UNIVERSITÉ PARIS VII

STRUCTURES ALGÉBRIQUES ORDONNÉES

SÉMINAIRE 1987 – 1988

F. Delon, M. Dickmann, D. Gondard

Séminaire de Structures Algébriques Ordonnées.

Delon - Dickmann - Gondard

1987 - 1988

Liste des exposés

13 10.87 - **F. Delon** (Univ. Paris 7).

$17^{ème}$ problème de Hilbert dans les corps chaîne-clos : suite.

20.10.87 - **D. Pecker.**

Elimination radicale des inégalités.

10.11.87 - **D. Gondard** (Univ. Paris 6).

Algèbre de chaîne : définitions et premiers résultats.

17.11.87 - **M. Dickmann** (Univ. Paris 7).

Symétries d'ordres et chaînabilité.

24.11.87 - **S. Kuhlmann.**

Une remarque sur la classification des structures ordonnées.

01.12.87 - **K. Keimel** (Univ. de Darmstadt (R.F.A.).

Cônes ordonnés et approximation.

09.01.88 - **M. Giraudet** (Univ. du Mans).

Interactions entre la loi et l'ordre dans des groupes d'automorphismes de chaîne.

23.02.88 - **R. Farré** (Univ. de Barcelone, Espagne).

Fonctions définies positives dans les corps chaîne-clos.

01.03.88 - **E. Becker** (Dortmund - R.F.A.).

The real holomorphy ring of a real function field over $\mathbb{R}$.

08.03.88 - **T. Recio** (Santander - Espagne).

Rational computation trees.

15.03.88 - **M.F. Coste-Roy** (Rennes).

Complexité des calculs sur les nombres algébriques réels.

19.04.88 - **A. Prestel** (Konstanz - R.F.A.).

Representation of polynomials as sums of 2m-th powers.

26.04.88 - **L.G. Bröcker** (Munster - R.F.A.).

On basic semialgebraic sets.

17.05.88 - **M. Giraudet et F. Lucas** (Univ. du Mans et Angers).

Groupes de permutations monotones de chaînes.

31.05.88 - **J. Heintz** (Buenos Aires, Argentine).

Théorème des zéros effectif et applications en complexité et calcul formel.

14.06.88 - **C. Scheiderer** (Univ. de Regensburg, R.F.A.).

On the stability index of real varieties.

Séminaire **Structures Algébriques Ordonnées.**

Delon - Dickmann - Gondard

1987 - 1988

Liste des contributions

- **F. Delon** (Univ. Paris 7).
  Compléments sur les corps chaîne–clos.

- **D. Pecker** (Univ. Paris 6).
  Elimination radicale des inégalités.

- **E. Becker** (Dortmund – R.F.A) et **D. Gondard** (Univ. Paris 6).
  Anneaux semi–chaînables.

- **M. Dickmann** (Univ. Paris 7).
  Couples d'ordres chaînables.

- **S. Kuhlmann** (R.F.A.).
  A remark on the classification problem for ordered structures.

- **K. Keimel** (Univ. de Darmstadt – R.F.A.) et **W. Roth** (Univ. de Bahrain) .
  Ordered cones and approximation.

- **R. Farré** (Univ. de Barcelone, Espagne).
  A positivstellensatz for chain–closed fields.

– **E. Becker** (Dortmund – R.F.A.).
The real holomorphy ring of a real function field.

– **T. Recio** (Santander – Espagne).
Rational computation trees.

– **M.F. Coste–Roy** (Rennes) et **A. Szpirglas** (Paris–Nord).
Complexity of the computation on real algebraic numbers.

– **L.G. Bröcker** (Munster – R.F.A.).
On basic open semialgebraic sets.

– **N. Fitchas** (Buenos Aires – Argentine) et **A. Galligo** (Nice).
Nullstellensatz effectif et conjecture de Serre pour le calcul formel.

– **F. Delon** (Univ. Paris 7).
La théorie élémentaire d'un corps ordonné ne détermine pas la théorie de son plongement dans sa clôture réelle.

– **C. Scheiderer** (Univ. de Regensburg – R F.A.).
On the stability index of real varieties.

COMPLÉMENTS SUR LES CORPS CHAÎNE-CLOS

Françoise Delon

Les corps chaîne-clos ont été abondamment décrits dans ce séminaire. On a vu qu'ils peuvent être définis comme des corps portant une chaîne et sans extension algébrique propre sur laquelle cette chaîne se prolonge fidèlement, ou bien comme des corps portant une valuation henselienne avec un corps de restes réels clos et un groupe de valeurs G impair-divisible et vérifiant $(G:2G) = 2$. Leur classe est élémentaire. Nous allons préciser ici quelques points de théorie des modèles à propos de ces structures: élimination des quantificateurs dans une extension par définition et coïncidence entre inclusion élémentaire et clôture existentielle relative. Nous reviendrons aussi sur la caractérisation, dans certains corps chaîne-clos, des fractions rationnelles à une seule indéterminée qui sont sommes de puissances 2^n (voir [DeG]), et donnerons des exemples et contre-exemples qui expliquent les hypothèses restrictives et la forme de la caractérisation. Les trois parties sont indépendantes.

1. Élimination des quantificateurs

Reprenons les différentes théories considérées par Dickmann [Di] :

T = théorie des corps chaîne-clos dans le langage $L = \{ 0, 1, +, -, . \}$

TC = théorie des corps <u>chaînés</u> chaîne-clos dans le langage

$$LC = L \cup \{ P_i \ ; \ i \in \omega \}$$

TCV = théorie des corps chaînés chaîne-clos munis de leur valuation de Jacob dans le langage $LCV = LC \cup \{ D \}$, où D est le prédicat de divisibilité: $D(x,y) \iff v(x) \leq v(y)$; rappelons que la valuation de Jacob sur un corps chaîne-clos K est le premier élément de l'ensemble $V(K) = \{ v$ valuation sur K ; K/v réel clos $\}$ ordonné par la relation $v \geq w$ ssi l'anneau de valuation de w contient celui de v , et qu'elle est définissable dans la seule structure de corps de K .

Dickmann a montré que TCV est modèle-complète [Di 2-3]. Nous allons montrer que cette théorie admet l'élimination des quantificateurs. Nous commençons par décrire les parties universelles des théories précédentes. Signalons que Harman a employé l'expression "extension de chaîne" en un sens qui contredit l'usage en théorie des modèles; nous n'utilisons qu'une fois cette terminologie et précisons alors "au sens de Harman".

Lemme 1-1. $T_\forall$ est la théorie des anneaux intègres ordonnables.

Démonstration. Pour une théorie S , l'ensemble $S_\forall$ de ses conséquences universelles est la théorie des sous-structures de ses modèles. Un corps chaîne-clos est ordonnable, et réciproquement un corps ordonnable est plongeable dans un corps réel clos, disons R , lequel se plonge dans $R((X^{\frac{1}{2^\infty}})) := \bigcup_{n \in \mathbb{N}} R((X^{\frac{1}{2n+1}}))$ qui est chaîne-clos. □

Lemme 1-2. $TC_\forall$ est axiomatisée par les propriétés suivantes:

1. anneau intègre;

2. P_0 et P_1 sont des ordres, c'est-à-dire:

$P_i + P_i \subseteq P_i$, $P_i . P_i \subseteq P_i$, $x^2 \in P_i$, $x \in P_i \vee -x \in P_i$, pour $i=0,1$;

3. pour $i \geq 2$, $x^{2^i} \subseteq P_i$, $P_i . P_i \subseteq P_i$, $[P_i(xy) \wedge P_i(x)] \longrightarrow P_i(y)$, $P_i + P_i \subseteq P_i$

$$P_o(x) \wedge \neg P_1(x) \longrightarrow \bigvee_{j=1}^{2^i} P_i(x^j y) \ ;$$

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

Démonstration. Soit T_o la conjonction des axiomes donnés dans l'énoncé. Clairement $T_o \subseteq T_\forall$. Soit réciproquement $A \models T_o$. On vérifie sans difficulté que l'unique prolongement des P_i sur le corps des quotients $Q(A)$ de A défini par $P_i(ab^{-1}) \leftrightarrow P_i(ab^{2^i-1})$ continue à satisfaire T_o. Les axiomes 3 impliquent que P_i est sur $Q(A)$ un ordre de niveau j pour un entier $j \leq i$. Cette situation a été étudiée par Harman ([H] lemme 1-7).

- Ou bien tous les P_i coïncident sur $Q(A)$. Dans ce cas, si R est la clôture réelle de $Q(A)$ pour cet ordre, et $(Q_i)_i$ l'unique chaîne de $K := R((X^{\frac{1}{2^\infty}}))$, on a $(A,(P_i)) \subseteq (K,(Q_i))$.

- Ou bien il y a un entier d tel que P_o, P_1 ... P_d coïncident sur $Q(A)$ et $(P_{d+i})_i$ est une chaîne de $Q(A)$. Si $d \geq 1$, prenons un point x de A vérifiant $P_d(x) \wedge \neg P_{d+1}(x)$ et considérons le corps $B = Q(A)[y]$, $y^2 = x$. Il y a sur B exactement deux ordres prolongeant $P_d(Q(A))$ et aucun prolongeant $P_{d+1}(Q(A))$. D'après [H] 3-7, il y a donc sur B une chaîne $(Q_i)_{i\in\omega}$, unique à échange de ses deux ordres vrais près, qui est extension de degré 2 au sens de Harman de $(P_{d+i}(Q(A))_{i\in\omega}$, c'est-à-dire vérifie

$$Q_o \cap Q(A) = Q_1 \cap Q(A) = P_d(Q(A))$$

$$Q_i \cap Q(A) = P_{d-1+i}(Q(A)) \ , \quad \text{pour} \quad i \geq 2 \ ,$$

ce qui nous permet de renommer $Q_i = P_{d-1+i}(B)$. On prolonge ainsi par induction les P_i sur $C = Q(A)[x^{2^{-d}}]$, où ils forment une chaîne. Et C muni de cette chaîne admet une clôture, ce qui montre $C \models T_\forall$ donc aussi $A \models T_\forall$. □

Lemme 1-3. Soient les axiomes:

5. $\neg D(0,1)$, $[\ D(x,y) \wedge D(y,z)\ ] \longrightarrow D(x,z)$, $D(x,y) \vee D(y,x)$,

$[\ D(x,y) \wedge D(x,z)\ ] \longrightarrow D(x,y+z)\ ,\quad z \neq 0 \longrightarrow [\ D(x,y) \leftrightarrow D(zx,zy)\ ]\ ,$

6. $[\ D(y,x) \wedge \neg D(x,y)\ ] \longrightarrow P_o(y^2+x)$

7. $[\ P_o(xy) \wedge D(x,y) \wedge D(y,x)\ ] \longrightarrow P_1(xy)\ .$

Alors $TCV_v = TC_v + 5 + 6 + 7\ .$

Démonstration. Il a déjà été expliqué dans [DrMM] pourquoi il convient de parler d'une valuation en termes de divisibilité lorsqu'on s'intéresse à l'élimination des quantificateurs. On trouve là aussi l'équivalence entre les axiomes 5 et la présentation habituelle d'une valuation. De la même façon l'axiome 6 n'est autre que l'expression, dans un anneau, de la convexité de v pour P_o , et l'axiome 7 l'expression de l'égalité des ordres résiduels définis par P_o et P_1 . Précisons. Comme il est usuel A_v désigne l'anneau de la valuation v , M_v son idéal maximal, K/v son corps résiduel et x/v le reste d'un élément $x \in A_v$. Soit T_1 la conjonction des axiomes ci-dessus. Clairement $T_1 \subseteq TCV_v$. Soit réciproquement $A \models T_1$; on sait déjà étendre les P_i sur $Q(A)$, où ils satisfont toujours TC_v . De même v s'étend de façon unique sur $Q(A)$, où il continue à satisfaire $5 + 6 + 7$. Nous allons donc désormais supposer que A est un corps. Par définition une valuation v est convexe pour un ordre de niveau éventuellement supérieur P_i lorsque $1 + M_v \subseteq P_i$; cela implique, pour $v(x)$ et $v(y) \geq 0$,

$$[\ x/v = y/v \longrightarrow (\ P_i(x) \leftrightarrow P_i(y)\ )\ ]$$

et permet de définir l'ordre quotient P_i/v sur K/v . Harman [H 1-8] a montré que, étant donnée une chaîne $(P_i)_i$ sur un corps, la valuation v_1 archimédienne pour P_o est convexe pour tous les P_i et telle que les P_i/v sont égaux. Une valuation v convexe pour P_o vérifie donc $v \leq v_1$ et est également convexe pour tous les P_i . De plus si P_o/v et P_1/v coïncident, d'après la relation $P_{i+1}/v \cup -P_{i+1}/v = (P_i/v \cap P_o/v) \cup -(P_i/v \cap P_o/v)$, on voit par induction sur i que chaque P_i/v est égal à P_o/v . En conséquence T_1 impose que v est convexe pour chacun des P_i et que les P_i/v sont

égaux. D'après le lemme 1-2 on sait déjà étendre A en un modèle K de TC. On avait distingué deux cas.

1. Les P_i coïncident sur A. On prolonge v de A à K en prenant pour anneau de valuation la clôture convexe de A dans K. On se rappelle que $K = R((X^{\frac{1}{2^\infty}}))$, où R est la clôture réelle de A. Sur K la valuation de Jacob v_K est la valuation associée à X, et $v \geq v_K$.

2. Sinon K est algébrique sur A, v admet un et un seul prolongement convexe de A à K. Si $v(K) < v_K$, K/v est chaîne-clos avec $(P_i(K)/v)_i$ pour chaîne (voir [DeG] proposition 11); mais K/v est algébrique sur A/v et donc, d'après [H theorem 4-12], $(P_{i+d}(K)/v \cap A/v)_{i\in\omega}$ est une chaîne de A/v pour un entier d ; cela contredit le fait que tous les $P_i(d)/v$ sont égaux.

On s'est ainsi ramené à un corps chaîne-clos avec une valuation $v \geq v_K$. Si $v(K) > v_K$, considérons le corps $K(x)$, où x est transcendant sur K et où on prolonge v en plaçant $v(x)$ dans la coupure 0^+ de vK. On a donc $K(x)/v = K/v$ et $vK(x) = vK \times \mathbb{Z}$ (produit lexicographique). On prend la clôture henselienne de ce corps, puis une clôture ordonnable par racines d'ordre impair, et enfin, pour un y fixé $\in K - \pm K^2$, on ajoute un système compatible de racines $(xy)^{2^{-n}}$, $n\in\omega$; il y a sur le corps L ainsi obtenu un unique prolongement de v. Alors (L,v) est un corps chaîne-clos et sa chaîne prolonge celle de K ; en effet, on a $P_n(K) = K^2 \cup -y^{2^{n-1}} K^{2^n}$ et les mêmes relations dans L, or K est relativement algébriquement clos dans L (car vK est pur dans vL). Parce que $v(x)$ est dans la première composante archimédienne de vL et n'est pas divisible par 2, on a $v(L) = v_L$. □

Théorème 1-4. TCV élimine les quantificateurs.

Démonstration. On sait déjà que cette théorie est modèle-complète. Il suffit

de vérifier que, pour $A \models TCV_v$, les différents plongements de A dans un modèle de TCV sont compatibles. On peut par exemple supposer A dénombrable et vérifier que le modèle que nous avons construit au-dessus de A dans le lemme 1-3 se plonge dans tout modèle ω_1-saturé et contenant A de TCV .

Considérons d'abord le modèle de TC .

- Dans le cas où tous les $P_i(A)$ sont égaux, un modèle de TC contenant A contient sa clôture réelle R pour P_i car $TC \vdash P_i \cap P_o = M^{2^i}$ pour tout $i \geq 1$, et un modèle ω_1-saturé M contient un infinitésimal par rapport à A qui n'est pas un carré, donc $R((X^{\frac{1}{2^r}}))$ se plonge dans M au sens de LC .
- Lorsque la chaîne ne se réduit pas sur A à un ordre unique et que $P_o(A) = \ldots = P_d(A)$ avec $d \geq 1$, un modèle de TC contient y car $TC \vdash P_o \cap P_1 = M^2$ et les prolongements de P_d à $A[y]$ sont conjugués au-dessus de A , donc aussi les deux familles (P_{d+i-1}) .

Pour obtenir un modèle de TCV on doit ensuite éventuellement ajouter le x de la seconde partie de la preuve de 1-3. Un groupe abélien ordonné 2-régulier satisfait pour tout entier n :

$$\forall \varepsilon > 0 \ \forall g \ \exists h \ [\ h \equiv g \ (2^n) \ \wedge \ 0 < h < g \ ] \ .$$

En conséquence, si M est un modèle ω-saturé de TCV contenant K , vM contient un h dans la coupure 0^+ sur vK et tel que, pour tout entier n , $2^n \mid h - v(y)$, donc, pour $x \in M$ avec $v(x) = h$, xy ou $-xy \in M^{2^n}$; nécessairement xy ou $-xy \in M^{2^\infty}$. Si on choisit x pour avoir $xy \in M^{2^\infty}$, cet x est celui qu'on cherche.□

Dans un corps chaîne-clos, chacun des prédicats D et P_i , $i \geq 2$, est définissable. Ce n'est pas le cas des ordres vrais P_o et P_1 , qui sont certes définissables avec un paramètre, mais que certains automorphismes échangent. On peut améliorer l'énoncé précédent et obtenir l'élimination pour

une extension par définition de la théorie des corps chaîne-clos. Définissons

$LCV' = \{ 0, 1, +, -, ., D \} \cup \{ S \} \cup \{ P_n ; n \geq 2 \}$

TCV' = théorie des corps chaîne-clos

+ $(P_n)_{n\geq 2}$ est une chaîne privée de ses deux ordres vrais

+ D est la relation de divisibilité de Jacob

+ $S(x) \longleftrightarrow \exists y\ (y^2=x)$.

Théorème 1-5. TCV' admet l'élimination des quantificateurs. En reprenant les notations des lemmes 1-2 et 1-3, $TCV'_\forall$ est axiomatisée par:

1.

2'. $S(x^2)$, $\neg S(-1)$, $[\ S(x) \wedge S(y)\ ] \longrightarrow [\ S(xy) \wedge S(x+y)\ ]$,

$[\ S(xy) \wedge S(x)\ ] \longrightarrow S(y)$, $[\ \neg S(\pm x) \wedge \neg S(\pm y)\ ] \longrightarrow [\ S(xy) \vee S(-xy)\ ]$;

3'. 3 avec remplacement du dernier schéma par $\neg S(\pm x) \longrightarrow \bigvee_{j=1}^{2^i} P_i(x^j y)$;

4'. $P_2 \cup -P_2 = S \cup -S$,

$P_{i+1} \cup -P_{i+1} = (\ P_i \cap S\ ) \cup -(\ P_i \cap S\ )$, pour $i \geq 2$;

5.

6'. $[\ D(y,x) \wedge \neg D(x,y)\ ] \longrightarrow S(y^2+x)$;

8. $[\ D(y,x) \wedge \neg D(x,y)\ ] \longrightarrow [\ S(xy) \vee S(-xy)\ ]$.

Démonstration. Pour $T_2 = 1 + 2' + 3' + 4' + 5 + 6' + 8$ et $A \models T_2$, la LCV'-structure de A s'étend de façon unique à $Q(A)$ de façon à en faire un modèle de T_2 . Si A est maintenant un corps, on définit sur A sans quantificateur dans LCV' une LCV-structure, unique à échange de P_o et P_1 près, qui en fasse un modèle de $TCV_\forall$, conserve D et les P_i pour $i \geq 2$, et vérifie $S = P_o \cap P_1$:

- si $A \subseteq \pm S(A)$, alors LCV , comme LCV' , se réduit au langage des anneaux ordonnés.

- Sinon A contient un point $a \notin \pm S(A)$, $S(A) \cup aS(A)$ et $S(A) \cup -aS(A)$ sont deux ordres de A (grâce au dernier axiome de 2') et ils constituent une

chaîne avec les $(P_i)_{i\geq 2}$ (grâce à 4'). Toujours grâce au dernier axiome de 2', l'ensemble de ces deux ordres ne dépend pas de a et ils sont donc les seuls ordres à constituer une chaîne avec les $(P_i)_{i\in\omega}$.

Réciproquement une LCV-structure peut être munie d'une LCV'-structure, qui est définie sans quantificateur en posant $S = P_0 \cap P_1$ et en conservant les P_i, $i\geq 2$, et D. □

La présentation des corps chaîne-clos dans le langage LCV est naturelle et pratique. Le théorème d'élimination des quantificateurs montre aussi sa richesse. Donnons une illustration: on sait maintenant que TCV_v est une t-théorie avec modèle-complétion et que s'appliquent tous les développements que van den Dries fait à ce sujet dans sa thèse. Il faut par contre remarquer que, contrairement à ce qui se passe pour les clôtures algébriques ou réelles, le plongement d'un corps chaîné dans sa clôture-chaîne n'a pas de bonne interprétation en théorie des modèles. Cela vient de ce que la théorie des corps chaînés n'est pas universelle; on peut la rendre universelle en ajoutant une constante c et l'axiome $\forall x\ (\ c \neq \pm x^2\ )$ (voir plus loin 2-3), mais l'interprétation de cette constante dans un modèle est arbitraire. On doit sinon ajouter au langage la valuation de Jacob; mais si K est un modèle et A une sous-structure, la trace sur A de la valuation de Jacob de K n'est pas la valuation de Jacob de A, ce qui détruit l'existence d'un modèle premier.

2. Inclusion élémentaire et clôture existentielle relative

On notera v_K la valuation de Jacob d'un corps chaîne-clos K.

Proposition 2-1. Soient deux corps chaîne-clos $K \subseteq L$. Sont alors équivalents:

1. K existentiellement clos dans L (" $K \prec_1 L$ ");

2. $K \prec L$;

3. $v_L \restriction K = v_K$ et K relativement algébriquement clos dans L (" K rac dans L ").

Démonstration. Trivialement $K \prec L \Rightarrow K \prec_1 L \Rightarrow$ K rac dans L ; et $K \prec L \Rightarrow v_L \restriction K = v_K$.

Montrons $3 \Rightarrow 1$. Si $v_L \restriction K = v_K$ on a une inclusion de corps valués henseliens $(K, v_K) \subseteq (L, v_L)$ avec $K/v_K \prec L/v_L$ car ces deux corps sont réels clos. Si on montre $v_K K \prec v_L L$, le principe d'Ax-Kochen-Ersov permettra de conclure $K \prec L$. Ces groupes ordonnés étant réguliers, il suffit de montrer que $v_K K$ est pur dans $v_L L$, c'est-à-dire 2-pur. Or pour $k \in K$, on a les équivalences: $2 \nmid v(k)$ dans $v_K K \Leftrightarrow k \in \pm cK^2$ pour un $c \in K - \pm K^2 \Leftrightarrow$ (si K est rac dans L) $2 \nmid v(k)$ dans $v_L L$.

Montrons $K \prec_1 L \Rightarrow K \prec L$. Supposons donc $K \prec_1 L$; certainement K est rac dans L et il suffit, d'après ce qu'on a vu précédemment, de montrer $v_L \restriction K = v_K$. Du fait que K est rac dans L on a $v_L \restriction K \in V(K)$, donc $v_L \restriction K \geq v_K$. Supposons par l'absurde $v_L \restriction K > v_K$. Fixons $k \in K - \pm K^2$ et choisissons sur L l'ordre qui rend k positif. Cet ordre est définissable de façon existentielle dans K : $x \geq 0 \Leftrightarrow x \in K^2 \cup kK^2$; et par la même formule dans L . Considérons sur L la valuation dont l'anneau est la clôture convexe de A_{v_K} dans L et continuons à l'appeler v_K . Donc $v_L > v_K$ sur L , et $v_K L$ est un quotient de $v_L L$ par un sous-groupe convexe propre H . Prenons $g \in v_L L$, $g > 0$, $g \notin H$ et $2 \nmid g$ dans $v_L L$ (cela est possible parce que $v_L L$ est 2-régulier), et $1 \in L$, $v_L(1) = g$ et $1 > 0$. On a $g \notin H$, donc $v_K(1) = 0$; $2 \nmid g$ dans $v_L L$, donc $1 \in \pm kL^2$. Par définition de v_K sur L et parce que $v_K(1) = 0$, il existe a et b dans K vérifiant $v_K(a) = v_K(b) = 0$ et $0 < a < 1 < b$. L'énoncé à paramètres k, a et b :

$$\exists l \, \exists u \quad a < l < b \wedge l = \pm k u^2$$

est satisfait dans L ; il ne l'est pas dans K car tout x coincé entre a et b a une v_K-valuation nulle et est positif, c'est donc un carré.□

Proposition 2-2. Soit un corps chaîne-clos K .

1. Si $V(K)$ a un seul élément, alors pour tout corps chaîne-clos L contenant K on a: K rac dans $L \Rightarrow K \prec L$.

2. Si $V(K)$ a plusieurs éléments, il existe un corps L chaîne-clos contenant K , avec K rac dans L et $K \not\prec L$.

Démonstration. 1. est un corollaire de la proposition précédente.

Pour montrer 2. on reprend la construction faite dans la preuve du lemme 1-3. Soit $K \models T$ et v la valuation archimédienne sur K . Si $v > v_K$ on adjoint à K un point x tel que $v(x)$ soit dans la coupure 0^+ de vK , et on considère le corps L construit comme dans le lemme 1-3. On a alors une inclusion de corps chaînés chaîne-clos avec $K \not\prec L$ puisque $v_L = v$ et $v \restriction K \neq v_K$.□

Corollaire 2-3 (Laslandes [L]). Dans le langage $LVc = \{ 0, 1, +, -, ., D, c \}$ la théorie $T \cup$ " D est la divisibilité de Jacob" $\cup$ " $c \notin \pm K^2$ " est modèle-complète.

Démonstration. Soient K et L des modèles de TVc , avec $K \subseteq L$ au sens de LVc . D'après ce qui précède il nous suffit de montrer que K est rac dans L , c'est-à-dire $L^2 \cap K = K^2$. Or, si $x \in K - \pm K^2$, on a $x \in \pm cK^2$ donc $x \in \pm cL^2$, donc $x \notin \pm L^2$.□

Proposition 2-4. 1. T n'a pas de modèle existentiellement clos.

2. Les modèles existentiellement clos de TC sont les corps chaînés chaîne-clos K avec un unique élément dans $V(K)$. Puisque cette classe n'est pas élémentaire, TC n'a pas de modèle-compagnon.

Démonstration. 1. Pour $K \models T$ et $c \in K - \pm K^2$, $L = K[c^{\frac{1}{2}}]$ est également chaîne-clos et K n'est pas existentiellement clos dans L.

2. Inclusion élémentaire et clôture existentielle relative coïncident entre modèles de T, donc a fortiori de TC. Si K et L sont des modèles de TC avec $K \subseteq L$ au sens de LC, K est rac dans L (en effet $K^2 = (P_1 \cap P_2)(K) = (P_1 \cap P_2)(L) \cap K = L^2 \cap K$). Le résultat découle alors de 1 et de la preuve de 2-2.2.□

3. Le XVIIème problème de Hilbert au niveau n

On peut énoncer la solution donnée par Artin au XVIIème problème de Hilbert sous la forme suivante : si R est un corps réel clos et $f \in R(\bar{X})$ avec $\bar{X} = (X_1, \ldots, X_m)$, alors $f \in \Sigma\, R(\bar{X})^2$ ssi $\forall\, \bar{x} \in R^n$, $f(\bar{x}) \in \Sigma\, R^2$. Danielle Gondard et moi-même avons cherché à généraliser ce résultat pour les puissances d'ordre 2^n, $n \geq 2$, dans un cadre où les corps réels clos avec leur unique ordre seraient remplacés par les corps chaîne-clos avec leur unique ordre de niveau 2^n. Là encore il est apparu que les corps chaîne-clos K avec un seul élément dans $V(K)$ se comportaient plus simplement que les autres. Énonçons le résultat que nous avions prouvé (voir [DeG]).

Définition. $f \in K(X)$ a la propriété $(*n)$ sur K lorsqu'elle vérifie : $\forall x \in K$, $f(x) \in \Sigma\, K^{2^n}$.

Théorème. Soit un corps K chaîne-clos avec un seul élément dans $V(K)$ et $f \in K(X)$. Alors $f \in \Sigma\, K(X)^{2^n}$ ssi f a la propriété $(*n)$ sur toute extension finie réelle de K.

Nous avions signalé les faits suivants.

- Pour $n = 1$ l'équivalence est vraie quel que soit le corps K. Elle peut être reformulée ainsi : f est une somme de carrés ssi elle est définie positive sur les extensions finies réelles de K pour chacun de leurs deux ordres.

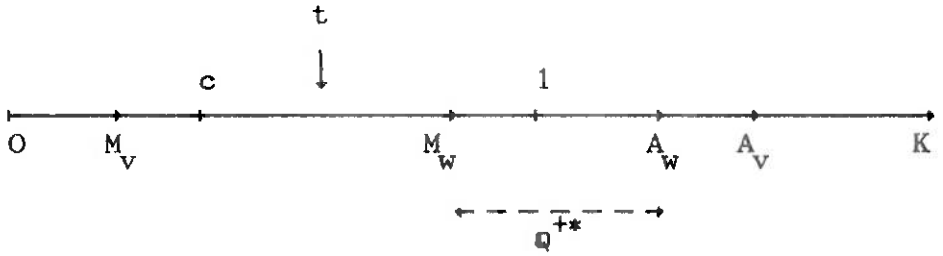
- Dès qu'on a $n \geq 2$, si K est chaîne-clos avec au moins deux éléments dans $V(K)$, il y a des contre-exemples.

Construction du contre-exemple. Soit K chaîne-clos avec $v \in V(K)$, K/v non archimédien. Soit w la valuation archimédienne sur K ; donc $w > v$. Prenons $c \in K$ vérifiant $v(c) = 0$, $w(c) > 0$ et $f = (X^2 + 1)(X^2 + c^2)$. Pour x dans K,

- si $v(x) < 0$, $f(x) \sim_v x^4$ (où "$a \sim_v b$", ou "$a \sim b$" quand il n'y a pas d'ambiguïté, signifie $v(a-b) > v(a) = v(b)$);

- si $v(x) \geq 0$, $f(x)/v = ((x/v)^2 + 1)((x/v)^2 + (c/v)^2) > 0$ donc $f(x) \in K^4$.

Le même raisonnement montre $f(L) \subseteq L^4$ pour toute extension finie réelle L de K car alors $L/v = K/v$ est réel clos et (L,v) est henselien. Si f était dans $\Sigma K(X)^4$ on aurait $f(L) \subseteq \Sigma L^4$ pour toute extension L de K. Or considérons le corps $L = K(t)$ ordonné de façon à ce que, en continuant à appeler v et w des prolongements convexes de v et w sur L, on ait $v(t) = 0$, $0 < w(t) < w(c)$, ce qui correspond à la situation suivante :



et $w(t)$ irrationnel sur wK. En tant que groupes, wL et $wK \oplus \mathbb{Z}.w(t)$ sont isomorphes, donc $w(t)$ n'est pas divisible par 2 dans wL. En conséquence $f(t)$, qui est w-équivalent à t^2, n'est pas dans L^4, ni dans ΣL^4 dès que $L/w = K/v$ est réel.

Expliquons maintenant pourquoi il est insuffisant de supposer que f a la propriété $(*n)$ sur K. On a montré dans [DeG] que si f vérifie $(*n)$ sur K, ses racines se regroupent par paquets de cardinalité multiple de 2^n, où toutes ont la même valuation. On peut être plus précis et regrouper les racines "indiscernables" sur K.

Définition. 1) Soit $(K \subseteq L, v)$ une extension de corps valués ; c et c' dans L sont dits indiscernables" sur (K,v) lorsqu'ils vérifient $v(c-k) = v(c'-k)$ pour tout $k \in K$.

2) Pour $x \in L$ on définit

$$J(x) = \{v(x-k) \ ; \ k \in K\}$$

$$I(x) = J(x) \cap vK .$$

On vérifie facilement que l'ultramétrique impose : ou bien $J(x) = I(x)$, ou bien $J(x)$ est égal à $I(x)$ plus un élément maximal qui n'appartient pas à vK. Si $J(x)$ a un élément maximal $g_x \notin vK$, x est dit valuationnel sur K ; on a alors $J(x) = I(x) \cup \{ g_x \}$. Si $J(x)$ a un élément maximal $g_x \in vK$, x est dit résiduel sur K ; on a $J(x) = I(x)$. Dans les deux cas, soit $k_x \in K$, vérifiant $g_x = v(x-k_x)$; si $g_x = v(x)$, on choisit $k_x=0$; sinon k_x est défini à $\sim$-équivalence près.

Lemme 3-1. 1. Si x et y sont résiduels ou valuationnels sur K, ils sont indiscernables ssi $g_x = g_y$ et $k_x \sim k_y$.

2. S'il existe $k \in K$ vérifiant $v(x-k) = v(y-k) \notin vK$, alors x et y sont (valuationnels et) indiscernables sur (K,v).

Démonstration sans problème utilisant l'ultramétrique.

Lemme 3-2. a. Soit L la clôture algébrique de K et v une valuation sur L ; alors vL est la clôture divisible de vK et L/v est la clôture algébrique de K/v.

b. Soit (K,v) henselien. Alors :

1) des éléments algébriques conjugués sur K sont indiscernables;

2) si x est algébrique sur K et K/v de caractéristique résiduelle nulle, J(x) a un plus grand élément ;

Démonstration. Nous renvoyons à [R] pour les éléments de théorie des valuations. (a) est classique, (b.1) se déduit de ce qu'une valuation henselienne se prolonge de façon unique sur toute extension algébrique; (b.2) de ce que, lorsque (K,v) est henselien et K/v de caractéristique nulle, un point algébrique sur K n'est jamais "limite", ce qui signifie exactement que J(x) a un élément maximal.□

Proposition 3-3. Soit K chaîne-clos et $f \in K[X]$ unitaire. Alors $\forall x \in K$ $vK \models 2^n | v(f(x))$ ssi les racines x_i de f se regroupent par paquets C_i de racines indiscernables sur K tels que:

- si $x_i \in K$ ou est résiduel, 2^n divise $|C_i|$
- si x_i est valuationnel et m est le premier entier pour lequel $m.g_{x_i} \in vK$, $2^n.m$ divise $|C_i|$.

Démonstration. 1) Preuve de "si".

Décomposons $f = \prod f_i$ où $f_i = \prod_{x \in C_i} (X-x)$ pour des C_i ayant les propriétés indiquées. D'après le lemme 3-2.1, f_i est à coefficients dans K .

- Si les x sont résiduels, $v(k-x) \in vK$ pour tout $k \in K$, donc 2^n divise $v(f_i(k))$ dans vK .
- Si les x sont valuationnels, on définit $g(X) = f(X+a) = \prod(X-(x-a))$ pour un $a \in K$ avec $a \sim k_x$; pour $k \in K$ et $v(k) < v(x-a)$, $g(k) \sim k^{|C_i|}$; et pour $v(k) > v(x-a)$, $g(k) \sim (x-a)^{|C_i|}$, d'où $v(g(k)) = |C_i|.g_x$.

2) Soit $f \in K[X]$ unitaire et tel que $K \models \forall x\ 2^n | v(f(x))$. Considérons une racine valuationnelle x de f, $(x_i)_i$ les racines de f indiscernables de

x , $(y_i)_i$ les autres racines, $k=k_x$. Définissons $g(X) = f(X+k)$. D'après le lemme 3-1.2, les $x_i - k$ sont les seules racines de g à avoir une valuation $\notin vK$. D'après le lemme 20 de [DeG] , les $(y_i-k)_i$ peuvent être séparés en groupes où tous ont la même valuation, et de cardinalité divisible par 2^n . En conséquence on a $2^n|v(\Pi(y_i-k))$, et $2^n|v(g(0))$ implique $2^n|v(\Pi(x_i-k)) = g_x$. nombre de x_i . Grâce à 1 et à ce qui précède, on peut maintenant supposer que toutes les racines de f sont résiduelles.

Décomposons $f = f_1 . \ldots . f_r$, où les racines de f_j sont indiscernables, celles de f_i discernables de celles de f_j pour $i\neq j$, et, si x_j est racine de f_j , $g_{x_{j+1}} \geq g_{x_j}$. Cela impose $v(x_j - k_{x_r}) < g_{x_r}$ pour $1 > j > r$, donc, si on translate en posant $g(X) = f(X+k_{x_r})$, les $x_r-k_{x_r}$ sont les seules racines de g ayant g_{x_r} comme valuation, et le lemme 20 de [DeG] donne le résultat (ce lemme est énoncé avec l'hypothèse plus forte $f(K) \subseteq K^{2^n}$, mais dans la preuve seule est utilisée la propriété $K \models \forall x\ 2^n|v(f(x)))$.□

Si nous nous rappelons l'équivalence $x \in K^{2^n} \iff [\ 2^n|v(x) \wedge x$ est positif pour un ordre de $K\ ]$, nous voyons maintenant comment construire un polynôme $f \in K[x]$ ayant la propriété $(*n)$ sur K et ne la conservant pas sur une extension finie réelle L de K, il suffit que les racines de f soient indiscernables sur K mais cessent de l'être sur L . Nous précisons dans l'exemple suivant.

Exemple. Soit $c \in K - \pm K^2$, $v(c) > 0$, $e^4 = c$ et $f \in K[X]$ le polynôme minimal de $e^2 + e^3$ sur K . Les quatre racines $a = e^2 \pm e^3$ et $-e^2 \pm ie^3$ de f sont valuationnelles indiscernables sur K ($k_a = 0$, $g_a = v(c)/2$) , mais cessent de l'être sur $K[e^2]$. Pour $x \in K$,

- si $v(x) < v(c)/2$, $f(x) \sim x^4$

- si $v(x) > v(c)/2$, $f(x) \sim c^2$

donc f a la propriété $(*1)$ sur K , alors que $f(e^2) \sim -4(e^2)^5 \notin (K[e^2])^2$.

Dans l'exemple précédent les racines sont valuationnelles ; c'est, d'après le lemme suivant, le seul cas où le phénomène décrit se produise.

Lemme 3-4. Soit $f \in K[X]$ unitaire, de degré $2^n.S$, avec toutes ses racines c vérifiant $v(c) = 0$ et $c/v \notin K/v$. Alors f a la propriété $(*n)$ sur toute extension algébrique réelle L de K .

Démonstration. Soit $f = \prod (X - c_i)$; pour $x \in K$,

- si $v(x) < 0$, $f(x) \sim x^{2^n.S}$

- si $v(x) \geq 0$ alors $v(f(x)) = 0$;

f/v est un polynôme unitaire et sans racine sur K/v réel clos ; il ne prend donc que des valeurs strictement positives, et $f(K) \subseteq K^{2^n}$.

Comme $L/v = K/v$, f satisfait les hypothèses du lemme sur L , ce qui achève la preuve.□

Proposition 3-5. f satisfait $(*n)$ sur toute extension algébrique réelle de K ssi il satisfait $(*n)$ sur toute extension finie réelle de dimension $\leq d(f)$, où $d(f)$ est le degré de f .

Démonstration. D'après la proposition 5 de [DeG], f a toutes ses racines dans $K'[i]$ où K' est n'importe quelle extension réelle de dimension $d(f)$ de K . Supposons $f(K') \subseteq K'^{2^n}$.

- Les racines qui sont dans K' sont alors de multiplicité divisible par 2^n .

- Parmi les autres, considérons un paquet C de racines indiscernables sur K' et $g = \prod_{c \in C} (X - c)$; ces racines sont résiduelles sur K', et donc il existe a et b dans K' tels que $g((X-a)b^{-1})$ satisfasse les hypothèses du lemme 3-4, donc $g(L) \subseteq L^{2^n}$ quelle que soit l'extension finie réelle L de K', on a donc aussi $f(L) \subseteq L^{2^n}$.
Comme K' est une extension réelle de degré $d(f)$ réelle arbitraire, on obtient $f(L) \subseteq L^{2^n}$ pour toute extension L finie réelle de K.□

Corollaire 3-6. " f a la propriété $(*n)$ sur toutes les extensions finies réelles de K " se dit par un énoncé sans paramètres sur les coefficients de f.

Démonstration. Les extensions réelles L de K de dimension 2^d sont toutes de la forme $K[c]$ avec $c^{2^d} \in K$.□

Cela nous permet de retrouver un cas particulier d'un résultat de Prestel ([P] théorème 2 + corollaire du théorème 1).

Corollaire 3-7. Définissons le degré de $f \in K(X)$, $D(f) = d(p) + d(q)$ où p et $q \in K[X]$ et $f = p/q$ est irréductible, et $K(X)_{\leq d} = \{ f \in K(X) ; D(f) \leq d \}$. Alors $\forall n \geq 2 \ \forall d \ \forall m \ \forall r \quad K(X)_{\leq d} \cap \Sigma K(X)^{2^n} \not\subseteq \overset{r}{\Sigma} [K(X)_{\leq m}]^{2^n}$.

Démonstration. Sinon $\exists n \geq 2 \ \exists d \ \exists m \ \exists r$, $K(X)_{\leq d} \cap \Sigma K(X)^{2^n} \subseteq \overset{r}{\Sigma} [K(X)_{\leq m}]^{2^n}$.
Mais alors le théorème impliquerait que K satisfait l'énoncé suivant :

$\forall f \in K(X)$ de degré $\leq d$

$[f \models (*n)$ sur les extensions ordonnées de degré $\leq d] \longrightarrow f \in \overset{r}{\Sigma} [K(X)_{\leq m}]^{2^n}$.
Parce que la théorie des corps chaîne-clos est complète, tout autre corps chaîne-clos le satisferait ; or on a vu qu'il y a des contre-exemples dès que

V(K) contient plus d'un élément.□

Bibliographie

[DeG] F. Delon et D. Gondard, 17ème problème de Hilbert sur les corps chaîne-clos, manuscrit.

[Di] M. Dickmann, The model-theory of chain-closed fields, J.S.L. 53 (1988), pp. 921-930.

[Dr] L. van den Dries, Model Theory of Fields, Thesis, Utrecht 1978.

[DrMM] L. van den Dries, A. Macintyre et K. McKenna, Elimination of quantifiers in algebraic structures, Adv. in Math. 47 (1983), pp. 74-87.

[H] J. Harman, Chains of higher level orderings, Contemporary Math. 8 (1982), pp. 141-174.

[L] B. Laslandes, Corps de Rolle portant un nombre fini de valuations, C.R.A.S. 302 (1986), série I , pp. 401-404.

[P] A. Prestel, Model theory of fields: An application to semidefinite polynomials, dans Logique (Delon, Lascar, Parigot et Sabbagh éditeurs), Mémoire de la S.M.F. n°16, Gauthier-Villars, Paris 1984, pp. 53-65.

[R] P. Ribenboim, Théorie des valuations, les Presses de l'Université de Montréal, Montréal 1964.

D.Pecker
Université Paris 6

L'ELIMINATION RADICALE DES INEGALITES .

§1 Introduction:

On remplace souvent l'inégalité $x \geqslant 0$ par la proposition "x a une racine carrée " ou par " $\exists\ t \in \mathbb{R}\ ,\ x^2 - t = 0$ ". C'est l'exemple le plus immédiat d'élimination d'une inégalité . Ce problème n'est pas toujours aussi facile : trouver par exemple un polynôme $P(x,y,T)$ qui a une racine réelle si et seulement si $x \neq 0$ ou $y \geqslant 0$ ...

C'est une réciproque du problème de l'élimination des quantificateurs. Géométriquement , il s'agit de trouver un ensemble algébrique se projetant sur un ensemble semi-algébrique donné . Comme le fait remarquer R.Thom, c'est le problème que devaient résoudre les habitants enchaînés de la caverne de Platon .

On démontre le résultat suivant :

Théorème :

Soit S un ensemble semi-algébrique de $\mathbb{R}^n$. Il existe un polynôme irréductible $P(X_1,..,X_n,T)$ tel que :

$$(x_1,..,x_n) \in S \iff \exists\ t \in \mathbb{R}\ ,\ P(x_1,..,x_n,t) = 0$$

et l'équation d'inconnue T : $P(X_1,..,X_n,T) = 0$ est résoluble par racines carrées .

On étudie d'abord le cas des coins obtus : $\left\{ x \in \mathbb{R}^n \mid x_1 \geqslant 0 \text{ ou } \ldots \text{ ou } x_n \geqslant 0 \right\}$, puis le cas des coins aigus $C_n = \left\{ x \in \mathbb{R}^n \mid x_1 \geqslant 0 \text{ et } \ldots \text{ et } x_n \geqslant 0 \right\}$ et enfin le cas général des semi-algébriques pas nécéssairement fermés .

Dans ce qui suit $x = (x_1,..,x_n) \in \mathbb{R}^n$ est le "paramètre" et T la "variable" ou "l'inconnue". On a aussi la "variable" $X = (X_1, .., X_n)$.

§2 Le cas des coins obtus :

Proposition 1 : Il existe une fonction ψ_n continue semi-algébrique sur $\mathbb{R}^n$, analytique sauf peut-être sur un ensemble de codimension 2 (strictement) positive ssi l'un des x_i est (strictement) positif .

