies

$$\beta \equiv d \bmod L^2$$

In particular we obtain that the 2-fold Pfister form $\langle 1,m;-m\beta,-\beta\rangle$ is zero in $W(L)$. But this implies that $\langle 1,m,-\beta\rangle$ is isotropic. Thus in case β is not a square in L, this tells us that $-m$ is a norm from $L(\sqrt{\beta})$.

5. More about NT

The remark at the end of the last section shows that NT is in some sense essential for the result of the Main Theorem. It will be thus interesting to ask in general which function fields are satisfying this property. For rational function fields we can give a complete answer.

THEOREM *Let k be a formally real field. Then the rational function field $k(t)$ satisfies NT if and only if k is hereditarily pythagorean, i.e. k and all its finite formally real extensions are pythagorean.*

Proof: In [B],Ch.III, Theorem 4, it is shown that if k is hereditarily pythagorean, in $k(t)$ every sum of squares β is equal to a sum of 2 squares. Thus the form $\langle 1,-\beta,1\rangle$ is isotropic over $k(t)$.

Conversely, let us assume that there is a finite formally real extension k_1 of k which is not pythagorean. Then there is some $\alpha \in k_1$ such that

$$\gamma = 1 + \alpha^2$$

is not a square in k_1. We consider the extensions

$$k_2 = k_1(\sqrt{\gamma}) \quad \text{and} \quad k_3 = k_2(\sqrt{\sqrt{\gamma}-\gamma}\,).$$

Observing that

$$(\sqrt{\gamma}-\gamma\,)(-\sqrt{\gamma}-\gamma\,) = \gamma^2-\gamma = \gamma(\gamma-1) = \gamma\alpha^2$$

we see that k_3/k_1 is cyclic with the automorphism

$$\sigma(\sqrt{\sqrt{\gamma}-\gamma}\,) = \sqrt{-\sqrt{\gamma}-\gamma}$$

generating the Galois group. The unique extension of k_1 of degree 2 in k_3 is k_2. Since k_2 is formally real, we find that for every $m \in \mathbb{N}$

$$\sqrt{-m} \notin k_3 .$$

On the other hand k_3 is not formally real. In fact, $\gamma > 1$ implies $\gamma > \sqrt{\gamma}$. Denoting by $f(t)$ the irreducible polynomial of some generator of k_3 over k, we thus find polynomials $f_1,\ldots,f_r \in k[t]$ such that

$$-1 \equiv f_1^2 + \ldots + f_r^2 \mod f$$

and

$$\deg f_i < \deg f .$$

If we now assume that $k(t)$ satisfies NT, we could find some $m \in \mathbb{N}$ and $g_1,g_2,h \in k[t]$ such that

$$-mh^2 = g_1^2 - (1+\sum_{i=1}^{r} f_i^2)g_2^2 \quad .$$

Since f divides $1+\Sigma f_i^2$, we may assume (after cancelling) that f does not divide h or g_1. Thus computing mod f we would get that $-m$ is a square in k_3. This contradiction proves the theorem.

This theorem in particular shows that the field $\mathbb{Q}(t)$ does not satisfy Theorem 2. More precisely, considering the fields $k = k_1 = \mathbb{Q}$, $k_2(\sqrt{2})$, $k_3 = \mathbb{Q}(\sqrt{\sqrt{2}-2})$ we see that $f = t^4+4t^2+2$ and

$$-1 \equiv (t^2)^2 + (2t)^2 + 1^2 \mod f \quad .$$

Thus we find that the sum of squares

$$\beta = t^4+4t^2+1 \in \mathbb{Q}(t)$$

is not Witt equivalent to any trace form of a finite extension of $\mathbb{Q}(t)$ given by some linear trinomial of odd degree.

According to [E-L-P] and [W] a formally real function field in one variable over a field k satisfies ED if and only if k is hereditarily euclidean, i.e. k and all its finite formally real extensions are pythagorean and have just one ordering. Thus the main theorem already holds for algebraic function fields in one variable over a hereditarily euclidean field, since also Witt's Theorem on totally indefinite quadratic forms of dimension ≥ 3 holds for such function fields (see [E-L-P])

References

[A-G] C. Andradas-J.M.Gamboa: On projections of real algebraic varieties. Pacific J.Math.121(1986),281-291

[B] E. Becker: Hereditarily pythagorean fields and orderings of higher level. Monografias de Matemática 29. IMPA, Rio de Janeiro 1978.

[C-P] P.E.Conner-R.Perlis: A survey of trace forms of algebraic number fields. Lecture Notes on Pure Math.2, World Scientifi Singapore 1984.

[E-L-P] R.Elman,Y.T.Lam-A.Prestel: On some Hasse principles over formally real fields. Math.Z. 134(1973),291-301.

[E-H-P] D.R.Estes-J.Hurrelbrink-R.Perlis: Total positivity and algebraic Witt classes. Comment.Math.Helvetici 60(1985), 284-290.

[L] T.Y. Lam: The algebraic theory of quadratic forms, Benjamin, Reading, Mass. 1973.

[P-W] A. Prestel-R.Ware: Almost isotropic quadratic forms. J. London Math.Soc.(2), 19(1979),241-244.

[Sch_1] W. Scharlau: On trace forms of algebraic number fields. (to appear in Math.Z.)

[Sch_2] W. Scharlau: Quadratic and hermitian forms. Springer, Berlin-Heidelberg-New York-Tokyo 1985

[S] J.-P. Serre: L'invariante de Witt de la forme $Tr(x^2)$. Comment.Math.Helvetici 59 (1984), 651-676

[W] R. Ware:Hasse principles and the u-invariant over formally real fields. Nagoya Math. J.61(1976), 117-125

[Wi] E. Witt: Theorie der quadratischen Formen in beliebigen Körpern. J.reine angew.Math. 176,31-44(1937).

Alexander Prestel
Fakultät für Mathematik
Universität Konstanz
West Germany