Pour chaque valeur du paramètre x , $\psi_n(x)$ est la plus grande des racines d'un polynôme $Q_n(x,T)$ qui a toutes ses racines réelles .

Démonstration: Par induction : pour n = 1 $\psi_1(x) = x$

$\psi_2(x_1,x_2) = x_1+x_2+\sqrt{x_1^2+x_2^2}$, $\psi_n(x_1,\dots,x_n) = \psi_2(\psi_{n-1}(x_1,\dots,x_{n-1}),x_n)$

La fonction ψ_n est analytique sauf sur un ensemble où deux au moins des x_i sont nuls . Les autres racines du polynôme de degré 2^{n-1} que satisfait ψ_n s'obtiennent en remplaçant dans la construction inductive certains des ψ_2 par $\psi_2'(x_1,x_2) = x_1 + x_2 - \sqrt{x_1^2 + x_2^2}$

et sont donc toutes réelles .

Remarque: On peut démontrer que $Q_n(X,T)$ est irréductible .

§3 Le cas des coins aigus:

Théorème 1 :

Pour chaque n = 1 , 2 ,... il existe un polynôme réel $P_n(X,U)$ unitaire en U ,homogène de degré 2^{n-1} ,tel que l'équation $P_n(x,U) = 0$ soit résoluble par racines carrées et tel que toutes les coordonnées de x sont positives ssi il existe un réel t tel que $P_n(x,t^2) = 0$. De plus il n'existe pas de tel polynôme de degré plus petit ; $P_n(X,T^2)$ est irréductible et $P_n(x,T^2)$ a toutes ses racines réelles quand toutes les coordonnées de x sont positives .

Démonstration: Par induction . $P_1(X_1,T^2) = T^2 - X_1$.

Pour P_2 ; considérons le cercle $\mathcal{V}_2'$: $(x-1)^2 + (y-1)^2 - 1 = 0$

Le cône positif sur $\mathcal{V}_2'$ est le coin aigu C_2 , on voit donc que $P_2(x,y,T^2) = (x-T^2)^2 + (y-T^2)^2 - T^4$ a une racine réelle ssi $(x,y) \in C_2$

Pour pouvoir faire la même construction pour n =3 il suffit de trouver un ensemble algébrique $\mathcal{V}_3'$ tel que le cône positif sur $\mathcal{V}_3'$ soit C_3 .

Soit $\Delta_2 = \{(x,y) \in \mathbb{R}^2 \mid 0 \leq x \leq 1 \ , \ 0 \leq y \leq 1 \ , \ x+y \leq 1\}$. On peut trouver deux polynômes de degré 2, $B_1(x,y)$ et $B_2(x,y)$ tels que :

$(x,y) \in \Delta_2 \Leftrightarrow B_1(x,y) \geq 0$ et $B_2(x,y) \geq 0$. L'ensemble algébrique compact $\mathcal{V}_3$ d'équation $P_2(B_1(x,y),B_2(x,y),z^2) = 0$ se projette verticalement sur Δ_2 . Si l'on fait une transformation projective qui ramène le point à l'infini sur l'axe des z à l'origine, et Δ_2 en

$\Delta_2' = \{(x,y,z) \in \mathbb{R}^3 \mid x \geqslant 0 , y \geqslant 0 , z \geqslant 0 , x+y+z = 1\}$. L'ensemble algébrique $\mathcal{V}_3$ se transforme en $\mathcal{V}_3'$ qui a la propriété voulue .

L'équation de $\mathcal{V}_3'$ est (Si $B_1 = x - x^2$, $B_2 = (1-x)y - y^2$) :

$(x+y+z-1)^4 - 2(xy+yz+zx)(x+y+z-1)^2 + (xy+xz)^2 + y^2z^2 = 0$

Ce qui nous donne comme précédemment :

$P_3(x,y,z,T^2) = (x+y+z-T^2)^4 - 2(xy+yz+zx)(x+y+z-T^2)^2 + (xy+xz)^2 + y^2z^2$

La méthode peut donc se faire par induction grâce au lemme :

Lemme: Il existe n polynômes de degré 2, $B_1(x)$,..., $B_n(x)$ tels que :

$$x \in \Delta_n \iff (B_1(x) \geqslant 0 \text{ et } \ldots \text{ et } B_n(x) \geqslant 0)$$

La démonstration est facile (C.f. [7]) .

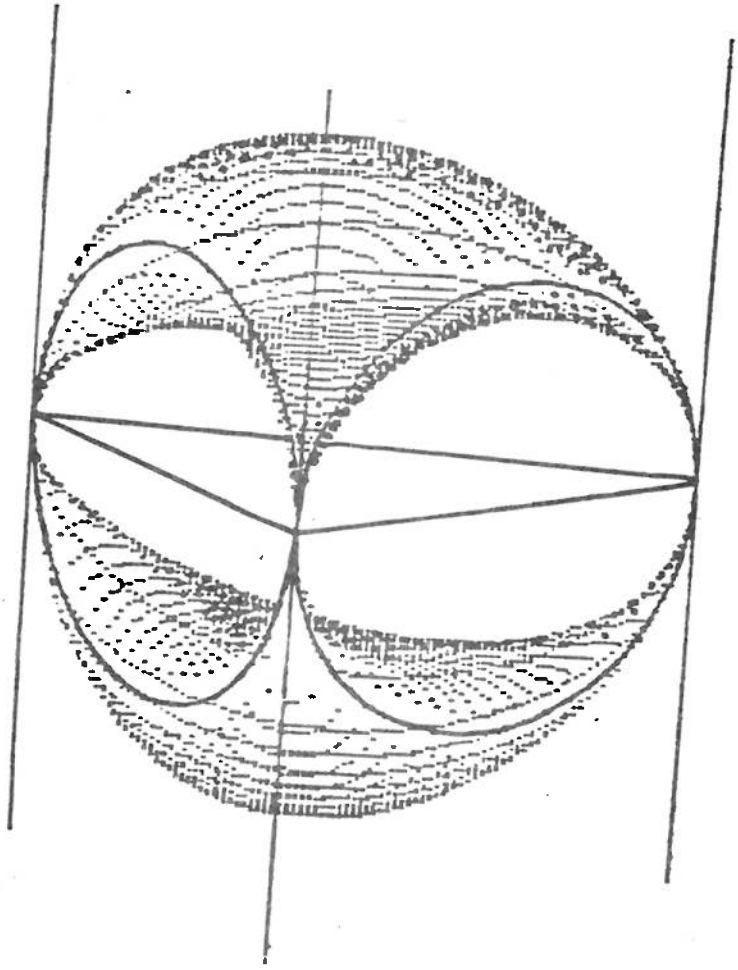


Figure : Surface $\mathcal{V}_3$ se projetant verticalement sur le triangle Δ_2

Montrons maintenant que le degré du polynôme obtenu est minimal , ce qui permettra aussi de voir son irréductibilité .

Proposition 2 : Soit $P(x,T)$ un polynôme unitaire en T qui a une racine réelle ssi $x \in C_n$. Alors P a au moins 2^n racines réelles qui sont distinctes dans un ouvert de C_n .

Démonstration : Par récurrence : clair pour $n = 1$.

Considérons le polynôme $P(x_1, \ldots, x_{n-1}, 0, T)$. Toutes ses racines réelles sont doubles si $x_1 \geqslant 0$ et ... et $x_{n-1} \geqslant 0$ (par le théorème des fonctions implicites) et elles correspondent à deux racines réelles de $P(x,T) = 0$ distinctes si x est dans un ouvert de C_n . Le nombre de racines réelles de P est donc le double du nombre de racines réelles de $P(x_1, \ldots, x_{n-1}, 0, T)$ or ce dernier réalise la projection sur C_{n-1} et , par récurrence, a au moins 2^{n-1} racines réelles distinctes dans un ouvert de C_{n-1} . ■

Cela permet de conclure que le polynôme P_n est irréductible : en effet , soit P un facteur irréductible de $P_n(x,T^2)$ non trivial . Comme $P_n(x,T^2)$ a toutes ses racines réelles ou bien aucune, P aussi et pour les mêmes valeurs du paramètre x . P réalise donc la projection sur C_n et est donc au moins de degré 2^n : $P = P_n(x,T^2)$. ■

Ce polynôme permet de donner une démonstration très simple d'un théorème de Hröcker (Cf: [4]) :

Corollaire : Si $A_1(x), \ldots, A_k(x)$ sont des polynômes réels tels que $C_n = \{x \in \mathbb{R}^n \mid A_1(x) \geqslant 0 \text{ et } \ldots \text{ et } A_k(x) \geqslant 0\}$; alors $k \geqslant n$.

Démonstration : $P_k(A_1(x), \ldots, A_k(x), T^2)$ qui est de degré 2^k , réalise la projection sur C_n , on a donc $2^k \geqslant 2^n$ par la proposition 2 . ■

En raffinant un peu la méthode précédente on peut même montrer que C_n n'est réunion finie de fermés $\{x \in \mathbb{R}^n \mid A_1(x) \geqslant 0, \ldots, \text{et } A_k(x) \geqslant 0\}$ que si l'un des k est au moins égal à n . Cela nous amène à la question : Tout fermé semi-algébrique est-il réunion finie de fermés du type $\{x \in \mathbb{R}^n \mid A_1(x) \geqslant 0 \text{ et } \ldots \text{ et } A_k(x) \geqslant 0\}$ avec $k \leqslant n$?

Pour ce genre de questions voir [4] [8] .

§4 Le cas général :

Définissons une fonction $\overline{\Psi}$ sur $\mathbb{R}^2 - \{(x,y)\in\mathbb{R}^2 \mid y = 0 \text{ et } x<0\}$:

$$\overline{\Psi}(x,y) = \frac{x + y + \sqrt{x^2+y^2}}{\left(x+\sqrt{x^2+y^2}\right)^2}(x^2+y^2) \text{ et } \overline{\Psi}(0,0) = 0 .$$

On a : $\overline{\Psi}(x,y)\geqslant 0$ si et seulement si $x\geqslant 0$ ou $y > 0$. Soit la fonction $\overline{\Theta}$ "conjuguée de $\overline{\Psi}$" donnée par :

$$\overline{\Theta}(x,y) = \frac{x+y-\sqrt{x^2+y^2}}{\left(x-\sqrt{x^2+y^2}\right)^2}(x^2+y^2)$$

Si $y\leqslant 0$ et $x<0$ on n'a pas $\overline{\Theta}(x,y)\geqslant 0$ .On voit donc que $\overline{\Psi}(x,y)$ Satisfait un polynôme $K(x,y,\overline{\Psi}) = 0$ du deuxième degré en $\overline{\Psi}$ et qui a une racine positive ssi $x\geqslant 0$ ou $y>0$. De plus $\overline{\Psi}$ est méromorphe sur $\mathbb{R}^2 - \{0\}$.

D'autre part , voyons que tout semi-algébrique S peut se mettre sous la forme $S = \bigcup_{k=1}^{N}(S_k)$ avec :

$S_k = \{x\in\mathbb{R}^n \mid A_1^k(x)\geqslant 0 \text{ ou } .. \text{ ou } B_1^k(x)>0 \text{ ou } ..\}$ où les polynômes A_i^k et B_i^k sont premiers entre eux . En effet on peut écrire (Cf [3])

(1) $S = \bigcup_i \{x\in\mathbb{R}^n \mid A_1^i(x)\geqslant 0 \text{ et } .. \text{ et } B_1^i(x)>0 \text{ et } ..\}$

Si $A = CD$, $\{A\geqslant 0\} = \{C\geqslant 0 \text{ et } D\geqslant 0\} \cup \{-C\geqslant 0 \text{ et } -D\geqslant 0\}$

et si $B = EF$ $\{B>0\} = \{E>0 \text{ et } F>0\} \cup \{-E>0 \text{ et } -F>0\}$.

On peut donc supposer que dans l'écriture (1) tous les polynômes sont irréductibles . En utilisant la distributivité on obtient la représentation annoncée du semi-algébrique S .

Définissons une fonction F_k associée à S_k :

Si aucune des familles A_i^k , B_j^k n'est vide :

$F_k(x) = \overline{\Psi}\left[\Psi_{\ell_1}(A_1^k(x),..A_{\ell_1}^k(x)),\ \Psi_{\ell_2}(B_1^k(x),.. B_{\ell_2}^k(x))\right]$

S'il n'y a pas de B_j^k : $F_k(x) = \Psi_{\ell_1}(A_1^k(x),.. A_{\ell_1}^k(x))$.

Et s'il n'y a pas de A_i^k : $F_k(x) = 1 / \Psi_{\ell_2}(B_1^k(x),.. B_{\ell_2}^k(x))$. F_k est le quotient de deux fonctions analytiques, sauf sur un fermé de codimension au moins deux .

Proposition 3 : Il existe un polynôme irréductible $R_k(X,T)$ tel que : pour tout x $F_k(x)$ est une des racines du polynôme $R_k(x,T)$ qui a toutes ses racines réelles . On a l'équivalence :

$$x \in S_k \iff F_k(x) \geqslant 0 \iff \exists t \geqslant 0 , \ R_k(x,t) = 0$$

Démonstration :

Soit $A = \psi_{\ell_1}(A_1^k(X),..,A_{\ell_1}^k(X))$, $B = \psi_{\ell_2}(B_1^k(X),..,B_{\ell_2}^k(X))$,et soit $R_1(X,F)$ le polynôme obtenu en éliminant A et B du système (I) :

$$(I) \quad \begin{cases} Q_{\ell_1}(A_1^k(X),..,A_{\ell_1}^k(X),A) = 0 \\ Q_{\ell_2}(B_1^k(X),..,B_{\ell_2}^k(X),B) = 0 \\ K(A,B,F) = 0 \end{cases}$$

On voit que $R_1(x,F_k(x)) = 0$ pour tout x . Soit R un facteur irréductible de R_1 tel que $R(x,F_k(x))=0$ sur un ouvert de $\mathbb{R}^n$,alors par prolongement analytique on aura $R(x,F_k(x))=0$ sur le domaine de définition de F_k , qui est un ouvert dense de $\mathbb{R}^n$ contenant S_k .

Si au point $x \in \mathbb{R}^n$, $R(x,F)$ a une racine positive , le système (I) a une solution α,β,f . Comme Q_{ℓ_1} et Q_{ℓ_2} n'ont que des racines réelles α et β sont réels et comme $K(\alpha,\beta,F)=0$ a une racine positive $\alpha \geqslant 0$ ou $\beta > 0$ ce qui montre que $x \in S_k$.

Réciproquement, si $x \in S_k$ $F_k(x)$ est une racine positive de $R(x,F)=0$. ■

Théorème :

Si S est un semi-algébrique de $\mathbb{R}^n$, il existe un polynôme irréductible $R(X,T)$ tel que :

$$x \in S \iff \exists t \in \mathbb{R} , \ R(x,t) = 0$$

Si S est fermé on peut supposer que R est unitaire en T .

Démonstration : Toujours avec les mêmes notations . Soit γ une racine de $P_N(F_1,\ldots,F_N,\Gamma^2) = 0$ dans une extension de $\mathbb{R}(F_1,..,F_N)$. Si $Q_1(X,F)$ est le polynôme obtenu en éliminant les U_i du système (II)

$$(II) \quad \begin{cases} R_1(X,U_1) = 0 \\ R_2(X,U_2) = 0 \\ \\ P_N(U_1,\ldots,U_N,\Gamma^2) = 0 \end{cases}$$

On voit que $Q_1(X,\gamma)=0$. Soit $R(X,\Gamma)$ un facteur irréductible de $Q_1(X,\Gamma)$ tel que $R(X,\gamma) = 0$ .Montrons que ce polynôme convient :
- Si $R(x,\Gamma)=0$ a une racine réelle, le système (II) a une solution : $u_1, \ldots, u_N, \gamma$ .Comme les $R_i(x,U)=0$ n'ont que des racines réelles les u_i sont réels et $P_N(u_1, \ldots, u_N, \Gamma^2)=0$ a une racine réelle; les u_i sont donc tous positifs .Tous les $R_i(x,U)=0$ ont une racine positive ce qui montre que $x \in \bigcap_{i=1}^{N} S_i = S$.
- Réciproquement si $x \in S$ montrons que $R(x,\Gamma)=0$ a une racine réelle . Les deux polynômes $R(x,\Gamma)$ et $P_N(F_1, \ldots, F_N, \Gamma^2)$ ont une racine commune γ .Soit P leur diviseur commun dans $R(F_1, \ldots, F_N)[\Gamma]$. $P(F_1(x), \ldots, F_N(x), \Gamma)$ a toutes ses racines réelles si $x \in S$ puisqu'il divise $P_N(F_1(x), \ldots, F_N(x), \Gamma^2)$ qui a toutes ses racines réelles les $F_i(x)$ étant tous positifs . $R(x,\Gamma)$ qui est multiple de $P(F_1(x), \ldots, F_N(x), \Gamma)$ a donc une racine réelle . ■

Remarquons comme dans [7] que cela implique :

Corollaire : Si S est un semi-algébrique de R^n d'intérieur non-vide ; S est projection d'un ensemble algébrique irréductible de R^{n+1}.

...

Tous les ensembles algébriques ainsi construits admettent des paramétrisations par radicaux : par exemple la surface $\gamma^3 = Q$ est donnée par $z = \pm\sqrt{B_1 + B_2 \pm \sqrt{2B_1B_2}}$ avec $B_1 = x - x^2$, $B_2 = (1-x)y - y^2$

Références bibliographiques :

[1] C. Andradas et J.M. Gamboa, *A note on projections of real algebraic varieties*, Pacific Journal of Mathematics, Vol.115, No.1,(1984) p.1-11 .

[2] C Andradas et J.M. Gamboa, *On projections of real algebraic varieties*, Pacific Journal of Mathematics, Vol.121, No.2,(1986) p.281-291 .

[3] J. Bochnak, M. Coste & M.F. Coste Roy, *Géométrie algébrique réelle*, Ergebnisse der Mathematik vol.12 ,Springer-Verlag (1987).

[4] L.Bröcker Description of semi-algebraic sets by few polynomials cours au CIMPA (1985)

[5] T.S.Motzkin ,Elimination theory of algebraic inequalities.B.A.M.S. 61 (1955),326

[6] T.S. Motzkin, *The real solution set of a system of algebraic inequalities is the projection of a hypersurface in one more dimension*, Inequalities II, Academic Press,(1970) p.251-254 .

[7] D.Pecker ,Sur l'équation d'un ensemble algébrique de R^{n+1} dont la projection dans R^n est un ensemble semi-algébrique fermé donné , C.R.A.S. , t.306,Série:II,p.265-268,1988 .

[8] Scheiderer , s'(n) , Séminaire DDG 1987-88,Université de Paris 7.

ANNEAUX SEMI-CHAÎNABLES

EBERHARD BECKER (Universität Dortmund)

DANIELLE GONDARD (Université Paris VI)

Orderings of higher level on a field have been introduced by Becker (1978) and chains of such orderings by Harman who also defined chain-closed fields (1982). Fields admitting orderings of higher level also admit chains of such orderings. Gondard (C.R.A.S., 304, 1987) gave axiomatizations, in the Artin-Schreier manner, for chainable fields : K is chainable iff K is real and there exists $\alpha \in K$ such that $\alpha^2 \notin \sum K^4$, and for chain-closed fields : K is chain-closed iff K is real and does not admit any algebraic extension of odd degree, $K^4 + K^4 = K^4$, and there exists $\alpha \in K$ such that $\alpha^2 \notin K^4$ and $K = K^2 \cup -K^2 \cup \alpha K^2 \cup -\alpha K^2$. Using these axioms we develop the theory of chain algebra : a ring A is *formally α-chainable* if A is real and $(\sum^n a_i^4 - \alpha^2 \sum^m b_j^4 = 0) \Rightarrow (\forall i \ a_i = 0$ and $\forall j \ b_j = 0)$; an ideal I is an *α-chain ideal* if it is real and $(\sum^n a_i^4 - \alpha^2 \sum^m b_j^4 \in I) \Rightarrow (\forall i \ a_i \in I$ and $\forall j \ b_j \in I)$; with these definitions we obtain that for a prime ideal I of A , I is an α-chain ideal iff the quotient field of A/I is formally $\bar{\alpha}$-chainable

For a ring A we define notions of *α-spectra of higher level* and of *α-preorder* (of level 4), and show that the spectra are non empty iff $\sum A^4$ is an α-preorder. We introduce the *α-chain radical* of an ideal I of A as $\sqrt[\alpha]{I} = \bigcap_{\mathfrak{P}} \mathfrak{p}$ where $\mathfrak{P} = \{ \mathfrak{p} , \mathfrak{p} \supseteq I , \mathfrak{p}$ prime and α-chain ideal $\}$ and give a description of it. Finally, for some chain-closed fields, we obtain a Nullstellensatz and study its validity.

Introduction

Le but de cet exposé est de construire ce que nous appelons l'Algèbre de chaîne à partir de la théorie des corps chaînables de manière analogue à la construction de l'algèbre réelle à partir de la théorie des corps ordonnables.

Rappelons d'abord que les ordres de niveau supérieur ont été introduits par Becker[B1] et qu'un corps chaînable est un corps qui admet une chaîne d'ordres de niveau supérieur telle que définie par Harman [H] ; une suite $(p_i)_{i\in\mathbb{N}}$ est une chaîne d'ordres de niveau supérieur du corps commutatif K si :

(i) p_0 et p_1 sont deux ordres vrais distincts (par ordre vrai on entend ordre total compatible avec la structure de corps) ;

(ii) pour tout $i \geqslant 2$, p_i est un ordre de niveau exact 2^i tel que défini par Becker dans [B1] ($p_i \subset K$ tel que $p_i + p_i \subset p_i$, $\dot{p}_i = p_i - \{0\}$ est un sous groupe de $\dot{K} = K - \{0\}$ tel que $\dot{K}/\dot{p}_i$ est un groupe cyclique et $|\dot{K}/\dot{p}_i| = 2^i$) ;

(iii) pour tout $i \geqslant 1$:

$$p_i \cup -p_i = (p_{i-1} \cap p_0) \cup -(p_{i-1} \cap p_0) \quad .$$

Rappelons également le théorème que nous avons obtenu dans [G1] et [G2] caractérisant les corps chaînables :

Proposition 1 -

Un corps K *est chaînable si et seulement si on peut y trouver un élément* α *tel que* (K,α) *satisfasse :*

(a) *les axiomes de corps commutatif ;*

(b) *pour chaque* $m \geqslant 1$ *l'axiome* $\Lambda X_1 \ldots \Lambda X_m \neg(-1 = X_1^2 + \ldots + X_m^2)$;

(c) *pour chaque* $n \geqslant 1$ *l'axiome* $\Lambda X_1 \ldots \Lambda X_n \neg(\alpha^2 = X_1^4 + \ldots + X_n^4)$.

Ceci conduit à poser la définition 1 :

Définition 1 :

Un corps chaînable K *tel que* $\alpha \in K$ *et* α^2 *ne soit pas somme de puissances quatrièmes dans* K *sera dit* α*-chaînable.*

La terminologie est justifiée par le fait qu'il existe alors dans K une α-chaîne $(p_i)_{i\in\mathbb{N}}$, c'est-à-dire une chaîne d'ordres de niveau supérieur $(p_i)_{i\in\mathbb{N}}$ telle que $\alpha^2 \notin p_2$. D'après [H] on sait que si K admet un ordre p_2 de niveau exact 4 tel que $\alpha^2 \notin p_2$ alors K est α-chaînable.

Par exemple $\mathbb{Q}(t)$ est un corps t-chaînable ; en effet nous verrons (lemme 2) que $\mathbb{Q}(t)$ t-chaînable est équivalent à $\mathbb{Q}[t]$ formellement t-chaînable (définition 2). Soit alors $\Sigma(p_i(t))^4 - t^2\,\Sigma(q_j(t))^4 = 0$ dans $\mathbb{Q}[t]$; si $\Sigma(p_i(t))^4 \neq 0$ a un degré $4n$ (les termes de plus hauts degrés, donc de degrés multiples de 4, ne pouvant s'annuler car leurs coefficients sont des puissances quatrièmes dans $\mathbb{Q}$ ordonnable) et $\Sigma(q_j(t))^4 \neq 0$ a un degré $4p$ on aurait alors un polynôme de degré effectif $4n$ égal à un polynôme de degré effectif $4p+2$ ce qui est impossible ; donc $\Sigma(p_i(t))^4 = 0$ et $\Sigma(q_j(t))^4 = 0$ et ceci entraîne dans $\mathbb{Q}[t]$ formellement réel que $\forall i\ p_i = 0$ et $\forall j\ q_j = 0$.

Remarquons aussi qu'il est clair qu'un corps α-chaînable est aussi $\alpha\beta^2$-chaînable et $(-\alpha\beta^2)$-chaînable pour tout $\beta \in K$ (et réciproquement).

I - Algèbre de chaîne : les premiers pas

On sait qu'un anneau A est formellement réel si et seulement si $\Sigma a_i^2 = 0 \Rightarrow \forall i\ a_i = 0$, et que A intègre est formellement réel si et seulement si son corps des quotients est ordonnable (donc bien sûr un corps est formellement réel si et seulement si il est ordonnable).

Rappelons également qu'un idéal I d'un anneau A est réel si et seulement si A/I est formellement réel, si et seulement si $\Sigma a_i^2 \in I \Rightarrow \forall i\ a_i \in I$.

Dans la suite A désignera toujours un anneau commutatif avec unité et α un élément de A.

Nous allons maintenant définir l'analogue des notions d'anneau formellement réel et d'idéal réel.

Définition 2 :

A *est un anneau formellement α-chaînable si*

(i) A *est formellement réel (i.e.* $\sum_{i=1}^{n} a_i^2 = 0 \Rightarrow \forall i\ a_i = 0$) ;

(ii) $\sum_{i=1}^{n} a_i^4 - \alpha^2 \sum_{j=1}^{m} b_j^4 = 0 \Rightarrow \forall i\ a_i = 0$ *et* $\forall j\ b_j = 0$.

Remarque 1

Si A est un corps on sait déjà que A ordonnable équivaut à A formellement réel et nous avons aussi ici que *si A est un corps, A α-chaînable équivaut à A formellement α-chaînable* ; en effet :

$\Leftarrow$ Si A est formellement α-chaînable et que $\alpha^2 = \Sigma c_i^4$ alors $\Sigma c_i^4 - \alpha^2 = 0$ et donc $\forall i\ c_i = 0$, A est donc bien α-chaînable.

$\Rightarrow$ Réciproquement, supposons A α-chaînable et soit une relation $\sum_{1}^{n} a_i^4 - \alpha^2 \sum_{1}^{m} b_j^4 = 0$ avec un b_j au moins non nul ; alors

$$\alpha^2 = \frac{\sum_1^n a_i^4}{\sum_1^m b_j^4} = \frac{(\sum_1^n a_i^4)\,(\sum_1^m b_j^4)^3}{(\sum_1^m b_j^4)^4}$$

A étant α-chaînable chacun des éléments de cette somme de puissances quatrièmes doit être nul. Or nous avons

$$\alpha^2 = \frac{(\sum_1^n a_i^4)(\sum_1^m (b_j^4)^3 + \ldots)}{(\sum_1^m b_j^4)^4} = \frac{\sum_{i=1}^n a_i^4\, b_{j_o}^{12} + \ldots}{(\sum_1^m b_j^4)^4}$$

où j_o désigne l'indice du b_j supposé non nul précédemment. On obtient donc $\forall i \;\; a_i\, b_{j_o}^3 = 0$ ce qui entraîne bien, puisque $b_{j_o} \neq 0$, que $\forall i \;\; a_i = 0$.

A étant ordonnable on déduit aisément ensuite de $-\alpha^2 \sum_1^m b_j^4 = 0$ que $\forall j \;\; b_j = 0$.

A est donc bien formellement α-chaînable.

Définition 3

Soit I *un idéal de* A . I *est un* <u>*idéal de α-chaîne*</u> *si*

(i) I *est un idéal réel (i.e.* $\sum_{i=1}^n a_i^2 \in I \Rightarrow \forall i \;\; a_i \in I$)

(ii) $\sum_{i=1}^n a_i^4 - \alpha^2 \sum_{j=1}^m b_j^4 \in I \Rightarrow \forall i \;\; a_i \in I$ *et* $\forall j \;\; b_j \in I$.

Par exemple, considérons $\mathbb{R}[X,Y]$; soit (Y) l'idéal engendré par Y. Alors $\mathbb{R}[X,Y]/(Y) = \mathbb{R}[\overline{X}] \simeq \mathbb{R}[X]$, or nous savons que $\mathbb{R}[X]$ est X-chaînable (cf. : $\mathbb{Q}(t)$). Le théorème 1 montrera alors que l'idéal (Y) est un idéal de X-chaîne de $\mathbb{R}[X,Y]$.

Remarquons qu'il peut exister des idéaux réels dans un anneau intègre dont le corps des quotients est chaînable qui ne soient idéal de α-chaîne pour aucun α :

par exemple soit $\mathbb{R}[X]$ et l'idéal réel $(X-a)$, alors $\mathbb{R}[X]/(X-a) \simeq \mathbb{R}$ dont on sait qu'il est non chaînable, donc $(X-a)$ n'est jamais idéal de α-chaîne.

Notons aussi que dans un anneau A intègre, si I est un idéal premier de α-chaîne alors I est un idéal de β-chaîne pour tout $\beta = \pm \alpha a^2$ avec $a \in A \setminus I$.

En effet soit I un idéal de α-chaîne. Supposons $\sum_{i=1}^{n} a_i^4 - \alpha^2 a^4 \sum_{j=1}^{n} b_j^4 \in I$, c'est aussi $\sum_{i=1}^{n} a_i^4 - \alpha^2 \sum_{j=1}^{m} (b_j a)^4 \in I$ et donc nous avons $\forall i \; a_i \in I$ et $\forall j \; b_j a \in I$. Puisque I est premier et $a \notin I$ alors $b_j \in I$ et I est bien un idéal de αa^2-chaîne.

La réciproque est vraie pour a inversible dans A.

Théorème 1

Soit I un idéal premier de A, les propriétés suivantes sont équivalentes :

(1) *I est un idéal de α-chaîne.*

(2) *le corps des quotients de A/I est formellement $\overline{\alpha}$-chaînable.*

Ce théorème est un corollaire immédiat des deux lemmes suivants :

Lemme 1 : *Soit I un idéal premier de A alors I est un idéal de α-chaîne si et seulement si A/I est formellement $\overline{\alpha}$-chaînable.*

Lemme 2 : *Soit B un anneau commutatif intègre avec unité et $\alpha \in B$; alors B est formellement α-chaînable si et seulement si le corps des quotients de B est formellement α-chaînable.*

Démonstration du lemme 1

$\Rightarrow$ Soit I un idéal de α-chaîne. Montrons que A/I est formellement $\overline{\alpha}$-chaînable :

(i) I est un idéal réel donc A/I est formellement réel ;

(ii) On suppose $\sum_{i=1}^{n} \overline{a}_i^4 - \overline{\alpha}^2 \sum_{j=1}^{m} \overline{b}_j^4 = 0$ dans A/I alors

$\sum_{i=1}^{n} a_i^4 - \alpha^2 \sum_{j=1}^{m} b_j^4 \in I$ et I étant un idéal de α-chaîne alors $\forall i \ a_i \in I$ et $\forall j \ b_j \in I$, d'où $\forall i \ \overline{a}_i = 0$ et $\forall j \ \overline{b}_j = 0$.

$\Leftarrow$ Supposons A/I formellement $\overline{\alpha}$-chaînable.

Alors (i) A/I est formellement réel donc I est réel

et (ii) Soit $\sum_{i=1}^{n} a_i^4 - \alpha^2 \sum_{j=1}^{m} b_j^4 \in I$ alors $\sum_{i=1}^{n} \overline{a}_i^4 - \overline{\alpha}^2 \sum_{j=1}^{m} \overline{b}_j^4 = 0$ dans A/I et donc $\forall i \ \overline{a}_i = 0$ et $\forall j \ \overline{b}_j = 0$ d'après l'hypothèse, d'où $\forall i \ a_i \in I$ et $\forall j \ b_j \in I$; I est bien un idéal de α-chaîne. □

Démonstration du lemme 2

$\Leftarrow$ est clair

$\Rightarrow$ Supposons B formellement α-chaînable.

Soit dans q.f.(B), corps des quotients de B , une relation

$$\sum_{i=1}^{n} \left(\frac{a_i}{b_i}\right)^4 - \alpha^2 \sum_{j=1}^{m} \left(\frac{c_j}{d_j}\right)^4 = 0 \quad \text{avec} \quad \forall i \ b_i \neq 0 \quad \text{et} \quad \forall j \ d_j \neq 0$$

alors nous obtenons dans B la relation :

$$\sum_{i=1}^{n} \left(a_i \left(\prod_{j=1}^{m} d_j \prod_{\substack{k=1 \\ k\neq i}}^{n} b_k\right)\right)^4 - \alpha^2 \sum_{j=1}^{m} \left(c_j \left(\prod_{i=1}^{n} b_i \prod_{\substack{k=1 \\ k\neq j}}^{m} d_k\right)\right)^4 = 0 \quad .$$

B étant formellement α-chaînable on en déduit

$$\forall i \quad a_i \left(\prod_{j=1}^{m} d_j \prod_{\substack{k=1 \\ k\neq i}}^{n} b_k\right) = 0$$

$$\forall j \quad c_j \left(\prod_{i=1}^{n} b_i \prod_{\substack{k=1 \\ k\neq j}}^{m} d_k\right) = 0 \quad .$$

Les b et d étant non nuls et B intègre on obtient :

$$\forall i \quad a_i = 0 \quad \text{et} \quad \forall j \quad c_j = 0 \ .$$

Donc q.f.(B) est formellement α-chaînable. □

Remarque 2

Si B *est un anneau intègre avec unité et* q.f.(B) *formellement* α*-chaînable alors* q.f.(B) *est formellement* α'*-chaînable pour un* $\alpha' \in B$.

En effet :

Si $\alpha = \frac{\alpha_1}{\alpha_2}$ avec $\alpha_2 \neq 0$, et q.f.(B) formellement $\frac{\alpha_1}{\alpha_2}$-chaînable.

Soit $\sum_1^n \left(\frac{a_i}{b_i}\right)^4 - \left(\frac{\alpha_1}{\alpha_2}\right)^2 \sum_1^m \left(\frac{c_j}{d_j}\right)^4 = 0$ alors $\forall i \ a_i = 0 \quad \forall j \ c_j = 0$

posons $\alpha' = \alpha_1 \alpha_2^2$ alors si on a une relation $\sum_1^n \left(\frac{a_i}{b_i}\right)^4 - \alpha'^2 \sum_1^m \left(\frac{c_j}{d_j}\right)^4 = 0$

c'est aussi $\alpha_2^4 \sum_1^n \left(\frac{a_i}{b_i}\right)^4 - \alpha'^2 \alpha_2^4 \sum_1^m \left(\frac{c_j}{d_j}\right)^4 = 0$ donc

$$\sum_1^n \left(\frac{a_i \alpha_2}{b_i}\right)^4 - \alpha^2 \sum_1^m \left(\frac{c_j}{d_j}\right)^4 = 0$$ et on obtient $\forall i \ a_i = 0$ et $\forall j \ c_j = 0$,

puisque B est intègre et $\alpha_2 \neq 0$.

II - Le spectre de niveau supérieur d'un anneau

Les anneaux sont toujours supposés commutatifs et avec unité. Pour un anneau A on connaît la notion de spectre réel défini par :

$$\mathrm{Sper}\, A = \{(I,p) \mid I \text{ idéal premier réel de } A \text{ et } p \text{ ordre de } q.f.(A/I)\}$$

Un des théorèmes de l'algèbre réelle donne alors que $\mathrm{Sper}\, A \neq \emptyset$ si et seulement si l'anneau A est semi-réel (i.e. $-1 \notin \Sigma A^2$) si et seulement si ΣA^2 est un préordre.

Nous allons ici poser les définitions permettant d'obtenir un théorème analogue dans le cadre de l'algèbre de chaîne.

Définition 4

Soit A *un anneau et* $\alpha \in A$.

Nous appelerons α-*chaîne-spectre réel de* A

$$\alpha\text{-}\mathrm{Sper}\, A = \{(I\ ,\ (p_i)_{i\in\mathbb{N}}) \mid I \text{ idéal premier de } \alpha\text{-chaîne de } A\ ,\ (p_i)_{i\in\mathbb{N}} \text{ chaîne de } q.f.(A/I) \text{ telle que } \overline{\alpha}^2 \notin p_2\}\ .$$

Définition 5

Soit A *un anneau et* $\alpha \in A$.

Nous appelerons α-*spectre réel de* A

$$\mathrm{Sper}^{\alpha}\, A = \{(I,\ p_2) \mid I \text{ idéal premier de } \alpha\text{-chaîne de } A\ ,\ p_2 \text{ ordre de niveau exact 4 de } q.f.(A/I) \text{ tel que } \overline{\alpha}^2 \notin p_2\}$$

pour la commodité des notations dans les démonstrations nous poserons ainsi :

Définition 6

Soit A *un anneau et* $\alpha \in A$.

Définissons le α-*spectre de* A *par :*

$$\mathrm{Spec}^{\alpha}\, A = \{I \mid I \text{ idéal premier de } \alpha\text{-chaîne de } A\}\ .$$

Les lemmes 3 et 4 suivants résultent immédiatement du théorème 1, du fait que par tout ordre p_2 de niveau 4 il passe une chaîne d'ordres $(p_i)_{i\in\mathbb{N}}$ (voir [H]) et que $\Sigma K^4 = \cap p_2 \cap \Sigma K^2$ (voir [B1] et [H]).

Lemme 3

Soit A *un anneau et* $\alpha \in A$.

$\mathrm{Spec}^{\alpha} A = \{I \mid \text{q.f.}(A/I)$ *admet un ordre* p_2 *de niveau exact 4 tel que* $\bar{\alpha}^2 \notin p_2\}$.

Lemme 4

Les propriétés suivantes sont équivalentes :

(i) α - $\mathrm{Sper}\ A \neq \emptyset$;

(ii) $\mathrm{Sper}^{\alpha}\ A \neq \emptyset$;

(iii) $\mathrm{Spec}^{\alpha}\ A \neq \emptyset$.

Pour l'étude d'une topologie du spectre de niveau supérieur c'est sans doute la notion de α-chaîne-spectre réel qu'il convient de prendre car c'est la plus riche puisqu'il existe une surjection de α-sper A sur Sper^{α} A (qui confond toutes les chaînes passant par un p_2 ordre de niveau 4 tel que $\bar{\alpha}^2 \notin p_2$) et une autre surjection de Sper^{α} A sur Spec^{α} A (qui confond tous les p_2 ordres de niveau 4 tels que $\bar{\alpha}^2 \notin p_2$).
Par contre pour l'étude qui suit la notion de Spec^{α} A est suffisante.
Il nous faut encore introduire deux autres notions correspondant aux notions d'anneau semi-réel et de préordre dans le cas de l'algèbre réelle.

Définition 7a

Soit A *un anneau et* $\alpha \in A$.

Une partie T *de* A *est un* α-*préordre (de niveau* 4*) si et seulement si*

$$T+T \subset T \quad , \qquad T.T \subset T \quad , \quad A^4 \subset T \quad ,$$

$$\forall k \in \mathbb{N} \quad \forall t \in T \quad \alpha^{4k+2}(1+t) \notin T - \alpha^2 T \quad .$$

Définition 8

Un anneau A *sera dit anneau* α-*semi-chaînable*
si $T = \Sigma A^4$ *est un* α-*préordre.*

Enonçons alors le théorème principal de cette partie :

Théorème 2

Les propriétés suivantes sont équivalentes :

(i) A *est* α*-semi-chaînable* ;

(ii) A *admet un* α*-préordre* ;

(iii) $\mathrm{Spec}^{\alpha}\ A \neq \emptyset$. (*ce qui équivaut par le lemme* 4 *à* $\mathrm{Sper}^{\alpha}\ A \neq \emptyset$ *ou à* α - $\mathrm{Sper}\ A \neq \emptyset$) .

(i) $\Rightarrow$ (ii) est clair.

(iii) $\Rightarrow$ (i) Supposons que ΣA^4 ne soit pas un α-préordre. Cela signifie qu'il existe $k \in \mathbb{N}$, $t, t', t'' \in \Sigma A^4$ tels que $\alpha^{4k+2}(1+t) = t' - \alpha^2 t''$.

Soit $I_\alpha \in \mathrm{Spec}^{\alpha} A$; dans $q.f.(A/I_\alpha)$ on obtient la relation

$$\bar{\alpha}^2\, \bar{\alpha}^{4k}(1+\bar{t}) = \bar{t}' - \bar{\alpha}^2 \bar{t}'' .$$

Soit p_2 un ordre de niveau exact 4 de $q.f.(A/I_\alpha)$ tel que $\bar{\alpha}^2 \notin p_2$. Alors automatiquement $-\bar{\alpha}^2 \in p_2$ et donc $\bar{t}' - \bar{\alpha}^2\, \bar{t}'' \in p_2$.
Le facteur $\bar{\alpha}^{4k}(1+\bar{t})$ appartient à $\Sigma\,(q.f.(A/I_\alpha))^4$ et est non nul.
On en déduit $\bar{\alpha}^2 \in p_2$ ce qui est impossible.

(ii) $\Rightarrow$ (iii) résulte immédiatement du lemme 5 ci-dessous qui est l'analogue de la proposition (4.1) de [B2] .

Lemme 5

Soit A *un anneau et* $\alpha \in A$.

Soit $T \subset A$ *tel que* $T+T \subset T$, $T.T \subset T$ *et* $A^4 \subset T$. *les propriétés suivantes sont équivalentes :*

(i) T *est un* α*-préordre ;*

(ii) *il existe* $I_\alpha \in \mathrm{Spec}^{\alpha} A$ *et* p_2 *ordre de niveau exact* 4 *de* $q.f.(A/I_\alpha)$ *tel que* $\bar{\alpha}^2 \notin p_2$ *et* $\bar{T} \subset p_2$ *où*
$\bar{T} = \{\Sigma\, \bar{t} x_t^4 \mid t \in T ,\ x_t \in q.f.(A/I_\alpha)\}$

(ii) $\Rightarrow$ (i) la démonstration est la même que celle de (iii) $\Rightarrow$ (i) du Théorème 2.

(i) $\Rightarrow$ (ii) Nous allons, comme dans le cas de l'algèbre réelle, définir une partie multiplicative S telle que $1 \in S$ et $0 \notin S$, et l'idéal I_α cherché apparaîtra comme un idéal maximal pour la propriété d'être disjoint de S.

Posons :

$$S_{2k+1} = T - \alpha^2 T - \alpha^{4k+2}(1+T) \quad , \quad k \geq 0$$

et $$S_{2k} = T - \alpha^2 T + \alpha^{4k}(1+T) \quad , \quad k \geq 0 \quad .$$

D'après l'hypothèse "T est un α-préordre", $0 \notin S_{2k+1}$; si $0 \in S_{2k}$ alors $0 \in (-\alpha^2) S_{2k}$, or nous avons $(-\alpha^2) S_{2k} \subset S_{2k+1}$, c'est donc impossible.

Soit $\beta = -\alpha^2$ et soit $S_\ell = T + \beta T + \beta^\ell (1+T)$ pour $\ell \geq 0$. Alors en utilisant $\beta^2 \in T$ on montre que $S_\ell \cdot S_m \subset S_{\ell+m}$.

Soit alors $S = \bigcup_{\ell \geq 0} S_\ell$, S est une partie multiplicative telle que $0 \notin S$ et $1 \in S$.

Soit I_α maximal parmi les idéaux I tels que $I \cap S = \emptyset$, I_α est un idéal premier.

Considérons alors $\overline{T} = \{ \Sigma \overline{t} \, x_t^4 \mid t \in T \, , \, x_t \in q.f.(A/I_\alpha) \}$ et montrons d'abord que $\overline{\alpha}^2 \in \overline{T} - \overline{\alpha}^2 \overline{T}$ est impossible.
Supposons donc $\overline{\alpha}^2 \in \overline{T} - \overline{\alpha}^2 \overline{T}$. En supprimant les dénominateurs et en revenant à l'anneau A on obtient l'existence de $r \in A \setminus I_\alpha$, $t, t' \in T$ tels que :

(1) $$r^4 \alpha^2 \equiv t - \alpha^2 t' \bmod I_\alpha \quad .$$

Comme $r \notin I_\alpha$ alors $I_\alpha + (r)$, d'après la maximalité de I_α, doit rencontrer S. Donc il existe $u \in I_\alpha$ et $v \in A$ tels que $u + vr = s \in S$. On en déduit

que $v^4 r^4 \equiv s^4 \bmod I_\alpha$ ce qui montre compte tenu de la relation (1) qu'il existe $s \in S$ et $t_1, t_2 \in T$ tels que

$$(2) \qquad s^4 \alpha^2 \equiv t_1 - \alpha^2 t_2 \bmod I_\alpha \ .$$

Ceci signifie que $t_1 - \alpha^2 t_2 - s^4 \alpha^2 \in I_\alpha$.
Soit k tel que $s^4 \in S_k$ puisque

$S_k = T + \beta T + \beta^k (1+T)$ où $\beta = -\alpha^2$ on obtient

$$t_1 + \beta t_2 + s^4 \beta \in T + \beta T + \beta(T + \beta T + \beta^k(1+T))$$

soit encore puisque $\beta^2 \in T$

$$t_1 + \beta t_2 + s^4 \beta \in T + \beta T + \beta^{k+1} (1+T) \subset S_{k+1} \subset S$$

d'où $t_1 - \alpha^2 t_2 - s^4 \alpha^2 = t_1 + \beta t_2 + s^4 \beta \in I_\alpha \cap S$ ce qui est impossible.

Donc $\overline{\alpha}^2 \notin \overline{T} - \overline{\alpha}^2 \overline{T}$. Il reste à montrer que I_α satisfait les conditions de (ii).
$-1 \notin T$, sinon on aurait $-\overline{\alpha}^2 \in \overline{\alpha}^2 \overline{T}$ et donc $\overline{\alpha}^2 \in -\overline{\alpha}^2 \overline{T} \subset \overline{T} - \overline{\alpha}^2 \overline{T}$ ce qui est impossible.

En particulier $-1 \notin \Sigma(q.f.(A/I_\alpha))^4$ ce qui montre que le corps $q.f.(A/I_\alpha)$ est ordonnable (voir [B1]).

De plus $-1 \notin \overline{T} - \overline{\alpha}^2 \overline{T}$, puisque sinon on en déduirait $\overline{\alpha}^2 \in \overline{T} - \overline{\alpha}^2 \overline{T}$ qui est faux ; ceci montre que $\overline{T} - \overline{\alpha}^2 \overline{T}$ est un préordre propre de niveau exact 4 et donc il existe p_2 un ordre de niveau exact 4 tel que $p_2 \supset \overline{T} - \overline{\alpha}^2 \overline{T}$.

Enfin cet ordre p_2 est bien tel que $\overline{\alpha}^2 \notin p_2$: d'abord $\overline{\alpha}^2 \neq 0$ puisque $\overline{\alpha}^2 \notin \overline{T} - \overline{\alpha}^2 \overline{T}$ ensuite puisque $-\overline{\alpha}^2 \in p_2$, $\overline{\alpha}^2$ ne peut appartenir à p_2 qui est un ordre.

L'idéal I_α est donc bien un idéal premier réel tel que $q.f.(A/I_\alpha)$ admette un ordre p_2 de niveau exact 4 tel que $\overline{\alpha}^2 \notin p_2$ (ce qui montre que $I_\alpha \in \mathrm{Spec}^\alpha A$) et tel que $\overline{T} \subset p_2$. □

Notons que la définition 7a est remplaçable par la définition 7b donnée ci-dessous.

Définition 7b :

Soit A *un anneau et* $\alpha \in A$.

Une partie T *de* A *est un* α*-préordre (de niveau 4) si et seulement si*

$$T + T \subset T \ , \ T.T \subset T \ , \ A^4 \subset T \ ,$$

$$\forall k \in \mathbf{N} \quad \alpha^{4k+2} \notin T - \alpha^2 T \quad .$$

Les définitions 7a et 7b sont équivalentes car si $\alpha^{4k+2}(1+t) = t_1 - \alpha^2 t_2$ (t, t_1, t_2 dans T) alors $\alpha^{4k+2} = t_1 - \alpha^2(t_2 + \alpha^{4k}t) = t_1 - \alpha^2 t_3$ où $t_3 = (t_2 + \alpha^{4k}t)$ est clairement dans T .

De même si $\alpha^{4k+2} = t' - \alpha^2 t''$ (avec t' et t'' dans T), soit $t \in T$ alors

$$\alpha^{4k+2}(1+t) = (t' - \alpha^2 t'')(1+t) = t_1 - \alpha^2 t_2$$

avec $t_1 = t'(1+t)$ et $t_2 = t''(1+t)$ qui appartiennent bien à T .

Une conversation avec R. Berr (Septembre 88) nous a conduit à ajouter une définition dans le cas où α est inversible, car la définition 7b de l'α-préordre peut alors prendre une autre forme :

Définition 7c

Soit A *un anneau et* $\alpha \in A$ *un élément inversible de* A . *Une partie* T *de* A *est un* α*-préordre (de niveau 4) si et seulement si :*

$$T + T \subset T \ , \ T.T \subset T \ , \ A^4 \subset T \ , \ -1 \notin T - \alpha^2 T \quad .$$

C'est clair car $\alpha^{4k+2} \notin T - \alpha^2 T$ est équivalent dans ce cas à $\alpha^2 \notin T - \alpha^2 T$ et donc à $-1 \notin T - \alpha^2 T$.

Remarque 3

La condition $-1 \notin T - \alpha^2 T$ de la définition 7c ne saurait convenir dans tous les cas. En effet si α est nilpotent, $\alpha^4 = 0$ par exemple, $T \subset A$ tel que $T \neq T \subset T$, $A^4 \subset T$ ne satisfait pas $\forall k \quad \alpha^{4k+2} \notin T - \alpha^2 T$ mais satisfait $-1 \notin T - \alpha^2 T$ dès que $-1 \notin T$.

En effet si $-1 = t - \alpha^2 t'$ alors $1 + t = \alpha^2 t'$ et donc $(1+t)^2 = \alpha^4 t'^2 = 0$; d'où $-1 = 2t + t^2 \in T$.

III - L'α-chaîne radical d'un idéal

Il paraît alors naturel d'introduire la définition suivante :

Définition 9

Soit A *un anneau commutatif avec unité et* $\alpha \in A$.

Soit I *un idéal de* A .

On appelle α*-chaîne radical de* I , *l'intersection des idéaux premiers de* α*-chaîne le contenant :*

$$\sqrt[\alpha]{I} = \bigcap_{\substack{I \subset I_\alpha \\ I_\alpha \in \mathrm{Spec}^\alpha}} I_\alpha$$

D'une manière analogue à la proposition 4.3 de [B2] nous utilisons le lemme 5 pour obtenir une description de l'α-chaîne radical d'un idéal.

Théorème 3

Soit A *un anneau commutatif avec unité et* $\alpha \in A$. *Soit* I *un idéal de* A

$$\sqrt[\alpha]{I} = \{f \in A \mid \exists k \in \mathbb{N}\ ,\ \exists t, t', t'' \in \Sigma A^4 \text{ tels que } \alpha^{4k}(f^{4k} + t) + t' - \alpha^2 t'' \in I\}$$

Désignons par $J = \{f \in A \mid \exists k \in \mathbb{N}\ ,\ \exists t, t', t'' \in \Sigma A^4$ tels que $\alpha^{4k}(f^{4k} + t) + t' - \alpha^2 t'' \in I\}$.

On démontre successivement les deux inclusions.

$J \subset \sqrt[\alpha]{I}$.

Soit $I_\alpha \in \mathrm{Spec}^\alpha A$ tel que $I_\alpha \supset I$, nous allons montrer que $f \in I_\alpha$.

En utilisant l'hypothèse sur f, $\alpha^{4k}(f^{4k} + t) + t' - \alpha^2 t'' \in I$ et en multipliant par α^2 on obtient que $\alpha^2 . \alpha^{4k}(f^{4k} + t) + \alpha^2 t' - \alpha^4 t'' \in I$.

Supposons que $f \notin I_\alpha$, alors puisque $\bar{\alpha} \neq 0$ dans A/I_α et que $I \subset I_\alpha$ on obtient

$$\bar{\alpha}^2 \in \Sigma(\mathrm{q.f.}(A/I_\alpha))^4 - \bar{\alpha}^2\ \Sigma(\mathrm{q.f.}(A/I_\alpha))^4$$

ce qui contredit le fait que $\mathrm{q.f.}(A/I_\alpha)$ est $\bar{\alpha}$-chaînable.

$\sqrt[\alpha]{I} \subset J$.

En passant à A/I on peut supposer $I = 0$.

Soit $f \in \sqrt[\alpha]{I}$. Si f est nilpotent alors $f^{4k} = 0$ pour un certain k et donc f appartient bien à J .

Supposons maintenant que f ne soit pas nilpotent et considérons l'anneau A_f .

Supposons que A_f est α-semi-chaînable, alors par le théorème 2, nous pouvons trouver un idéal $I_\alpha \in \mathrm{Spec}^\alpha A_f$. La trace $I_\alpha \cap A$ appartient à $\mathrm{Spec}^\alpha A$ et pourtant $f \notin I_\alpha$, c'est donc impossible.

L'anneau A_f n'est donc pas α-semi-chaînable ce qui signifie que ΣA_f^4 n'est pas un α-préordre et donc qu'il existe une relation

$$\alpha^{4k+2} \left(1 + \frac{t}{f^{4\ell}}\right) = \frac{t' - \alpha^2 t''}{f^{4m}}$$

où $k, \ell, m \in \mathbb{N}$ et $t, t', t'' \in \Sigma A^4$.

Revenant à l'anneau A , en multipliant par α^2 et si nécessaire par les puissances convenables de α^4 et f^4 , on obtient une expression du type

$$\alpha^{4k} (f^{4k} + t) + t' - \alpha^2 t'' = 0 \quad \text{avec}$$

$k \in \mathbb{N}$ et $t, t', t'' \in \Sigma A^4$, ce qui signifie que $f \in J$. □

Remarque 4

Dans le cas où $\alpha \in A$ est inversible, l'expression du radical donnée au théorème 3 devient :

$$\sqrt[\alpha]{I} = \{f \in A \mid \exists k \in \mathbb{N} , \exists t , t' \in \Sigma A^4 \text{ tels que } f^{4k} + t - \alpha^2 t' \in I\} \quad .$$

Il est connu qu'un idéal est réel si et seulement si il est égal à son radical réel. Nous pouvons ici obtenir un résultat analogue avec les définitions que nous avons données :

Théorème 4 :

Soit I *un idéal d'un anneau commutatif* A ; *alors sont équivalentes les propriétés :*

(1) I *est un idéal de* α*-chaîne* ;

(2) $I = \sqrt[\alpha]{I}$.

La démonstration utilise le lemme suivant :

Lemme 6 : *Soit* $\mathfrak{p}$ *un idéal de* A . .

Alors $\mathfrak{p}$ *est un idéal de* α*-chaîne si et seulement si* $\mathfrak{p} = \bigcap_i \mathfrak{p}_i$ *où les* $\mathfrak{p}_i$ *sont des idéaux premiers de* α*-chaîne.*

⇒ La propriété de $\mathfrak{p}$ d'être un idéal de α-chaîne entraîne que $\mathfrak{p}$ est un idéal réel et donc que $\mathfrak{p} = \bigcap_i \mathfrak{p}_i$ avec $\mathfrak{p}_i$ idéaux premiers réels. Montrons que ces idéaux premiers $\mathfrak{p}_i$ vérifient aussi la propriété (ii) des idéaux de α-chaîne (Nous supposons la représentation $\mathfrak{p} = \bigcap_i \mathfrak{p}_i$ minimale).

Supposons que :

$$\left(\sum_1^m a_k^4 - \alpha^2 \sum_1^q b_\ell^4\right) \in \mathfrak{p}_i \quad .$$

Soit $h \in \bigcap_{j \neq i} \mathfrak{p}_j$ et $h \notin \mathfrak{p}_i$ on forme $h^4\left(\sum_1^m a_k^4 - \alpha^2 \sum_1^q b_\ell^4\right)$ ceci est dans $\mathfrak{p}_i$ comme la parenthèse et aussi dans $\bigcap_{j \neq i} \mathfrak{p}_j$ comme h .

Donc $\sum_{1}^{m} (h\, a_k)^4 - \alpha^2 \sum_{1}^{q} (h\, b_\ell)^4 \in \bigcap_i \mathfrak{p}_i = \mathfrak{p}$. Puisque $\mathfrak{p}$ est un idéal de α-chaîne alors chaque $h\, a_k$ et $h\, b_\ell$ est dans $\mathfrak{p}$.

Mais

$\forall k \quad h\, a_k \in \mathfrak{p} = \bigcap_i \mathfrak{p}_i$ avec $h \notin \mathfrak{p}_i \Rightarrow a_k \in \mathfrak{p}_i$

$\forall \ell \quad h\, b_\ell \in \mathfrak{p} = \bigcap_i \mathfrak{p}_i$ " " $\Rightarrow b_\ell \in \mathfrak{p}_i$.

$\mathfrak{p}_i$ est donc bien un idéal de α-chaîne.

$\Leftarrow$ La réciproque est évidente. □

Le théorème 4 résulte alors de la définition 9 et du lemme 6.

IV - Un Nullstellensatz pour certains corps chaîne-clos

Nous savons que si K est un corps réel clos il existe un Nullstellensatz réel qui affirme que le radical réel d'un idéal I est égal à $J(V(I))$ où nous utilisons les notations classiques : $V(I) = \{\overline{x} \in K^n , \forall f \in I \ f(\overline{x}) = 0\}$ est la variété de K^n définie par l'idéal I et $J(W) = \{f \in K[\overline{X}], \forall \overline{x} \in W \ f(\overline{x}) = 0\}$ est l'idéal des polynômes s'annulant sur le sous-ensemble W de K^n .

Afin de pouvoir obtenir sur les corps chaîne-clos un analogue du Nullstellensatz sur les corps réel-clos, on peut aussi retrouver la notion de α-chaîne radical d'un idéal en suivant la méthode générale indiquée par Cherlin dans [C] .

Définition 10 :

Soit K *un corps* α*-chaînable et soit* I *un idéal de* $K[\overline{X}]$. *La* α*-chaîne radical de* I *est défini par*

$$\sqrt[\alpha]{I} = \bigcap_{\mathfrak{p} \in P} \mathfrak{p} \quad \text{où}$$

$P = \{\mathfrak{p}, \mathfrak{p}$ *idéal premier de* $K[\overline{X}]$, $\mathfrak{p} \supset I$ *et* $K[\overline{X}]/\mathfrak{p}$ *est plongeable dans un corps* α*-chaînable*$\}$.

Théorème 5 :

Soit I *un idéal de* $K[\overline{X}]$ *où* K *est un corps* α*-chaînable alors*

$$\sqrt[\alpha]{I} = \bigcap_{\mathfrak{p} \in Q} \mathfrak{p} \quad \text{où}$$

$Q = \{\mathfrak{p}$, $\mathfrak{p}$ *idéal premier de* $K[\overline{X}]$, $\mathfrak{p} \supset I$ *et* $\mathfrak{p}$ *est un idéal de* α*-chaîne*$\}$.

Ce théorème montre bien qu'il s'agit de la même notion d'α-chaîne radical d'un idéal que celle définie en III-9.

Démonstration :

$$K \subset K[\overline{X}]/\mathfrak{p} \subset q.f.(K[\overline{X}]/\mathfrak{p})$$

on sait que $q.f.(K[\overline{X}]/\mathfrak{p})$ est (formellement) α-chaînable ssi $K[\overline{X}]/\mathfrak{p}$ est formellement α-chaînable (lemme 2), donc si et seulement si l'idéal $\mathfrak{p}$ (qui est premier par hypothèse) est un idéal de α-chaîne (théorème 1). □

Rappelons également qu'un corps chaîne-clos K est un corps admettant une seule chaîne d'ordres de niveau supérieur $(p_i)_{i\in\mathbb{N}}$ et tel que $(K, (p_i)_{i\in\mathbb{N}})$ n'admette pas d'extension algébrique fidèle (on dit que $(L, (\overline{p}_i)_{i\in\mathbb{N}})$ est une extension fidèle de $(K, (p_i)_{i\in\mathbb{N}})$ si $(\overline{p}_i)_{i\in\mathbb{N}}$ est une chaîne d'ordres de niveau supérieur de L et si pour tout $i\in\mathbb{N}$ $\overline{p}_i \cap K = p_i$).

Dans [G1] et [G2] nous avons montré qu'un corps K chaîne-clos était caractérisé par : K ordonnable et pythagoricien, tel que tout polynôme de degré impair a une racine dans K et il existe $\alpha \in K$ satisfaisant $\alpha^2 \notin \Sigma K^4$ et $K = K^2 \cup -K^2 \cup \alpha K^2 \cup -\alpha K^2$.

Enfin dans [D-G] écrit en collaboration avec F. Delon, nous avons démontré le résultat suivant que nous allons utiliser pour obtenir le théorème 6 :

Proposition 2

Soit K *et* L *deux corps chaîne-clos* α*-chaînables. Supposons que* K *n'admette qu'une seule valuation hensélienne à corps des restes réel clos, alors* $K \prec L$.

F. Delon ayant remarqué que le Nullstellensatz général donné par Cherlin pouvait s'appliquer dès que l'on avait une inclusion élémentaire, voir [D] (proposition 3 ci-dessous), les définitions et résultats précédents permettent alors d'obtenir :

Théorème 6 (Nullstellensatz)

Soit K *un corps chaîne-clos* α*-chaînable ayant une seule valuation hensélienne à corps des restes réel-clos. Soit* I *un idéal de* $K[\overline{X}]$ *alors*

$$J(V(I)) = \sqrt[\alpha]{I}$$

où nous notons toujours :

$$V(I) = \{\overline{x} \in K^n \ , \ \forall f \in I \quad f(\overline{x}) = 0\}$$

$$J(W) = \{f \in K[\overline{X}] \ , \ \forall \overline{x} \in W \quad f(\overline{x}) = 0\} \ .$$

Le théorème résulte du Nullstellensatz général de Cherlin (proposition 3 ci-dessous) et des définitions et résultats précédents.

Proposition 3 (d'après [D])

Soit K *un corps quelconque,* T *sa théorie dans le langage des anneaux plus éventuellement un nombre fini de constantes.*

Pour un idéal I *de* $K[\overline{X}]$ *on définit :*

$$T\text{-}Radical\ (I) = \bigcap_{\mathscr{P}} \mathfrak{p} \quad où$$

$\mathscr{P} = \{\mathfrak{p}$ *idéal premier de* $K[\overline{X}]$, $\mathfrak{p} \supset I$ *et* $K[\overline{X}]/\mathfrak{p}$ *se plonge dans un modèle* L *de* T *avec* $K \prec L\}$.

Alors $J(V(I)) = T\text{-}Radical\ (I)$.

Démonstration du théorème 6 :

En effet $K[\overline{X}]/I$, avec I idéal premier de α-chaîne, peut se plonger dans un corps L chaîne-clos α-chaînable tel que $K \prec L$ car nous avons :

$$K \subset K[\overline{X}]/I \subset qf.(K[\overline{X}]/I) \quad ;$$

$qf.(K[\bar{X}]/I)$ étant (formellement) α-chaînable, il existe une chaîne d'ordres de niveau supérieur $(p_i)_{i\in\mathbb{N}}$ telle que $\alpha^2 \notin p_2$. Soit alors L la clôture de chaîne de ce corps pour la chaîne fixée, L est un corps chaîne-clos α-chaînable. Si nous supposons de plus que K n'admet qu'une seule valuation hensélienne à corps des restes réel clos nous obtenons $K \prec L$ (grâce à la proposition 2). □

Remarque 5

L'hypothèse faite sur le corps K chaîne-clos que celui-ci n'admet qu'une seule valuation hensélienne à corps des restes réel-clos équivaut au fait que K n'admet qu'une seule valuation hensélienne à corps des restes réel-clos avec groupe des valeurs impair-divisible et $|vK/2vK| = 2$.

Cette condition peut donc aussi être vue comme $A(p_2) = O(p_2)$ où $A(p_2)$ désigne l'anneau de Becker et $O(p_2)$ l'anneau de Jacob, le premier correspondant à la plus fine des valuations ayant les propriétés énoncées ci-dessus et le second à la plus grossière de ces valuations (voir [B3I]).

En combinant le théorème 3 et le théorème 6 modifié par la remarque 4, nous pouvons obtenir un Nullstellensatz plus descriptif sous la forme du théorème 7 donné ci-dessous :

Théorème 7

Soit K *un corps chaîne-clos* α*-chaînable tel que* $A(p_2) = O(p_2)$. *Alors pour tout idéal* I *de* $K[X_1, \ldots, X_n]$ $n \geq 1$

$$\mathcal{I}(V(I)) = \{f \in K[X_1, \ldots, X_n] \mid \exists k \in \mathbb{N}, \exists t, t' \in \Sigma (K[X_1, \ldots, X_n])^4$$

tels que $f^{4k} + t - \alpha^2 t' \in I\}$.

Remarque 6

Pour un autre Nullstellensatz (sur les corps réels clos généralisés) on pourra consulter [B-J].

V - La validité du Nullstellensatz

Nous montrons ici que les énoncés du Nullstellensatz donnés dans la partie précédente aux théorèmes 6 et 7 peuvent être généralisés à un corps chaîne-clos quelconque dans le cas d'une seule variable et ne peuvent être améliorés pour plus de variables.

Théorème 8

Soit K *un corps chaîne-clos* α*-chaînable ;*

Soit I *un idéal de* $K[X_1]$; *alors*

$$\mathcal{I}(V(I)) = \sqrt[\alpha]{I} \quad .$$

De $\sqrt[\alpha]{I} = \bigcap_{I \subset I_\alpha} I_\alpha$ $\quad I_\alpha \in \mathrm{Spec}^\alpha K[X_1]$ et de $\mathcal{I}(V(I)) = \bigcap_{K[X_1]/\mathcal{M} = K} \mathcal{M}$.

On déduit puisque de tels $\mathcal{M}$ sont dans $\mathrm{Spec}^\alpha K[X_1]$ que

$$\mathcal{I}(V(I)) \supset \sqrt[\alpha]{I} \quad .$$

Mais dans le cas de $n = 1$, $K[X_1]/I_\alpha$ est une extension finie α-chaînable du corps K .

K étant chaîne-clos on a $K[X_1] / I_\alpha = K$ pour tout $I_\alpha \in \mathrm{Spec}^\alpha K[X_1]$.

Théorème 9

Soit K *un corps chaîne-clos tel que* $A(p_2) \neq O(p_2)$, *où* $A(p_2)$ *désigne l'anneau de Becker et* $O(p_2)$ *celui de Jacob (voir* [B3]*) ;*

Alors le Nullstellensatz $\mathcal{I}(V(I)) = \sqrt[\alpha]{I}$ *n'est pas vérifié dans* $K[X_1, \ldots, X_n]$ *pour* $n \geq 2$.

La condition $A(p_2) \neq O(p_2)$ est équivalente au fait que le groupe des valeurs Γ de la valuation v correspondant à $A(p_2)$ admet un sous groupe convexe divisible non trivial. Notons Δ le sous groupe convexe divisible maximal de Γ .

D'après l'hypothèse on peut trouver t tel que $v(t) > 0$ et $v(t) \in \Delta$.

Considérons le polynôme $f(X) = (1+X^2)(t^2+X^2)$. Montrons que pour tout $x \in K$, $f(x) \in K^{\star 4}$. Il est clair que $f(x) \neq 0$.

Si $v(x) < 0$ alors $f(x) = x^4.\varepsilon$ avec $v(\varepsilon) = 0$; ε est alors une puissance quatrième puisque la valuation v est hensélienne avec corps des restes réel-clos ; donc si $v(x) < 0$ alors $f(x) \in K^{\star 4}$.

Si $0 < v(t) \leqslant v(x)$, alors $f(x) = t^2.\varepsilon_1 . (1 + (xt^{-1})^2)$. Le dernier facteur est une unité et une somme de carrés, c'est donc une puissance quatrième.

Puisque $v(t) \in 2\Gamma$, alors $t = \varepsilon_2 x^2$ où ε_2 est une unité, donc $t^2 = \varepsilon_2^2 x^4 \in K^{\star 4}$ et donc dans ce cas encore $f(x) \in K^{\star 4}$.

Il reste le cas $0 < v(x) < v(t)$. Alors $f(x) = x^2.\varepsilon$ avec ε une unité.

Puisque Δ est convexe nous avons $v(x) \in \Delta \subset 2\Gamma$ et donc, comme pour t ci-dessus $x^2 \in K^{\star 4}$, d'où encore $f(x) \in K^{\star 4}$.

Comme conséquence du fait que pour tout $x \in K$, $f(x) \in K^{\star 4}$ nous obtenons que le polynôme $g(X,Y) = (1+X^2)(t^2+X^2) - \alpha^2 Y^4$ n'admet pas de zéro dans K^2 (puisque $\alpha^2 \notin K^4$ le corps K étant chaîne-clos α-chaînable).

Supposons que l'on ait $\mathscr{T}(V(I)) = \sqrt[\alpha]{I}$ alors on pourrait trouver une identité

$$\alpha^{4k}(1+t_1) + t_2 - \alpha^2 t_3 = h.g$$ où les

$t_i \in \Sigma(K[X,Y])^4$, $h \in K[X,Y]$ et $k \in \mathbb{N}$.

Supposons maintenant que g admette un zéro $(a,b) \in L^2$, avec L extension ordonnable de K . Alors, puisque $t_3(a,b) \neq 0$ on obtient que $\alpha^2 \in \Sigma L^4$.

Il nous suffit alors de construire un corps $L \supset K$ tel que $\alpha^2 \notin \Sigma L^4$ et que g admette un zéro sur L , pour montrer que le Nullstellensatz n'est pas valable.

Pour cela étendons la valuation v à $K(X)$ en posant

$$\omega(\Sigma a_j X^j) = \min_j \{(v(a_j), j)\} \in \Gamma \times \mathbb{Z}$$

avec $\mathbb{Z}$ le plus petit facteur.

Puisque $v(\alpha) + 2\Gamma$ engendre $\Gamma/2\Gamma$ on trouve

$$\Gamma \times \mathbb{Z} \,/\, 4(\Gamma \times \mathbb{Z}) = < \omega(X\,\alpha^{-1}) > \times < \omega(\alpha) > .$$

Alors il existe un caractère $\eta : \Gamma \times \mathbb{Z}/4(\Gamma \times \mathbb{Z}) \twoheadrightarrow \mu(4)$ tel que $\eta\omega(X\,\alpha^{-1}) = 1$ et $\eta\omega(\alpha) = i$.

Ceci entraîne l'existence d'un ordre $p' \subset K(X)$ tel que $X\,\alpha^{-1} \in p'$, $-\alpha^2 \in p'$, et le niveau exact de p' est 4 .

Considérons maintenant une clôture réelle $(L, \tilde{p})$ de $(K(X), p')$.

Puisque $0 < \omega(X) < \omega(t)$ nous obtenons

$$f(X) = X^2 . \varepsilon = X^2 . u^4 \quad \text{avec} \quad u \in L .$$

De $(X\,\alpha^{-1})^2 \in \tilde{p} \cap L^2 = L^4$ on déduit que $f(X) = \alpha^2 . v^4$ avec $v \in L$.

Le polynôme $g(X,Y)$ admet alors le zéro (X,v) sur L .
De plus puisque $-\alpha^2 \in \tilde{p}$, alors $\alpha^2 \notin \Sigma L^4$.
Ceci termine la démonstration et montre que le Nullstellensatz n'est pas valable dès que $A(p_2) \neq 0(p_2)$. □

BIBLIOGRAPHIE

[B1] E. Becker :*"Hereditarily pythagorean fields and orderings of higher types"*, I.M.P.A., Lectures Notes # 29 (1978), Rio de Janeiro.

[B2] E. Becker :*"On the real spectrum of a ring and its application to semialgebraic geometry"*, Bull A.M.S., 15 (1986), pp. 19-60.

[B3] E. Becker :*"Extended Artin-Schreier theory of fields"*, Rocky Mountain Journal of Mathematics, vol 14, # 4, Fall 1984.

[B-J] E.Becker et B.Jacob :*"Rational points on algebraic varieties over a generalized real closed field : a model theoretic approach"*, J. für die reine und angew.Math., 357, 1985, pp.77-95.

[C] G.Cherlin :*"Model Theoretic Algebra. Selected Topics"*, Lectures Notes in Mathematics 521, Springer-Verlag, 1976.

[D] F.Delon :*"Théorème général des zéros d'après McKenna"*, in Séminaire D.D.G., 1985-86, Université Paris 7.

[D-G] F. Delon et D. Gondard :*"17ème problème de Hilbert au niveau n dans les corps chaîne-clos"*, Séminaire (D.D.G.) 1986-87, Université Paris VII ; Soumis J.S.L..

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

[G2] D. Gondard :*"Axiomatisations à la Artin-Schreier des théories des corps chaînables et des corps chaîne-clos"*, in Séminaire D.D.G., 1986-87, Université Paris 7.

[G3] D. Gondard :*"Foundations of chain algebra and chain closed fields"*, Abstracts A.M.S., # 56, vol. 9, n° 2, Mars 1988.

[G4] D. Gondard :*"Fields with chains : axiomatizations, algebra, Hilbert's 17th problem and Nullstellensatz"*, Abstract for the Logic Colloquium 87 (Granada July 1987), to be published in J.S.L..

[G5] D. Gondard :"*Foundations of chain algebra and a Nullstellensatz*", à paraître in proceedings de la Journée de l'Association Française d'Algèbre ordonnée (Le Mans 30-11-1987)

[H] J. Harman :"*Chains of higher level orderings*", Contemporary Mathematics, vol. 8, 1982, pp. 141-174, A.M.S..

[J] B. Jacob :"*The model theory of generalized real closed fields*", J. für die reine und ang. Mathematik, 323 (1981), pp.213-220.

[L] T. Y. Lam :"*An introduction to real algebra*", Rocky Mountain Journal of Mathematics, vol. 14, Fall 1984, pp.767-814.

[R] J.J. Risler :"*Une caractérisation des idéaux des variétés algébriques réelles*", C.R.A.S. Paris, t.271, 1970, série A,pp. 1171-1173.

[S] C. Saliba :"*Pour une classification des différentes formes de théorème des zéros et de théorème des éléments positifs*", Thèse de 3ème cycle, 1983, Université de Rennes I.

COUPLES D'ORDRES CHAÎNABLES

M. A. DICKMANN
CNRS – Université Paris VII

RESUMÉ. Dans cet exposé nous abordons les questions suivantes:

(1) Premièrement, nous nous demandons quelles sont les paires d'ordres P_0, P_1 sur le corps k(X) des fonctions rationnelles à une variable et coefficients dans un corps ordonné $<k, \leq>$ qui constituent le début d'une *chaîne* d'ordres de niveau supérieur sur k(X) (dans le sens de Harman [3]); on suppose, sans perte de généralité, que P_0, P_1 prolongent l'ordre $\leq$ sur k.

L'étude de cette situation a pour objectif de maîtriser un certain nombre d'exemples simples. Pour certains corps k il est possible de determiner toutes les paires de tels ordres en exploitant la connaissance de toutes les valuations sur k(X); c'est, notamment, le cas lorsque k n'admet pas de valuation réelle non–triviale, p. ex., lorsque k est archimédien.

Notons qu'une paire d'ordres totaux P_0, P_1 sur K est *chaînable* —i.e., le début d'une chaîne sur K— ssi il existe une valuation v sur K avec les propriétés suivantes:
(i) v est compatible avec P_0 et P_1, i.e., $1 + M_v \subseteq P_0 \cap P_1$;
(ii) $\overline{A_v \cap P_0} = \overline{A_v \cap P_1}$ et ceci est un ordre total sur le corps résiduel $\overline{A_v}$.

En utilisant ce critère nous avons:

Exemple et Proposition 1. ($k \subseteq \mathbb{R}$). *Une paire d'ordres P_0, P_1 sur k(X) est chaînable ssi ils ont l'une des formes suivantes:*
—$P_0 = P_{a+}$, $P_1 = P_{a-}$, avec $a \in \bar{k}$ (= clôture réelle de $<k, \leq>$), où P_{a+} (resp. P_{a-}) désigne la restriction à k(X) de l'ordre sur $\bar{k}(X)$ qui rend X infinitésimalement proche à droite (resp. à gauche) de a, c'est–à–dire, l'ordre tel que $a < X < b$ (resp. $b < X < a$) pour tout $b \in \bar{k}$, $a < b$ (resp. $b < a$).;
—$P_0 = P_{+\infty}$, $P_1 = P_{-\infty}$, où $P_{+\infty}$ (resp. $P_{-\infty}$) désigne l'ordre sur k(X) qui rend X plus grand (resp. plus petit) que tous les éléments de k. □

Remarquez la "symétrie" des paires d'ordres chaînables dans ce cas. La méthode utilisée permet également de traiter certains cas où k n'est pas forcément archimédien. La situation se complique rapidement dès que l'on considère d'autres corps de coefficients k, à cause de l'excessive complexité de l'ensemble des ordres, voire l'ensemble des valuations, de k(X). Pour information, le lecteur peut consulter la discussion informelle du cas $\mathbb{R}(X, Y)$ contenue dans Brumfiel [2; §8.12].

(2) Deuxième question abordée dans cet exposé. Existe–t–il une description explicite et relativement simple —ne serait–ce que dans certains cas— des ordres de niveau supérieur qui forment la (ou les) chaîne(s) d'un corps K commençant par deux ordres donnés P_0, P_1?. Plus précisément, nous cherchons une construction en termes de P_0, P_1, et de l'une des valuations v vérifiant le critère de chaînabilité ci–dessus.

Dans le contexte des ordres de niveau supérieur, Becker [1; pp. 23–25] donne une construction de ce type pour le cas plus général; mais, justement à cause de sa généralité, cette construction paraît peu maniable dans des cas concrets.

Remarquons, en passant, que l'ensemble $\mathscr{V}^*(K) = \mathscr{V}^*(K, P_0, P_1)$ des valuations ayant les propriétés (i) et (ii) ci–dessus est totalement ordonné par la relation d'inclusion de leurs anneaux de valuation; si $\mathscr{V}^*(K) \neq \phi$, il a un premier et un dernier élément.

Dans le cas où l'ensemble $\mathscr{V}^*(K)$ possède une valuation v telle que $|\Gamma_v/_{2\Gamma_v}| = 2$, où Γ_v désigne le groupe de valeurs de v, on obtient une caractérisation assez "parlante". [Notez que la condition $|\Gamma_v/_{2\Gamma_v}| = 2$ est vérifiée par un $v \in \mathscr{V}^*(K)$ ssi elle est vérifiée par la valuation d'anneau maximal dans $\mathscr{V}^*(K)$.]

Proposition 2. *Soient P_0, P_1 des ordres totaux sur un corps K et $v \in \mathscr{V}^*(K)$. Désignons par U_v^+ l'ensemble des unités (résiduellement) positives de v, $U_v^+ = \{x \in K \mid v(x) = 0 \text{ et } \bar{x} \gneq_{\bar{P}} 0\}$, où P désigne l'ordre résiduel $\overline{A_v \cap P_0}$ $(= \overline{A_v \cap P_1})$. Soit $a \in P_0 \cap -P_1$ un élément quelconque. Pour $n \geq 2$, posons:*

$$P_n = (P_0 \cap P_1)^{2^{n-1}} U_v^+ \cup -a^{2^{n-1}} (P_0 \cap P_1)^{2^{n-1}} U_v^+.$$

Alors, on a:

(i) P_n est un préordre propre de niveau exact n (cf. Becker [1; pp. 1 et 5]); *P_n ne dépend pas du choix de l'élément a dans $P_0 \cap P_1$.*

(ii) $\{P_n\}_{n\in\omega}$ *est une chaîne de K ssi* $|\Gamma_v/2\Gamma_v| = 2$; *la même chaîne est obtenue en augmentant la valuation v dans* $\mathcal{V}^*(K)$.

(iii) La valuation v est compatible avec tout P_n, *et résiduellement on a* $\overline{A_v \cap P_n} = \overline{A_v \cap P_0}$ *pour* $n \geq 1$.

(iv) Réciproquement, si $\{P_0, P_1, Q_n\}_{n\geq 2}$ *est une chaîne de K commençant par* P_0, P_1 *telle qu'il existe une valuation* $w \in \mathcal{V}^*(K)$ *compatible avec tous les* Q_n, *avec* $|\Gamma_w/2\Gamma_w| = 2$, *et telle que* $\overline{Q_n \cap A_w} = \overline{P_0 \cap A_w}$ *pour tout* $n \geq 2$, *alors* $Q_n = P_n$ *pour* $n \geq 2$. □

Pour les corps de Pasch (ou corps SAP) les préordres P_n définis ci–dessus constituent une chaîne quels que soient les ordres chaînables P_0, P_1 et la valuation $v \in \mathcal{V}^*(K)$, et toute chaîne est de cette forme; cf. Becker [1; Thm. 17, p. 41].

Références.

[1] Becker, E., **Hereditarily–pythagorean fields and orderings of higher level**, Monografias de Matemàtica 29, IMPA, Rio de Janeiro, 1978.

[2] Brumfiel, G. W., **Partially ordered rings and semi–algebraic geometry**, London Math. Soc. Lecture Notes 37, 1979.

[3] Harman, J., Chain of higher level orderings, in **Ordered fields and real algebraic geometry** (D. W. Dubois and T. Recio, eds.), Contemporary Maths. 8, Amer. Math. Soc., 1982, pp. 141–174.

A remark on the classification problem for ordered structures

Salma Kuhlmann

1 Introduction

In [H], Hausdorff introduces the notion of an η_α-set: let $\kappa = \aleph_\alpha$ be an infinite cardinal and A a linear ordering; A is an *η_α-set* (or: is *κ-dense*) if given A_1 and A_2 subsets of A s.t. $A_1 < A_2$ and $\text{card}(A_i) < \aleph_\alpha$ for $i = 1, 2$, then there exists $a \in A$ s.t. $A_1 < a < A_2$. For example A is a DLOWEP (dense linear ordering without endpoints) iff A is an $\aleph_0$-set. Hausdorff also proves that: two η_α-sets of power $\aleph_\alpha$ are isomorphic.

The Hausdorff η_α-sets were later on examined in the context of ordered algebraic structures: Erdös, Gillman and Henriksen prove in 1955 that for $\alpha > 0$, any two RCF (real closed fields) that are η_α-sets of power $\aleph_\alpha$ are isomorphic (c.f. [E-G-H]), and in 1960, Alling proves the corresponding result for DOAG (divisible ordered Abelian groups): for $\alpha > 0$, any two DOAG that are η_α-sets of power $\aleph_\alpha$ are isomorphic (c.f. [ALL 1]). In their article, Erdös, Gillman and Henriksen ask the following question: what are the possible invariants characterizing a real closed field? Does the order type determine the RCF up to isomorphism?

In the next section, we will answer this question negatively, indeed for every infinite κ we shall construct 2^κ RCF which are isomorphic as ordered sets, but not as ordered fields; in fact we shall examine that question in the following more general context: Let L be a countable first order language and T a theory in L extending the theory of linear orders, T is *o-minimal* iff for every model M of T and every formula ϕ with one free variable and parameters in M, ϕ is equivalent to a finite union of intervals (cf. [P-S]). The most important examples are DLOWEP, DOAG, RCF, and many theorems now follow easily via this model theoretic property that they share, for example the following theorem holds for any o-minimal model M:

Theorem 1.1 *For $\kappa > \aleph_0$, M is κ-saturated iff M is κ-saturated as an ordered set.*

From general model theory and from this theorem, the above mentioned results of Hausdorff, Erdös, Gillman and Henriksen, and that of Alling follow immediately. The question now translates as follows: does the order characterize the o-minimal model? An o-minimal theory being unstable, looking for invariants (a classification problem) is rather risky, but is in some sense motivated by the good model theory that has been done for these theories: some theorems that are true for ω-stable theories, like "existence and uniqueness of prime models", "Vaught's conjecture" were proved for o-minimal theories (cf. [P-S] and [MA]). To the above question we will give however a negative answer by giving counterexamples in DOAG and RCF. The following strengthening of the hypothesis was proposed by D. Lascar: Does the order characterize the κ-saturated o-minimal models, at least for large enough κ? The last part of this talk will be devoted to give a negative answer to that question as well, some theorems will be stated and used without proofs, those are to be read elsewhere.

2 Construction of 2^κ DOAG of cardinality κ, isomorphic as ordered sets, but not as ordered groups

We first need some definitions. Let G be a DOAG and $g \in G$, put $|g| = \max(g, -g)$. For $g_1 \in G$, $g_2 \in G$, g_1 is *archimedean equivalent* to g_2 (we denote it by: $g_1 \sim g_2$) iff there exists $n \in \omega$ s.t. $n|g_1| > |g_2|$ and $n|g_2| > |g_1|$, g_1 is *infinitely smaller* than g_2 iff for all $n \in \omega, n|g_1| < |g_2|$ (we denote it by: $g_1 \ll g_2$). G is *archimedean* iff any two nonzero elements are archimedean equivalent; an archimedean group is a subgroup of $\mathbb{R}$. Given $g \in G$, $g \neq 0$, let C_g be the smallest convex subgroup containing g, and D_g the largest convex subgroup not containing g, then C_g/D_g is archimedean, it is called the *archimedean component corresponding to* g. We order the set of equivalence classes of nonzero elements as follows: $[g_1] < [g_2]$ iff $g_2 \ll g_1$; the *rank* of G, denoted by I_G, is the order type of this ordered set. For $i \in I_G$, we let B_i be the archimedean component corresponding to any element of the equivalence class i. This is well defined because $g_1 \sim g_2$ iff $C_{g_1} = C_{g_2}$ iff $D_{g_1} = D_{g_2}$. The *skeleton* of G is $[I_G\,;\, B_i\,,\, i \in I_G]$; it is an invariant: if $G \simeq G'$, there exists an order isomorphism ϕ of I_G onto $I_{G'}$, and for every $i \in I_G$, an isomorphism ϕ_i of archimedean ordered groups from B_i onto $B'_{\phi(i)}$. Given an ordered set I and a choice B_i, $i \in I$ of archimedean groups, we form the group $\Gamma_{i\in I}B_i$: it consists of all functions f from I into $\bigcup_{i\in I} B_i$ s.t. $f(i) \in B_i$ and f has well ordered support in I. Addition is pointwise,

and the order is lexicographic: $f > 0$ iff $f(i) > 0$ where $i = \min(\text{support}(f))$. The subgroup consisting of the functions with finite support is denoted by $\bigoplus_{i\in I} B_i$. Clearly, both $\Gamma_{i\in I} B_i$ and $\bigoplus_{i\in I} B_i$ have skeleton $[I\,;\, B_i\,,\, i \in I]$. Finally, we note that if given $[I\,;\, A_i\,,\, i \in I]$ and $[J\,;\, B_j\,,\, j \in J]$ s.t. there is an isomorphism ϕ from I onto J, and for every $i \in I$, an isomorphism ϕ_i from A_i onto $B_{\phi(i)}$, then $\Gamma_{i\in I} A_i \simeq \Gamma_{j\in J} B_j$ and $\bigoplus_{i\in I} A_i \simeq \bigoplus_{j\in J} B_j$.

Now let an infinite cardinal κ be given. Let A_1 and A_2 be two countable archimedean DOAG which are isomorphic as ordered sets, but not as ordered groups (e.g. $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}) = \{p + q\sqrt{2}\,;\, p, q \in \mathbb{Q}\}$ as ordered sets are countable DLOWEP and so are isomorphic, but $\dim[\mathbb{Q} : \mathbb{Q}] = 1$ and $\dim[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$). For every function $f \in 2^\kappa$, put $G_f = \bigoplus_{\alpha\in\kappa} A_{f(\alpha)}$. It is not difficult to verify that since the archimedean components are all isomorphic as ordered sets, then also for all $f, f' \in 2^\kappa$, G_f and $G_{f'}$ are isomorphic as ordered sets. However if $f \neq f'$, then G_f and $G_{f'}$ are not isomorphic as ordered groups, for if they were, then by a previous remark, we should have that for every $\alpha \in \kappa$, $A_{f(\alpha)}$ and $A_{f'(\alpha)}$ are isomorphic as ordered groups (the only automorphism of κ being the identity), but since $f \neq f'$, there exists $\alpha \in \kappa$ s.t. $f(\alpha) \neq f'(\alpha)$ and thus $A_{f(\alpha)} \not\simeq A_{f'(\alpha)}$.

We now proceed to answer the question of Erdös, Gillman and Henriksen about RCF. We need some definitions: Let $(K, +, ., 0, 1, <)$ be an ordered field and consider the set G of equivalence classes of the equivalence relation "archimedean equivalence" defined on the ordered abelian group $(K, +, 0, <)$. On G we define the following addition: $[x] + [y] = [xy]$; in this way, G becomes an ordered abelian group, and the map $v : K \setminus \{0\} \longrightarrow G$ defined by $v(x) = [x]$ is a *valuation* on K, i.e. it satisfies the following properties: $v(ab) = v(a) + v(b)$ and $v(a + b) \geq \min(v(a), v(b))$. The *valuation ring*, denoted by R_v, is the set $\{x \in K \setminus \{0\}\,;\, v(x) \geq 0\}$; the *valuation ideal*, denoted by M_v, is the set $\{x \in K \setminus \{0\}\,;\, v(x) > 0\}$; the *residue field*, denoted by $\overline{K}$, is the field R_v/M_v; finally the *valuation group* is G. $\overline{K}$ and G are invariants for isomorphisms of ordered fields. Given an ordered abelian group G, *the field of formal power series* with coefficients in $\mathbb{R}$ and exponents in G, denoted by $\mathbb{R}((G))$, is the set of all functions from G into $\mathbb{R}$ with well ordered support in G; addition is pointwise and the order lexicographic; multiplication is given by: $(f \cdot f')(g) = \sum_{g'\in G} f(g')f'(g - g')$. It is clear that the residue field of $\mathbb{R}((G))$ is $\mathbb{R}$ and its valuation group is G. Now let κ an infinite cardinal be given, and let $\{G_\alpha\,;\, \alpha \in 2^\kappa\}$ be a set of DOAG which are order isomorphic but not isomorphic, and put: $R_\alpha = \mathbb{R}((G_\alpha))$. Since G_α is divisible, R_α is real closed (for a proof see [PR]). For every $\alpha, \beta \in 2^\kappa$, R_α and R_β are isomorphic as ordered sets (even $(R_\alpha, +, 0, <)$ and $(R_\beta, +, 0, <)$

are isomorphic), but if $\alpha \neq \beta$ then R_α and R_β are not isomorphic as ordered fields since they have nonisomorphic value groups.

3 The case of the κ-saturated structures

For every infinite κ we shall construct two κ-saturated DOAG (RCF) isomorphic as ordered sets but not as ordered groups (fields). We need some definitions and some theorems. Let λ be a limit cardinal and $(a_\rho)_{\rho\in\lambda}$ a sequence of elements of a DOAG (or a RCF), $(a_\rho)_{\rho\in\lambda}$ is *pseudo- cauchy* iff for all $\nu < \rho < \mu < \lambda$ we have $a_\rho - a_\mu \ll a_\nu - a_\rho$. a is a *pseudo-limit* of $(a_\rho)_{\rho\in\lambda}$ iff for all $\nu \in \lambda$, $a - a_{\nu+1} \ll a - a_\nu$. For $\kappa > \aleph_0$, the following two theorems characterizing the κ-saturated DOAG and RCF can be deduced from Alling's theorem about DOAG which are η_α-sets (c.f. [ALL 2]), a proof treating also the case $\kappa = \aleph_0$ is given in [KU].

Theorem 3.1 *Let G be a DOAG and κ an infinite cardinal, then G is κ-saturated iff:*
its rank is κ-dense
all its archimedean components are $\mathbb{R}$
every pseudo-cauchy sequence indexed by $\lambda < \kappa$ has a pseudo-limit in G.

Theorem 3.2 *Let F be a RCF and κ an infinite cardinal, then F is κ-saturated iff:*
its value group is a κ-saturated DOAG
its residue field is $\mathbb{R}$
every pseudo-cauchy sequence in a subfield of absolute trancendence degree $< \kappa$ has a pseudo-limit in F.

The following theorem computes the rank of the group of positive elements of an ordered field, the proof is given in [KU].

Theorem 3.3 *Let $(K, +, ., 0, 1, <)$ be an ordered field, and G its valuation group. Then* $\mathrm{rank}(K^{>0}, ., 1, <) = \mathrm{rank}(G) + 1 + G^{>0}$, *this last sum being a sum of ordered sets, and 1 being the ordered set consisting of one element.*

A corollary to this theorem is

Corollary 3.4 *If $(K, +, ., 0, 1, <)$ admits an exponential function, then*

$$\mathrm{rank}(G) \simeq G^{<0}$$

as ordered sets.

The following three propositions are easily verified.

Proposition 3.5 *Let $(R,+,.,0,1,<)$ be a real closed field, then*

$$(R,<) \simeq (R^{>0},<)$$

as ordered sets.

Proof: In fact $\phi : R \longrightarrow R^{>0}$ defined by

$$\phi(x) = \begin{cases} \frac{1}{x^2+1} & \text{if } x < 0 \\ x+1 & \text{if } x \geq 0 \end{cases}$$

is an order preserving bijection. □

Proposition 3.6 *Let η be a κ^+-saturated DLOWEP of cardinality 2^κ and let η' be the sum of 2^κ copies of η, then η' is again κ^+-saturated.*

Proposition 3.7 *Let I be an infinite chain of cardinality λ, and suppose that I contains a well ordered subset of cardinality λ, then* $\mathrm{card}(\Gamma_{i\in I}\mathbb{R}) = 2^\lambda$.

We now have all the material needed to construct the counterexample: Let κ be an infinite cardinal and η' like in 3.6. Let $G = \Gamma_{i\in\eta'}\mathbb{R}$. It is known (c.f. [KR]) that such groups are *maximal*, i.e. every pseudo-cauchy sequence has a pseudo-limit in G, and so by 3.1 G is κ-saturated. Clearly, η' contains a well ordered subset of cardinality 2^κ, so by 3.7, $\mathrm{card}(G) = 2^{\mathrm{card}(\eta')} = 2^{2^\kappa}$. Now let $F = (\mathbb{R}((G)),+,.,0,1,<)$. Then F is a RCF. Put $G_1 = (\mathbb{R}((G)),+,0,<)$ and $G_2 = (\mathbb{R}((G))^{>0},.,1,<)$. then G_1 and G_2 are DOAG. By 3.2, F is κ-saturated, hence also G_1 and G_2, and by 3.5 G_1 and G_2 are isomorphic as ordered sets. Now if they were isomorphic as ordered groups, we should have $\mathrm{rank}(G_1) \simeq \mathrm{rank}(G_2)$ as ordered sets, and it would then follow by 3.3 that $G \simeq \mathrm{rank}(G) + \mathbf{1} + G^{>0}$, or equivalently $\mathrm{rank}(G) \simeq G^{<0}$ as ordered sets, but $\mathrm{rank}(G) = \eta'$ so $\mathrm{card}(\mathrm{rank}(G)) = 2^\kappa$ whereas $\mathrm{card}(G^{<0}) = \mathrm{card}(G) = 2^{2^\kappa}$, so $G_1 \simeq G_2$ is impossible.

Finally to produce two κ-saturated RCF isomorphic as ordered sets but not as ordered fields, let G_1 and G_2 be the two DOAG of the counterexample above and set $F_1 = \mathbb{R}((G_1))$ and $F_2 = \mathbb{R}((G_2))$. Then F_1 and F_2 are κ-saturated, isomorphic as ordered sets but have nonisomorphic value groups.

References

[ALL1] N.L. Alling, On ordered divisible groups, TAMS 94 (1968), 498–514

[ALL2] N.L. Alling, On the existence of real closed fields that are η_α-sets of power $\aleph_\alpha$, TAMS 103 (1962), 341–352

[E–G–H] Erdös, Gillman and Henriksen, An isomorphism theorem for real-closed fields, Ann. of Math. 61 (1955), 542-554

[H] Hausdorff, Grundzüge der Mengenlehre, Verlag von Veit, Leipzig, 1914

[KU] S. Kuhlmann, Manuscript, Paris 1987

[KR] Krull, Allgemeine Bewertungstheorie, J. Reine Angew. Math. 167 (1936), 160-196

[MA] L. Mayer, Dissertation, Yale University 1985

[P-S] A. Pillay and C. Steinhorn, Definable sets in ordered structures I, Preprint 1984

[PR] A. Prestel, Lectures on formally real fields, Lecture Notes in Mathematics 1093, Berlin (1984)

Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
D–6900 Heidelberg

ORDERED CONES AND APPROXIMATION

Klaus Keimel and Walter Roth

Introduction.

Using order theoretical concepts instead of topological structures has proved to be useful in quite a number of situations in analysis. In our investigations on Korovkin type theorems in approximation theory we were led to introduce a new concept of locally convex (partially) ordered cones which might be of independent interest.

Looking for a unified presentation of Korovkin type theorems for positive linear operators (see e.g. [2], [3], [4], [23]) and for linear contractions (see e.g. [1], [17]), as well as for order preserving linear operators on spaces of set-valued functions (see [22], [9]), we were indeed forced to leave the setting of vector spaces and to turn to more general structures which we call locally convex ordered cones. Our prime example is the set $Conv(E)$ of all non-empty convex subsets of a locally convex topological vector space E which has a natural addition and a scalar multiplication by *non-negative* reals; it is ordered by inclusion and it carries a topology which is induced in a canonical way by a subset $V \subset Conv(E)$, namely an arbitrary base of convex neighborhoods of 0 in E.

In this vein, a *locally convex ordered cone* will be a set P with an addition, a scalar multiplication by non-negative reals, a partial order $\leq$ and a distinguished subset V of positive elements $v \in P$ which act as abstract neighborhoods of 0. The axioms that we impose look very natural. They allow to derive a canonical topology on P, the properties of which justify the term "locally convex".

For our purposes, it was essential to include cones with unbounded elements as $P = Conv(E)$, which are not embeddable in vector spaces. At the other hand, we

cannot use a very general notion of a cone as e.g. Fuchssteiner and Lusky in their monograph [6]. As we need to apply functional analytic methods, we need an appropriate duality theory and, in particular Hahn-Banach type extension and separation theorems. We believe that the concept introduced here has the desired generality but is close enough to the classical theory of locally convex vector spaces in order to work with the analogues of the classical functional analytical methods.

In this paper, we present the basic theory of locally convex ordered cones as ordered algebraic structures. A more detailed study of its duality theory and the applications to approximation theory will be dealt with at a different place.

1. Cones and preordered cones.

1.1 Cones. We define a *cone* to be a set P endowed with an addition $(a,b) \to a+b$ and a scalar multiplication $(\alpha,a) \to \alpha a$ for real numbers $\alpha>0$. The addition is only supposed to be associative and commutative and a neutral element 0_P (shortly 0) is required to exist, i.e.:

$$\begin{aligned} (a+b)+c &= a+(b+c) && \text{for all } a,b,c \in P,\\ a+b &= b+a && \text{for all } a,b \in P,\\ 0+a &= a && \text{for all } a \in P. \end{aligned}$$

For the scalar multiplication we require as usual:

$$\begin{aligned} \alpha(\beta a) &= (\alpha\beta)a && \text{for all } \alpha,\beta>0 \text{ and } a \in P,\\ (\alpha+\beta)a &= \alpha a+\beta a && \text{for all } \alpha,\beta>0 \text{ and } a \in P,\\ \alpha(a+b) &= \alpha a+\alpha b && \text{for all } \alpha>0 \text{ and } a,b \in P,\\ 1\cdot a &= a && \text{for all } a \in P. \end{aligned}$$

In this definition of a cone P, the scalar multiplication is only required to be defined for real numbers $\alpha>0$. We may - and we shall do this in the sequel - extend the scalar multiplication to $\alpha = 0$ by defining $0\cdot a = 0$ for all $a \in P$, and all of the above rules remain valid. At the other hand, $\alpha\cdot 0 = 0$ for all $\alpha>0$ is a consequence of these rules. Indeed, for all $a \in P$ we have

$$a = \alpha(\alpha^{-1}a+0) = a+\alpha 0,$$

whence $\alpha\cdot 0 = 0$ by the unicity of the neutral element.

1.2 Subcones. A subset Q of a cone P is called a *subcone* if

$$a+b \in Q \quad \text{and} \quad \alpha a \in Q \qquad \text{for all } a,b \in Q \text{ and } \alpha\geq 0.$$

Note that every subcone of P contains 0.

Of course, cones in real vector spaces are cones in the above sense. They have the *cancellation property*

(C) $\qquad a+c = b+c \qquad$ implies $\qquad a = b$

for arbitrary elements a,b,c. Conversely, cones which satisfy the cancellation property are embeddable in real vector spaces. It is important to note that cones in our sense are in general far from being embeddable in vector spaces, as the addition is not supposed to be cancellative. This is essential, as we want to include examples like the following:

1.3 Example. With its straightforward addition and multiplication with $\alpha\geq 0$, the set

$$\overline{\boldsymbol{R}} = \boldsymbol{R} \cup \{+\infty\} \qquad \text{is a cone.}$$

1.4 Example: Cones of convex sets. Let $\boldsymbol{P}$ be a cone. A subset A of $\boldsymbol{P}$ is called *convex*, if $\alpha a+(1-\alpha)b \in A$, whenever $a,b \in A$ and $0\leq\alpha\leq 1$.
We denote by $Conv(\boldsymbol{P})$ the set of all non-empty convex subsets of $\boldsymbol{P}$. With the addition and scalar multiplication defined as usual by

$$A+B = \{a+b \mid a \in A \text{ and } b \in B\} \quad \text{for } A,B \in Conv(\boldsymbol{P}),$$
$$\alpha A = \{\alpha a \mid a \in A\} \quad \text{for } A \in Conv(\boldsymbol{P}) \text{ and } \alpha\geq 0,$$

it is easily verified that $Conv(\boldsymbol{P})$ is again a cone. Convexitiy is required to show that $(\alpha+\beta)A$ equals $\alpha A+\beta A$: Clearly $(\alpha+\beta)A$ is a subset of $\alpha A+\beta A$. To show the converse, consider an arbitrary element $c \in \alpha A+\beta A$; it can be written $c = \alpha a+\beta b$ with $a, b \in A$; as

$$c = (\alpha+\beta)\left(\frac{\alpha}{\alpha+\beta}a + \frac{\beta}{\alpha+\beta}b\right); \quad \text{(the case } \alpha=\beta=0 \text{ is trivial.)}$$

and as

$$\frac{\alpha}{\alpha+\beta}a+\frac{\beta}{\alpha+\beta}b \in A \quad \text{by the convexity of } A,$$

we conclude that $c \in (\alpha+\beta)A$.

Note that every subcone $\boldsymbol{Q}$ of $\boldsymbol{P}$ is convex and satisfies $\boldsymbol{Q}+\boldsymbol{Q} = \boldsymbol{Q}$. In particular, the non-empty convex subsets of a real vector space form a cone in our sense which is far from being cancellative.

1.5 Example: Cones of cone-valued functions. Let $\boldsymbol{P}$ be a cone, X any a set. For $\boldsymbol{P}$-valued functions on X the addition and scalar multiplication may be defined pointwise. The set $\boldsymbol{F}(X,\boldsymbol{P})$ of all such functions then is a cone in our sense. But again the addition is in general not cancellative, as it is not in $\boldsymbol{P}$.

1.6 Preordered cones. *A preordered cone* is a cone $\boldsymbol{P}$ with a reflexive transitive relation $\leq$ such that

$$a \leq b \text{ implies } a+c \leq b+c \text{ and } \alpha a \leq \alpha b \text{ for all } a,b,c \in \boldsymbol{P} \text{ and all } \alpha\geq 0.$$

If $\leq$ is in addition antisymmetric, i.e. $\leq$ is a partial ordering, then $\boldsymbol{P}$ is called an *ordered cone.*

Examples of preordered cones are $\overline{\boldsymbol{R}}$ with its usual order (Ex.1.3), the set $Conv(\boldsymbol{P})$ of non-empty convex subsets of a cone $\boldsymbol{P}$ ordered by inclusion (Ex 1.4) and

if P is a preordered cone, the set of P-valued functions on a given set X endowed with the pointwise ordering (Ex. 1.5). Every cone P is preordered by its *natural preorder* defined by $a \leq_n b$ if $a+c=b$ for some $c \in P$.

Convex sets in cones may look rather peculiar. For example in $\overline{R}$ all the two element sets $\{a,+\infty\}$ are convex. This phenomenon is somehow remedied by considering only increasing or decreasing sets, or more generally convex sets that are also order convex:

1.7 Example: Cones of decreasing convex sets. A subset a of a preordered cone is called *decreasing*, if $a \in A$ and $b \leq a$ for some $b \in P$ imply $b \in A$. For a subset B of P we denote by:

$$\downarrow B = \{a \in P \mid a \leq b \text{ for some } b \in B\},$$

the decreasing subset generated by B. In a dual way one defines the notion of an *increasing* subset and $\uparrow B$, the increasing subset generated by B. It is easily verified, that $\downarrow B$ and $\uparrow B$ both are convex, whenever B is convex. We denote by *DConv(P)* the set of all non-empty decreasing convex subsets of P.

For a decreasing convex set A and $\alpha>0$, the set αA is also decreasing and convex. But $A+B$ need not be decreasing, if A and B are. We therefore modify the addition on *DConv(P)* and define

$$A \oplus B = \downarrow(A+B) = \{c \in P \mid c \leq a+b \text{ for some } a \in A, b \in B\}.$$

With this addition and the usual scalar multiplication DConv(P) becomes a cone ordered by inclusion; the set $\{0\}$ acts as the additive zero element. There is a natural map

$$a \to \downarrow\{a\} \text{ of } P \text{ into } DConv(P),$$

which is order preserving. It is an embedding, i.e. injective, if and only if the preorder on P is in fact an order. If not, the image

$$\downarrow P = \{ \downarrow\{a\} \mid a \in P \}$$

is called the *ordered cone associated with P*.

2. Locally convex cones.

We want to endow our cones with a locally convex structure. Our definition will be guided by the example of the cone *Conv(E)* of all non-empty convex subsets of a locally convex topological vector space E. In this case we can choose a base V of convex neighborhoods V of 0 in E. We may suppose that $U+V \in V$ and $\alpha V \in V$ whenever $U,V \in V$ and $\alpha>0$. Note that V is a "cone without zero" down directed towards 0. A neighborhood base for a convex set A is given by the sets

$$A + V, \quad V \in V$$

This induces three hyperspace topologies on $Conv(E)$ given by the respective neighborhood bases for $A \in Conv(E)$

in the *upper topology* $\quad V(A) = \{B \in Conv(E) \mid B \subset A+V\}, \ V \in \boldsymbol{V},$

in the *lower topology* $\quad (A)V = \{B \in Conv(E) \mid A \subset B+V\}, \ V \in \boldsymbol{V},$

in the *symmetric topology* $\quad V(A) \cap A(V), \quad V \in \boldsymbol{V}.$

On a subcone Q of $Conv(E)$, we shall consider the induced topologies, also in the case where Q does not contain V. On $Q = E$ all the three topologies coincide with the given locally convex topology.

We now present an abstract formulation:

2.1 Abstract 0-neighborhood systems. Let P be a preordered cone. A subset V of P is called an *(abstract) 0-neighborhood system,* if the following properties hold:

$0 < v$ for all $v \in V$;

for all $u,v \in V$ there is $w \in V$ with $w \leq u$ and $w \leq v$;

$u+v \in V$ and $\alpha v \in V$ whenever $u,v \in V$ and $\alpha > 0$.

One could say that V is a "subcone without zero directed towards 0". The elements

$$a+v, \quad v \in V,$$

may be called abstract neighborhoods of $a \in P$.

2.2 Locally convex topologies. Let P be a cone with a 0-neighborhood system V. For every $a \in P$ we define

$$v(a) = \{b \in P \mid b \leq a+v\}$$

to be a neighborhood of a in the *upper topology*, and

$$(a)v = \{b \in P \mid a \leq b+v\}$$

to be a neighborhood of a in the *lower topology*. One easily verifies that these neighborhood systems define indeed topologies on P. The common refinement of these two topologies is called the *symmetric topology* on P.

Note that the $v(a)$ are decreasing convex sets and the $(a)v$ are increasing convex sets. The neighborhoods in the symmetric topology are both convex and order convex. Thus, all of these three toplologies merit to be called locally convex. Of course the upper and the lower topology are far from being Hausdorff. Since all of the three topologies are defined in terms of the preorder on P, we will not need to work with them expicitely. Continuity properties etc. will be expressible by means of the ordering and the 0-neighborhoods alone.

We also consider subcones Q of P not necessarily containing V. They will be endowed with the topologies induced from P. Thus, for $a \in Q$, the neighborhood bases for the upper and lower topologies on Q will be given by

$$v_Q(a) = v(a) \cap Q = \{b \in Q \mid b \leq a+v\}, \quad v \in V$$

$$(a)_Q v = (a)v \cap Q = \{b \in Q \mid a \leq b+v\}, \quad v \in V,$$

respectively.

2.3 Bounded elements. Let P be a preordered cone with a 0-neighborhood system V. For $v \in V$, an element $a \in P$ is called

upper v-bounded, if $a \leq \alpha v$ for some $\alpha>0$,

lower v-bounded, if $0 \leq a+\beta v$ for some $\beta>0$,

v-bounded, if it is both lower and upper v-bounded.

An element a is called *upper (lower) bounded*, if it is upper (lower) bounded for every $v \in V$. The following is straightforward:

2.4 Proposition. *The set $B(v)$ of all upper v-bounded and likewise the set B of all upper bounded elements is a decreasing subcone in P.*

Now we are ready for our main definition which proceeds in two steps:

2.5 Locally convex cones. Let P be a preordered cone and $V \subset P$ an abstract 0-neighborhood system. The pair (P,V) is called a *full locally convex cone*, if every element of P is lower bounded. In a full locally convex cone the bounded elements therefore coincide with the upper bounded ones.

Finally, a *locally convex cone* is a pair (Q,V), where Q is a subcone and V the 0-neighborhood system of some full locally convex cone (P, V). Of course, Q inherits the preorder and the topological structure of P. We have neglected to indicate P in the notation, as only those elements of P play a role for Q which are of the form $a+v$ with $a \in Q$ and $v \in V \cup \{0\}$, and these elements form a subcone of P already containing V. But one has to keep in mind that Q in general does not contain the 0-neighborhood system.

Clearly every locally convex topological vector space E with 0-neighborhood base V is a locally convex cone (E,V) in this sense, as it is a subcone of the full locally convex cone $Conv(E)$ ordered by inclusion, which contains V and in which every element is bounded below. The preorder induced on E is just the equality.

If, on the other hand, the locally convex cone Q is a vector space, i.e. contains all negatives of its elements, then $b \leq a+v$, if and only if $b-a \leq v$. All elements of Q are bounded, as they and their negatives are bounded below, and the neighborhoods of 0 with respect to the symmetric topology

$$v_0 = (0)v \cap v(0) = \{b \in Q \mid b \leq v \text{ and } 0 \leq b+v\}$$
$$= \{b \in Q \mid b \leq v \text{ and } -b \leq v\}$$

form the basis for a locally convex vector space topology on Q (not necessarily Hausdorff). But it is obvious that distinct abstract neighborhood systems V in our sense may lead to the same symmetric topology. So even in the case of vector spaces there is a substantially larger variety of locally convex cone topologies than vector space topologies.

The following are our standard examples for locally convex cones to which we will frequently refer in the sequel:

2.6 Example. The cone $\overline{R} = R \cup \{+\infty\}$ will always be endowed with the abstract neighborhood system $V = \{\varepsilon \in R \mid \varepsilon > 0\}$. For $a \in R$ the intervals $(-\infty, a+\varepsilon)$ are the upper and the intervals $(a-\varepsilon, +\infty)$ the lower neighborhoods, while for $a = +\infty$ the entire cone $\overline{R}$ is the only upper neighborhood, and $\{+\infty\}$ is open in the lower topology. The symmetric topology on $\overline{R}$ is the usual topology on R with $\{+\infty\}$ as an isolated point.

2.7 Example. Let $(E,\leq)$ be an locally convex ordered topological vector space with 0-neighborhood base V. For $A,B \in Conv(E)$, the cone of non-empty convex subsets of E, we define

$$A \leq B \text{ if for every } a \in A \text{ there is some } b \in B \text{ such that } a \leq b.$$

Since $Conv(E)$ contains V, and all its elements are bounded below in this sense, $(Conv(E),V)$ is a full locally convex cone. E may be considered as a subcone of $Conv(E)$, hence (E,V) is a locally convex cone. Note that the upper neighborhoods of $a \in E$ contain all elements smaller then a, the lower neighborhoods all larger ones. The symmetric toplology on E coincides with the original one if the neighborhoods $v \in V$ are order convex.

2.8 Example. Let (P,V) be a full locally convex cone. If we identify the elements of V with singleton sets, then V is a subset of $Conv(P)$, which can be preordered using the preorder of P. For $A,B \in Conv(P)$ we define

$$A \leq B \text{ if for all } a \in A \text{ there is some } b \in B \text{ such that } a \leq b.$$

Since its elements clearly are bounded below as are the elements of P, $(Conv(P),V)$ becomes a full locally convex cone.

If (Q,V) is a locally convex cone, i.e. a subcone of some full locally convex cone (P,V), $Conv(Q)$ is a subcone of $Conv(P)$, hence for any cone D of non-empty convex subsets of Q, the pair (D,V) is a locally convex cone.

We shall also consider the families $DConv(Q)$ and $\overline{DConv(Q)}$ of decreasing convex subsets, respectively closed decreasing convex subsets of Q, where closure is meant with respect to the lower topology on Q. If we slightly modify the addition (c.f. Example 1.7), both sets will become cones as well:

$$A \oplus B = \downarrow(A+B) \qquad \text{for } A,B \in DConv(Q),$$
$$A \overline{\oplus} B = \overline{\downarrow(A+B)} \qquad \text{for A,B} \in \overline{DConv(Q)},$$

where $\overline{\downarrow(A+B)}$ denotes the closure with respect to the lower topology. (We shall see in the following section that the closure in this topology is decreasing for any subset of Q.) With the preorder and the abstract neighborhood system induced by

$Conv(Q)$ (For decreasing sets this preorder coincides with inclusion), both $(DConv(Q), V)$ and $(\overline{DConv(Q)}, V)$ then are locally convex cones.

2.9 Example. Let $F(X,P)$ be the cone of P-valued functions on the set X, where (P,V) is a full locally convex cone. If we consider its pointwise preorder and identify the elements $v \in V$ with the constant functions $x \to v$ for all $x \in X$, then V is a subset of $F(X,P)$ and defines an abstract neighborhood system there. Of course, not all functions in $F(X,P)$ will be bounded below. So we have to restrict ourselves to the subcone $B_l(X,P)$ of elements with this property, and $(B_l(X,P),V)$ then is a full locally convex cone.

Again, if (Q,V) is a locally convex cone, every subcone of $B_l(X,Q)$ is seen to be a locally convex cone as well. If in particular X is a topological space, we may consider the following subcones of $F(X,Q)$:

The cone $C_u(X,Q)$ of functions continuous with respect to the upper topology on Q,

the cone $C_l(X,Q)$ of functions continuous with respect to the lower topology on Q,

the cone $C_s(X,P)$ of functions continuous with respect to the symmetric topology on Q.

Their respective subcones of elements bounded below then are locally convex cones. If X is compact, then obviously all functions in $C_l(X,Q)$ and in $C_s(X,Q)$ are bounded below.

3. Local and global preorder. Closure.

Throughout this section we assume that Q is a locally convex cone, i.e. a subcone of the full locally convex cone (P,V). By means of the abstract neighborhood system V we shall define a new preorder on P, hence on Q, which in general will not coincide with the original one. It will however turn out to be more appropriate to describe the topological properties of a locally convex cone. We shall proceed in two steps:

3.1 The local preorder $\preceq_v$. For a fixed element $v \in V$ we define a relation $\preceq_v$ on P by:

$$a \preceq_v b \text{ if and only if } a \leq b+\rho v \text{ for all } \rho>0.$$

It is easily seen that $\preceq_v$ is a preorder on P called the *v-local preorder* and that P endowed with this preorder and the abstract 0-neighborhood system V is again a full locally convex cone. And again, as a subcone of P, Q is a locally convex cone. Clearly $a \leq b$ in the original preorder implies $a \preceq_v b$.

3.2 The global preorder $\lesssim$. *The global preorder* is defined as the intersection of all local preorders, i.e.

$$a \lesssim b \quad \text{iff} \quad a \leq a+v \text{ for all } v \in V,$$
$$\text{iff} \quad a \lesssim_v b \text{ for all } v \in V.$$

Endowed with this preorder and the abstract neighborhood system V, P is again a full locally convex cone, Q a locally convex cone, and $a \leq b$ in the original preorder implies $a \lesssim b$.

3.3 Closure. In Example 1.7 we studied decreasing convex subsets of a preordered cone and in particular the sets $\downarrow\{a\}$ generated by a single element $a \in P$. We shall do the same now with respect to the global preorder:
For every $a \in P$, the *closure of* a is defined to be the set

$$\begin{aligned} \overline{a} &= \{b \in P \mid b \lesssim a\} \\ &= \{b \in P \mid b \leq a+v \text{ for all } v \in V\}. \\ &= \bigcap_{v \in V} v(a). \end{aligned}$$

By definition, $\overline{a}$ is the intersection of all the upper neighborhoods of a. Clearly, $\overline{a}$ is convex and decreasing with respect to both of the preorders $\leq$ and $\lesssim$. The collection

$$\overline{P} = \{\overline{a} \mid a \in P\}$$

of all one point closures is again a full locally convex cone, if we endow $\overline{P}$ with the operations

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \lambda\overline{a} = \overline{\lambda a} \quad \text{for } \lambda > 0,$$

with the inclusion order and the abstract 0-neighborhood system $\overline{V} = \{\overline{v} \mid v \in V\}$.
There is a canonical map $a \to \overline{a} : P \to \overline{P}$ which preserves the whole structure of P.
For a subcone Q of P we may restrict the closure to Q and consider $\overline{a} \cap Q$ instead of $\overline{a}$, and we obtain again a locally convex ordered cone $\overline{Q}$.

3.4 Lemma. *If $c \not\in \overline{a}$, then there is a lower neighborhood of c and an upper neighborhood of a which are disjoint.*

Proof. If $c \not\lesssim a$, then there is a $v \in V$ such that $c \not\leq a+2v$. We claim that $(c)v$ and $v(a)$ are disjoint. Indeed, if x were an element in the intersection, then we had $c \leq x+v$ and $x \leq a+v$, which would imply $c \leq a+2v$.

3.5 Corollary. *The closure $\overline{a}$ is the closure of $\{a\}$ with respect to the lower topology.*

Proof. Indeed, the complement of $\overline{a}$ is open for the lower topology by the preceding Lemma. Conversely, if $c \lesssim a$, then every lower neighborhood of c contains a; thus every lower closed set containing a must contain c as well.

3.6 Remark. This shows in particular that the original preorder $\leq$ and the global preorder $\preceq$ on a locally convex cone coincide if and only if the sets $\downarrow\{a\} = \{b \mid b \leq a\}$ are all closed in the lower topology, i.e. $\overline{a} = \downarrow\{a\}$.

In a similar way, one shows that the set $\{b \mid a \preceq b\}$, which is the intersection of all lower neighborhoods of a, is nothing but the closure of $\{a\}$ with respect to the upper topology. Finally, the set $\{b \mid b \preceq a \text{ and } a \preceq b\}$, which is the intersection of all symmetric neighborhoods of a, is nothing but the closure of $\{a\}$ with respect to the symmetric topology.

3.7 Proposition. *For a subset $A \subset Q$ its closure $\overline{A}$ with respect to the lower topology is given by*

$$\overline{A} = \{b \in Q \mid \text{for all } v \in V \text{ there is } a \in A \text{ such that } b \leq a+v\}.$$

In particular, $\overline{A}$ is decreasing with respect to the global preorder of Q, and convex if A is.

Proof. Clearly $b \in \overline{A}$ if and only if $(b)v \cap A \neq \emptyset$ for all $v \in V$; i.e. there is some $a \in A$ such that $b \leq a+v$. Now let $b \in \overline{A}$ and $c \preceq b$. Then for $v \in V$, we have $c \leq b+v/2$ and $b \leq a+v/2$ for some $a \in A$, whence $c \leq a+v$, and $c \in \overline{A}$ as well.

Again, a similar statement can be made for the closure of A in the upper topology. The following observation will be crucial for our further investigations in locally convex cones. It demonstrates the importance of the global preorder:

3.8 Proposition. Let Q and Q' be locally convex cones. Then every mapping $f: Q \to Q'$, which is continuous with respect to the upper (or lower) topologies on both cones, is monotone with respect to their global preorders.

Proof. Since a continuous mapping between topological spaces maps the closure of a subset into the closure of its image, this renders $f(\overline{a}) \subset \overline{f(a)}$ for all $a \in Q$, whenever f is continuous with respect to the lower topologies on Q and Q'. So clearly $b \preceq a$, i.e. $b \in \overline{a}$ implies $f(b) \in \overline{f(a)}$, hence $f(b) \preceq f(a)$. If f is continuous for the upper topologies the same argument holds for the sets $\{b \mid a \preceq b\}$.

3.9 Definition. A locally convex cone is called *separated* if $\overline{a} = \overline{b}$ implies $a = b$, i.e. if different elements have different closures.

This property corresponds to the Hausdorff axiom in locally convex vector spaces. The following is clear from the above:

3.10 Proposition. *For a locally convex cone (Q,V) the following properties are equivalent:*

(i) (Q,V) *is separated.*

(ii) *The upper topology on Q is T_0.*

(iii) *The lower topology on Q is T_0.*

(iv) *The symmetric topology on Q is T_0.*

(v) *The symmetric topology on Q is Hausdorff.*

Moreover, on a separated cone the global preorder $\leq$ is in fact an order and the canonical map $a \to \bar{a}$ from Q with this order into $\overline{Q}$ is an isomorphism.

3.11 Corollary. *For every locally convex cone (Q,V), the cone $(\overline{Q},\overline{V})$ of one point closures is separated.*

We shall call $(\overline{Q},\overline{V})$ the *separated reflection* of (Q,V). This terminology is justified by the fact that continuous linear mappings from Q into separated locally convex cones all factor through $\overline{Q}$. This will be dealt with in detail in section 6.

3.12 Examples. Reviewing our standard Examples 2.6 through 2.9 for locally convex cones reveals the following:

The cone $\overline{R}$ clearly is separated (Example 2.6).

In Example 2.7 the locally convex ordered vector space $(E,\leq)$ is separated as a locally convex cone (E,V) as well, if only its positive cone E^+ is proper, i.e. $E^+ \cap (-E^+) = \{0\}$: For elements $a,b \in E$ $a \leq b$ translates into $b-a \in E^+ + V$, for all 0-neighborhoods $V \in \mathcal{V}$. Since E^+ is closed, this means $a \leq b$ in the given order of E, which therefore coincides with the global preorder. $\bar{a} = \bar{b}$ then implies $a = b$ because of the condition on E^+. Note that in the light of Proposition 3.8 this implies that mappings between locally convex ordered vector spaces, considered as locally convex cones, which are continuous with respect to their upper (or lower) topologies, need to be monotone with respect to the original orderings.

For any locally convex cone (Q,V) and $A,B \in (Conv(Q),V)$ one has $A \leq B$ if A is contained in the closure $\overline{A}$ of A with respect to the lower topology (c.f. Proposition 3.7). So in fact $(\overline{DConv(Q)},V)$ is the separated reflection of $(Conv(Q),V)$ and likewise, of $(DConv(Q),V)$ (Example 2.8).

Finally in $(B_l(X,Q),V)$ (Example 2.9) for two Q-valued functions $f,g \in B_l(X,Q)$ we have $f \leq g$ if $f(x) \leq g(x)$ for all $x \in X$. So $B_l(X,Q)$ is a separated locally convex cone, whenever Q is.

4. Cancellation.

Let $a,b\ c$ be elements of an arbitrary preordered cone Q. In section 1 we insisted on the fact that we do not require the cancellation law

(C) $\qquad a+c = b+c \qquad$ implies $\quad a = b,$

as we wanted to include examples like the cone *Conv(E)* of all non-empty convex subsets of a real vector space E. In this section we want to show that certain restricted cancellation laws hold in a locally convex cone (Q,V). For the proofs, it is no restriction to assume this cone to be full. The first property holds in any preordered cone:

4.1 Lemma. $a+c \le b+c$ *implies* $a+\rho c \le b+\rho c$ *for all* $\rho \ge 0$.

Proof. Suppose $a+c \le b+c$. Adding a and b, respectively, we obtain $2a+c \le a+b+c$ and $a+b+c \le 2b+c$, whence $2a+c \le 2b+c$ or else $a+c/2 \le b+c/2$. Repeating the same argument, we obtain

$$a+\frac{c}{2^n} \le b+\frac{c}{2^n}$$

for all natural numbers . If ρ is an arbitrary positive real number, choose an n such that $1/2^n \le \rho$; adding $(\rho-1/2^n)c$ to the last inequality, we obtain $a+\rho c \le b+\rho c$ as desired.

If $c \ge 0$, then $a \le a+\rho c$, and we may conclude:

4.2 Lemma. *If* $c \ge 0$, *then* $a+c \le b+c$ *implies* $a \le b+\rho c$ *for all* $\rho>0$.

From now on we place ourselves in a locally convex preordered cone (Q,V):

4.3 Lemma. *Let c be v-bounded for some* $v \in V$. *Then*

$$a+c \le b+c \quad \textit{implies} \quad a \le b+\rho v \ \textit{for a}$$

i.e. $\quad a+c \le b+c$ *implies* $\quad a \le_v b.$

Proof. As c is v-bounded, there is a $\lambda>0$ such that $c+\lambda v \ge 0$ and $c \le \lambda v$. Suppose $a+c \le b+c$. Then $a+(c+\lambda v) \le b+(c+\lambda v)$. By Lemma 4.2 we conclude $a \le b+\rho(c+\lambda v) \le b+2\rho\lambda v$ for all $\rho>0$.

4.4 Proposition. *For every bounded element c one has :*

$$a+c \le b+c \quad \textit{implies} \quad a+v \le b+v \ \textit{for all} \ v \in V,$$

i.e. $\quad a+c \le b+c$ *implies* $\quad a \le b,$ *where* $\le$ *is the global preorder.*

This is an immediate consequence of 4.3. We may apply this to the global preorder on Q, and we obtain the

4.5 Order cancellation for bounded elements:

$$a+c \leq b+c \quad \textit{implies} \quad a \leq b, \quad \textit{whenever } c \textit{ is bounded.}$$

For the closure of the elements we obtain (cf. section 3):

4.6 Corollary. *Whenever c is bounded, one has:*

$$\overline{a}+\overline{c} \subset \overline{b}+\overline{c} \quad \textit{implies} \quad \overline{a} \subset \overline{b},$$
$$\overline{a}+\overline{c} = \overline{b}+\overline{c} \quad \textit{implies} \quad \overline{a} = \overline{b}.$$

As in separated cones the global preorder is an order, i.e. antisymmetric, we conclude:

4.7 Corollary. *For bounded elements c in a separated locally convex cone one has:* $a+b = b+c$ *implies* $a = b$. *(cancellation for bounded elements c).*

Now we are in a position to embed a separated locally convex cone (Q,V) with its global preorder into a locally convex preordered cone (Q',V'), in which the bounded elements form a vector space which is locally convex with respect to the symmetric topology:

4.8 Embedding. Let us consider first a full locally convex cone (P,V). By $\leq$ we denote the global preorder on P and by B the subcone of all bounded elements. In order to embed B into a cone, in which the bounded elements become invertible, we perform the usual construction:

On the cone $P\times B$ of all pairs (a,b) with $a \in P$, $b \in B$, we define

$$(a,b) \leq (a',b') \text{ iff } a+b' \leq a'+b.$$

This relation on $P\times B$ clearly is reflexive. Let us verify that it is transitive as well: Let $(a,b) \leq (a',b')$ and $(a',b') \leq (a'',b'')$. Then $a+b' \leq a'+b$ and $a'+b'' \leq a''+b'$. Adding b'' and b to these inequalities, respectively, we obtain

$$a+b'+b'' \leq a'+b+b'' \quad \text{and} \quad a'+b''+b \leq a''+b'+b,$$

whence $a+b'+b'' \leq a''+b'+b$ by transitivity. As b' is bounded, we may cancel b' by 4.5 and we obtain $a+b'' \leq a''+b$, i.e. $(a,b) \leq (a'',b'')$.

Thus, $\leq$ is a preorder on $P\times B$ which clearly is compatible with the addition and scalar multiplication. We have an obvious embedding

$$a \to (a,0) \; : \; P \to P\times B$$

which allows to consider P as a subcone of $P\times B$. Moreover, the set $V\times\{0\}$ of all pairs $(v,0)$, $v \in V$, is an abstract neighborhood system on the preordered cone $P\times B$. Using the cancellation property for bounded elements again, one proves that $(P\times B, V\times\{0\})$ is indeed a locally convex cone. We now pass to its separated

reflection $\overline{P \times B}$ of one point closures $(\overline{a,b})$ as in section 3. For every bounded element b, the relations $(b,b) \leq (0,0) \leq (b,b)$ imply $(\overline{b,b}) = (\overline{0,0})$. Thus $(\overline{b,0}) + (\overline{0,b}) = (\overline{b,b}) = (\overline{0,0})$. We see that $(\overline{b,0})$ has an additive inverse, namely $(\overline{0,b})$. We may write shortly $\overline{a}$ for $(\overline{a,0})$ and $-\overline{b}$ for $(\overline{0,b})$, and $\overline{a}-\overline{b}$ for $(\overline{a,b})$. Finally, we write $\overline{P}-\overline{B}$ for $\overline{P} \times \overline{B}$. If P is separated, the canonical map $a \to \overline{a} : P \to \overline{P}$ is an isomorphism with respect to the global preorder on P, and considering this, we may omit the bars: We have embedded (P,V), preserving ist global preorder, into the locally convex cone $(P-B,V)$ in which the bounded elements form a vector space $E = B - B$. As we mentioned before (Section 2.5), the topology on E induced from the symmetric topology on the locally convex cone $(P-B,V)$ is given by neighborhoods of 0 in E :

$$\begin{aligned} v_0 = (0)v \cap v(0) &= \{b \in E \mid b \leq v \text{ and } 0 \leq b+v\} \\ &= \{b \in E \mid b \leq v \text{ and } -b \leq v\}. \end{aligned}$$

For $v \in V$, these sets are convex and order convex and form the 0-neighborhood basis for a Hausdorff locally convex vector space topology on E. For an arbitrary element $c \in E$, the respective neighborhoods obviously are

$$v_c = (c)v \cap v(c) = c + v_0$$

Thus, the symmetric topology on $E = B-B$ is the Hausdorff locally convex vector space topology with the v_0, $v \in V$, as 0-neighborhood base. Note that the negative (hence also the positive) cone is closed in E by Lemma 3.5.

Until now, we have considered a full cone (P,V). For a subcone Q of P we may consider its set B_Q of bounded elements. Inside $P-B$ we form $Q-B_Q$ and we have embedded Q in a cone where the bounded elements form a vector space $E_Q = B_Q - B_Q$. Thus we have proved:

4.9 Embedding Theorem. *Every separated locally convex cone (Q,V) can be embedded in a separated locally convex cone (Q',V') in which the bounded elements form a vector subspace $E_{Q'}$. With respect to the symmetric topology $E_{Q'}$ is a locally convex ordered topological vector space. The embedding is an isomorphism for the global preorders on Q and Q'.*

4.10 Remark. If we start with a Hausdorff locally convex topological vector space E and if we consider the cone $P = Conv(E)$ of all non-empty convex subsets of E, the cancellation laws 4.3 through 4.7 are well-known (c.f. Hörmander [7], Pinsker [12], Rådström [15], Rabinovich [13], [14], K. D. Schmidt [19]. Also the embedding of the cone $\overline{B}$ of non-empty closed bounded convex subsets into a locally convex topological vector space has been investigated by the same authors. It has been done in particular detail in [19].

We want to investigate now separated locally convex cones (Q,V) which may be represented as a cones of closed decreasing convex subsets of a locally convex ordered vector space. This representation should be injective and faithful with respect to the global preorder. It will represent the scalar multiplication as well, but unfortunately, without additional requirements on Q, the addition of unbounded elements as well as the abstract 0-neighborhoods do not seem to be reflected in a nice way

By 4.9 we may suppose that the bounded elements of Q form a vector space E, which we endow with the abstract 0-neighborhoods inherited by Q-B_Q. With the symmetric topology, E is a locally convex ordered vector space as shown in 4.8. This is the vector space that we use. For every $a \in Q$, let

$$C(a) = \{b \in E \mid b \leq a\}.$$

The set $C(a)$ clearly is convex and decreasing. It is closed with respect to the lower topology (hence also for the symmetric topology), by 3.5. Thus, we have a mapping $a \to C(a)$ of Q into the cone $\overline{DConv(E)}$ of closed and decreasing (with respect to the global preorder and the lower topology) subsets of E. Recall that $\overline{DConv(E)}$ is a locally convex cone with its addition $\overline{\oplus}$, the canonical preorder $\leq$ and the abstract neighborhoods via those in E, as described in Example 2.8. Moreover, as the separated reflection of $Conv(E)$ (Examples 3.12), $\overline{DConv(E)}$ is separated itself, its given and its global preorders coincide and are nothing but the inclusion.
Our mapping $a \to C(a)$ clearly is monotone with respect to this preorder on $\overline{DConv(E)}$ and the global preorder on Q. But this embedding will not necessarily be injective and an order isomorphism without additional requirements: Q should contain sufficiently many bounded elements, which already describe its abstract 0-neighborhood system.

4.11 Tight coverage by bounded elements. A locally convex cone (Q,V) is said to be *tightly covered by its bounded elements* if for all $a,a' \in Q$ and $v \in V$ such that $a \notin v(a')$ there is some *bounded element* $b \in Q$ such that $b \leq a$ and $b \notin v(a')$.

Obviously, now, this property will guarantee that $a \not\leq a'+v$ for some $v \in V$, implies the existence of some bounded element $b \in C(a)$, but $b \not\leq a'+v$, i.e. $C(a) \notin v(C(a'))$; our embedding is indeed an order isomorphism.

Considering the algebraic operations, we clearly have $C(\lambda a) = \lambda C(a)$ for $\lambda > 0$. For the addition, in general, we only can prove $C(a) \oplus C(a') \subset C(a+a')$, but not equality. Furthermore, our representation is not yet faithful for the abstract 0-neighborhoods of Q and $\overline{DConv(E)}$. In order to obtain this we shall require the

4.12 Continuous decomposition property. If in addition Q has the *continuous decomposition property for bounded elements*

(CDB) If d is bounded and $d \leq a+a'+v$ for $a,a' \in Q$, $v \in V$ then there are bounded elements $b,b' \in Q$ such that $b \leq a$, $b' \leq a'$ and $d \leq b+b'+v$.

then for every element $d \in C(a+a')$, i.e. $d \leq a+a'$ and $v \in V$ we choose b,b' as in (CDB). So, $b+b' \in C(a)+C(a')$, $d \in C(a) \overline{\oplus} C(a')$ by the definition of the operation $\overline{\oplus}$, and indeed $C(a+a') = C(a)+C(a')$.

Now suppose that $a \leq a'+v$ for $a,a' \in Q$. Then for $d \in C(a)$ we have $d \leq a'+v$. Applying (CDB) with $a = 0$, this renders bounded elements $b' \leq a'$, $b \leq 0$, whence $b+b' \in C(a')$, and $d \leq b+b'+v$, whence $C(a) \in v(C(a'))$ as well. The converse was shown to be a consequence of property 4.11.

Summarizing this, yields:

4.13 Representation Theorem. *Every separated locally convex cone Q which is tightly covered by its bounded elements may be represented as a cone of closed decreasing subsets of a locally convex ordered vector space E. This representation is an isomorphism with respect to the global preorders on Q and $\overline{DConv(E)}$. It represents the scalar multiplication and, if Q has property* (CDB), *the addition and the abstract neighborhood system as well.*

4.14 Examples. Reviewing our standard examples for the properties 4.11 and 4.12, this renders:

$\overline{R}$ clearly is tightly covered by its bounded elements and has property (CDB) (Example 2.6).

The same obviously holds for the locally convex ordered vector space $(E,\leq)$ as a locally convex cone (Example 2.7).

As in Example 2.8, let (Q,V) be a locally convex cone with its global preorder, B the subcone of its bounded elements. If D is any a subcone of $Conv(B)$, which contains all singleton sets $\{b\}$, $b \in B$, then properties 4.11 holds for D:
Suppose $A \not\leq A'+v$ for sets $A,A' \in D$, and $v \in V$, i.e. there is some $a \in A$, such that $a \not\leq a'+v$ for all $a' \in A'$. Since a is bounded in Q, so is $\{a\}$ in D, and we have $\{a\} \leq A$, but $\{a\} \not\leq A'+v$.
No general statement seems possible for (CDB) in this case.

The same holds for cones of cone-valued functions (Example 2.9) But in many applications of this we will restrict ourselves to bounded functions anyway, for which both 4.11 and 4.12 are trivial.

5. Locally convex cones via convex semiuniform structures.

We want to show that the notion of a locally convex cone can be defined in a natural way via semiuniform structures in the sense of Nachbin [10]. For this, we use the notation $R \circ S = \{(a,c) \mid$ there is b such that $(a,b) \in R$ and $(b,c) \in S\}$ for the relational product for two binary relations R and S on a set Q, and R^{-1} for the converse relation $\{(b,a) \mid (a,b) \in R\}$; the diagonal is denoted by $\triangle$. We recall the following:

5.1 Semiuniform structures. A collection $\mathcal{U}$ of subsets of $Q \times Q$ is called a *semiuniform structure on* Q, if the following hold:

(U1) $\triangle \subset U$ for every $U \in \mathcal{U}$;

(U2) for all $U,V \in \mathcal{U}$ there is a $W \in \mathcal{U}$ such that $W \subset U \cap V$;

(U3) for all $U \in \mathcal{U}$ there is a $V \in \mathcal{U}$ such that $V \circ V \subset U$.

Nachbin has called this a basis of a semiuniform structure, as we require $\mathcal{U}$ to be a filter basis only and not a filter.

To every uniform structure $\mathcal{U}$ on Q we associate

(a) a preorder defined by $a \leq b$ iff $(a,b) \in U$ for all $U \in \mathcal{U}$; the graph of this preorder is the set $\gamma = \bigcap_{U \in \mathcal{U}} U$.

(b) two topologies: The neighborhood bases for an element a for the *upper* and *lower* topology are given by the sets

$$U(a) = \{b \in Q \mid (b,a) \in Q\}, \quad U \in \mathcal{U},$$
$$(a)U = \{b \in Q \mid (a,b) \in Q\}, \quad U \in \mathcal{U},$$

respectively.

(c) a *uniform structure* $\mathcal{U}_s = \{U \cap U^{-1} \mid U \in \mathcal{U}\}$; the topology associated with this uniform structure is the common refinement of the lower and upper topology; it is Hausdorff iff the preorder $\leq$ is in fact an order.

5.2 The semiuniform structure of a locally convex cone. Let Q be a preordered cone and $\mathcal{V}$ an abstract neighborhood system (contained in some preordered cone $P \supset Q$). For every abstract neighborhood $v \in \mathcal{V}$, we put

$$\tilde{v} = \{(a,b) \in Q \times Q \mid a \leq b+v\}$$

The collection $\tilde{\mathcal{V}}$ of all $\tilde{v}$, $v \in \mathcal{V}$, is a semiuniform structure:

As $0 \leq v$, we have $a \leq a+v$ for all a, whence (U1). As $\mathcal{V}$ is directed downward, we also have (U2). Furthermore, we have the property

(U'3) $(\lambda v)^{\sim} \circ (\mu v)^{\sim} \subset ((\lambda+\mu)v)^{\sim}$ for all $\lambda,\mu > 0$;

indeed, $a \le b+\lambda v$ and $b \le c+\mu v$ imply $a \le c+(\lambda+\mu)v$. Choosing $w = v/2$ in (U'3) we obtain $\tilde{w} \circ \tilde{w} \subset \tilde{v}$, whence (U3).

In addition, it is easy to see that all the $\tilde{v}$ are convex subsets of $Q \times Q$, and

(U4) for $U \in \boldsymbol{U}$, $\lambda > 0$, we have $\lambda U \in \boldsymbol{U}$ as well.

Finally, if (Q,V) is a locally convex cone, the condition that every element has to be bounded below, translates into:

(U5) For all $a \in Q$ and $U \in \boldsymbol{U}$ there is some $\rho > 0$ such that $(0,a) \in \rho U$.

So we have a convex semiuniform structure in the following sense:

5.3 Convex semiuniform structures. Let Q be a cone. A collection $\boldsymbol{U}$ of convex subsets $U \subset Q \times Q$ is called a *convex semiuniform structure*, if $\boldsymbol{U}$ satisfies the properties (U1), (U2), (U'3) and (U4).

If we start with an abstract neighborhood system V on a preordered cone as above, the lower and upper topologies on Q are precisely the lower and upper topologies associated with the semiuniform structure $\tilde{\boldsymbol{V}}$. The preorder associated with this semiuniform structure coincides with the global preorder on Q; indeed, $(a\, b) \in \tilde{v}$ for every $v \in \boldsymbol{V}$ means $a \le b+v$ for every $v \in V$. Thus, the global preorder and the various topologies on a locally convex preordered cone are all described by the semiuniform structure $\tilde{\boldsymbol{V}}$.

5.4 The abstract neighborhood system for a convex semiuniform structure. Let $\boldsymbol{U}$ be a convex semiuniform structure on a cone Q. We shall embed Q in a preordered cone P containig an abstract neighborhood system $\boldsymbol{V}$ in such a way that the canonical semiuniform structure $\tilde{\boldsymbol{V}}$ associated with $\boldsymbol{V}$ is equivalent to the original semiuniform structure $\boldsymbol{U}$ on Q.

For this, let $\boldsymbol{B}$ be any 'subbasis' of $\boldsymbol{U}$, which means that for every $U \in \boldsymbol{U}$ one can find $U_1,\dots,U_n \in \boldsymbol{B}$ and $\lambda_1,\dots\lambda_n > 0$ such that $\lambda_1 U_1 \cap \dots \cap \lambda_n U_n \subset U$. Let $\boldsymbol{V}$ be the set of all families

$r = (r_U)_{U \in \boldsymbol{B}}$ where r_U is a strictly positive real number for finitely many $U \in \boldsymbol{B}$ and $r_U = +\infty$ else.

Adjoining a zero (0) to $\boldsymbol{V}$, we obtain an ordered cone $\boldsymbol{V}_0$ with componentwise defined operations and order.

Let P be the direct sum $P = Q \oplus \boldsymbol{V}_0$ with the usual addition and scalar multiplication. Define a preorder on P in the following way:

$x \oplus r \le y \oplus s$ if $r \le s$ and $(x,y) \in \lambda U$ for all $\lambda > s_U - r_U$ whenever $s_U < +\infty$.

This relation clearly is reflexive. Let us show transitivity: Let $x \oplus r \le y \oplus s \le z \oplus t$. Then firstly $r \le s \le t$; secondly, consider any U with $t_U < +\infty$, and let $\lambda > t_U - r_U$. Then there are λ_1, λ_2 such that $\lambda = \lambda_1 + \lambda_2$, $\lambda_1 > s_U - r_U$, $\lambda_2 > t_U - s_U$. We conclude

that $(x,y) \in \lambda_1 U$ and $(y,z) \in \lambda_2 U$, whence $(x,z) \in \lambda_1 U \circ \lambda_2 U \subset (\lambda_1+\lambda_2)U = \lambda U$ by (U'3). Thus $x \oplus r \leq z \oplus t$.

Let us show the compatibility of this preorder with the algebraic operations: Let $x \oplus r \leq y \oplus s$. Clearly, $\lambda(x \oplus r) \leq \lambda(y \oplus s)$. Let us show that $(x \oplus r)+(z \oplus t) \leq (y \oplus s)+(z \oplus t)$: Firstly, $r \leq s$ implies $r+t \leq s+t$. Secondly, take any U such that $s_U+t_U < +\infty$. Then r_U, s_U, t_U are all finite and for every $\lambda > (s_U+t_U)-(r_U+t_U) = s_U-r_U$ we have $(x,y) \in \lambda U$. As $(z,z) \in \varepsilon U$ for all $\varepsilon>0$ we conclude that $(x+z,y+z) \in (\lambda+\varepsilon)U$, whence the assertion.

Now we have proved that $P = Q \oplus V_0$ is a preordered cone. It is easy to see that V (identified with $\{0\} \oplus V$) is an abstract neighborhood system on P.

When is $x \leq y \oplus r$ for $x,y \in Q$ and $r \in V$? Let $U_1,\ldots U_n$ be the members of B such that r_U is finite. Then

$x \leq y \oplus r$ iff $(x,y) \leq \lambda_i U_i$ for all $\lambda_i > r_{U_i}$ and all i,

i.e. $x \leq y \oplus r$ iff $(x,y) \in \lambda(r_{U_1} U_1 \cap \ldots \cap r_{U_n} U_n)$ for all $\lambda>1$.

As B was chosen to be a 'subbasis' of the semiuniform structure U, we see that U is equivalent to the semiuniform structure $\tilde{V}$ consisting of all $\tilde{v} = \{(x,y) \mid x \leq y \oplus r\}$.
We summarize:

5.5 Proposition. *The notions of an abstract neighborhood system V and a convex semiuniform structure U for a cone Q are equivalent in the following sense:*

For every abstract neighborhood system V for a preordered cone Q there is a convex semiuniform structure $\tilde{V}$ on Q which induces the global preorder on Q and the same upper, lower and symmetric topologies.

If Q is a cone with a convex semiuniform structure U, then one can find a preorder and an abstract neighborhood system V for Q such that the semiuniform structure $\tilde{V}$ is equivalent to U.

As we mentioned above, the condition of lower boundedness for elements of a locally convex cone translates into condition (U5) in terms of the convex semiuniform structure. Thus, the two approaches to locally convex cones firstly via a preorder and an abstract neighborhood system and secondly via convex semiuniform structures turned out to be equivalent. In fact, in applications the second approach will often arise more naturally, as it avoids the explicit construction of a full cone containing the abstract neighborhood system.

6. Uniformly continuous operators.

6.1 Linear operators. For cones Q and P, a map $T : Q \to P$ is called a *linear operator*, if

$$T(a+b) = T(a)+T(b) \qquad \text{for all } a,b \in Q \text{ and}$$
$$T(\alpha a) = \alpha T(a) \qquad \text{for all } a \in Q \text{ and } \alpha \leq 0.$$

Note that this implies $T(0_Q) = 0_P$.

6.2 Uniformly continuous linear operators. In the following let (Q,V) and (P,W) be two preordered locally convex cones. A linear operator $T : Q \to P$ is called *uniformly continuous* or *u-continuous* for short, if for every $w \in W$ one can find a $v \in V$ such that

$$a \leq b+v \text{ implies } T(a) \leq T(b)+w.$$

Uniform continuity is not just continuity. It is immediate from the definition that it combines continuity with respect to the upper, lower and symmetric topologies on Q and P.

6.3 Remarks. (a) Let us consider on Q and P the semiuniform structures $\tilde{V}$ and $\tilde{W}$ as in section 5, i.e. $\tilde{V}$ is the collection of all

$$\tilde{v} = \{(a,b) \in Q \times Q \mid a \leq b+v\}, \quad v \in V$$

and likewise for $\tilde{W}$. Then a linear operator $T : Q \to P$ is u-continuous if and only if it is uniformly continuous with respect to these semiuniform structures in the sense that for every $\tilde{w} \in \tilde{W}$ there is a $\tilde{v} \in \tilde{V}$ such that $(a,b) \in \tilde{v}$ implies $(T(a),T(b)) \in \tilde{w}$.

(b) If Q is a full cone, then a monotone linear operator $T : Q \to P$ is u-continuous, if for every $w \in W$ there is a $v \in V$ such that $T(v) \leq w$. Indeed, if $T(v) \leq w$, then $a \leq b+v$ implies $T(a) \leq T(b+v) = T(b)+T(v) \leq T(b)+w$.

As an immediate consequence from Proposition 3.8 we have:

6.4 Monotonicity Lemma. *Let $T : Q \to P$ be a u-continuous linear operator. Then $a \lesssim b$ implies $T(a) \lesssim T(b)$, where $\lesssim$ denotes the global preorder on Q and P, respectively.*

Since for the original preorder $\leq$ on Q $a \leq b$ implies $a \lesssim b$ we conclude that $a \leq b$ implies $T(a) \lesssim T(b)$ as well. Using the notations of sections 3 and 4 we obtain:

6.5 Proposition. *Let $T : Q \to P$ be u-continuous. There is a unique corresponding u-continuous operator*

$$\overline{T} : \overline{Q}\text{-}\overline{B}_Q \to \overline{P}\text{-}\overline{B}_P$$

such that $\overline{T}(\overline{a}) = \overline{T(a)}$ *for all* $a \in Q$, *where* $\overline{B}_Q$ *and* $\overline{B}_P$ *denote the subcones of bounded elements in* Q *and* P, *respectively, and* $\overline{a}$ *and* $\overline{T(a)}$ *the closures of* a *and* $T(a)$.

Proof. Firstly, we observe that under T the image of each bounded element of Q is bounded in P: Indeed, let $a \in B_Q$ and $w \in W$. Then there is $v \in V$ such that $a \le b+v$ implies $T(a) \le T(b)+w$. As $a \le \rho v$ for some $\rho>0$, this shows $T(a) \le \rho w$. Secondly, if $\overline{a} = \overline{b}$ for $a,b \in Q$ then $T(a) \le T(b)$ as well as $T(b) \le T(a)$. Thus, $\overline{T(a)} = \overline{T(b)}$, and $\overline{T}$ is well defined; u-continuity is easily checked. Thirdly, any linear operator on $\overline{Q}\text{-}\overline{B}_Q$ obviously is already determined by its values on $\overline{Q}$.

6.6 Examples. (a) Addition $(a,b) \to a+b$ is a u-continuous operator from $Q \times Q$ into Q. Indeed, given $w \in V$, we choose $v = w/2$ and we obtain that $a \le c+v$ and $b \le d+v$ imply $a+b \le c+d+w$.

(b) For fixed $\lambda \ge 0$, the operator $a \to \lambda a : Q \to Q$ is u-continuous.

(c) For every bounded element $b \ge 0$, the map $\lambda \to \lambda b : R_+ \to Q$ is u-continuous. Indeed, given $w \in V$, choose an $\varepsilon>0$ such that $b \le \varepsilon w$. Then $\mu \le \lambda+\varepsilon$ and $b \ge 0$ imply $\mu b \le (\lambda+\varepsilon)b = \lambda b+\varepsilon b \le \lambda b+w$.

(d) As an immediate consequence of (a) and (b) we obtain: For finitely many bounded positive elements $b_1,\dots,b_n$ in Q the map

$$(\lambda_1,\dots,\lambda_n) \to \sum_i \lambda_i b_i \ : \ R_+^n \to Q$$

is u-continuous.

(e) Let E and F be locally convex topological vector spaces and $T : E \to F$ a continuous linear operator. We extend T to non-empty convex subsets by defining $\tilde{T}(A) = \{ T(a) \mid a \in A \}$. In this way we obtain a linear operator $\tilde{T} : Conv(E) \to Conv(F)$ which is readily verified to be u-continuous.

The same procedure can be applied more generally to extend any u-continuous operator $T : Q \to P$ between arbitrary locally convex cones to a u-continuous linear operator $\tilde{T} : Conv(Q) \to Conv(P)$. Extension to the cones $DConv(Q)$ and $\overline{DConv(Q)}$ (for their locally conves structures, see Example 2.8), however turns out to be less straightforward: It will require properties similar to 4.12.

6.7 The cone of u-continuous linear operators. For two linear operators S and T from Q into P and for $\lambda \ge 0$, the sum $S+T$ and λT are also linear. If both S and T are u-continuous, so are $S+T$ and λT by 6.5(a,b). Thus, the u-continuous linear operators from Q into P form a cone $L(Q,P)$. We do not intend to discuss locally convex structures for this cone in this paper.

7. Linear functionals and the dual cone.

Throughout this section, let (Q,V) be a locally convex cone with its preorder $\leq$ and the global preorder $\preceq$. A *linear functional* on Q is a linear operator $\mu : Q \to \overline{R}$.

7.1 The dual cone. According to 6.1, a linear functional μ on Q is called *uniformly continuous* or simply *u-continuous*, if there is a $v \in V$ such that

(O) $\qquad a \leq b+v$ implies $\mu(a) \leq \mu(b)+1$.

Every u-continuous linear functional is monotone by 6.4, even with respect to the global preorder on Q. The u-continuous linear functionals on Q form again a cone (c.f. 6.7), denoted by Q^* and called the *dual cone* of Q. We shall endow Q^* with the topology $w(Q^*,Q)$ of pointwise convergence of the elements of Q, considered as functions on Q with values in $\overline{R}$ with its usual topology. (Studying duality theory, later on we shall consider $\overline{R}$ with its symmetric topology, which isolates $+\infty$, and the resulting finer topology $s(Q^*,Q)$ on Q^* as well.)

If Q is a full cone and μ a monotone linear functional on Q, then the definition of u-continuity becomes particularly simple: μ will be u-continuous if and only if there is a $v \in V$ such that $\mu(v) \leq 1$. Proposition 6.5 renders for linear functionals:

7.2 Proposition *For every $\mu \in Q^*$ there is a unique $\overline{\mu} \in (Q-B_Q)^*$ such that*

$$\overline{\mu}(\overline{a}-\overline{b}) = \mu(a) - \mu(b).$$

If Q is separated then Q^* and $(Q-B_Q)^*$ may be identified.

7.3 Polars. For every $v \in V$, the *polar* of v is defined to be the set v_Q° of all linear functionals μ on Q satisfying (O), i.e.

$$v_Q^\circ = \{\mu \in Q^* \mid a \leq b+v \text{ implies } \mu(a) \leq \mu(b)+1\}$$

We simply write v° instead of v_Q°, if no confusion is possible. If Q is a full cone, the definition of the polar becomes particularly simple: v_Q° is the set of all monotone linear functionals on Q such that $\mu(v) \leq 1$.

7.4 Proposition. *The polar v° of any $v \in V$ is a compact convex subset of Q^* in the topology $w(Q^*,Q)$.*

Proof. Clearly, v° is convex and closed for pointwise convergence in the set of all functions $f : Q \to \overline{R}$. Remember that every $a \in Q$ is bounded below, i.e. there is a real number $\lambda_a > 0$ such that $0 \leq a+\lambda_a v$. For every μ in v° we then have $0 = \mu(0) \leq \mu(a)+\lambda_a$, whence $\mu(a) \geq -\lambda_a$. Thus, v° is in fact a closed subset of the compact space $\prod_{a \in Q} [-\lambda_a, +\infty]$ and hence compact.

It is an important feature of our notion of locally convex cones that with only slight additional requirements, such as 4.11, we are able to prove all of the desired Hahn-Banach type theorems on the existence of sufficiently many u-continuous linear functionals. Our prime model *Conv(E)* for locally convex cones has plenty of them, indeed: Every continuous linear functional μ on a locally convex topological vector space E may be extended by defining

$\overline{\mu}(A) = \sup\{ \mu(a) \mid a \in A \}$ for every non-empty convex subset A of E.

Thus, we obtain a functional $\overline{\mu} : Conv(E) \to \overline{R}$ which is easily verified to be linear and u-continuous. For deriving our Hahn-Banach type theorems in general we cannot apply directly the corresponding results that one finds e.g. in the book of Fuchssteiner and Lusky [6]; the reason is that in the literature mostly linear and sublinear functionals with values in $R \cup \{-\infty\}$ are considered, whilst we have to deal with functionals which have values in $\overline{R} = R \cup \{+\infty\}$. The difference between those two points of view is essential and not just a question of reversing the order on R. We have to begin with a few remarks on sublinear functionals:

7.5 Sublinear functionals. A map $p : Q \to \overline{R}$ is *sublinear* if

$p(a+b) \le p(a)+p(b)$ and $p(\lambda a) = \lambda p(a)$ for all $a,b \in Q$ and $\lambda \ge 0$.

A a sublinear functional p is called *u-continuous*, if there is a neighborhood $v \in V$ such that

(O) $a \le b+v$ implies $p(a) \le p(b)+1$ whenever $a,b \in Q$.

Every u-continuous sublinear functional is monotone by Proposition 3.8, even monotone with respect to the global preorder on Q.

If Q is a full cone and p a monotone sublinear functional on Q, then the definition of u-continuity becomes particularly simple: p will be u-continuous if and only if there is a $v \in V$ such that $p(v) \le 1$.

7.6 Lemma. *Let Q be a subcone of the preordered locally convex cone (P,V). Every u-continuous sublinear functional on Q can be extended to a u-continuous sublinear functional on P; more precisely: Let p be a sublinear functional on Q and $v \in V$ such that*

(O) $a \le b+v$ *implies* $p(a) \le p(b)+1$, *whenever* $a,b \in Q$,

then there is a sublinear functional $\tilde{p}$ on P extending p such that

(O') $x \le y+v$ *implies* $\tilde{p}(x) \le \tilde{p}(y)+1$, *whenever* $x,y \in P$.

Proof. For every $x \in P$ we define

$$\tilde{p}(x) = \inf\{ p(a)+\lambda \mid x \le a+\lambda v \text{ for some } a \in Q \text{ and } \lambda > 0 \}.$$

We verify:

(*i*) $\tilde{p}$ is an extension of p: Let $x \in Q$. Clearly, $\tilde{p}(x) \le p(x)$. For the converse inequality consider any α such that $\tilde{p}(x) < \alpha$. Then there is an $a \in Q$ and a

$\lambda>0$ such that $x \le a+\lambda v$ and $p(a)+\lambda < \alpha$. Condition (O) implies $p(x) \le p(a)+\lambda < \alpha$. As this holds forevery $\alpha > \tilde{p}(x)$, we infer $p(x) < \tilde{p}(x)$.

(*ii*) $\tilde{p}$ satisfies (O'): Let $x,y \in P$ with $x \le y+v$. We want to show $\tilde{p}(x) \le \tilde{p}(y)+1$. This is clear if $\tilde{p}(y) = +\infty$. So suppose $\tilde{p}(y) < +\infty$. For every $\alpha > \tilde{p}(y)$ we may find $a \in Q$ and $\lambda>0$ such that $y \le a+\lambda v$ and $p(a)+\lambda \le \alpha$. We conclude $x \le y+v \le a+(\lambda+1)v$, Whence $\tilde{p}(x) \le p(a)+\lambda+1 < \alpha+1$. As this holds for every $\alpha > \tilde{p}(y)$, we obtain $\tilde{p}(x) \le \tilde{p}(y)+1$.

(*iii*) $\tilde{p}$ is sublinear: The proofs are similar to the above, and we leave them to the reader.

7.7 Superlinear functionals. A map $q : Q \to \boldsymbol{R} \cup \{+\infty,-\infty\}$ is *superlinear* if

$$q(\lambda a) = \lambda q(a) \text{ for all } \lambda \ge 0,\ a \in Q \text{ and}$$

$$q(a+b) \ge q(a)+q(b) \text{ for all } a,b \in Q \text{ such that both } q(a) \text{ and } q(b) \text{ are finite.}$$

7.8 Sandwich Theorem. *Let (Q,V) be a preordered locally convex cone. Let $q : Q \to \boldsymbol{R} \cup \{+\infty,-\infty\}$ be superlinear and $p : Q \to \overline{\boldsymbol{R}} \cup \{+\infty\}$ sublinear with $q(a) \le p(a)$ for all $a \in Q$. If p is u-continuous, then there is a u-continuous linear functional $\mu : Q \to \overline{\boldsymbol{R}}$ such that $q(a) \le \mu(a) \le p(a)$ for all $a \in Q$,*

more precisely: If, for some $v \in V$, the functional p satisfies

(O) $\quad a \le b+v$ *implies* $p(a) \le p(b)+1$ *whenever* $a,b \in Q$,

then there is a linear functional μ in the polar v_Q° of v such that $q(a) \le \mu(a) \le p(a)$ for all $a \in Q$.

Proof. We may suppose that Q is a full cone. In fact, by Lemma 7.6 we can extend p to a full cone containig Q without disturbing hypothesis (O), and q may be extended by defining its value to be $-\infty$ on the new elements. Now we consider the subset of Q

$$Q_f = \{\, a \in Q \mid p(a) < +\infty \,\}.$$

As p is sublinear and monotone, Q_f is a decreasing subcone of Q. Let us show that Q_f is a face of Q: Let a,b be elements of Q such that $a+b \in Q_f$, i.e. $p(a+b) < +\infty$. Recall that in a locally convex cone every element is bounded below. Hence there is a $\lambda>0$ such that $0 \le a+\lambda v$, whence $b \le a+b+\lambda v$. As p satisfies (O), we infer that $p(b) \le p(a+b)+\lambda$, whence $p(b) < +\infty$, i.e. $b \in Q_f$.

On Q_f the sublinear functional p does not take the value $+\infty$, and we may apply the Theorem 1.2.5 in [6] which assures the existence of a monotone linear functional μ on Q_f with values in $R \cup \{-\infty\}$ such that $q(a) \le \mu(a) \le p(a)$ for all $a \in Q_f$. By (O) we have $p(v) \le 1$, whence $\mu(v) \le 1$. This shows that in fact μ does not attain the value $-\infty$: As every $a \in Q$ is bounded below, there is $\lambda_a>0$ such that $0 \le a+\lambda_a v$; i.e. $0 = \mu(0) \le \mu(a)+\lambda_a$ and $\mu(a) \ge -\lambda_a$. We extend μ to Q by $\mu(a) = +\infty$ for all $a \notin Q_f$. As Q_f is a decreasing face, μ is still monotone and linear, and obviously $q(a) \le \mu(a) \le p(a)$ holds for all $a \in Q$. Finally, $\mu(v) \le 1$ implies $\mu \in v_Q^\circ$.

7.9 Extension Theorem. *Let Q be a subcone of the locally convex cone (P,V). Then every u-continuous linear functional on Q can be extended to a u-continuous linear functional on P; more precisely: For every $\mu \in v_Q^\circ$ there is a $\tilde{\mu} \in v_P^\circ$ such that $\mu = \tilde{\mu}_{|Q}$.*

Proof. By Lemma 6.5 we may extend μ to a sublinear functional p on P which satisfies (O) for all $a,b \in P$. We define a superlinear functional q on P by

$$q(a) = \begin{cases} \mu(a) & \text{if } a \in Q \\ -\infty & \text{else.} \end{cases}$$

By the Sandwich Theorem 6.6 we find a linear functional $\tilde{\mu} \in v_Q^\circ$ such that $q(a) \le \tilde{\mu}(a) \le p(a)$ for all $a \in P$. As $q(a) = \mu(a) = p(a)$ for all $a \in Q$, the functional $\tilde{\mu}$ extends μ.

7.10 Weak separation. *Let $a,b \in Q$ with $b \ge 0$ and let $v \in V$ such that $a \not\le b+v$. Then there is a linear functional μ on Q such that*

$$\mu(a) \ge 1 \quad \textit{and} \quad \mu(x) \le 1 \ \textit{whenever}\ x \le b+v;$$

more generally:

$$\mu(x) \le \mu(y)+1 \ \textit{whenever}\ x \le y+b+v.$$

Proof. Let $w = b+v$. We may suppose that $w \in V$, as $b \ge 0$. Let $Q_o = \{\alpha a \mid \alpha \ge 0\}$. and define $\mu_0 : Q_o \to \overline{R}$ by

$$\mu_0(\alpha a) = \alpha \inf\{\lambda > 0 \mid a \le \lambda v\}.$$

Then μ_0 is a linear functional on Q_o contained in the polar of w in Q_o^*. By the extension Theorem 7.9, μ_0 has a linear extension μ to Q which is contained in the polar of w in Q^*. The extension μ has the desired properties.

In order to obtain strict separation, we have to reinforce the hypothesis:

7.11 Lemma. *Let $v \in V$, let a be a v-bounded and b an arbitrary element of Q such that $a \not\le b+\rho v$ for some $\rho > 1$, then there is a linear functional $\mu \in v_Q^\circ$ such that*

$$\mu(a) > \mu(b)+1.$$

Proof. We may suppose that Q is a full cone. First we choose an α such that $0 \le b+\alpha v$. We then have

$$a+\alpha v \not\le b+\alpha v+\sigma v \quad \text{whenever } 1 < \sigma < v.$$

Indeed, the inequality $a+\alpha v \le b+\alpha v+\sigma v$ would imply $a \le b+\rho v$ for all $\rho > \sigma$ by the cancellation Lemma 4.2. Replacing a by $a+\alpha v$ and b by $b+\alpha v$ in 4.10, we may find a linear functional $\nu \in Q^*$ such that

(i) $\nu(a+\alpha v) \ge 1$ and (ii) $\nu(b+\alpha v+\sigma v) \le 1$.

From these inequalities we conclude that

$$\nu(a)+\alpha\nu(v) \ge \nu(b)+\alpha\nu(v)+\sigma\nu(v), \quad \text{whence}$$

(iii) $\nu(a) \ge \nu(b)+\sigma\nu(v)$.

From (ii) we also get that $\nu(v) \neq +\infty$. Indeed, if $\nu(v) = 0$, then we choose $\lambda>0$ such that $a \leq \lambda v$ (which is possible, as a is supposed to be v-bounded) and we get $\nu(a+\alpha v) \leq \nu(\lambda v+\alpha v) = 0$ which contradicts (i). So (iii) implies

(iv) $\nu(a) > \nu(b)+\nu(v)$.

Now we put $\mu = \nu/\nu(v)$. Then (iv) becomes $\mu(a) > \mu(b)+1$ and μ is contained in the polar of v as $\mu(v) =1$.

7.12 Strict separation. The separation property as formulated in the preceding lemma will in general not hold for unbounded elements a in an arbitrary locally convex cone (Q,V). This property, however, turns out to be crucial in the investigation of Korovkin type approximation.

We shall say that (Q,V) has the *strict separation property* , if

(S P) for all $a,b \in Q$ and $v \in V$ such that $a \not\leq b+v$, i.e $a \not\leq b+\rho v$ for some $\rho>1$, there is a linear functional $\mu \in v_Q^\circ$ such that $\mu(a) > \mu(b)+1$.

(Note that $\mu(x) \leq \mu(y)+1$, whenever $x \leq y+v$, as $\mu \in v_Q^\circ$.) In view of the preceding lemma, we will obtain strict separation if we have sufficiently many bounded elements in Q. This will be guaranteed by property 4.11:

7.13 Separation Theorem. *Every locally convex cone (Q,V) which is tightly covered by its bounded elements (c.f.* 4.11*) has the strict separation property* (SP).

Proof. By (4.11) choose a bounded element $a' \leq a$ such that $a' \not\leq b+\rho' v$ for some $\rho'>1$. Lemma 7.11 yields a linear functional $\mu \in v_Q^\circ$ such that $\mu(a') \geq \mu(b)+1$. As $\mu(a) \geq \mu(a')$, we have the desired result.

The Sandwich Theorem and its corollaries will provide the main tools for further studies of the duality theory of locally convex cones. Korovkin type approximation theorems may be derived using the preceding separation results. We shall deal with those subjects at a different place.

References.

[1] **Altomare, F.:** *On Korovkin type theorems in spaces of continuous complex-valued functions.* Bolletino U.M.I. (6) 1-B, 75-86 (1982).

[2] **Bauer, H.:** *Theorems of Korovkin type for adapted spaces.* Ann. Inst. Fourier 23, 245-260 (1973).

[3] **Behrens, H. and Lorentz, G.G.:** *Theorems of Korovkin type for positive linear operators on Banach lattices.* In: Approximation Theory (ed.: G.G. Lorentz), Academic press, New York, 1-30 (1973).

[4] **Donner, K.:** *Extensions of positive operators and Korovkin Theorems.* Lecture Notes in Math. 904, Springer Verlag, Heidelberg - Berlin - New York.

[5] **Flösser, H.O., Irmisch, R. and Roth, W.:** *Infimum-stable convex cones and approximation.* Proc. London Math. Soc. (3) 42, 104-120 (1981).

[6] **Fuchssteiner, B. and Lusky, W.:** *Convex Cones.* North Holland Math. Studies 56, (2881).

[7] **Hörmander, L.:** *Sur la fonction d'appui des ensembles convexes dans un espace localement convexe.* Arkiv Mat. 3, 181-286 (1954).

[8] **Hudzik, H., Musielak, J.and Urbansky, R.:** *Lattice properties of the space of convex closed and bounded subsets of a topological vector space.* Bull. Acad. Polon. Sci. Sér. Sci. Math 27, 157-162 (1979).

[9] **Keimel, K. and Roth, W.:** *A Korovkin type approximation theorem for set-valued functions.* Proc. Amer. Math. Soc. (to appear).

[10] **Nachbin, L.:** *Topology ond order.* Van Nostrand, Princeton (1969).

[11] **Pannenberg, M.:** *Topics in qualitative Korovkin approximation.* Math. Inst. Univ. Münster, Preprint (1987).

[12] **Pinsker, A.G.:** *The space of convex sets of a locally convex space* (Russian). Trudy Leningrad. Inzh.-Ekon. In-ta 63, 13-17 (1966).

[13] **Rabinovich, M.G.:** *An embedding theorem for spaces of convex sets* (Russian). Sibirsk. Mat. Zh. 8, 376-383 (1967). (English transl. Siberian Math. J. 8, 275-279 (1067).

[14] **Rabinovich, M.G.:** *Some classes of spaces of convex sets and their extensions* (Russian). Sibirsk. Mat. Zh. 8, 1405-1415 (1967). (English transl.Siberian Math. J. 8, 1064-11070 (1067).

[15] **Rådström, H.:** *An embedding theorem for spaces of convex sets.* Proc. Amer. Math Soc. 3, 165-169 (1952).

[16] **Roth, W.:** *Families of convex subsets and Korovkin type theorems in locally convex spaces.* Rev. Roum. Math. Pures et Appl. (to appear).

[17] **Scheffold, E.:** *Über Konvergenz linearer Operatoren.* Mathematica 20 (43), 193-198 (1975).

[18] **Schirotzek, W.:** *Extensions of additive non-negatively homogeneous functionals in quasilinear spaces.* Demonstratio Math. 10, 241-260.

[19] **Schmidt, K.D.:** *Embedding theorems for classes of convex sets.* Acta Appl. Math 5, 209-237 (1986).

[20] **Topsøe, F.:** *The naive approach to the Hahn-Banach Theorem.* Comment. Math. Special Issue 1, 315-330 (1978).

[21] **Urbanski, R.:** *A generalization of the Minkowsky-Rådström-Hörmander theorem.* Bull. Acad. Polon. Sc., ser. sc. math., astr. et phys. 24, 709-725 (1976).

[22] **Vitale, R.A.:** *Approximation of convex set-valued functions.* J. Approximation Theory 26 ,301-316 (1979).

[23] **Wolff, M.:** *On the theory of approximation by positive linear operators in vector lattices.* In: Functional Analysis: Surveys and recent results (eds.: K. D. Bierstedt, B. Fuchssteiner), North Holland Math. Studies 27, 73-87 (1977).

K. Keimel
Fachbereich Mathematik
Technische Hochschule
D-6100 Darmstadt
West-Germany

W. Roth
Department of Mathematics
University of Bahrain
P.O. Box 3082
State of Bahrain

A Positivstellensatz for Chain-closed Fields

*Rafael Farré**
Facultat de Matemàtiques, Universitat de Barcelona
Gran Via 585, 08007 Barcelona, SPAIN

A Chain-closed field admits two different orders. We shall fix one of these orders and determine all the functions definite positive. in addition to sums of squares, other definite positive functions will turn out generated by operators in the style of the Kochen operator [6] for p-adic fields.

1.Algebraic preliminaries

We shall start with a general theorem which characterizes equationally the existence of valuations and orders compatible with certain prescribed conditions. In order to do it we need two lemmas.

In the following if B is any subset of k, S(B) will denote the semi-ring (closed under addition and multiplication) generated by B.

LEMMA 1.1. *Let k be any field of characteristic 0, A a subring of k, M an ideal of A and B any subset of k. If $-1 \notin S(k^2, B, 1+M)$ then there exists $\overline{M}$ a prime ideal of A extending M and satisfying $-1 \notin S(k^2, B, 1+\overline{M})$.*

Proof. For the sake of simplicity we shall suppose B closed under multiplication and $1 \in B$. We take by Zorn's Lemma $\overline{M}$ a maximal ideal of A with the property $-1 \notin S(k^2, B, 1+\overline{M})$. We will have finished if we prove $\overline{M}$ prime. If not, there exist $x, y \in A$ with $xy \in \overline{M}$, $x \notin \overline{M}$, $y \notin \overline{M}$. By the maximality of $\overline{M}$ we have $-1 \in S(k^2, B, 1+\overline{M}+(x))$ and $-1 \in S(k^2, B, 1+\overline{M}+(y))$:

$$-1 = \sum a_i^2 b_i (1 + m_i + \lambda_i x) \tag{1}$$

* *Work partially supported by grant PB86-0269 Dirección General de Investigación Cientifica y Técnica. The author would like to thank Françoise Delon for her help during the preparation of this work.*

$$-1 = \sum c_j^2 d_j (1 + n_j + \mu_j y) \tag{2}$$

with $a_i, c_j \in k$, $b_i, d_j \in B$, $m_i, n_j \in \overline{M}$ and $\lambda_i, \mu_j \in A$. It is sufficient to obtain $-1 \in S(k^2, B, 1 + \overline{M})$ from (1) and (2). Multiplying (2) by x we obtain:

$$-x(1 + \sum c_j^2 d_j) = \sum c_j^2 d_j (x n_j + \mu_j x y) = \sum c_j^2 d_j \nu_j$$

with $\nu_j \in \overline{M}$. Making $a = \sum c_j^2 d_j$, $b = \sum c_j^2 d_j \nu_j$ we have

$$-x(1 + a) = b \tag{3}$$

Now multiplying (1) by $1 + a$:

$$-1 = a + \sum a_i^2 b_i (1 + a)(1/2 + m_i) + \sum a_i^2 b_i (1 + a)(1/2 + \lambda_i x)$$

were a and the first $\sum$ clearly belong to $S(k^2, B, 1 + \overline{M})$:

$$1/2 + m_i = (1/2)^2 2(1 + 2m_i)$$

To see that the third term also belongs to it, we put

$$(1 + a)(1/2 + \lambda_i x) = 1/2(1 + a + 2(1 + a)\lambda_i x) =$$

by (3)

$$= 1/2(1 + a - 2b\lambda_i) = 1/2(1 + \sum c_j^2 d_j (1 - 2\lambda_i \nu_j))$$

and consequently $-1 \in S(k^2, B, 1 + \overline{M})$. ■

LEMMA 1.2. *Let k be any field of characteristic 0, A a subring of k, M an ideal of A and B any subset of k. If $-1 \notin S(k^2, B, 1 + M)$, then for every $\alpha \in k$ one of the following assertions holds*:

$$-1 \notin S(k^2, B, 1 + M[\alpha])$$

$$-1 \notin S(k^2, B, 1 + M[\alpha^{-1}])$$

Proof. If not we take n and m minimal such that

$$-1 \in S(k^2, B, 1 + M[\alpha]_n)$$

$$-1 \in S(k^2, B, 1 + M[\alpha^{-1}]_m)$$

were $M[\alpha]_n$ is the set of polynomials over M in α of degree less or equal to n. Without loss of generality we can suppose $n \geq m$. Then

$$-1 = \sum a_i^2 b_i (1 + f_i(\alpha)) \tag{1'}$$

$$-1 = \sum c_j^2 d_j (1 + g_j(\alpha^{-1})) \tag{2'}$$

were $a_i, c_j \in k$, $b_i, d_j \in B$ and $f_i, g_j \in M[x]_n$. Multiplying (2') by α^n we obtain

$$-\alpha^n (1 + \sum c_j^2 d_j (1 + g_j(0))) = \sum c_j^2 d_j \tilde{g}_j(\alpha)$$

with $g_j(0) \in M$, $\tilde{g}_j(\alpha) \in M[\alpha]_{n-1}$. Making $a = \sum c_j^2 d_j (1 + g_j(0))$ and $b = \sum c_j^2 d_j \tilde{g}_j(\alpha)$ we obtain

$$-\alpha^n (1 + a) = b \tag{3'}$$

Now multiplying (1') by $1 + a$ we have that

$$-1 = a + \sum a_i^2 b_i (1 + a)(1/2 + \overline{f}_i(\alpha)) + \sum a_i^2 b_i (1 + a)(1/2 + m_i \alpha^n)$$

were $m_i \alpha^n$ is the term of degree n of $f_i(\alpha)$ and $\overline{f}_i(\alpha) \in M[\alpha]_{n-1}$ is the rest. It is clear that a and the first $\sum$ belong to $S(k^2, B, 1 + M[\alpha]_{n-1})$. But

$$(1 + a)(1/2 + m_i \alpha^n) = 1/2(1 + \sum c_j^2 d_j (1 + g_j(0) - 2 m_i \tilde{g}_j(\alpha)))$$

also belongs to $S(k^2, B, 1 + M[\alpha]_{n-1})$ which implies $-1 \in S(k^2, B, 1 + M[\alpha]_{n-1})$, contradiction. ■

If (k, v) is a valued field and $x \in k$ with $v(x) \geq 0$, $\overline{x}$ will denote the class of x modulo M_v. Also we will use the same symbol to denote the class of an element of an ordered abelian group modulo a convex subgroup. If in addition $\leq$ is an order of k and P its positive cone, we shall say that v and $\leq$ are compatible or v is convex with respect to $\leq$ if $1 + M \subseteq P$. This condition is equivalent to $|x| < |y|$ for every $x, y \in k$ such that $v(x) > v(y)$. In this case the order of k induces an order $\leq_{/v}$ in k/v by putting $\overline{x} \geq_{/v} 0$ if and only if $x \geq 0$ (it is easily seen that this condition does not depend on the representant of $\overline{x}$ chosen).

THEOREM 1.3. *Let k be any field of characteristic 0, A a subring of k, M an ideal of A and B any subset of k. Then the following are equivalent:*

(i) $-1 \notin S(k^2, B, 1 + M)$

(ii) There exist an order $\leq$ *and a valuation* v *compatible such that* $B \geq 0$, $A \subseteq A_v$ *and* $M \subseteq M_v$.

Proof. To see i⇒ii we consider $\mathcal{C} = \{(A, M)/\ M$ an ideal of the ring A, $A \subseteq k$, such that $-1 \notin S(k^2, B, 1 + M)\}$, $\mathcal{C}$ ordered by the relation $(A_i, M_i) \leq (A_j, M_j)$ if and only if $A_i \subseteq A_j$ and $M_i \subseteq M_j$. By Zorn's Lemma we take $(\overline{A}, \overline{M})$ maximal. As a consequence of Lemma 1.1 we obtain that $\overline{M}$ is a prime ideal of $\overline{A}$ and by Lemma 1.2 we have that $\overline{A}$ is a valuation ring. But the localisation $\overline{A}_{\overline{M}}$ is also a valuation ring with maximal ideal $\overline{M}$, thus $(\overline{A}_{\overline{M}}, \overline{M})$ is an extension of $(\overline{A}, \overline{M})$ belonging to $\mathcal{C}$. Therefore $\overline{A} = \overline{A}_{\overline{M}}$ and $\overline{M}$ is the maximal ideal of $\overline{A}$. Finally the condition $-1 \notin S(k^2, B, 1 + \overline{M})$ implies the existence of an order $\leq$ over k compatible with the valuation associated to $\overline{A}$ and such that $B \geq 0$. ■

We are now going to develop some consequences of Theorem 1.3.

COROLLARY 1.4. *Let $(k, \leq)$ be an ordered field, A a subring of k and M any ideal of A. Then the following are equivalent:*

(i) $1 + M \geq 0$

(ii) There exists a valuation v compatible with $\leq$ such that $A \subseteq A_v$ and $M \subseteq M_v$.

Proof. Trivial applying Theorem 1.3 with $B = P$ (the positive cone of the order) and observing that $-1 \notin S(k^2, P, 1 + M)$ if and only if $1 + M \subseteq P$. ■

LEMMA 1.5. *Let k be any field, B a subset of k and f an element of k , $f \neq 0$. If $-1 \notin S(k^2, B)$ then the following are equivalent:*

(i) $f \in S(k^2, B)$

(ii) $-1 \in S(k^2, B, -f)$

Proof. W.l.o.g. we may suppose B closed under multiplication and $1 \in B$. To see i⇒ii it suffices to observe $-1 = (-f)f(1/f)^2$. In the other side if $-1 = \sum a_i^2 b_i - f \sum c_i^2 d_i$ with $a_i, c_i \in k$ and $b_i, d_i \in B$, isolating f ($\sum c_i^2 d_i \neq 0$, otherwise $-1 \in S(k^2, B)$) $f = \frac{1+\sum a_i^2 b_i}{\sum c_i^2 d_i} \in S(k^2, B)$ because $S(k^2, B)$ is closed under inverse. ■

THEOREM 1.6. *Let k be any field of characteristic 0, A a subring of k, M an ideal of A and B any subset of k. Then $S(k^2, B, 1 + M) = \bigcap \mathcal{P}$ were $\mathcal{P} = \{$ P, P is the positive cone of an order in k containing B and such that there exists a compatible valuation v with $A \subseteq A_v$ and $M \subseteq M_v\}$.*

Proof. Trivially $S(k^2, B, 1 + M) \subseteq \bigcap \mathcal{P}$. To see the other inclusion we may suppose $-1 \notin S(k^2, B, 1 + M)$, if not $k = S(k^2, B, 1 + M)$ because $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$. If $f \notin S(k^2, B, 1 + M)$ then $-1 \notin S(k^2, B, 1 + M, -f)$ and by Theorem 1.3 there exists $P \in \mathcal{P}$ such that $-f \in P$, i.e. $f \notin P$. ■

COROLLARY 1.7. *Let k be any field of characteristic 0, A a subring of k, B a subset of k and M a multiplicatively closed subset of k such that $AM \subseteq M$. Then $S(k^2, B, 1+M) = \bigcap \mathcal{P}$ were $\mathcal{P} = \{$ P, P is the positive cone of an order in k containing B and such that there exists a compatible valuation v with $A \subseteq A_v$ and $M \subseteq M_v\}$.*

Proof. We apply theorem 1.6 with $A' = A[M] = A + \sum M$ were $\sum M$ means sums of elements of M and M' the ideal generated by M in A', $M' = MA' = \sum M$. It is enough to prove $S(k^2, B, 1 + M) = S(k^2, B, 1 + \sum M)$. But $1 + \sum_1^n m_i = (1/n)^2 n \sum_1^n (1 + nm_i)$, and therefore $1 + \sum M \subseteq S(k^2, 1 + M)$. ■

COROLLARY 1.8. *Let k be any field of characteristic 0, B a subset of k and M a multiplicatively closed subset of k such that $\mathbb{Z}M \subseteq M$. Then $S(k^2, B, 1 + M) = \bigcap \mathcal{P}$ were $\mathcal{P} = \{$ P, P is the positive cone of an order in k containing B and such that there exists a compatible valuation v with $M \subseteq M_v\}$.*

Proof. Corollary 1.8 is a particular case of Corollary 1.7 for $A = \mathbb{Z}$. ■

We are now going to give a general theorem on extensions of valuations and compatible orderings.

Notation. $(k, v, \leq)$ will always be a valued and ordered field with compatibility between v and $\leq$.

LEMMA 1.9. *Let $(k, v, \leq_0)$ be a valued and ordered field, (L, w) an extension of (k, v) with $v(k) = w(L)$ and $\leq_1$ an order over L/w such that $(L/w, \leq_1)$ is an extension of $(k/v, \leq_0 /v)$. Then there exists an order $\leq_2$ over L compatible with w, extending $\leq_0$ and inducing $\leq_1$ on L/w.*

Proof. We define $P_2 = \{x \in L/$ there exists an $x' \in k$ such that $w(x) = v(x')$, $x' >_0 0$ and $\overline{x/x'} >_1 0\}$. $L = P_2 \cup -P_2 \cup \{0\}$ and P_2 is closed under multiplication. To see that $P_2 \cup \{0\}$ is the positive cone of an order it suffices to prove that P_2 is closed under addition. Let $x, y \in P_2$ and w.l.o.g. suppose $v(x) \leq v(y)$. We distinguish two cases.

I. If $v(x + y) = v(x)$ then

$$\overline{\frac{x+y}{x'}} = \overline{x/x'} + \overline{y/x'} = \overline{x/x'} + \overline{y'/x'} \cdot \overline{y/y'} >_1 0$$

and thus $x + y \in P_2$.

II. If $v(x + y) > v(x)$ then $v(x) = v(y)$. Assume $-(x + y) \in P_2$, then we have that $-y = -(x + y) + x \in P_2$ by case I and we arrive to a contradiction. ■

If H is an ordered abelian group (o.a.g.) $\tilde{H}$ will denote its divisible hull $H \otimes_{\mathbf{Z}} \mathbf{Q}$.

PROPOSITION 1.10. *Let $(k, v, \leq)$ be an ordered and valued field and H an o.a.g. such that $v(k) \subseteq H \subseteq \widetilde{v(k)}$. Then there exists $(L, v, \leq)$ an algebraic extension of $(k, v, \leq)$ with (L, v) henselian, $(L/v, \leq_{/v})$ real-closed and $v(L) = H$.*

Proof. First we take (L, v) a henselian extension of (k, v) with residue field $(\widetilde{k/v}, \leq)$ the real closure of $(k/v, , \leq_{/v})$ and $v(k) = v(L)$ (this is alwais posible: [7] prop 3 pag 146). Applying Lemma 1.9 we take an order in L extending the order of k compatible with (L, v) and inducing the order of $\widetilde{k/v}$. Extending v to $(\widetilde{L}, \leq)$ the real closure of $(L, \leq)$ we have a henselian valuation and therefore compatible [5]. Then $v(\widetilde{L})$ is divisible and $(\widetilde{L}/v, \leq) = (\widetilde{k/v}, \leq)$ real-closed. We finally take an extension L_0 of L into $\widetilde{L}$ maximal with the property $v(L_0) \subseteq H$. We will have finished if we prove $v(L_0) = H$. Otherwise let h be an element of $H - v(L_0)$ and n its order into $H/v(L_o)$. Taking $b \in L_0$, $b > 0$ with $v(b) = nh$ and $c = \sqrt[n]{b}$ we have $v(c) = h$. We then note that the following natural inequalities

$$n \leq (v(L_0) + (h), v(L_0)) \leq (v(L_0(c)) : v(L_0)) \leq [L_0(c) : L_0] = n$$

are equalities and therefore $v(L_o(c)) = v(L_o) + (h) \subseteq H$, contradicting the maximality of L_o. ■

2. A Positivstellensatz for Chain-closed fields

A chain-closed field [3] may be characterized as a field carrying a henselian valuation v with real-closed residue field, odd-divisible value group and $(v(k) : 2v(k)) = 2$. We shall call an ordered abelian group H 2-regular if $2H$ is dense into H. The theory of the o.a.g. H odd-divisible, 2-regular and such that $(H : 2H) = 2$ is model-complete in the language $(+, \leq, 0, D)$ were D is a monadic predicate with the following interpretation: $D(x)$ if and

only if $(\exists y)(x = 2y)$ [8]. Equivalently the model-completeness may be formulated in the language $(+, \leq, 0, \alpha)$ were α is a constant satisfying the condition $\alpha \notin 2H$.

If following [1] $V(k) = \{v,\ v$ henselian valuation with real-closed residue field, odd-divisible value group and $(v(k) : 2v(k)) = 2\}$, $V(k)$ is totally ordered by the reverse inclusion of its valuation rings i.e. $v \geq w$ if and only if $A_v \subseteq A_w$. Furthermore $V(k)$ has maximum and minimum. The minimum corresponds to the greatest valuation ring , the Jacob ring $\mathcal{O}(k)$ of k [4], [2], for which $v(k)$ is 2-regular. This ring is defined as follows:

$$\mathcal{O}_1(k) = \{\ x \in k/\ x \notin \pm k^2 \text{ and } 1 + x \in k^2\ \}$$

$$\mathcal{O}_2(k) = \{\ x \in k/\ x \in \pm k^2 \text{ and } x\mathcal{O}_1(k) \subseteq \mathcal{O}_1(k)\ \}$$

$$\mathcal{O}(k) = \mathcal{O}_1(k) \cup \mathcal{O}_2(k)$$

Let us take $a \in k - (\pm k^2)$ (which is equivalent to $v(a) \notin 2v(k)$ for every $v \in V(k)$). There exist in k only two orders fixed by the conditions $a > 0$ and $a < 0$. The positive cones of these orders are $k^2 \cup ak^2$ and $k^2 \cup -a\,k^2$ respectively.

If H is an o.a.g. $H/2H$ is a vector space over the two-element field; we shall call a basis of $H/2H$ over this field a 2-basis.

LEMMA 2.1. *Let H be an o.a.g. and $\alpha \in H - 2H$. Then there exists G an o.a.g. extension of H into $\widetilde{H}$, odd-divisible with $\overline{\alpha}$ as 2-basis of $G/2G$*

Proof. We may suppose H odd-divisible, otherwise we take its odd-divisible hull which preserves the property $\alpha \notin 2H$. Taking G maximal with the condition $\alpha \notin 2G$ we will prove $G = 2G + (\alpha)$. Otherwise we take $\beta \in G - (2G + (\alpha))$ and put $G_0 = G + \mathbb{Z}\beta/2 = \{\ g + k\beta/2$ with $k = 0, 1\ \}$. We should have finished if we prove $\alpha \notin 2G_0$. Suppose $\alpha \in 2G_0$:

$$\alpha = 2(g + k\beta/2) = 2g + k\beta$$

with $g \in G$ and $k = 0$ or $k = 1$. Neither $k = 0$ is posible because then $\alpha \in 2G$, nor $k = 1$ because then $\beta \in 2G + (\alpha)$. ■

THEOREM 2.2. *Let $(k, v, \leq)$ be an ordered an valued field and $a \in k$ such that $a > 0$, $v(a) \notin 2v(k)$. Then there exists $(L, v, \leq)$ an extension of $(k, v, \leq)$ with v henselian, L/v real-closed, $v(L)$ odd-divisible and $v(a)$ a 2-basis of $v(L)/2v(L)$.*

Proof. This theorem follows from Proposition 1.10 and Lemma 2.1. ■

LEMMA 2.3. *Let (k, v) be a valued field, $a \in k^*$ and δ the operator defined by $\delta(x) = \frac{ax^2}{x^4 - a^2}$. Then the following are equivalent:*
(i) $v(a) \notin 2v(k)$
(ii) $\delta(k) \subseteq M_v$

Proof. $v(a) \notin 2v(k)$ if and only if $v(x^2/a) \neq 0$ for every $x \in k$. But δ may be expressed $\delta(x) = \frac{x^2/a}{(x^2/a)^2 - 1}$ and we need only to prove that $v(t) \neq 0$ if and only if $v\left(\frac{t}{t^2-1}\right) > 0$. This is easily seen by distinguishing the cases $v(t) > 0$, $= 0$ or < 0. ■

The following Lemma is in fact a particular case of a result of algebraic geometry which says that a regular local ring is dominated by a place with the same residue field.

LEMMA 2.4. *Let k be any field, $k(\overline{X}) = k(X_1, \ldots, X_n)$. Let $\overline{x} = (x_1, \ldots, x_n)$ be an element of k^n. Then there exists a place $P : k(\overline{X}) \to k \cup \{\infty\}$ with $P_{|k} = Id$ and $X_i P = x_i$ for $i = 1, \ldots, n$.*

Proof. We have to find a valuation on $k(\overline{X})$ with residue field k, $v(k^*) = \{0\}$ and $v(X_i - x_i) > 0$. We take as value group $\bigotimes_{i=1}^{n} \mathbf{Z}_i$, the lexicographic product of n copies of $\mathbf{Z}$ and we define v on $k[\overline{X}]$:

$$v(\sum_i b_i(X_1 - x_1)^{i_1} \ldots . (X_n - x_n)^{i_n}) = \min_i \{\sum_{j=1}^{n} i_j 1_j\}$$

were $b_i \in k$ and 1_j is the unit of $\mathbf{Z}_j$. Then v extends uniquely to a valuation over $k(\overline{X})$ satisfying the required conditions. ■

LEMMA 2.5. *Let $P : L \to k \cup \{\infty\}$ be a place and $\leq$ an order over k. Let $a_i, b_i \in L$ such that $\infty \neq b_i P > 0$. Then $(\sum a_i^2 b_i)P \neq \infty$ implies $a_i P \neq \infty$ and $(\sum a_i^2 b_i)P = \sum (a_i P)^2 b_i P \geq 0$.*

Proof. If v is the valuation defined by P it suffices to prove that $v(\sum a_i^2 b_i) = \min_i \{v(a_i^2)\}$. For the sake of simplicity we may suppose $v(a_1) = \min_i \{v(a_i)\}$. Then $v\left(\frac{a_i^2}{a_1^2} b_i\right) \geq 0$ and $\left(\sum_1^k \frac{a_i^2}{a_1^2} b_i\right) P = b_1 P + \sum_2^k \left(\frac{a_i}{a_1} P\right)^2 b_i P > 0$ showing that $v\left(\frac{\sum a_i^2 b_i}{a_1^2}\right) = 0$ and $v(\sum a_i^2 b_i) = v(a_1^2)$. ■

Notation. If B is any subset of k, $\prod(B)$ will denote the multiplicative semigroup generated by B.

THEOREM 2.6. *Let k be a chain-closed field, $a \in k - (\pm k^2)$ and $\leq$ the order for which $a > 0$. Let $f, g_1, \ldots, g_r \in k(\overline{X})$. Then the following are equivalent:*

(i) $f(\overline{x}) \geq 0$ for every $\overline{x} \in k^n$ such that $f(\overline{x}), g_1(\overline{x}), \ldots, g_r(\overline{x})$ are defined and $g_i(\overline{x}) > 0$, $i = 1, \ldots, r$.

(ii) There exist $k \in \mathbf{N}$, $\delta_i, \delta_{i,j} \in \{0, 1\}$ for $i = 1, \ldots, k, j = 1, \ldots, r$, $h_1, \ldots, h_k \in k(\overline{X})$, $u_1, \ldots, u_k \in \mathcal{O}(k) \prod \delta(k(\overline{X}))$ such that $f = \sum_{i=1}^{k} h_i^2 a^{\delta_i} g_1^{\delta_{i,1}} \ldots g_r^{\delta_{i,r}} (1 + u_i)$

Proof. Suppose f has this form and let $\overline{x} \in k^n$ such that $f(\overline{x}), g_1(\overline{x}), \ldots, g_r(\overline{x})$ are defined and $g_i(\overline{x}) > 0$, $i = 1, \ldots, r$. Taking a place P like in Lemma 2.4 we have $fP = f(\overline{x})$, $g_i P = g_i(\overline{x})$, $i = 1, \ldots, r$. Distinguishing the cases $hP = \infty$, $hP \neq \infty$, for every $h \in k(\overline{X})$ and by Lemma 2.3 we see that $\delta(h)P \in M_v$, were v is the Jacob valuation over k. Thus if $u \in \mathcal{O}(k) \prod \delta(k(\overline{X}))$, $uP \in M_v$ and $(1 + u)P > 0$. Now applying Lemma 2.5. to $f = \sum_{i=1}^{k} h_i^2 a^{\delta_i} g_1^{\delta_{i,1}} \ldots g_r^{\delta_{i,r}} (1 + u_i)$ we have that $f(\overline{x}) = fP \geq 0$. This proves ii⇒i.

To prove i⇒ii, if $f \notin S(k(\overline{X})^2, a, g_1, \ldots, g_r, 1 + \mathcal{O}(k) \prod \delta(k(\overline{X})))$ then by Corollary 1.7 and Lemma 2.3 there exist in k a valuation w and an order $\leq$ compatible such that $f < 0$, $g_1, \ldots, g_r > 0$, $w(a) \notin 2w(k(\overline{X}))$ and $\mathcal{O}(k) \subseteq A_w$. By Theorem 2.2 there exists an extension $(L, w, \leq)$ with w henselian, L/w real-closed and $w(L)$ odd-divisible such that $\overline{w(a)}$ is a 2-basis of $w(L)/2w(L)$. By the definition of the Jacob ring we have $\mathcal{O}(k) \supseteq \mathcal{O}(L) \cap k$ and by

construction $\mathcal{O}(k) \subseteq A_w \subseteq \mathcal{O}(L)$, thus $\mathcal{O}(k) = \mathcal{O}(L) \cap k$. Denoting v_0 and w_0 the Jacob valuations of k and L respectively we have $(k, v_0) \subseteq (L, w_0)$. By the model-completeness of the o.a.g. H odd-divisible, 2-regular an such that $(H : 2H) = 2$ and using the Ax-Kochen-Ershov Theorem we obtain the elementary inclusion $(k, v_0) \preceq (L, w_0)$. In the two fields the order for which $a > 0$ is defined by the same formula, hence $(k, \leq) \preceq (L, \leq)$. Finally because of $f(\overline{X}) < 0$, $g_i(\overline{X}) > 0$, $i = 1, \ldots, r$ in $(L, \leq)$ the sentence expressing

$$(\exists \overline{x})(f(\overline{x}), g_1(\overline{x}), \ldots, g_r(\overline{x}) \text{ are defined and } f(\overline{x}) < 0,\ g_i(\overline{x}) > 0,\ i = 1, \ldots, r)$$

holds. By the elementary inclusion this is transferred to k showing (i) false. ■

In the case of chain-closed fields for which $V(k)$ is a singleton we have a simpler form of the positively defined functions. In order to do this we should keep in mind the following fact: taking one of the two orders of k and if we denote $W(k)$ the set of all valuations convex for this order, $W(k)$ is totally ordered (with the inverse inclusion of its valuation rings) and contains $V(k)$. Further ([1] prop 11) $V(k)$ is a final segment of $W(k)$ and we have the following equivalences:

1. $v \in V(k)$ if and only if $(v(k) : 2v(k)) = 2$
2. $v \notin V(k)$ if and only if $v(k)$ is divisible

THEOREM 3.5. *Let k be any chain-closed field such that $V(k)$ is a singleton. Let $a \in k - (\pm k^2)$ and $\leq$ the order for which $a > 0$. Let $f, g_1, \ldots, g_r \in k(\overline{X})$. Then the following are equivalent:*

(i) $f(\overline{x}) \geq 0$ for every $\overline{x} \in k^n$ such that $f(\overline{x}), g_1(\overline{x}), \ldots, g_r(\overline{x})$ are defined and $g_i(\overline{x}) > 0$, $i = 1, \ldots, r$.

(ii) There exist $k \in \mathbb{N}$, $\delta_i, \delta_{i,j} \in \{0, 1\}$ for $i = 1, \ldots, k, j = 1, \ldots, r$, $h_1, \ldots, h_k \in k(\overline{X})$, $u_1, \ldots, u_k \in \mathbf{Z} \prod \delta(k(\overline{X}))$ such that $f = \sum_{i=1}^{k} h_i^2 a^{\delta_i} g_1^{\delta_{i,1}} \ldots g_r^{\delta_{i,r}} (1 + u_i)$

Proof. The proof is the same as in Theorem 2.6 but for two points: we use Corollary 1.8 instead of Corollary 1.7 and to prove $\mathcal{O}(k) = \mathcal{O}(L) \cap k$ we will use the condition $|V(k)| = 1$ instead of imposing $\mathcal{O}(k) \subseteq A_w$. This is done in the following way: the order making $a > 0$ in k is the restriction of the order in L with $a > 0$. Then from the convexity of w_0 we deduce the convexity of $w_{0|k}$. Furthermore $w_0(k)$ is not divisible ($w_0(a) \notin 2w_0(L)$), hence $w_{0|k} = v_0$ and thus $(k, v_0) \subseteq (L, w_0)$. ■

REFERENCES

1. F. DELON and D. GONDARD, *17ème problème de Hilbert au niveau n pour les corps Chaine-clos*, preprint.
2. M. A. DICKMANN, *The Model Theory of Chain-closed Fields*, to appear in The Journal of Symbolic Logic.
3. J. HARMAN, *Chains of higher level orderings*, Contemporary Mathematics vol 8 (1982), pp.141-174.

4. B. JACOB, *The model theory of generalized real closed fields*, Journal für die reine und angewandte Math. 323 (1981), pp. 213-220.
5. M. KNEBUSCH and M. WRIGHT, *Bewertungen mit reeller henselisierung*, Journal für die reine und angewandte Math. 286-7 (1976), pp. 314-321.
6. S. KOCHEN, *Integer Valued Rational Functions over the p-adic numbers*, Proceedings of the Symp. in pure Math. XII, American Math. Society, Providence R.I. (1969), pp. 57-73.
7. P. RIBENBOIM, *Théorie des Valuations*, Les presses de l'Université de Montréal 9 (1965), Montréal, Canada.
8. A. ROBINSON and E. ZAKON, *Elementary properties of ordered abelian groups*, Transactions of the A. M. S. 96 (1960), pp. 222-236.

The real holomorphy ring of a real function field

by Eberhard Becker

By definition, the real holomorphy ring H = H(K) of a formally real field is the intersection of all valuation rings with formally real residue fields. This ring plays an important role in the theory of Witt rings [B-R], [Schw], [P], in the study of sums of powers in a field [B2], [B3], [K] and in real algebraic geometry [K], [Schü 2], [Schü 4]. For applications to ring theory cf. [Schü 1], [K], [Schü 4]. Related subjects are also dealt with in [B1], [Br-S], [Ku-Pr], [Schü 3].

[B1] E. Becker, "Valuations and places in the theory of formally real fields", Géométrie Algébrique Réelle et Formes Quadratiques, Lecture Notes in Math. vol. 959, 1-40, Berlin, Heidelberg, New York: Springer 1982.

[B2] E. Becker, "The real holomorphy ring and sums of 2n-th powers", Géométrie Algébrique Réelle et Formes Quadratiques, Lecture Notes in Math. vol. 959, 139-181, Berlin, Heidelberg, New York: Springer 1982.

[B3] E. Becker, "Local global theorems for diagonal forms of higher degree", J. Reine Angew. Math. 318 (1980), 36-50.

[B-R] E. Becker, A. Rosenberg, "The graded Witt ring of higher level, in preparation.

[Br-S] L. Bröcker, H.-W. Schülting, "Valuations of function fields from the geometrical point of view", J. Reine Angew. Math. 365 (1986), 12-32.

[K] W. Kucharz, "Invertible ideals in real holomorphy rings", J. Reine Angew. Math., to appear.

[Ku-Pr] F.-V. Kuhlmann, A. Prestel, "On places of algebraic function fields", J. Reine Angew. Math. 353 (1984), 181-195.

[P] Powers, V., "The real holomorphy ring of skew fields, preprint 1988.

[Schü 1] H.-W. Schülting, "Über die Erzeugendenanzahl invertierbarer Ideale in Prüferringen", Comm. Algebra 7 (1977), 1331-1349.

[Schü 2] H.-W. Schülting, "Real holomorphy rings in real algebraic geometry", Géométrie Algébrique Réelle et Formes Quadratiques, Lecture Notes in Math. vol 959, 433-442, Berlin, Heidelberg, New York: Springer 1982.

[Schü 3] H.-W. Schülting, "Prime divisors on real varieties and valuation theory", J. Algebra 98 (1986), 499-514.

[Schü 4] H.-W. Schülting, "Cycles on real varieties and birational aspects of real algebraic geometry", Habilitationsschrift, Dortmund 1988.

[Schw] N. Schwartz, "Chain signatures and real closures", J. Reine Angew. Math. 347 (1984, 1-20.

RATIONAL COMPUTATION TREES

T. Recio (*)

&1. Algebraic computation trees (as in [B-O]) are usually introduced in Computational Geometry to obtain lower bounds of the complexity of solving the membership problem for a (necessarily) semialgebraic subset $W \subset \mathbf{R}^N$. At each node of the tree an arithmetical operation or comparison (test instruction of the form $f>0$, $f\geq 0$ or $f=0$) is performed. In this model of computation, exact real arithmetic is assumed. Then lower bounds for the height of any tree that decides correctly for every $x \in \mathbf{R}^N$ whether $x \in W$ or $x \notin W$ are obtained -using the Milnor-Thom Theorem- as a function of N and the number of connected components of $W \subset \mathbf{R}^N$.

&2. Usually, arithmetic operations performed in an operational vertex of the tree are $+, -, \times, \div$, plus real root extractions of polynomials (at the cost of the complexity of evaluating the polynomial at a given point; for example roots of x^2-f at cost 1, where f has been previously computed in the path leading to the node which performs the extraction $\sqrt{f}$). The terms of the operations are either all precomputed along the path or some of them are constants of $\mathbf{R}$ (for example, dividing $f/2$, extracting the root of $x^2-\pi x+f$, or multiplying $f \times g$).

Despite of the fact that the rational numbers $\mathbf{Q}$ are not closed for all these arithmetic operations one can easily show the following: "*For every set $W \subset R^N$ such that there is an algebraic computation tree solving the membership to W using no trascendental constants, there is also an algebraic computation tree solving W which uses only the four elementary operations $+, -, \times, \div$, and rational constants. Moreover there exists another (maybe different) elementary operations tree for solving $W \cap Q^N$*"

In general one needs higher elementary algebraic computation trees for solving a given $W \subset \mathbf{R}^N$ than if one is allowed to use trees which perform more complex operations, but nothing is said about the height of the elementary tree for solving $W \cap \mathbf{Q}^N$.

&3. But we are thinking of applying this elementary algebraic computation trees (rational computation trees) for solving the membership problem for sets $W \subset \mathbf{Q}^N$. The philosophy is that most of the sets W that arise in Computational geometry can be described by trees that use only rational constants; and to compute these sets with exact

(*) Partially supported by P. B. 62/86 CICYT.

arithmetic it is more realistic to restrict to rational inputs and elementary operations; else to restrict to real algebraic numbers suitably codified (c. f. [C-R], [L]), allowing some specific weight to the performance of exact operations, even if elementary. Thus, the remark in &2 says that the consideration of rational computation trees does not diminish essentially the set of problems in Computational Geometry that can be studied with this restricted model of computation.

&4. In order to bound the height of a rational computation tree T that computes a set $W \subset \mathbf{Q}^N$ one considers the description -in terms of equalities and inequalities- given by T of W, namely W=W(T). Now, W(T) can be interpreted as a system over $\mathbf{R}^N$, and we write $W(T)(\mathbf{R}^N)$ to represent the solution set, thus $W(T)(\mathbf{R}^N) \cap \mathbf{Q}^N = W$. Clearly the height of T, h(T) is bounded -using Thom-Milnor- by the number of connected components of $W(T)(\mathbf{R}^N)$. But this number has *a priori* little relation with the closure in $\mathbf{R}^N$ of W, $\overline{W}$; connected components of $\overline{W}$ can be less that the ones of $W(T)(\mathbf{R}^N)$ (for example, two tangent open circles); or more (the case of $[(x-1)(x-2)(x+1) - y^2][x^4+y^4-1]^2 \geq 0$ in $\mathbf{Q}^2$). It is therefore relevant the following result that connects the number γ of compact connected components of $\overline{W}$ with non empty interior with the height of T, h(T):

Theorem [B-O] : $h(t)=\Omega(\log \gamma - N)$.

Stated without proof in [B-O], it is just a matter of bounding γ with the number of connected components of some subsets $W(T)(\mathbf{R}^N)$ -the ones defined without equalities through the tree T (c. f. [P-R] for details) .

& 5. One useful way of using the Theorem above is to obtain better lower bounds for the membership problem of certain semialgebraic sets $W \subset \mathbf{R}^N$. In fact , if W is defined with rational coefficients but if it is connected, the Milnor-Thom method does not give an estimation of complexity. Here we can consider , for every rational computation tree solving W the same tree solving the rational set $W \cap \mathbf{Q}^N$. Now the closure of $W \cap \mathbf{Q}^N$. in $\mathbf{R}^N$ can well have several connected components with non empty interior (as in the second example of &4); therefore we obtain better lower bounds for the height of the trees solving W. On the other hand, it is clear that given a semialgebraic set $W \subset \mathbf{R}^N$, with a number of equalities and inequalities of bounded degree, one can construct a tree solving W with height bounded by a certain function of the degree and the number of conditions. Thus we can obtain an upper bound for the number of connected components with non empty interior corresponding to the closure of $W \cap \mathbf{Q}^N$.

REFERENCES:

[B-O] - Ben-Or M., Lower Bounds for Algebraic Computation Trees. *Proceedings 15th A.C.M. Annual Symp. Theory of Comp. 1983*

[C-R] - Coste M., Roy M. F., Thom's Lemma, the Coding of Real Algebraic Numbers and the Computation of the Topology of Semialgebraic Sets. *Journal of Symbolic Computation. Numbers 1 & 2. Vol. 5. Academic Press. 1988*

[L] - Loos, R., Computing in Algebraic Extensions.*Computer Algebra. Symbolic and Algebraic Computation. Springer-Verlag. 1982*

[P-R] - Pardo L.M.,Recio T., Arboles Algebraicos: Un Modelo de Computación en Geometría. *" Homenaje al profesor E. Villar ". Universidad de Cantabria. 1988.*

T.Recio
Departamento de Matemáticas, Estadística y Computación.
Universidad de Cantabria.
39005 SANTANDER.

Complexity of the computation on real algebraic numbers

Marie-Françoise Roy, IRMAR, Université de Rennes I
Aviva Szpirglas, CSP, Université Paris Nord

A new method for coding the real algebraic numbers , based on the study of simultaneous inequalities coming from [B K R],has ben introduced in [C R].This leads to various applications in the field of computational real algebraic geometry: study of the topology of a real algebraic curve ([R]), or of the analytic branches of a real algebraic curve ([Cu P 3R]).

In this paper we give some improvment of the algorithms in [C R] and we study their complexity. We will apply our results to the study of the complexity of some algorithms on curves: cylindrical decomposition and topology by the methods in [R] , in an another paper.

In the first paragraph we introduce some basic tools we need, based on the techniques of computer algebra (mainly results on subresultants and divisors). In the second paragraph, we study simultaneous inequalities at the real roots of a polynomial,in the third paragraph, we consider the coding of real algebraic numbers.

I)Basic tools and notations

In all the paper, for $P = a_0X^p+...+a_p$ a polynomial with integer coefficients we define the norm of P, $N(P)$, by $N(P)=(a_0^2+.....+a_p^2)^{1/2}$. The **size** of P is the log of $N(P)$. The **length** of an integer is the log of the integer.

Our algorithms are based on a generalization of Sturm theorem, hence on divisions of polynomials, taking care of signs. So we shall need various notions of signed remainders.

In this paragraph we denote by :

P a polynomial with integer cefficients of degree p ;

Q a polynomial with integer cefficients of degree q with leading coefficient $b_0 \neq 0$, $q \leq p$.

1) Signed pseudo-remainders

We denote by rem(P,Q) the remainder of P and Q in the euclidian division process: so rem(P,Q) has rational coefficients.

In order to perform division of polynomials with only integer coefficients, one uses classically the pseudo-division process:

The **pseudo-remainder** of P and Q prem(P,Q) is the remainder of the quotient of $b_0^{p-q+1} P$ by Q .

The **signed pseudo-remainder** of P and Q sprem(P,Q) is the remainder of the quotient of $| b_0^{p-q+1} | P$ by Q .

The **pseudo-remainder sequence** of P and Q is by definition the following sequence:

$$prem_0(P,Q) = P$$

$$prem_1(P,Q) = Q$$

$$prem_j(P,Q) = prem(prem_{j-2}(P,Q) , prem_{j-1}(P,Q)) \text{ for } j \leq j_0$$

where j_0 is such that $prem_{j_0}(P,Q)$ is of degree 0 (so $j_0 \leq p-2$).

The **signed pseudo-remainder sequence** is obtained by replacing in the preceeding definition each pseudo-remainder by the corresponding signed pseudo-remainder .

2) Signed subresultant sequence

One defect of the pseudo-division process is the growth of the size of the coefficients. Is is well known (see for example [Lo]) that the subresultants techniques allow to make divisions with integer computations and with a good controll of the size of intermediate results.

Let us recall the definition of the **subresultants :**

If Q_1 ,.... , Q_k are k polynomials with integer coefficients ,of respective degrees

q_1 ,... ,q_k , $Q_i = \sum_{j=1}^{q_i+1} a_{i,j} x^{j-1}$, denote by l the number $\max(q_i)+1$. We can write :

$Q_i = \sum_{j=1}^{l} a_{i,j} x^{j-1}$ with $a_{i,j}=0$ for $j>q_i+1$. Then denote by $mat(\ Q_1$,.... , $Q_k\ )$ the

$k \times l$–matrix of elements $(b_{i,j})$ where $b_{i,j}=a_{i,l-j}$

For $0 \le k < q$,the k-th **subresultant** of P and Q , S_k is defined as follows : denote by M_k the $(p+q-2k, p+q-k)$-matrix $mat(x^{q-k-1}P,....,P,\ x^{p-k-1}Q,.... ,Q\ )$. Then the k–th subresultant of P and Q, S_k , is $\sum_{p+q-2k}^{p+q-k} \det M_{k,j}\, x^{p+q-k-j}$, where $M_{,kj}$ is the minor of M_k obtained by taking the first $p+q-2k-1$ columns and the j-th column.

The **subresultant sequence** of P and Q is obtained by considering Q as a polynomial of degree $p-1$ (the first $p-1-q$ coefficients being equal to 0) and by taking for S_p the polynomial P , for S_{p-1} the polynomial Q and for S_k the k-th subresultant of P and Q , for $0 \le k \le p-2$.

Let us recall the subresultant theorem, which indicates the relation between the subresultant sequence and the pseudo-remainder-sequence:

Subresultant heorem :

If the degre of S_{j+1} is equal to $j+1$ and the degree of S_j is equal to s , then :

(i) $S_{j-1} = ... = S_{s+1} = 0$ for $-1 \le s < j < p-1$

(ii) $(R_{j+1})^{j-s} S_s = lc\,(S_j)^{j-s} S_j$ for $0 \le s \le j \le p-1$

(iii) $(-1)^{j-s}(R_{j+1})^{j-s+2} S_{s-1} = prem(S_{j+1}, S_j)$

where R_{j+1} is the leading coefficient of S_{j+1} except for $j=p-1$ $(R_p = 1)$ and $lc(S_j)$ the leading coefficient of S_j.

proof: see [Lo].

We deduce immediately the following corollary for signed pseudo-remainders.

Corollary :

For each j , $j_0 \le j \le p-2$, there exists i_j $0 \le i_j \le p$ and $C_j \in \mathbb{Z}$ such that

$C_j S_{i_j} = sprem_j(P,Q)$.

With the notations of the corollary the **signed subresultant sequence** is by definition ,

$$ssub_j(P,Q) = \varepsilon_j S_{i_j} \text{ for } j_0 \leq j \leq p \text{ where } \varepsilon_j \text{ is the sign of } C_j.$$

3) Generalized subresultant Sturm sequence

The **generalized Sturm sequence** associated to P and Q , denoted by is defined by :

$$P_0 = P$$

$$P_1 = Q$$

$$P_j = -rem_j(P,Q).$$

One notes $v_{P,Q}(-\infty)$ and $v_{P,Q}(+\infty)$ the number of sign changes in the sequences of the signs of the P_i at $-\infty$ and $+\infty$.

The **Sturm sequence** of P is the generalized Sturm sequence associated to P and P'.

We have the following property,due to Sylvester ([S]).

Proposition 1:

Denote by $c_{>0}(P;Q)$ (resp. $c_{<0}(P;Q)$) the number of real roots ξ of P such that $Q(\xi)$ is >0 (resp. <0) . With the above definitions and notations , if P and Q are coprime, one has $c_{>0}(P;Q) - c_{<0}(P;Q) = v_{P,P'Q}(-\infty) - v_{P,P'Q}(+\infty)$)

proof: It is similar to the classical proof of Sturm theorem (see for example [J] or [B C R]): look at the sign variations in the generalized Sturm sequence when passing through a root of P .

In order to get only integer computations with a good controll on their size we define the **generalized subresultant Sturm sequence** associated to P and Q , denoted by GSS(P,Q) by :

$$P_0 = P$$

$$P_1 = Q$$

$$P_j = -ssub_j(P,Q).$$

It is clear by the definition of the signed subresultant sequence that the number of sign changes in the sequences of the signs of the P_i at $-\infty$ and $+\infty$ are equal to $v_{P,Q}(-\infty)$ and $v_{P,Q}(+\infty)$.

The **subresultant Sturm sequence** of P is the generalized subresultant Sturm sequence associated to P and P'.

Remark 1

The computation of the generalized subresultant Sturm sequence associated to P and Q takes $O(pq)$ arithmetic operations.

By Hadamard inequality ([Mi]), the coefficients of all the subresultants of P and Q are bounded by $N(P)^q N(Q)^p$, hence the size of the coefficients of the polynomials in the generalized subresultant Sturm sequence associated to P and Q is in $O(q\log(N(P))+p\log(N(Q)))$.

4) Divisors

Let P and R be polynomials with no content (such that their coefficients have no factor in common). Then R is a divisor of P over $\mathbb{Q}$ if and only if it is a divisor of P over $\mathbb{Z}$ [La]). This implies that the coefficients of R are bounded by $2^p N(P)$, hence that $\log(N(R))$ is $O(p+\log(N(P)))$ [Mi].

5) GCD

Using signed subresultant algorithm, we get the following way for computing the GCD of P and Q (supposed with no content):

-compute the signed subresultant Sturm sequence of P and Q,

-get the last polynomial in this sequence, G,

-take the GCD , g, of its coefficients, define $\mathrm{GCD}(P,Q) = G/g$.

The polynomial $\mathrm{GCD}(P,Q)$ is a polynomial with integer coefficients, which is (up to a rational) a multiple of the GCD of P and Q computed with ordinary euclidean division, and a divisor of P and Q.

The number of arithmetical operations for computing $\mathrm{GCD}(P,Q)$ is in $O(pq)$. The size of coefficients of polynomials in the computation is $O(E)$ with

$E=q\log(N(P))+p\log(N(Q)$, hence the complexity of the computation is is $O(pqE^2)$ using classical arithmetic, and using "fast multiplication" in $O(pqE\log E)$. Moreover, using 4, the norm of GCD(P,Q) is in $O(p+\log(N(P))$.

II) Simultaneaous inequalities

All algorithms are based on proposition 1, a result due to Sylvester ([S]) revisited by Ben-Ore, Kozen and Reif ([B K R]).

Let $P, Q_1,...,Q_k$ be polynomials with integer coefficients and let $\varepsilon=(\varepsilon_1,...,\varepsilon_k)$ be a sequence of sign conditions $(>0,<0,=0)$. The subject of this paragraph is to study the number of real roots of P giving to $Q_1,...,Q_k$ fixed signs.

One denotes by $c_\varepsilon(P;Q_1,...,Q_k)$ the number of real roots of P giving to $Q_1,...,Q_k$ the signs $\varepsilon_1,...,\varepsilon_k$. The **sign conditions realized by $Q_1,...,Q_k$ at the real roots of** P are the k-uples of signs conditions ε such that

$\{x\in\mathbb{R} \mid P(x)=0 \text{ and } Q_j(x)\varepsilon_j, j=1,...,k\}$

is non empty.

1) Basic situation. strict simultaneous inequalities: algorithm SSI

In this paragraph,

P will denote a squarefree polynomial with integer coefficients, of degree p,

r will denote the number of real roots of P, $r\leq p$

$Q_1,...,Q_k$ will denote a finite list of polynomials with integer coefficients of respective degrees $q_1,...,q_k$, prime to P.

In this situation, any real root ξ of P gives strict signs $(>0, <0)$ to P', $Q_1,...,Q_k$.

Algorithm SSI is a detailed version of algorithm b_3 of [C R].

Presentation of SSI

The **aim** of the algorithm is to determine the number of real roots of P giving to $Q_1,...,Q_k$ fixed signs.

Let us consider the case $k=1$. Let Q be a polynomial with integer coefficients, prime to P. We want to compute $c_{>0}(P;Q)$ and $c_{<0}(P;Q)$. Using proposition 1, we

have

$$A_1\begin{bmatrix} c_{>0}(P;Q) \\ c_{<0}(P;Q) \end{bmatrix} = \begin{bmatrix} v_{P,PQ}(-\infty)+v_{P,PQ}(+\infty) \\ v_{P,PQ}(-\infty)-v_{P,PQ}(+\infty) \end{bmatrix}$$

$$\text{with } A_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

We can easily deduce $c_{>0}(P;Q)$ and $c_{<0}(P;Q)$ from $v(1)= v_{P,P'}(-\infty)-v_{P,P'}(+\infty)$ and $v(2)=v_{P,P'Q}(-\infty)-v_{P,P'Q}(+\infty)$.

The **idea** for $k\neq 1$ is to compute the generalized subresultant Sturm sequences associated to the products of the polynomials in subsets of $\{Q_1,...,Q_k\}$ and use the sign variations of these generalized subresultant Sturm sequences and some linear algebra (generalizing $k=1$) to deduce the values of the $c_\varepsilon(P;Q_1,...,Q_k)$. If done without care, this leads to an exponential algorithm, since we have 2^k subsets of $\{Q_1,...,Q_k\}$, hence 2^k generalized Sturm sequences to compute, to get the values c_ε for the 2^k sign conditions ε. To avoid this exponential growth the idea ([B K R]) is to remark that the number r_k of distinct sign conditions realized by $Q_1,..., Q_k$ at the real roots of P is, for any k, smaller than the number r of real roots of P.

We shall give a description of the algorithm and then an example to enlighten the situation. Precisely one wants to determine the sign conditions $\varepsilon(k,1),...,\varepsilon(k,r(P;Q_1,...,Q_k))$, with $r(P;Q_1,...,Q_k)=r_k\leq r$, realized by $Q_1,..., Q_k$ at the real roots of P and the number $c_{k,j}=c_{\varepsilon(k,j)}(P;Q_1,...,Q_k)$ of elements of the non empty set

$\{x\in\mathbb{R} \mid P(x)=0 \text{ and } Q_i(x)\varepsilon(k,j)_i,\ i=1,...,k\}$.

The **input** of the algorithm consists of P, $Q_1,...,Q_k$.

The **output** SSIout$(P,Q_1,...,Q_k)$ of the algorithm is the following:

(1_k) the list $\varepsilon_k=(\varepsilon(k,1),...,\varepsilon(k,r(P;Q_1,...,Q_k)))$, $r(P;Q_1,...,Q_k)=r_k\leq r$, of the k–uples of sign conditions realized by $Q_1,..., Q_k$ at the real roots of P,

(2_k) the numbers $c(k,1),..., c(k,r_k)$

(3_k) a list of polynomials $(Q_{k,j})_{j=1,...,r_k}$ which are some product of the Q_m 's and the numbers $v(k,j)=v_{P,P'Q_{k,j}}(-\infty) - v_{P,P'Q_{k,j}}(+\infty)$,

(4_k) an invertible matrix $A(P;Q_1,...,Q_k)=A_k$ of dimension r_k such that $A_k c_k = v_k$, where c_k is the vector $(c(k,1),...,c(k,r_k))$ and v_k the vector $v(P;Q_1,...,Q_k)=(v(k,1),...,v(k,r_k))$.

Description of SSI

We are going to compute by induction on l, $1 \le l < k$ SSIout$(P,Q_1,...,Q_l)$

The case l=0 is given by r_0=0.

The passage from l to l+1 is given by the following procedure SSIadd.

The input of SSIadd$((P;Q_1,...,Q_l),Q_{l+1})$ is SSIout$(P;Q_1,...,Q_l)$, its output is SSIout$(P;Q_1,...,Q_{l+1})$.

Procedure SSIadd

We compute the r_l generalized subresultant Sturm sequences associated to the $Q_{l,r_l+j}=Q_{l+1}Q_{l,j}$, $j=1,...,r_l$ and $v(l,m)=v_{P,P'Q_{l,m}}(-\infty) - v_{P,P'Q_{l,m}}(+\infty)$, $m=r_l+1,...,2r_l$. One considers the $2r_l$ dimension matrix

$$A'=\begin{bmatrix} A_l & A_l \\ A_l & -A_l \end{bmatrix}$$

and the equality $A'.c'=v'$, obtained from (4_l) and proposition 1 where c' is the vector

$(c_{\varepsilon(l,j),>0}(P;Q_1,...,Q_{l+1}),j=1,...,r_l\ ,\ c_{\varepsilon(l,j),<0}(P;Q_1,...,Q_{l+1}),j=1,...,r_l)$

and v' the vector $(v(l,1),...v(l,2r_l))$.

The matrix A' is invertible. One computes c' by inverting A'.

We define r_{l+1} as the number $(\le r)$ of non zero elements in c' and let $m_1,...,m_{r_{l+1}}$

$(m_1<...<m_{r_{l+1}} \leq 2r_l)$ be such that the m_i'th coordinate of c', for $j=1$, ... , r_{l+1} , is different from 0. The sign conditions $\varepsilon(l+1,1),...,\varepsilon(l+1,r_{l+1})$ realized by $Q_1,...,Q_{l+1}$ at the real roots of P are the m_j 'th elements ,$j=1,...,r_{l+1}$, of the list

$((\varepsilon(l,1),>0),...,(\varepsilon(l,r_l),>0),(\varepsilon(l,1),<0),...,(\varepsilon(l,r_l),<0))$.

One can then extract from A' the m_1'th column, ... , the $m_{r_{l+1}}$'th column , which gives a $2r_l$, r_{l+1} matrix A''. The r_l first lines of A'' are independant, since at least one of the columns of number j and $r_l + j$ of A' appears in A''. An invertible matrix A_{l+1}, of dimension r_{l+1} can be extracted from A''. Let us denote

$m'_1,...,m'_{r_{l+1}-r_l}$, $m'_1<...<m'_{r_{l+1}-r_l}$ the elements of $\{1,....,r_{l+1}\}$ such that the $(r_l+m'_i)$'th line of A'' appears in A_{l+1}.

The list $(Q_{l,j})_{j=1,...,r_{l+1}}$ is obtained by adding to the list $(Q_{l,j})_{j=1,...,r_l}$ the polynomials $Q_{l+1}\,Q_{l,j}$ $j=m'_1,...,m'_{r_{l+1}-r_l}$

It is easy to verify $(1_{l+1}),...,(4_{l+1})$.

Remark 2

The polynomials $Q_{l,j}$ are always products of a number smaller or equal to r of polynomials among $Q_1,...,Q_k$: the polynomial Q_{l+1} appears in some $Q_{l+1,j}$ if and only if r_{l+1} is greater than r_l , and there is at most r such values of l.

Example 1:

Let us consider

$$P = (X^3-1)(X^2-9)$$

$$Q_1 = X$$

$$Q_2 = X+1$$

$$Q_3 = X - 4$$

$$Q_4 = X - 2$$

$$Q_5 = X + 2$$

We have $v_{P,P'}(-\infty) - v_{P,P'}(+\infty) = 3$: P has 3 real roots

Also $v_{P,P'Q_1}(-\infty) - v_{P,P'Q_1}(+\infty) = 1$: P has 2 roots with $Q_1>0$ and 1 with $Q_1<0$. So we have $r_1=2$

and $A_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Let us add Q_1:

$$v_{P,P'Q_2}(-\infty) - v_{P,P'Q_2}(+\infty) = 1$$

and $$v_{P,P'Q_1Q_2}(-\infty) - v_{P,P'Q_1Q_2}(+\infty) = 3,$$

hence P has 2 roots with $Q_1>0$ and $Q_2>0$ and 1 root with $Q_1<0$ and $Q_2<0$. So we have $r_2 = r_1$ and the list of $Q_{2,j}$ is just $(1,Q_1)$, also $A_2=A_1$.

Let us add Q_3:

$$v_{P,P'Q_3}(-\infty) - v_{P,P'Q_3}(+\infty) = -3$$

and $$v_{P,P'Q_1Q_3}(-\infty) - v_{P,P'Q_1Q_3}(+\infty) = -1,$$

hence P has 2 roots with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and 1 root with $Q_1<0$ and $Q_2<0$ and $Q_3<0$. So we have $r_3=r_2 = r_1$ and the list of $Q_{3,j}$ is just $(1,Q_1)$, also $A_3=A_1$.

Let us add Q_4:

$$v_{P,P'Q_4}(-\infty) - v_{P,P'Q_4}(+\infty) = -1$$

and $$v_{P,P'Q_1Q_4}(-\infty) - v_{P,P'Q_1Q_4}(+\infty) = 1,$$

hence P has 1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4>0$

1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4<0$

and 1 root with $Q_1<0$ and $Q_2<0$ and $Q_3<0$ and $Q_4<0$.

So we have $r_4=3$ and the list of $Q_{4,j}$ is $(1,Q_1,Q_4)$,

$$\text{also } A_4 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & -1 \end{bmatrix}$$

We add Q_5:

$$v_{P,P'\,Q_5}(-\infty) - v_{P,P'\,Q_5}(+\infty) = 1$$

$$v_{P,P'\,Q_1Q_5}(-\infty) - v_{P,P'\,Q_1Q_5}(+\infty) = 3,$$

and $$v_{P,P'\,Q_4Q_5}(-\infty) - v_{P,P'\,Q_4Q_5}(+\infty) = 1,$$

hence P has 1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4>0$ and $Q_5>0$

1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4<0$ and $Q_5>0$

and 1 root with $Q_1<0$ and $Q_2<0$ and $Q_3<0$ and $Q_4<0$ and $Q_5<0$.

So we have $r_5=3$ and the list of $Q_{5,j}$ is just $(1,Q_1,Q_4)$, also $A_5=A_4$.

Complexity of the computation

Let us denote by

P a squarefree polynomial with integer coefficients, of degree p,

r the number of real roots of P, $r\leq p$

$Q_1,\ldots,Q_k$ a finite list of polynomials with integer coefficients of respective degrees $q_1,\ldots,q_k$, prime to P,

d the maximum of $p,q_1,\ldots,q_k$;

N the maximum of $N(P),N(Q_1),\ldots,N(Q_k)$,

Q a polynomial with integer coefficients of degree q

n an integer bigger than d, log(N), k.

Proposition 2:

The complexity of SSI is in $O(n^{11})$, or using "fast multiplication", in $O(n^8 \log n \log\log n)$.

proof:

In SSIadd, which is done k times, the number of generalized subresultant Sturm sequences to compute is bounded by r. Each computation of a generalized subresultant Sturm sequence takes $O(rd^2)$ arithmetical operation, since the $\boldsymbol{Q}_{i,j}$ are of degree $\leq p+rd$.

So, the total number in SSI of arithmetic operations is in $O(kr^2d^2)$.

A bound for $N(P'\boldsymbol{Q}_{l,j})$ is $N(P')N^r$, hence a bound for $\log(N(P'\boldsymbol{Q}_{l,j}))$ is $\log(p)+\log(N(P))+r\log(N)$. So applying c) the size of the coefficients of the polynomials computed in SSIadd is in $O(rd\log(N))$.

So, using classical arithmetic, our total computation, after b) and d) is in $O(kr^4d^4log(N)^2)$, that is $O(n^{11})$.Using the "fast multiplication" [A H U], we get $O(kr^3d^3\log(N)\log(rd\log(N))\log\log(rd\log(N))$, that is $O(n^8 \log n \log\log n)$.

Remark 3

We get a complexity which is **linear in the number k of polynomials** and where the **number of real roots r plays an important role.**

2) General situation: simultaneous inequalities: algorithm SI

In this paragraph, let us denote by

P a square free polynomial with integer coefficients, of degree p,

r the number of real roots of P, $r \leq p$

$Q_1,\ldots,Q_k$ a finite list of polynomials with integer coefficients of respective degrees $q_1,\ldots,q_k$.

Presentation of SI

The aim of the algorithm is to determine the number of real roots of P giving to $Q_1,...,Q_k$ fixed signs. We first replace P by the square free polynomial $P/\mathrm{GCD}(P,P')$.

The algorithm SI is an improvment of b_4 in [C R], and as b_4 is based on SSI as well as a splitting process, to take care of the situation where P and the Q_i's have common real roots. So we shall have in the splitting process to introduce divisors of P.The improvment is based on the following remark

Remark 4

Let P_1 be a divisor of P ; if $c_\varepsilon(P; Q_1,...., Q_k)=0$ then $c_\varepsilon(P_1; Q_1,...., Q_k)=0$ .This means that if we are in the hypotheses of SSI and have already computed $\mathrm{SSIout}(P,Q_1,...,Q_k)$, we just need the following procedure SSIdiv to know $\mathrm{SSIout}(P_1;Q_1,...,Q_k)$.

Procedure SSIdiv

The input of SSIdiv is $\mathrm{SSIout}(P;Q_1,...,Q_k)$ and a divisor P_1 of P.

The output of SSIdiv is $\mathrm{SSIout}(P_1;Q_1,....,Q_k)$ and $\mathrm{SSIout}(P/P_1;Q_1,....,Q_k)$.

The computations in SSIdiv are the following:

-compute $v_{1,k}=(v_{P_1,P_1'Q_{k,j}}(-\infty)- v_{P_1,P_1'Q_{k,j}}(-\infty))_{j=1,..r_k}$

-compute $c_{1,k}=(c_{\varepsilon(k,j)}(P_1;Q_1,...,Q_k))_{j=1,..r_k}$ by inverting the system $A_k c_{1,k}=v_{1,k}$

-determine the j's such that $c_{\varepsilon(k,j)}(P_1;Q_1,...,Q_k)\neq 0$ which gives $r_{1,k}=r_k(P_1;Q_1,...,Q_k)$

-compute the invertible $r_{1,k}$, $r_{1,k}$ matrix $A_{1,k}$ obtained by extracting from A_k the corresponding $r_{1,k}$ columns and finding $r_{1,k}$ independant lines.

It is clear that after SSIdiv we have the information to determine SSIout(P_1;Q_1,...,Q_k), as well as, easily, SSIout(P/P_1,Q_1,...,Q_k) since

$c_\varepsilon(P;Q_1,...Q_k)=c_\varepsilon(P_1;Q_1,...,Q_k)+c_\varepsilon(P/P_1;Q_1,...,Q_k)$.

We go back to the algorithm SI .

<u>case k=1 .</u>

Let Q be a polynomial with integer coefficients. Let us indicate how to compute $c_{>0}(P;Q)$, $c_{<0}(P;Q)$ and $c_{=0}(P;Q)$.

-compute R= $GCD(P,Q)$

-if R is of degree 0 , apply SSI to P and Q with k=1

-if R is of degree >0

take $S = P/R$

apply SSI to S and Q with k=1 to determine $c_{>0}(S;Q)$ and $c_{<0}(S;Q)$, respectively equal to $c_{>0}(P;Q)$ and $c_{<0}(P,Q)$.

-compute $c_{=0}(P;Q) = r-(c_{>0}(P;Q)+ c_{<0}(P;Q))$

<u>case $k\neq1$</u> . We want to determine SIout(P;Q_1,...Q_k), which will consist of

($1'_k$) a splitting of P into P_1,... ,$P_{s(k)}$ (this means that P is the product of P_1,...,$P_{s(k)}$)

($2'_k$) for each $s\leq s(k)$ the list $Q_{s,1}$,...,$Q_{s,k(s)}$,$k(s) \leq k$ of the polynomials taken from the list Q_1,...,Q_l which are prime to P_s , and such that if ε is a k-uple of sign conditions with $c_\varepsilon(P;Q_1,...,Q_k)$ different from zero, there exists s and ε' with ε' composed of the non zero elements of ε and $c_\varepsilon(P;Q_1,...,Q_k) = c_{\varepsilon'}(P_s;Q_{s,1},...,Q_{s,n(s)})$.

($3'_k$) for each $s\leq s(k)$ SSIout(P_s;$Q_{s,1}$,...,$Q_{s,k(s)}$)

Description of SI

We suppose the problem solved for P,Q_1,...,Q_l and we add the polynomial Q_{l+1} by the following procedure SIadd.

Procedure SIadd

The input of SIadd is SIout($P;Q_1,\ldots,Q_l$) and Q_{l+1} and its output is SIadd($P;Q_1,\ldots Q_{l+1}$).

- define for each $s \leq s_l$, $R_s = GCD(P_s , Q_{l+1})$

-apply SSIdiv with the inputs SSIout(P_s; $Q_{s,1}$, ... , $Q_{s,l(s)}$) and R_s (we get by this SSIout(P_s/R_s; $Q_{s,1}$, ... , $Q_{s,l(s)}$) and SSIout(R_s; $Q_{s,1}$, ... , $Q_{s,l(s)}$))

-apply SSIadd to SSIout(P_s/R_s; $Q_{s,1}$, ... , $Q_{s,l(s)}$) and Q_{l+1}(we get by this SSIout(P_s/R_s; $Q_{s,1}$, ... , $Q_{s,l(s)}$,Q_{l+1}))

On the real roots of R_s one has $Q_{l+1} = 0$.

During this process, the P_s have been splitted (eventually) in P_s/R_s and R_s for the next step of the algorithm.

Example 2

We consider again

$$P = (X^3-1)(X^2-9)$$

$$Q_1 = X$$

$$Q_2 = X+1$$

$$Q_3 = X-4$$

$$Q_4 = X-2$$

$$Q_5 = X+2$$

and now $Q_6 = X^4 - X$.

We have already computed SIout($P;Q_1,\ldots,Q_5$), which coincides with SSIout($P;Q_1,\ldots,Q_5$) since $Q_1,\ldots,Q_5$ are prime to P:

P has 1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4>0$ and $Q_5>0$

1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4<0$ and $Q_5>0$

and 1 root with $Q_1<0$ and $Q_2<0$ and $Q_3<0$ and $Q_4<0$ and $Q_5<0$.

We have $r_5=3$ and the list of $Q_{5,j}$ is just $(1,Q_1,Q_4)$, also $A_5=A_4$.

Let us add Q_6 that is let us apply SIadd to SIout$(P;Q_1,...,Q_5)$ and Q_6.

The GCD of P and Q_6 is X^3-X. So we have a splitting of P in $P_1=X^3-X$ and $P_2=X^2-9$.

We apply SSIdiv to P_1; we compute :

$$v_{P_1,P'_1}(-\infty) - v_{P_1,P'_1}(+\infty) = 2$$

$$v_{P_1,P'_1\,Q_1}(-\infty) - v_{P_1,P'_1Q_1}(+\infty) = 0,$$

and $$v_{P_1,P'_1Q_4}(-\infty) - v_{P_1,P'_1Q_4}(+\infty) = 0.$$

So P_1 has 1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4>0$ and $Q_5>0$

and 1 root with $Q_1<0$ and $Q_2<0$ and $Q_3<0$ and $Q_4<0$ and $Q_5<0$,

P_2 has 1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4<0$ and $Q_5>0$.

The output of SSIdiv applied to P_1 is $r_{1,5}=2$, $A_{1,5}=A_1$,and the list of the $Q_{1,5,j}$ is $(1,Q_1)$.

We now apply SSIadd to P_1 and Q_6: we compute

$$v_{P_1,P'_1\,Q_6}(-\infty) - v_{P_1,P'_1\,Q_6}(+\infty) = 0$$

and $$v_{P_1,P'_1Q_1Q_6}(-\infty) - v_{P_1,P'_1Q_1Q_6}(+\infty) = 2.$$

Hence

P_1 has 1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4>0$ and $Q_5>0$ and $Q_6>0$

and 1 root with $Q_1<0$ and $Q_2<0$ and $Q_3<0$ and $Q_4<0$ and $Q_5<0$ and $Q_6<0$,

P_2 has 1 root with $Q_1>0$ and $Q_2>0$ and $Q_3<0$ and $Q_4<0$ and $Q_5>0$ and $Q_6=0$.

Complexity of the algorithm SI

In this paragraph we will denote by

P a polynomial with integer coefficients, of degree p,

r the number of real roots of P, $r \leq p$

$Q_1,...,Q_k$ a finite list of polynomials with integer coefficients of respective degrees $q_1,...,q_k$,

d the maximum of $p,q_1,...,q_k$;

N the maximum of $N(P),N(Q_1),...,N(Q_k)$,

Q a polynomial with integer coefficients of degree q

n an integer bigger than d, log(N), k.

Proposition 3:

The complexity of SI is in $O(n^{11})$, or , using "fast multiplication" , in $O(n^8 \log n \log\log n)$.

proof:

We first replace P by $\underline{P}$,the quotient of P by GCD(P,P'). The degree of $\underline{P}$ is less than p and the number of real roots of $\underline{P}$ is equal to r. We have $N(\underline{P}) \leq 2^p N(P)$ [Mi].The computation of $\underline{P}$ takes $O(p^2)$ arithmetic operations.

In SIadd, the number of generalized subresultant Sturm sequences to compute is bounded by $2r$ (in the worst case where GCD($\underline{P}$,Q_{l+1}) is of degree >0). Each computation of a generalized subresultant Sturm sequence takes at most $O(rd^2)$) arithmetic operations.

So, the total number of arithmetic operations is in $O(kr^2d^2)$.

In SIadd we compute subresultants of a factor of P and products of a number smaller or equal to r of Q_i 's. So applying Remark 2 the size of the coefficients of the polynomials computed in SIadd is bounded by $rd(d+log(N))$.

The computation of $\underline{P}$ is in $O(p^2(p(p+\log(N(P))+p\log N(P))^2)$, i.e in $O(p^4(p+\log(N(P)))^2)$ using classical arithmetic , and , using "fast multiplication"

in $O(p^2(p(p+\log(N(P))\log(p(p+\log(N(P))\log\log(p(p+\log(N(P))))$.

Using classical arithmetic, our total computation is in $O(kr^4d^4(d^2+log(N)^2))$, that is $O(n^{11})$.

Using the "fast multiplication" [A H U] the total computation is in $O(kr^3d^3(d+\log(N))\log(rd(d+\log(N))\log\log(rd(d+\log(N)))$,that is $O(n^8 \log n \log\log n)$.

Remark 5:

The complexity of b_4 in [C R] ,involving one more loop ,is in $O(n^{12})$.

III) Real algebraic numbers

Algorithms proposed before [CR] to work on real algebraic numbers were semi-numerical: one characterizes a real algebraic number by means of a squarefree defining polynomial P with integer coefficients and an interval that isolates ξ from all other roots of P ([Col]). The new approach is purely formal and relies on Thom's lemma. We shall present a slight improvment to b_5 in [C R].

1) Real algebraic numbers coding

In this paragraph let us denote by
P a polynomial with integer coefficients, of degree p,
r the number of real roots of P, $r \leq p$,
n an integer bigger than $p, \log(N(P))$

Principle of the coding

It is based on the following proposition:

Proposition 4 :

Let P be a polynomial of degree p with integer coefficients. Let ξ and ξ' be two real roots of P. Suppose the signs $\varepsilon(\xi)_{p-i}$ and $\varepsilon(\xi')_{p-i}$ of $P^{(i)}(\xi)$ and $P^{(i)}(\xi')$, $i=1,...,p-1$, are given. Then

(i) If $\varepsilon(\xi)_i = \varepsilon(\xi)_i$ for all $i=1,...,p-1$ then $\xi = \xi'$.

(ii) In the other case one can decide whether $\xi<\xi'$ or $\xi>\xi'$:

let k be the smallest integer such that $\varepsilon(\xi)_k$ and $\varepsilon(\xi')_k$ are different ;

(ii a) $\varepsilon(\xi)_{k-1} = \varepsilon(\xi')_{k-1}$ is different from =0,

(ii b) if $\varepsilon(\xi)_{k-1} = \varepsilon(\xi')_{k-1}$ is >0 one has $\xi > \xi'$ if and only if $P^{(p-k)}(\xi)$ is bigger than $P^{(p-k)}(\xi')$ (which is known by looking at $\varepsilon(\xi)_k$ and $\varepsilon(\xi')_k$,

(ii c) if $\varepsilon(\xi)_{k-1} = \varepsilon(\xi')_{k-1}$ is <0 one has $\xi > \xi'$ if and only if $P^{(p-k)}(\xi)$ is smaller than $P^{(p-k)}(\xi')$ (which is known by looking at $\varepsilon(\xi)_k$ and $\varepsilon(\xi')_k$,

proof: cf [C R]

Algorithm RAN

As seen in proposition 2, a real root ξ of P is characterized by the sequence of signs it gives to the derivatives $P^{(i)}$ of P . So a possible coding of ξ is this sequence of signs .The algorithm b_5 given in [C R] for coding the real roots of a polynomial was simply, after proposition 4, b_4 applied to $P;P',\ldots, P^{(p-1)}$.

We could here use SI (which is an improvment of b_4) applied to $P;P',\ldots, P^{(p-1)}$.

The algorithm RAN is an improvement of this strategy, based on the following remarks :

Remarks 6 :

a) It is better to introduce the derivatives in the order $P^{(p-1)},\ldots,P'',P'$, since after proposition 2 (ii), if condition $(*,Q,l)$ holds :

"for all l-uples ε' of sign conditions on $P^{(p-1)},\ldots,P^{(p-l-1)}$ we have

$c_{\varepsilon'}(Q;P^{(p-1)},\ldots,P^{(p-l-1)})$ equal to 0 or 1 , with Q a divisor of P "

(i) : we have an individual code of length $\leq d$ of all the roots of P which are roots of Q

(ii): if we code all real roots of P as indicated in *(i)* we can still compare them using proposition 4 .

With the notation introduced in the description of SI this will allow us to stop the branch of the computation in SI corresponding to P_k as soon as $(*,P_k,l)$ is fulfilled.

b) Situation (*, P_k, l) is automatically verified when we consider P_k a common divisor to P and $P^{(p-1-l)}$ and sign conditions on the derivatives $P^{(p-1)},...,P^{(p-l-1)}$.

So the code of a root ξ of P will be a list of length $l(\xi)$ ($\leq d$) of the signs of $P^{(d-1)}(\xi),...,P^{(d-l(\xi))}$, and hence will be shorter in some cases than the code given by b_5 in [C R].

Let us take an example to illustrate this situation.

Example 3

Let us consider $P=X^5-X$. The polynomial P has three real roots ξ_1, ξ_2 and ξ_3. If we apply b_5 in [C R] we shall have to compute the signs of P', P'', $P^{(3)}$ and $P^{(4)}$ at ξ_1, ξ_2 and ξ_3.

Now, we apply SI to P and $P^{(4)}$. We compute $P_1 = \mathrm{GCD}(P,P^{(4)}) = X$. We compute the generalized Sturm sequence of $P_2 = P/P_1 = X^3 - X$ and X. The polynomial P_2 has two real roots, ξ_1 with $X>0$ and ξ_2 with $X<0$. The polynomial P_1 has one root ξ_3 with $X=0$.

So we have an individual coding for each real root of P just using $P^{(4)}$. This code allows to compare ξ_1, ξ_2 and ξ_3, since $P^{(5)}$ is constant and positive: we have $\xi_2 < \xi_3 < \xi_1$,

Presentation of RAN

We want to determine the following output of RAN applied to P , RANout(P), which will consist of :

($1'_d$) a splitting of P into $P_1,...,P_{s(d)}$ (this means that P is the product of $P_1,...,P_{s(d)}$)

($2'_d$) for each $s \leq s(d)$ a list $P_{s,1},..., P_{s,d(s)}$ of polynomials ,taken from the list $P^{(d-1)},...,$ $P^{(j(s))}$ in this order, with $j(s) \geq 1$ and $P_{s,d(s)} = P^{(j(s))}$, which are prime to P_s , and

such that for every s and for every sign condition ε' ,with $c_{\varepsilon'}(P_s;P_{s,1},\ldots,P_{s,d(s)})$ different from 0, $c_{\varepsilon'}(P_s;P_{s,1},\ldots,P_{s,d(s)})=1$

$(3'_d)$ for each $s\leq s(d)$ SSIout$(P_s;P_{s,1},\ldots,P_{s,d(s)})$

Description of RAN

We suppose that we have computed the output of RAN applied to P at step k RANout(P,k), which consists of :

$(1'_k)$ a splitting of P into $P_1,\ldots,P_{s(k)}$

$(2'_k)$ for each $s\leq s(k)$ a list $P_{s,1},\ldots, P_{s,k(s)}$ of polynomials , taken from the list $P^{(d-1)},\ldots, P^{(i(s))}$ in this order , with $j(s)\geq d-k$ and $P_{s,k(s)}=P^{(i(s))}$, which are prime to P_s, and such that for every s , we have :

either (*, P_s, $d-j(s)+1$): for every sign condition ε' with $c_{\varepsilon'}(P_s;P_{s,1},\ldots,P_{s,k(s)})$ different from 0 , $c_{\varepsilon'}(P_s;P_{s,1},\ldots,P_{s,k(s)})=1$

or (C_s): $j(s)=d-k$.

$(3'_k)$ for each $s\leq s(k)$ SSIout$(P_s;P_{s,1},\ldots,P_{s,k(s)})$

We suppose the problem solved for step k and we add the polynomial $P^{(d-k-1)}$ by the following procedure RANadd.

Procedure RANadd

The input of RANadd is RANout(P,k) and its output is RANout$(P,k+1)$.

-If for every $s\leq s(k)$ (*, P_s, $d-j(s)+1$) holds, then RANout$(P,k+1)$ = RANout(P,k).

-Else , for each $s\leq s(k)$ such that (C_s) holds

-take $R_s = GCD(P_s, P^{(d-k-1)})$.

-apply SSIdiv to P_s/R_s , $P_{s,1}$, ..., $P_{s,k(s)}$

–apply SSIadd to P_s / R_s and $P^{(d-k-1)}$

(this gives SSIout (P_s/R_s ,$P_{s,1}$,...,$P_{s,l(s)}$, $P^{(d-k-1)}$)).

On the real roots of R_s , $P^{(d-k-1)}$= 0. During this process, the P_s have been splitted (eventually) in P_s/R_s and R_s for the next step of the algorithm. We get a new splitting P_1,...,$P_{s(k+1)}$ of P and we can check for all $s \leq s(k+1)$ whether (*,P_s , k+1) holds or not.

Notations :

For any real root ξ, we denote by $\zeta(\xi)$ the $l(\xi)$-uple of <0 , >0, =0 coding ξ by algorithm RAN.

Complexity of the algorithm RAN

Proposition 5:

The complexity of algorithm RAN is in $O(n^{11})$ (using classical arithmetic, or , using "fast multiplication" , in $O(n^8 \log n \log\log n)$.

proof:

The complexity of RAN is smaller or equal to the complexity of SI applied to P; P',.. ,$P^{(d-1)}$.

Instead of the signs given by the real roots of P to $P^{(i)}$'s we shall consider equivalently the signs given by the real roots of P to $\underline{P}^{(i)}=P^{(i)}/i!$ ($i!$ is a common divisor of the $P^{(i)}$'s coefficients) . Remark that $N(\underline{P}^{(i)}) \leq 2^i N(P)$

A bound for the products of r $N(P^{(i)})$ is $2^{pr}N(P)^r$, hence a bound for their log is $r(p+\log(N(P)))$. So the size of the coefficients of the polynomials computed is bounded by $O(pr(p+\log(N(P)))$.

After proposition 3 the total complexity using classical arithmetic is in $O(r^4p^5E^2)$, with $E=p+\log(N(P)$ and using "fast multiplication" $O(r^3p^4E\log E\log\log E)$.

So the complexity of RAN is in $O(n^{11})$ using classical arithmetic, $O(n^8 \log n \log\log n)$ using "fast multiplication" .

2)Simultaneous inequalities at real algebraic numbers

Algorithm RANI :

One wants to compute the signs taken by Q at any real root of P .
We denote by :
P a polynomial with integer coefficients , of degre p ;
r the number of real roots of P;
Q a polynomial with integer coefficients of degree q
d the maximum of p and q;
n an integer bigger than d , $\log(N(P))$, $\log(N(Q))$;
ξ_i for $1 \leq i \leq r$ the r real roots of P .

Description of RANI

The input of RANI is RANout(P). Its output is for every real root ξ of P the sign of Q at ξ. With the notations used in RAN, RANI consists just in $s(d)$ applications of SIadd applied to SSIout(P_s;$P_{s,1}$,...,$P_{s,d(s)}$) and Q.

Complexity of the algorithm RANI

Proposition 6:

The complexity of RANI is in O (n^{10}) using classical arithmetic, and in O($n^7 \log n \log\log n$) using "fast multiplication".

proof :

The complexity of RANI is in O(r^2pqE^2) , with $E=qr(p+\log(N(P)))+p\log(N(Q))$ using classical arithmetic, that is O (n^{10}) , and O($r^2pqE\log E\log\log E$) that is O($n^7 \log n \log\log n$) using "fast multiplication".

Algorithm RANSI

We denote by :

P a polynomial with integer coefficients , of degre p ;

r the number of real roots of P;

$Q_1,...,Q_k$ polynomials with integer coefficients, of degree less than q;

d the maximum of p and q;

n an integer bigger than d , $\log(N(P))$, $\log(N(Q_i))$.

One wants to compute the signs taken by $Q_1,..., Q_k$ at any real root of P .

Description of RANSI

The input of RANSI is RANout(P). Because each root of P is individually coded, RANSI consists just of k applications of RANI.

Complexity of RANSI

Proposition 7 :

The complexity of RANSI is in O (n^{11}) , and in O($n^7 \log n \log\log n$) using "fast multiplication".

proof :

The complexity of RANSI is in O(kr^2pqE^2), with $E=qr(p+\log(N(P)))+p\log(N(Q))$ using classical alrthmetic, that is O (n^{11}) , and O($kr^2pqE\log E\log\log E$) that is O($n^7 \log n \log\log n$) using "fast multiplication".

An application of RANSI : the comparison of two real algebraic numbers.

Algorithm RANSIis fundamental in the computation of topoloy of curves for example (see [R]). We give here another application.

We want to compare two real algebraic numbers ξ_1 and ξ_2 coded by RAN as real roots of the polynomial P_1 of degree n_1 and P_2 of degree n_2: we apply RANSI to P_1 and the derivatives of P_1P_2, then RANSI to P_2 and the derivatives of P_1P_2 .

Then , the coding of ξ and ξ' as real roots of P_1P_2 is known and those two algebraic numbers can be compared by proposition 4 as real roots of P_1P_2.

References

[A H U] A. Aho, J. Hopcroft, J. Ullman: *The design and analysis of computer algorithms.* Addison Wesley, Reading (1974).

[B K R] M. Ben-Or, D. Kozen, J. Reif: *The complexity of elementary algebra and geometry.* J. of Computation and Systems Sciences **32** 251-264 (1986).

[B C R] J. Bochnak, M. Coste, M.F. Roy: *Géométrie algébrique réelle.* Ergebnisse der Mathematik, Springer-Verlag, Berlin (1987).

[Col] G. Collins: *Quantifier elimination for real closed fields by cylindric algebraic decomposition.* In Second GI Conference on Automata Theory and Formal Languages. Lecture Notes in Computer Sciences, vol. 33, pp. 134-183, Springer-Verlag, Berlin (1975).

[C R] M. Coste, M.-F. Roy: *Thom's lemma, the coding of real algebraic numbers and the topology of semi-algebraic sets.* J. of Symbolic Computation (to appear in january 1988).

[Cu P 3R] F. Cucker, L. M. Pardo, M. Raimondo,T. Recio, M.-F. Roy: *On the computation of the local and global analytic branches of a real algebraic cuve.* To appear in A.A.E.C.C.-5 Conference of Minorca (1987).

[J] N. Jacobson:*Basic algebra.* San Francisco Freeman (1974).

[La] S. Lang: *Algebra.* Reading, Addison Wesley (1965).

[Lo] R. Loos: *Generalized polynomial remainder sequences.* In Computer algebra, symbolic and algebraic computation. Springer Verlag, Berlin (1982)

[Mi] M. Mignotte: *Some useful bounds.* In Computer algebra, symbolic and algebraic computation. Springer Verlag, Berlin (1982)

[R] M.-F. Roy: *Computation of the topology of a real algebraic curve.* To appear in Computational geometry and topology, Congress in Sevilla 1987.

[S] J. J. Sylvester: *On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function.* Trans. Roy. Soc. London (1853).

On Basic Open Semialgebraic Sets

by
Ludwig Bröcker

Throughout this article a ring A will be commutative with unit. We denote by Sper(A) its real spectrum and by Spec(A) its Zariski-spectrum. Note that

$$\mathrm{Sper}(A) = \bigcup_{p \in \mathrm{Spec}(A)} \mathrm{Sper}(A(p))$$

where $A(p)$ is the resicue field of A at p . Moreover, $\mathrm{Sper}(A(p))$ is the space of all orderings of $A(p)$ [L], which admits the structure of an abstract space of orderings [M 1], [M 2], [M 3], [M 4].
For $a_1,\ldots,a_r \in A$ let $U(a_1,\ldots,a_r) := \{\alpha \in \mathrm{Sper}(A) \mid a_i(\alpha) > 0 \ , \ i = 1,\ldots r\}$ and $V(a_1,\ldots a_r) := \{\alpha \in \mathrm{Sper}(A) \mid a_i(\alpha) = 0 \ , \ i = 1,\ldots,r\}$. For a real prime ideal p of A let $V(p) := \bigcap_{f \in p} V(f) = \{\alpha \in \mathrm{Sper}(A) \mid \mathrm{supp}(\alpha) \supset p\}$.

Now assume (for simplicity) that R is a real closed field and A is an algebra of finite type over R . Thus, if $S \subset \mathrm{Sper}(A)$ is constructible, then so is its closure $\bar{S}$ and its boundary δS [B-C-R, 7.2]. We denote by $\bar{S}^Z$ the Zariski-closure of S in Sper(A) , that is, $\bar{S}^Z = \bigcap_{S \subset V(f)} V(f)$. Also for a subset $X \subset \mathrm{Spec}(A)$ let $\bar{X}^Z := \cap V(f)$ where f ranges over $\bigcap_{p \in X} p$. Our main result is the following

Theorem 1: *Let* $S \subset \mathrm{Sper}(A)$ *be constructible such that* $S \cap \overline{\delta S}^Z = \emptyset$ *and let* $f_1,\ldots f_r \in A$. *Suppose that for all real prime ideals* p *of* A *there exist* $g_{r+1},\ldots,g_m \in A$ *(depending on* p*), such that* $S \cap \mathrm{Sper}(A(p)) = U(f_1,\ldots,f_r,g_{r+1},\ldots,g_m) \cap \mathrm{Sper}(A(p))$. *Then there exist* $f_{r+1},\ldots,f_m \in A$ *with* $S = U(f_1,\ldots,f_m)$.

Corollary 2: (See also [Sch]). *Let* V *be an algebraic affine real* R*-variety of dimension* n *and let* $S \subset V(R)$ *be a basic open semialgebraic set. Then* $S = \{x \in V(R) \mid f_1(x) > 0,\ldots,f_n(x) > 0\}$ for suitable $f_1,\ldots,f_n \in R[V]$.

Proof of the Corollary: Note that we have a canonical 1-1 correspondence between the semialgebraic sets in V(R) and the constructible sets in Sper(A) where $A = R[V]$. Moreover, for a real prime ideal p of A , $A(p)$ is a real function field over R of dimension $\leq n$. Thus the stability index of $\mathrm{Sper}(A(p))$ is $\leq n$ [Bro 1, §4], that is, in $\mathrm{Sper}(A(p))$ each basic set is generated by $\leq n$ elements. Now, setting $r = 0$, the Corollary follows from the Theorem.

For the proof of the Theorem we need a corresponding result, first in an abstract and then in the semilocal situation.

Theorem 3: *Let* (X,G) *be a space of orderings. Let* $S \supset X$ *be constructible and let* $f_1,\dots,f_r \in G$ *such that* $S \subset X(f_1,\dots,f_r)$. *If for all finite fans* $F \subset X(f_1,\dots,f_r)$ *one has* $\#(S \cap F) \mid \#(F)$ *and* $2^m(S \cap F) \equiv 0 \bmod \#(F)$, *then there exist* $f_{r+1},\dots,f_m \in G$ *such that* $S = X(f_1,\dots,f_m)$.

Here, for $g_1,\dots,g_n \in G$, $X(g_1,\dots,g_n) = \{\sigma \in X \mid \sigma(g_i) = 1,\ i = 1,\dots,n\}$.

Proof: See [Brö 2, §4], [Brö 3, Th. 5.4].

Proposition 4: *Let* (X,G) *be a space of orderings and let* $f_i, g_j, h_j \in G$, $i = 1,\dots,r$, $j = r+1,\dots,m$, *such that* $S = X(f_1,\dots,f_r, g_{r+1},\dots,g_m) = X(f_1,\dots,f_r,h_{r+1},\dots,h_m)$ *and let* $k_{r+1} \in D(\langle g_{r+1},h_{r+1}\rangle)$. *Then there exist* $k_{r+2},\dots,k_m \in G$ *such that* $S = X(f_1,\dots,f_r,k_{r+1},\dots,k_m)$.

This follows easily from [M 3, Cor. 3.5 and L. 6.3].
See also [Brö 3, Prop. 4.14].
It was discovered by Scheiderer [Sch] that this result is crucial for the proof of Th. 1.

Theorem 5: *Let* A *be a semilocal ring. Let* $S \subset \mathrm{Sper}(A)$ *be open and closed and let* $f_1,\dots,f_r \in A^*$. *If for all real prime ideals* p *of* A *there are* $g_{r+1},\dots,g_m \in A$ *such that* $S \cap \mathrm{Sper}(A(p)) = U(f_1,\dots,f_r,g_{r+1},\dots,g_m) \cap \mathrm{Sper}(A(p))$ *then there exist* $f_{r+1},\dots,f_m \in A^*$ *such that* $S = U(f_1,\dots,f_m)$.

Sketch of the Proof: Let $T := \{a \in A \mid a(\alpha) > 0 \text{ for all } \alpha \in \mathrm{Sper}(A)\}$ and $T^* = A^* \cap T$. Then $(\mathrm{Spermax}(A), A^*/T^*)$ is a space of orderings. Moreover, for all non trivial fans $F \subset \mathrm{Spermax}(A)$ there exists a real prime ideal p of A such that $p = \mathrm{supp}(\alpha)$ for all $\alpha \in F$ [Kn]. Thus, from our assumption follows that the numerical conditions of Th. 3 hold for S , from which we get the result.

Proof of Theorem 1: We try to move the assumption from r to $r+1$. For $f_{r+1} \in A$ let Y be the collection of all real prime ideals p of A such that $S \cap \mathrm{Sper}(A(p))$ is not of the form $U(f_1,\dots,f_r,f_{r+1},g_{r+2},\dots,g_m) \cap \mathrm{Sper}(A(p))$ and let $Z := \overline{Y}^Z \subset \mathrm{Sper}(A)$. We choose f_{r+1} such that Z has smallest possible dimension d. We claim that $Z = \emptyset$ .So assume $\emptyset \neq Z$ and $Z_1,\dots,Z_k$ are the components of Z with generic points $z_1,\dots,z_k$. Then $Z_i \not\subset \overline{\delta S}^Z \cup V(f_1) \cup \dots \cup V(f_r)$, $i = 1,\dots,k$, since for $Z_i \subset \overline{\delta S}^Z \cup V(f_1) \cup \dots \cup V(f_r)$ one can choose $g_j = 0$,

$j = r+1,\ldots,m$, in $A(z_i)$. Let $B := A_{z_1,\ldots,z_k}$ (semilocalization). Then $f_i \in B^*$, $i = 1,\ldots,r$ and $S \cap \mathrm{Sper}(B)$ is open and closed in $\mathrm{Sper}(B)$ by [Brö 2, L. 6.1]. So by Th. 5 we find $h_{r+1},\ldots,h_m \in B^*$ such that $S \cap \mathrm{Sper}(B) = T \cap \mathrm{Sper}(B)$ for $T := U(f_1,\ldots,f_r,h_{r+1},\ldots,h_m)$. Let $D := (S \cup T) \setminus (S \cap T)$. Then $V(z_i) \not\subset \overline{D}^Z$ for $i = 1,\ldots,h$. By multiplication with positiv equations for Z and $\overline{D}$ respectively we may assume that f_{r+1} vanishes on Z and h_{r+1} on $\overline{D}^Z$. Now let Y' be the set of all real prime ideals p of A such that $S \cap \mathrm{Sper}(A(p))$ is not of the form $U(f_1,\ldots,f_r,h_{r+1}+f_{r+1},g_{r+2},\ldots,g_m) \cap \mathrm{Sper}(A(p))$

and $Z' := \overline{Y'}^Z$ correspondingly. Then $Z' \cap Z_i \subset \overline{D}^Z \cap Z_i$ is a proper subvariety of Z_i for $i = 1,\ldots,k$. On the other hand, if $V(p) \not\subset Z$ for a real prime ideal, then either $V(p) \subset \overline{D}^Z$, so $h_{r+1} \in p$ and $f_{r+1}+h_{r+1} = f_{r+1}$ fullfills already the assertion over $A(p)$, or we have $S \cap \mathrm{Sper}(A(p)) = U(f_1,\ldots,f_r,f_{r+1},g_{r+2},\ldots g_m) \cap \mathrm{Sper}(A(p)) = U(f_1,\ldots,f_r,h_{r+1},h_{r+2},\ldots,h_m) \cap \mathrm{Sper}(A(p))$ for suitable g_i , $i = r+2,\ldots,m$, depending on p . But in the space of orderings, which is associated to $A(p)$ we have $\overline{f_{r+1}+h_{r+1}} \in D(\langle \overline{f}_{r+1}, \overline{h}_{r+1} \rangle)$ where $\bar{}$ denotes the residue class modulo sums of squares. Now by Prop. 4 we find $k_{r+2},\ldots,k_m$ such that $S \cap \mathrm{Sper}(A(p)) = U(f_1,\ldots,f_r,f_{r+1}+h_{r+1},k_{r+2},\ldots,k_m) \cap \mathrm{Sper}(A(p))$. Thus $Z' \subset Z$ and $\dim(Z') < d$. Contradiction.

References

[B-C-R] Bochnak, J.; Coste, M; Roy, M.F.: Géométrie Algébrique Réelle. Ergeb. Math., Berlin, Heidelberg, New York: Springer 1987

[Brö 1] Bröcker, L.: Zur Theorie der quadratischen Formen über formal reellen Körpern. Math. Ann. 210, 233-256 (1974)

[Brö 2] ~ : Minimale Erzeugung von Positivbereichen. Geom. Dedicata 16, 335-350 (1984).

[Brö 3] ~ : On basic semialgebraic sets. to appear

[Kn] Knebusch, M.: On the local theory of signatures and reduced quadratic forms. Abh. Math. Sem. Univ. Hamburg 51, 149-195 (1981)

[L] Lam, T.Y.: Orderings, valuations and quadratic forms. Conference Board of the mathematical sciences, regional conference series in mathematics 52 - A.M.S. 1983

[M 1] Marshall, M.: Classification of finite spaces of orderings, Canad. J. Math. 31, 320-330 (1979)

[M 2] ~ : Quotients and inverse limits of spaces of orderings. Canad. J. Math. 31 604-616 (1979)

[M 3] ~ : The Witt ring of a space of orderings. Trans. Amer. Math. Soc. 298, 505-521 (1980)

[M 4] ~ : Spaces of orderings IV. Canad J. Math. 32, 603-627 (1980

[Sch] Scheiderer, C.: Stability index of real varieties. To appear.

Ludwig Bröcker
Mathematisches Institut
Einsteinstraße 62
D-4400 Münster

Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel.

Noaï Fitchas [1] (Buenos Aires)

André Galligo [2] (Nice)

1. Introduction.

Le Nullstellensatz de Hilbert démontre que, sur un corps algébriquement clos, l'idéal de polynômes définissant une variété algébrique affine contient 1 si et seulement si la variété est vide. L'objet de ce travail est d'étudier des versions effectives de cet énoncé en vue d'applications en Calcul Formel et en théorie de la Complexité.

Soit k un corps (commutatif) quelconque et $X_0,\dots,X_n$ des indéterminées sur k.

Nous notons deg(F) le degré total du polynôme F de $k[X_0,\dots,X_n]$.

Nous appelons Nullstellensatz effectif relatif à la fonction $\psi : N^2 \longrightarrow N$ (qu'on appelle une borne) l'énoncé suivant :

soient $F_1,\dots,F_s \in k[X_0,\dots,X_n]$ et $d=\max \deg(F_i)$,

alors $1\in(F_1,\dots,F_s)$ ssi il existe des polynômes $P_i\in k[X_0,\dots,X_n]$ tels que :

$$1=\sum_{1\leqslant i\leqslant s} P_iF_i \quad \text{et} \quad \max(\deg(P_iF_i)) \leqslant \psi(d,n).$$

---

1) Groupe de travail constitué par Leandro Caniglia, Guillermo Cortiñas, Silvia Danón, Joos Heintz, Teresa Krick, Pablo Solerno.
Instituto de Matematica, Consejo Nacional de Investigationes Científicas y Tecnicas; Viamonte 1636, (1055) Buenos Aires – Argentina.

2) Département de Mathématiques, Université de Nice, Parc Valrose, 06034 Nice cedex , France.

Des versions de Nullstellensatz existent depuis le début du siècle, de façon implicite chez Macaulay (voir par exemple [23], chapter I, Art 16) puis de façon complètement explicite relativement à des fonctions ψ doublement exponentielles en n et polynomiales en d (voir [16] et [26]). Ces résultats s'obtiennent essentiellement en bornant les degrés de certains résultants après avoir convenablement préparé les données.

Une borne $\psi(d,n) = d^n$ a été conjecturé depuis longtemps. Un exemple de Masser et Philipon (voir dans [3]) montre qu'il n'existe pas de borne inférieure à $d^n - d^{n-1}$.

Le premier Nullstellensatz effectif relativement à une ψ simple exponentielle en n : $\psi(d,n) = 3n^2d^n$ mais pour un corps k de caractéristique 0, est du à Brownawell [3]. La démonstration est difficile : elle utilise des connaissances spécialisée d'analyse complexe notamment un théorème de Skoda(voir [3]) et une théorie de l'élimination assez spécifique [25].

Après cette percée, nous avons démontré dans [4] et [5] un Nullstellensatz effectif pour un corps de caractéristique quelconque et relativement à des bornes ψ simples exponentielles :

$$\psi(d,n) = d^{(n+1)(n+2)/2} \text{ et } \psi(d,n) = d^{n(n+3)/2}.$$

Enfin, J. Kollar a démontré dans [19] le meilleur résultat actuellement connu: pour un corps de caractéristique quelconque, une borne

$$\psi(d,n) = \max\{d^n, 3^n\}.$$

La démonstration de [19] est élégante mais fait appel à de la géométrie algébrique approfondie : théorie des faisceaux, cohomologie à support, théorie de l'intersection. Elle reste donc hermétique à la plupart des non spécialistes, notamment aux chercheurs en Calcul Formel qui utilisent plutôt de l'algèbre "classique".

Du point de vue du Calcul Formel, la connaissance d'un Nullstellensatz effectif avec une borne simple exponentielle permet d'améliorer la compléxité de nombreux algorithmes séquentiels ou parallèles. Par exemple le calcul de la dimension d'une variété algébrique affine, le calcul d'une base standard d'une variété affine de dimension zéro, le test d'appartenance d'un polynôme à un idéal équidimensionel (voir [4], [7]). Egalement, sur un corps algébriquement clos, l'élimination des quantificateurs dans les formules prénexes à nombre d'alternations de quantificateurs fixé (voir [8], [11]) ou le test de "consistence" d'un ensemble semi-algébrique (voir [15]).
Pour illustrer ce type d'application nous donnons, dans la deuxième partie du présent travail, une version effective et tout à fait élémentaire de l'ex-conjecture de Serre (démontrée en 1976 indépendamment par Suslin et Quillen). Notre résultat peut être amélioré : une version plus générale et plus précise que nous énonçons sera publiée ultérieurement par le premier auteur [9]. Voir aussi [27].

Quoiqu'il existe encore une petite différence entre les bornes de l'exemple de Masser-Philippon et les bornes de Kollar, du point de vue de la théorie de la compléxité et du Calcul Formel le pas essentiel est fait. Nous pensons que dans ces domaines, la recherche va plutôt s'orienter vers l'étude d'algorithmes adaptés à des situations spécifiques : polynômes creux ou donnés par des straight-line-programs (voir [13], [14], [18]).

Dans la première partie de ce travail, nous démontrons un Nullstellensatz effectif relativement à une fonction en $O(d^n)$, plus précisément

$$\psi(d,n) = 3\,d^n .$$

Notre preuve est complète et élémentaire : nous n'utilisons que des connaissances usuelles que l'on trouve dans les manuels d'algèbre commutative. Nous pensons que cette démonstration pourra être comprise

par les chercheurs en Calcul Formel et nous espérons qu'elle contribuera à améliorer les algorithmes existants.
Nous discutons ensuite du lien entre le Nullstellensatz effectif et l'existence d'une syzygie finale (voir aussi [28] et [4]) qui correspond à la notion d' "inconsistance stable" d'une famille de polynômes.

Une autre méthode de recherche explicite d'une famille $\{P_i\}$ telle que $1 = \sum P_i F_i$ est décrite dans [1]. Cette approche a été exploitée dans [3] et paraît très prometteuse.

Schéma de notre preuve du Nullstellensatz effectif.

1ère étape : On se ramène au cas $1 \in I$ où $I = (F_1,\dots,F_s)$ est une intersection complète de $k[X_1,\dots,X_n]$, avec $s \leqslant n + 1$ et $\deg(F_i) \leqslant d$. On homogénéise chaque F_i en un polynôme de même degré G_i de $R = k[X_0,\dots,X_n]$.
On veut alors majorer m tel que $X_0^m \in (G_1,\dots,G_s)$.
Pour chaque i=1 à s, on regroupe les composantes primaires de $(G_1,\dots,G_i)$ en composantes à "distance finie" et composantes contenues dans l'hyperplan à l'infini. On note B_i l'intersection des composantes "à distance finie".
On remarque que $B_1 = (G_1)$ et $B_s = (1)$.

2ème étape : Pour chaque i = 1 à s, on décompose de même

$$(B_i, G_{i+1}) = B_{i+1} \cap \Gamma_{i+1} \cap \Delta_{i+1}$$

Γ_{i+1} désigne l'intersection des composantes isolées "à l'infini" et

Δ_{i+1} l'intersection des composantes immergées "à l'infini".

Une inégalité de Bézout permet alors de borner ℓ_{i+1} tel que

$X_0^{\ell_{i+1}} B_{i+1} \subset \Gamma_{i+1}$.

Plus précisément si b_i désigne la somme des "degrés" des composantes de B_i on a $b_{i+1} + \ell_{i+1} \leqslant d\, b_i$, donc par récurrence $\ell_{i+1} \leqslant d^{i+1}$.

3ème étape : On démontre que pour c_i satisfaisant la formule de récurrence $c_{i+1} \leqslant 4c_i + \ell_{i+1}$, et $c_1 = 0$; on a :

$X_0^{2c_i+\ell_{i+1}} B_{i+1} \subset \Delta_{i+1}$; d'où $X_0^{2c_i+\ell_{i+1}} B_{i+1} \subset (B_i, G_{i+1})$.

La preuve procède par "dualité" : on montre facilement qu'il suffit de majorer c tel que $X_0^{\,c}\ \mathrm{Hom}_R(R/\Delta_{i+1}, R/(B_i, G_{i+1})) = 0$, et nécessite l'utilisation d'un argument élémentaire d'algèbre homologique que nous avons complètement explicité.

4ème étape : On utilise cette dernière inclusion pour construire une suite de polynômes $R_i \in B_i$ et une suite de polynômes A_i tels que

$X_0^{2c_{i+1}+\ell_{i+1}} R_{i+1} = R_i + A_i G_{i+1}$ avec $R_s = 1$ et $R_1 \in (G_1)$.

D'où $X_0^{\,m} \in (G_1, \ldots, G_s)$, avec $m = \sum 2c_i + \ell_{i+1}$ que l'on sait borner par d^s lorsque $d \geqslant 3$.

5ème étape : On améliore cette borne en majorant directement ℓ_{n+1} lorsque $s = n+1$.

Cette preuve reprend donc l'approche inductive que nous avions décrit dans [4] et [5]. La différence essentielle provient de la 3ème étape, qui a été inspirée par la lecture du pré-print de J.Kollar [19]. Cette étape permet de profiter complètement des majorations obtenues à chaque pas de la récurrence .

2. Un Nullstellensatz effectif.

Dans toute la suite k sera un corps commutatif fixé, de caractéristique positive ou nulle. Nous désignerons par $\overline{k}$ la clôture algébrique de k, et par $X_0,\ldots X_n$ des indéterminées sur k.

On considère des polynômes $F_1,\ldots,F_s \in k[X_1,\ldots,X_n]$ dont le maximum des degrés est égal à un entier d, on désigne comme d'habitude par $(F_1,\ldots,F_s)$ l'idéal qu'ils engendrent. Nous allons démontrer le théorème suivant.

Théorème 1 (Hilbert Nullstellensatz effectif; voir [3], [4], [5], [19]) :
$1 \in (F_1,\ldots,F_s)$ si et seulement si
il existe des polynômes $P_1,\ldots,P_s \in k[X_1,\ldots,X_n]$ tels que
$1 = \sum_{1\leqslant i\leqslant s} P_iF_i$ et $\max_{1\leqslant i\leqslant s} \deg(P_iF_i) \leqslant 3\,d^n$.

Démonstration. Comme nous l'avons indiqué à la fin de l'introduction, la démonstration est constituée de 5 étapes.
La *1ère étape* consiste en une préparation des données.
Comme il s'agit de trouver des polynômes P_i de degrés majorés par une constante explicite, la question peut être reformulée en termes d'algèbre linéaire sur k, et ne dépend que du plus petit sous-corps qui contient les coéfficients des F_i. Nous allons donc supposer, sans restriction de généralité, que k est algébriquement clos, soit $k = \overline{k}$, qui est donc infini.
Soit r le degré de transcendance de l'extension de corps $k \subset k(F_1,\ldots,F_s)$, alors $r\leqslant n$ et $r\leqslant s$. Il existe alors r combinaisons linéaires des F_i (à coéfficients dans k) qui sont algébriquement indépendantes et forment une suite régulière $F'_1,\ldots,F'_r$;le degré maximum des F'_i est d . D'où une suite d'idéaux équidimensionels de hauteurs 1, 2, ..., r :
$(F'_1) \subset (F'_1, F'_2) \subset \ldots \subset (F'_1,\ldots, F'_r)$ inclus dans $(F_1,\ldots, F_s) = (1)$. (Voir [17].)

De plus $k[F'_1,\ldots,F'_r] \subset k[F_1,\ldots,F_s]$ est une extension algébrique finie. Sur chaque composante irréductible de l'ensemble des zéros $\{F'_1 = \ldots = F'_r = 0\}$, chacune des F_i est nécessairement constante (éventuellement nulle). Donc il existe une autre combinaison linéaire "générique" F'_{r+1} des F_i qui écarte les composantes superflues, i.e. telle que $\{F'_1 = \ldots = F'_{r+1} = 0\} = \{F_1 = \ldots = F_s = 0\} = \varnothing$. Donc $1 \in (F'_1,\ldots,F'_{r+1})$. On peut alors supposer, sans restriction de généralité, $s = r+1$ et $F'_i = F_i$. ◆

Pour $1 \leqslant i \leqslant s$, soit $G_i \in k[X_0,\ldots,X_n]$, l'homogénéisé de F_i, on a $\deg(G_i)=d$.

Pour chaque i, $1 \leqslant i \leqslant s$, on note B_i l'intersection des composantes primaires de $(G_1,\ldots,G_i)$ qui ne contiennent pas X_0 dans leur radical, on dira qu'elles sont à "distance finie". En particulier, on a $B_1 = (G_1)$ et $B_s = (1)$.

Dans toute la suite, on est donc réduit à un problème projectif, on utilisera la terminologie et les notations suivantes (voir [24]) :

cf(A) désignera le corps de fraction d'un anneau intègre A.

$R = k[X_0,\ldots,X_n]$, R est une k-algèbre munie de la graduation par le degré total.

I étant un idéal homogène de R, on notera rad(I) le radical de I et $\{ I=0 \}$ la sous-variété fermée de $\mathbb{P}^n$ définie par I, à laquelle correspond une dimension $\dim \{ I=0 \}$ et un degré $\deg \{ I=0 \}$.

Soit $A = R/I$, A est une k-algèbre graduée et un R-module, nous noterons dim(A) la dimension de Krull (affine) de A et deg(A) le degré défini par la fonction d'Hilbert de A. On a alors $\dim(A) = 1 + \dim \{ I=0 \}$. Explicitons dans les seuls cas que nous utiliserons dans cet article.

Si I est un idéal premier donc A une algèbre intègre, dim(A) est le degré de transcendance de cf(A) sur k, et $\deg(A) = \deg \{ I = 0 \}$.

Si I est primaire, $\pi = \mathrm{rad}(I)$ est premier, $\dim(R/I) = \dim(R/\pi)$, $\deg(R/I)$ est un multiple de $\deg(R/\pi)$. Plus précisément, notons R_π la localisation de R en π

et ℓ la longueur du localisé de R/I en π (considéré comme module sur R_π), ℓ est la longueur maximum d'une suite :

$$0 \subset S_1 \subset \ldots \subset S_\ell = R/I \quad \text{telle que } S_j/S_{j-1} \simeq R/\pi \text{ pour } 1 \leqslant j \leqslant \ell \ ;$$

on a alors :

$$\deg(R/I) = \ell \deg(R/\pi) .$$

Dans le cas où I est de dimension pure (i.e. toutes les composantes primaires donnent la même dimension), le degré est la somme des degrés correspondant aux composantes primaires .

Soit M un R-module gradué de type fini, on notera dim(M) la dimension de Krull de M, soit dim(R/ann(M)). On notera M_{X_0} le localisé de M en X_0.

Avec ces notations, remarquons que pour tout i, $1 \leqslant i \leqslant s$,

(1) $B_i = (G_1,\ldots,G_i)_{X_0} \cap R$,

(2) $B_1 = (G_1)$

(3) R/B_i est de dimension pure $n-i+1$;

et G_{i+1} n'est pas diviseur de zéro dans R/B_i .

Notations : Pour chaque i, $1 \leqslant i \leqslant s$, on considère une décomposition primaire irrédondante, puis on regroupe les composantes en :

$$(B_i,G_{i+1}) = B_{i+1} \cap \Gamma_{i+1} \cap \Delta_{i+1}$$

Γ_{i+1} est l'intersection des composantes isolées dont le radical contient X_0, Δ_{i+1} l'intersection des composantes "immergées dont le radical contient X_0 . Ce sont des idéaux homogènes, Δ_{i+1} n'est pas uniquement déterminé.

Lorsque l'on fixera i, on notera $A = R/B_i$, $B = B_{i+1}/B_i$, $\Gamma = \Gamma_{i+1}/B_i$, $\Delta = \Delta_{i+1}/B_i$, et g la classe de G_{i+1} dans A. D'où

$$A\,g = B \cap \Gamma \cap \Delta .$$

En raisonnant sur les composantes irréductibles, on voit que $A/\Gamma = R/\Gamma_{i+1}$ est de dimension pure n-i.

Dans la $2^{ème}$ *étape* nous allons démontrer une version simple et utile de l'inégalité de Bézout (voir aussi [12] Theorem 1, et [4] Proposition 5). Ce résultat est difficilement accessible dans les livres spécialisés tel que celui de Fulton[10] qui ne traite et même n'énonce que des résultats sur des situations plus sophistiquées . Commençons par bien préciser la définition du degré et à démontrer un lemme simple .

Soient A une k-algèbre graduée, $\pi_1,\ldots,\pi_t$ ses idéaux premiers minimaux de hauteur minimale (géométriquement cela correspond aux composantes irréductibles de dimension maximale). On sait qu'il existe une suite de composition $(M_i)_{0\leqslant i\leqslant m}$ de A , i.e. $0\subset M_m\subset\ldots\subset M_0=A$, telle que M_i/M_{i+1} soit isomorphe à A/p_i où p_i est un idéal premier de A. Pour j fixé, $1\leqslant j\leqslant t$, le nombre de fois où $p_i = \pi_j$ est la longueur $\text{long}(A_{\pi_j})$ du localisé de A en π_j .

Définition : $\deg(A) = \sum_{1\leqslant j\leqslant t} \text{long}(A_{\pi_j})\ \deg(A/\pi_j)$.

Lemme 2 : Soit K un corps (commutatif) et D une K-algèbre de dimension finie. Soit $I_1\cap\ldots\cap I_t$ une décomposition primaire irrédondante de l'idéal (0) de D. Posons $\pi_j = \text{rad}(I_j)$, $\lambda_j = \min\{\lambda\ ;\ \pi_j^{\lambda}\subset I_j\}$ et considérons $\text{long}(D_{\pi_j})$ pour tout j, $1\leqslant j\leqslant t$. Alors :

$$\sum_{1\leqslant j\leqslant t} \lambda_j \dim_K(D/\pi_j) \leqslant \sum_{1\leqslant j\leqslant t} \text{long}(D_{\pi_j})\dim_K(D/\pi_j) = \dim_K D .$$

Preuve: Remarquons tout d'abord que puisque D est de dimension 0, $\deg(D) = \dim_K(D)$ et pour $1\leqslant j\leqslant t$, π_j est un idéal maximal, $\deg(D/\pi_j) = \dim_K(D/\pi_j)$, de plus $D/I_j = D_{\pi_j}$.

Par le Théorème du Reste Chinois, on a $D \simeq D/I_1\oplus\ldots\oplus D/I_t$ ce qui entraine $\dim_K D = \sum_{1\leqslant j\leqslant t}\dim_K(D/I_j)$. Il suffit donc de considérer le cas t=1, c'est à dire le cas où D est local .

Notons alors π l'idéal maximal de D et soit λ entier tel que $\pi^{\lambda}=(0)$ et $\pi^{\lambda-1}\neq(0)$. Dans ce cas nous avons les λ inclusions strictes :

$$(0) = \pi^{\lambda} \subset \pi^{\lambda-1} \subset \pi^{\lambda-2} \subset \ldots \subset \pi \subset D$$

il est alors clair que $\lambda \leqslant \text{long}(D_{\pi_j})$. ◆

Proposition 3 : Soit $\Gamma = J_1 \cap \ldots \cap J_s$ une décomposition primaire irrédondante dans l'algèbre A.

Pour tout j, $1 \leqslant j \leqslant s$, posons $\lambda_j = \min \{ \lambda \, ; (\text{rad}(J_j)^{\lambda} \subset I_j \}$. Alors,

$\sum_{1 \leqslant j \leqslant s} \deg(A/\pi_j) \cdot \lambda_j + \deg(A/B) \leqslant \deg(A)\, d$.

Conséquence : Comme $X_0 \in \pi_j$ pour tout $1 \leqslant j \leqslant t$, on obtiendra $X_0{}^{\lambda_j} \in I_j$; donc en posant $\ell = \max(\lambda_j)$, on obtiendra $X_0{}^{\ell} \in \Gamma$ et $\deg(A/B) + \ell \leqslant \deg(A)\, d$.

Preuve : Rappelons que A est gradué de dimension pure $n-i+1$, et que g, homogène de degré d , est non-diviseur de zéro dans A.

Soient $x_0,\ldots,x_n$ les images de $X_0,\ldots,X_n$ dans A et $y_0,\ldots,y_{n-i}$ des combinaisons linéaires "génériques" de $x_0,\ldots,x_n$; elles sont homogènes de degré 1. Les ensembles $\{g, y_1,\ldots,y_{n-i}\}$ et $\{y_0, \ldots, y_{n-i}\}$ sont chacun algébriquement indépendants sur k.

Notons $C = k[g,y_1,\ldots,y_{n-i}]$ et $E = k[y_0,\ldots,y_{n-i}]$, ce sont des sous algèbres graduées de A.

Par une forme convenable du Théorème de normalisation de Noether (voir par exemple [12], Lemma 1) A est un E-module de type fini, autrement dit l'extension de k-algèbres graduées $E \subset A$ est entière.

Par conséquent, il existe une relation de dépendance intégrale de degré minimal r de g sur E :

$$(*)\quad g^r + a_{r-1}g^{r-1} + \ldots + a_0 = 0 .$$

Les a_j pour $1 \leqslant j \leqslant r-1$ sont nuls ou homogènes de degré $(r-j)\, d$

et a_0 est non nul de degré $r\, d$.

On considère les $a_j \neq 0$ comme des polynômes homogènes en $y_0,\ldots,y_{n-i}$ de degré $(r-j)$ d. Quitte à effectuer encore un changement linéaire générique des $y_0,\ldots,y_{n-i}$, on peut supposer que le degré en y_0 de $a_j \neq 0$ est $(r-j)$ d.

On interprète maintenant (*) comme une relation de dépendance intégrale (de degré r d) de y_0 sur C. Donc y_0 est entier sur C, ce qui implique que :

A est une extension entière de C.

Soient $(0) = I_1 \cap \ldots \cap I_t$ une décomposition primaire irrédondante dans A et soient $\pi_1,\ldots,\pi_t$ les idéaux premiers minimaux de A. Fixons momentanément j, $1 \leqslant j \leqslant t$, $\pi = \pi_j$, c'est un idéal homogène. Comme g est non diviseur de zéro et que les $y_0,\ldots y_n$ sont génériques, les applications canoniques $E \to A/\pi$ et $C \to A/\pi$ sont injectives. Elles définissent donc des extensions entières d'algèbres graduées. Nous identifierons g, $y_0,\ldots,y_n$ avec leurs images dans A/π.

En considérant les corps de fractions, on obtient des extensions algébriques de corps : $cf(E) \subset cf(A/\pi)$ et $cf(C) \subset cf(A/\pi)$.

g comme élément de A/π est entier sur E et E comme anneau de polynômes sur k, est intégralement clos. On en déduit que le polynôme minimal de $g \in A/\pi$ sur cf(E) est de la forme (*) avec $r = [cf(E[g]) : cf(E)]$.

On peut de nouveau interpréter ce polynôme comme une relation de dépendance intégrale de y_0 sur C. D'où :

$$[cf(C[y_0]) : cf(C)] \leqslant [cf(E[g] : cf(E)]\, d.$$

Notons par ailleurs que $C[y_0] = E[g]$ et que le choix générique des $y_0,\ldots,y_{n-i}$ implique, par le théorème de normalisation, que $[cf(A/\pi) : cf(E)] = deg(A/\pi)$.

En rassemblant ces résultats, on obtient :

$$[cf(A/\pi) : cf(C)] = [cf(A/\pi) : cf(C[y_0])] \,.\, [cf(C[y_0]) : cf(C)]$$

$$\leqslant [cf(A/\pi) : cf(E[g])] \,.\, [cf(E[g]) : cf(E)]\, d$$
$$\leqslant deg(A/\pi)\, d\,.$$

En reprenant les anciennes notations, nous énonçons :

pour tout j , $1 \leqslant j \leqslant t$, $[cf(A/\pi_j) : cf(C)] \leqslant deg(A/\pi_j)$.

Soient $K' = cf(C)$ et $D' = A \otimes_C K'$. Montrons que $\dim_{K'} D' \leqslant deg(A)\, d$.

Comme A est entier sur C, on voit que D' est une K'-algèbre de dimension finie. On voit que $\pi'_1 = \pi_1 D'$, ..., $\pi'_t = \pi_t D'$ sont les idéaux maximaux de D', soit $(0) = I'_1 \cap \ldots \cap I'_t$ la décomposition primaire irrédondante de (0), avec $rad(I'_j) = \pi'_j$. Pour $1 \leqslant j \leqslant t$, on a :

$D'/\pi'_j = A/\pi_j \otimes_C cf(C) = cf(A/\pi_j)$ d'où :

$\dim_{K'}(D'/\pi'_j) = [cf(A/\pi_j) : cf(C)] \leqslant deg(A/\pi_j)\, d$, et $long(D'_{\pi'_j}) = long(A_{\pi_j})$

donc :

$\dim_{K'}(D'/I'_j) = long(D'_{\pi'_j})\, \dim_{K'}(D'/\pi'_j)$

$\leqslant long(A_{\pi_j})\, deg(A/\pi_j)\, d = deg(A/I_j)\, d,$

En sommant puisque $D' = \oplus_j D'/I'_j$, on obtient :

$$\dim_{K'} D' \leqslant \Sigma_{1 \leqslant j \leqslant t}\ deg(A/I_j)\, d = deg(A)\, d\,.$$

Soient $K = k(y_1, \ldots, y_{n-i})$ et $D = A/Ag \otimes_{k[y_1,\ldots,y_n]} \acute{K}$. Montrons que $\dim_K(D) \leqslant deg(A)\, d$.

On a $C/Cg \simeq k[y_1, \ldots, y_{n-i}]$, on la considère comme une sous-algèbre de A/Ag car les images des y_j sont algébriquement indépendantes dans A/Ag. On obtient ainsi un diagramme commutatif :

$$\begin{array}{ccc} A/Ag & \simeq & A\otimes_C C/Cg \\ | & & | \\ k[y_1,\dots,y_{n-i}] & \simeq & C/Cg \end{array}$$

Comme A est un C-module de type fini et que C est intégralement clos, il existe un $b \in C$ tel que A_b est un C_b module libre de rang égal à $\dim_{K'} D'$. Donc $(A/Ag)_b \simeq A_b\otimes_{C_b}(C/Cg)_b$ est un $(C/Cg)_b$ -module libre de même rang. D'où :

$$\dim_K D = \dim_{cf(C/Cg)} A\otimes_C cf(C/Cg) = \dim_{K'} D' \leqslant \deg(A)\, d\,.$$

D est une K-algèbre de dimension finie, nous pouvons donc appliquer le lemme 2. Vérifions qu'on trouve bien le résultat cherché.

Pour tout idéal J de A, notons $\underline{J}$ son extension JD dans D . Reprenons les décompositions :

$$Ag = B \cap \Gamma \cap \Delta \quad \text{et} \quad B \cap \Gamma = J_1 \cap \dots \cap J_r\,, \text{ dont } \Gamma = J_1 \cap \dots \cap J_s\,.$$

Comme Δ contient une intersection de composantes immergées, donc de dimension inférieures, on obtient une décomposition primaire de $\underline{(0)}$ dans D :

$$\underline{(0)} = \underline{(Ag)} = \underline{B} \cap \underline{\Gamma} = \underline{J}_1 \cap \dots \cap \underline{J}_r\ ;$$

D étant une localisation de A/Ag , on voit que :

$$\lambda_j = \min\{\lambda\ ; \mathrm{rad}(J_j)^\lambda \subset J_j\} = \min\{\lambda\ ; \mathrm{rad}(\underline{J}_j)^\lambda \subset \underline{J}_j\}$$

rappelons que par le choix générique des $y_1,\dots, y_{n-i}$ on a :

$$\deg(A/\pi_j) = [cf(A/\pi_j) : K]\,.$$

On conclue en regroupant les composantes de B et en appliquant le lemme 2 aux composantes de Γ . ◆

La $3^{ème}$ *étape* contient le résultat essentiel qui permet d'améliorer les bornes de [4] et [5]. Comme nous l'avons expliqué dans le schéma de la démonstration, il s'agit de montrer que les entiers $\{ c_i \}$ qui vérifient la relation de récurrence $c_{i+1} = 4 c_i + \ell_{i+1}$, $c_1 = 0$, satisfont : $X_0^{c_{i+1}+\ell_{i+1}} B_{i+1} \subset (B_i, G_{i+1})$. Autrement dit, avec les notations posées pour i fixé (i.e. $A = R/B_i$ etc...) et le résultat de la $2^{ème}$ étape qui entraine $X_0^{\ell} B \subset \Gamma$, on doit montrer $X_0^{c_{i+1}+\ell} B \subset Ag$ ou de façon équivalente $X_0^{c_{i+1}+\ell} B \subset \Delta$.

Soit c un entier arbitraire.

Lemme 4 : On a les implications suivantes (4) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1) $\Leftrightarrow$ (1') :

(1) $X_0^{c+\ell} B \subset \Delta$, (1') $X_0^{c+\ell} (B/Ag) = 0$,

(2) $X_0^{c} \mathrm{Hom}_R(A/\Delta , A/Ag) = 0$,

(3) $X_0^{c} \mathrm{Ext}^j_R(A/\Delta , A/Ag) = 0$, pour $j = 0$ à $\dim (A/Ag) - \dim (A/\Delta) - 1$,

(4) $X_0^{c} \mathrm{Ext}^j_R(R/I , A/Ag) = 0$, pour $j = 0$ à $\dim (A/Ag) - \dim (R/I) - 1$,

et pour tout les idéaux I de R tels que $(G_1, \dots , G_{i+1}) \subset I$, $X_0 \in \mathrm{rad}(I)$, et $\dim (R/I) < \dim (A/Ag)$.

Preuve. (1) $\Leftrightarrow$ (1') et (3) $\Rightarrow$ (2) sont triviales. (4) $\Rightarrow$ (3) s'obtient en considérant l'image inverse I de Δ par le morphisme $\pi : R \to A = R/B_i$, on se rappelle que $(G_1,\dots,G_i) \subset B_i$ que $\pi(G_{i+1}) = g \in \Delta$, et on remarque que $\dim(A/\Delta) < \dim(A/\Gamma) = \dim(A/Ag) = n-i$, puisque les idéaux premiers associés à Δ contiennent les idéaux premiers associés à Γ.

(2) $\Rightarrow$ (1) s'obtient par un argument de "dualité" : pour tout $b \in B$, on sait que $X_0^{\ell} b$ appartient à $B \cap \Gamma$ donc pour tout $\delta \in \Delta$, $X_0^{\ell} b\delta \in B \cap \Gamma \cap \Delta = (g)$. Ainsi la multiplication par $X_0^{\ell} b$ est un élément bien défini φ_b de $\mathrm{Hom}_R(A/\Delta, A/Ag)$. De plus $X_0^{c} . \varphi_b = 0$ si et seulement si $X_0^{c+\ell} b \in (g)$ soit si et seulement

si $X_0^{c+\ell}\, b \in \Delta$, pour tout $b \in B$. ◆

Notation Pour tout R-module de type fini M, et pour tout i , $1 \leqslant i \leqslant s$, on définit l'entier $c(i,M)$ en posant :

$c(i,M) = \min \{ c ; X_0^{c}.\mathrm{Ext}^j_R(R/I, M) = 0$, pour tout les idéaux I de R tels que

$(G_1,\ldots, G_i) \subset I$, $X_0 \in \mathrm{rad}(I)$, $\dim(R/I) < \dim(M)$,

et pour tout les j tels que $0 \leqslant j \leqslant \dim(M) - \dim(R/I)$ $\}$

Remarque : Pour tout M, $c(i+1,M) \leqslant c(i,M)$.

Lemme 5: Soient $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de R-modules de type fini avec $\dim(M'') < \dim(M')$ et i , $1 \leqslant i \leqslant s$.

Alors $c(i,M) < \infty$ et $c(i,M') < \infty$ impliquent $c(i,M'') \leqslant c(i,M) + c(i,M')$.

Preuve : Remarquons tout d'abord que $\dim(M) = \dim(M')$. Pour tout I tel que dans la définition de $c(i,M'')$, on considère la suite exacte longue des $\mathrm{Ext}_R(R/I,-)$. Pour tout $j < \dim(M'') - \dim(R/I)$, on en extrait la suite exacte suivante de R-modules (on note φ et ψ les morphismes) :

$$\mathrm{Ext}^j_R(R/I,M) \to \mathrm{Ext}^j_R(R/I,M'') \to \mathrm{Ext}^{j+1}_R(R/I,M').$$

Comme $X_0^{c(i,M)}\mathrm{Ext}^j_R(R/I,M) = 0$ et $X_0^{c(i,M')}\mathrm{Ext}^{j+1}_R(R/I,M') = 0$,

pour tout $\alpha \in \mathrm{Ext}^j_R(R/I,M'')$ on a $X_0^{c(i,M')}\alpha \in \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$, donc $X_0^{c(i,M)+c(i,M')}\alpha = 0$. ◆

Corollaire : $c(1,R/G_1) = 0$.

Preuve : On déduit le résultat de la considération de la résolution libre de R/G_1 : $0 \to R \to R \to R/G_1 \to 0$ et du fait que $\mathrm{Ext}^j_R(R/I,R) = 0$ pour tout j .

◆

Corollaire : Pour $1 \leqslant i < s$, si $c(i,R/B_i) < \infty$, on a

$$c(i+1, R/(B_i,G_{i+1})) \leqslant 2\, c(i, R/B_i).$$

Preuve : Du fait que G_{i+1} n'est pas diviseur de zéro dans R/B_i, on déduit que $\dim(R/(B_i,G_{i+1})) < \dim(R/B_i)$ et que l'on a la suite exacte courte associée à la multiplication par G_{i+1} :

$$0 \to R/B_i \to R/B_i \to R/(B_i,G_{i+1}) \to 0 .$$

D'où $c(i+1,R/(B_i,G_{i+1})) \leqslant c(i, R/(B_i,G_{i+1})) \leqslant 2\, c(i, R/B_i)$. ♦

Lemme 6: Pour $1 \leqslant i < s$, si $c(i+1,R/(B_i,G_{i+1})) < \infty$, on a

$$c(i+1, R/B_{i+1}) \leqslant \ell_{i+1} + 2\, c(i+1, R/(B_i,G_{i+1})).$$

Preuve : Avec les notations abrégées, il s'agit de prouver que $c(i+1,A/B) \leqslant \ell + 2\, c(i+1,A/Ag)$. D'après le lemme 4, $X_0^{\ell + c(i+1,A/Ag)}$ est dans l'annulateur du R-module B/Ag , il est donc dans l'annulateur de $\mathrm{Ext}^j_R(R/I,B/Ag)$ pour tout j et tout I. Considérons la suite exacte courte induite par l'inclusion de B dans Ag :

$$0 \to B/Ag \to A/Ag \to A/B \to 0$$

et le fragment suivant de la suite exacte longue associée :

$$\mathrm{Ext}^j_R(R/I,A/Ag) \to \mathrm{Ext}^j_R(R/I,A/B) \to \mathrm{Ext}^{j+1}_R(R/I,B/Ag)$$

pour tous I et j comme dans la définition de $c(i+1,A/B)$. Un raisonnement identique à celui de la preuve du lemme précédent donne $c(i+1,A/B) \leqslant c(i+1,A/Ag) + \ell + c(i+1,A/Ag)$. ♦

On résume la situation dans la proposition suivante.

Proposition 7 : Pour $1 \leqslant i < s$ on a :

(1) $X_0^{\ell_{i+1}+2c_i} B_{i+1} \subset (B_i, G_{i+1})$

(2) $c_1 = 0$ et $c_{i+1} \leqslant 4\, c_i + \ell_{i+1}$.

Preuve : On pose $c_i = c(i,R/B_i)$, les nombres ℓ_i pour $1 \leqslant i \leqslant s$ sont déterminés par la $2^{\text{ème}}$ étape. D'après le premier corollaire , $c_1 = 0$. Le second corollaire

et le Lemme 6 mis bout à bout donne :

$$c(i+1, R/B_{i+1}) \leqslant \ell_{i+1} + 2\, c(i+1, R/(B_i, G_{i+1})) \leqslant \ell_{i+1} + 4\, c(i, R/B_i).$$

Ceci montre inductivement que tous les $c(i,R/B_i)$ et $c(i+1,R/(B_i,G_{i+1}))$ sont finis et justifie l'utilisation de ces résultats. Le (1) est alors démontré par le Lemme 4 .

Dans *la 4ème étape* on résoud les relations de récurrence liant d, n, la borne cherchée m et les ℓ_i, c_i, et b_i. On a posé $b_i = \deg(B_i)$.

Pour cela on introduit les nombres intermédiares $d_1,\ldots,d_s$ définis de la façon suivante, et qui seront les degrés de polynômes que nous allons construire :

$$d_s = 0$$

$$d_i = d_{i+1} + \ell_{i+1} + 2\,c_i .$$

Ils sont liés par les relations :

$$c_{i+1} \leqslant \ell_{i+1} + 4\,c_i \quad \text{avec } c_1 = 0,$$

$$b_{i+1} + \ell_{i+1} \leqslant b_i d \quad \text{avec } b_1 = d .$$

Pour $s = 2$, on a $d_1 = \ell_2 \leqslant d^2$.

Pour $s > 2$, on a $d_1 = \ell_s + \sum_{2\leqslant i\leqslant s-1} \ell_i + 2 \sum_{2\leqslant i\leqslant s-1} c_i$;

la première inégalité de liaison donne pour $2 \leqslant i \leqslant s-1$:

$$4^{-i} c_i \leqslant \sum_{2\leqslant j\leqslant i} 4^{-j} \ell_j \text{ , d'où}$$

$$\sum_{2\leqslant i\leqslant s-1} c_i \leqslant \sum_{2\leqslant i\leqslant s-1} \sum_{2\leqslant j\leqslant i} 4^{i-j} \ell_j = \sum_{2\leqslant j\leqslant s-1} (4^{s-j} - 1)\ell_j /3 \ ;$$

en regroupant on trouve :

$$d_1 \leqslant \ell_s + 1/3 \sum_{2\leqslant i\leqslant s-1} \ell_i + 8/3 \cdot 4^{s-1} \sum_{2\leqslant i\leqslant s-1} \ell_i/4^i .$$

En sommant de i=1 à s−2 les instances de la deuxième inégalité de liaison :

$$\sum_{2\leqslant i\leqslant s-1} \ell_i \leqslant (d-1) \sum_{2\leqslant i\leqslant s-2} b_i - b_{s-1} + d^2$$

en portant pour $i \leqslant s-2$, $b_i \leqslant d^i$ et en effectuant la somme on obtient :

$$\sum_{2\leqslant i\leqslant s-1} \ell_i \leqslant d^{s-1} - b_{s-1} \ ;$$

de même en remplaçant ℓ_i par $4^{-i}\ell_i$, b_i par $4^{-i}b_i$ et d par d/4 ,

$$\Sigma_{2\leqslant i\leqslant s-1}\, 4^{-i}\ell_i \leqslant 4^{-s+1}(d^{s-1} - b_{s-1})\ ;$$

en gardant $\ell_s \leqslant b_{s-1}d$, on obtient alors :

$$d_1 \leqslant b_{s-1}d + 3(d^{s-1} - b_{s-1}) = d^s - (d-3)(d^{s-1} - b_{s-1}).$$

Résumons :

si d=1 le problème est trivial, $d_1 = 1$;

si d = 2 on trouve $d_1 \leqslant 2^s + 2^{s-1} - b_{s-1} \leqslant 3.2^{s-1}$;

si $d \geqslant 3$ on trouve $d_1 \leqslant d^s$.

Construisons, par récurrence sur i, des polynômes homogènes R_i qui satisfont pour $1\leqslant i\leqslant s$ les conditions suivantes :

$R_i \in B_i$, $\deg(R_i) = d_i$,

$R_i = X_0^{d_i} + \Sigma_{i<j\leqslant s} A_j^{(i)} G_j$ pour certains polynômes $A_j^{(i)}$.

Comme $B_s = (1)$, posons $R_s = 1$. Supposons construit R_{i+1} pour $s>i\geqslant 1$.

Appliquons la proposition de la 3ème étape,

$$X_0^{\ell_{i+1} + 2c_i}\, R_{i+1} \in (B_i, G_{i+1})$$

donc il existe des polynômes homogènes R_i dans B_i et A_i tels que :

$$X_0^{\ell_{i+1} + 2c_i}\, R_{i+1} = R_i + A_i\, G_{i+1}$$

on pose $A_{i+1}^{(i)} = -A_i$; et on remarque que :

$$\deg(R_i) = d_i = d_{i+1} + \ell_{i+1} + 2\, c_i\ .$$

Comme $B_1 = (G_1)$, il existe un polynôme homogène A_0 tel que :

$$R_1 = X_0^{d_1} + \Sigma_{1<j\leqslant s} A_j^{(1)} G_j = A_0 G_1\ ,$$

Donc

$$X_0^{d_1} \in (G_1, \ldots, G_s).$$

La $5^{ème\ étape}$ consiste à améliorer, lorsque s=n+1, la majoration de d_1 trouvée dans la $4^{ème}$ étape . on avait établi que :

$$d_1 \leqslant \ell_{n+1} + 2\,c_n + \ell_n + 3(d^{n-1} - b_{n-1}).$$

Dans ce cas $\{B_{n-1} = 0\}$ est formé de courbes de k^n, son prolongement à l'infini n'a donc que des points, qui ne peuvent intersecter $\{G_n = 0\}$ qu'en des points. Reprenons les notations : $(B_{n-1}, G_n) = B_n \cap \Gamma_n \cap \Delta_n$, $\{ B_n = 0 \}$ est aussi formé de points, $\{ \Delta_n = 0 \}$ est vide . On a aussi $(B_n, G_{n+1}) = \Gamma_{n+1}$.

En reprenant complétement l'étude géométrique et en la précisant, on conçoit bien que l'on peut remplacer le terme $(\ell_{n+1} + 2\,c_n + \ell_n)$ par une borne fine.

Nous nous contenterons ici de démontrer que ℓ_{n+1} est majoré par $b_n + d$ et d'utiliser les inégalités précédentes, ce qui donnera :

$$c_{n-1} \leqslant 4^{n-1} \sum_{2 \leqslant j \leqslant n-1} \ell_j / 4^j \leqslant d^{n-1} - b_{n-1} ,$$

$$2\,c_n \leqslant 2\,(\ell_n + 4\,c_{n-1}) \leqslant 2\,\ell_n + 8\,(d^{n-1} - b_{n-1}) ,$$

$$d_1 \leqslant b_n + d + 3\,\ell_n + 11\,(d^{n-1} - b_{n-1}) \leqslant 3\,b_{n-1} d - 2\,b_n + 11\,(d^{n-1} - b_{n-1}) + d$$

soit $d_1 \leqslant 3\,d^n - 2\,b_n - (3d - 11)(d^{n-1} - b_{n-1}) + d$.

Si d = 3 on avait déja $d_1 \leqslant d^{n+1} = 3\,d^n$,

si $d \geqslant 4$ on a $(3d - 11) \geqslant 1$, donc dans tous les cas on aura :

$$d_1 \leqslant 3\,d^n .$$

Reste donc à montrer que $\ell_{n+1} \leqslant b_n + d$.

Pour cela, on considère l'idéal $I = (F_1, \ldots, F_n)$ de $k[X_1, \ldots, X_n]$, il correspond à une intersection complète affine formée par des points dont la somme des

degrés est égale à b_n. On a donc $\dim_k[X_1,\ldots,X_n]/(F_1,\ldots,F_n) = b_n$.

Soit $H_1,\ldots,H_t$ une base standard réduite de I relativement au degré total raffiné, par exemple, par l'ordre lexicographique inverse ———— . Notons $\underline{H}_i$ les homogénéisés des H_i, $1\leqslant i\leqslant t$ et $\underline{I}$ l'idéal de $R = k[X_0,\ldots,X_n]$ qu'ils engendrent. Alors, $(\underline{H}_1,\ldots,\underline{H}_t)$ est une base standard réduite de $\underline{I}$ relativement à l'ordre lexicographique inverse :

en effet s'il y avait un élément $\underline{H}$ de $\underline{I}$ dont le terme dominant ne serait pas multiple du terme dominant de l'un des $\underline{H}_i$ (qui d'après nos choix, ne contient pas de X_0) il en serait de même en faisant $X_0 = 1$.

On en déduit que $(\underline{I} : X_0) = \underline{I}$, autrement dit $\underline{I}$ n'a pas de composante à l'infini, donc $\underline{I}$ est égal à notre ancien B_n.

De plus, puisque l'idéal des termes dominant $lt(B_n)$ est engendré par des monômes qui ne dépendent pas de X_0, on peut borner par b_n (qui est le nombre de points "sous l'escalier") la régularité de la fonction de Hilbert de $M = R/B_n$ ceci signifie que, en notant $M = \oplus_{0\leqslant i\leqslant\infty} M_i$ la graduation de M, on a $\dim_k(M_i) = \dim_k(M_j)$ pour tout i et $j \geqslant b_n$. (Voir [2] ou [22].)

Considérons enfin G_{n+1} qui induit dans M un élément g non diviseur de zéro et de degré d. Notons φ la multiplication par g dans M, c'est un morphisme injectif et gradué de degré d; φ définit donc une application k-linéaire bijective en degrés $a \geqslant b_n$

$$\varphi : M_a \to M_{a+d}$$

Le R-module gradué $N = R/(B_n, G_{n+1})$ est le conoyau de φ , on déduit de ce qui précède que N est nul en degré $a \geqslant b_n + d$, c'est à dire

$(X_0,\ldots,X_n)^a = (B_n, G_{n+1})$. Donc , $\ell_{n+1} \leqslant b_n + d$. cqfd.

Le lecteur pourra remarquer que dans la démonstration du théorème 1 on a seulement utilisé le fait que $G_1,\dots,G_s$ forment une suite régulière à distance finie, c'est à dire hors de l'hypersurface $\{ X_0 = 0 \}$. En particulier, le fait que X_0 est de degré 1 n'intervient pas. Dans notre démonstration on peut donc remplacer X_0 par un polynôme homogène G et obtenir la version projective suivante du (Hentzelt) Nullstellensatz effectif :

Théorème 10 : Soit k un corps quelconque et soient $G,G_1,\dots,G_s$ des polynômes homogènes de $k[X_0,\dots,X_n]$ tels que $d = \max_{1\leqslant i\leqslant s}\deg(G_i)$. Posons $\psi(d,n) = 3\,d^n$. Si $G \in \mathrm{rad}(G_1,\dots,G_s)$ alors

$$G^{\psi(d,n)} \in (G_1,\dots,G_n) .$$

La seule précaution à prendre est, dans la première étape, de bien multiplier les G_i par de monomes en $X_0,\dots,X_n$ pour égaliser les degrés à d , afin de pouvoir considérer des combinaisons linéaires génériques qui remplaceront les G_i. ♦

3. Remarques sur l'inconsistance stable

Dans ce paragraphe on supposera k algébriquement clos.

Définitions : Par analogie avec le vocabulaire utilisé en logique, on dira qu'une famille de polynômes $F_1,\dots,F_s$ de $k[X_1,\dots,X_n]$ est inconsistante si $1 \in (F_1,\dots,F_s)$. On dira qu'elle est stablement inconsistante s'il existe un ouvert de Zariski U de k^s , tel que $0 \in U$ et pour tout $\lambda = (\lambda_1,\dots,\lambda_s) \in U$ on ait $1 \in (F_1-\lambda_1,\dots,F_s-\lambda_s)$.

On appelle syzygie finale (voir [28]) de $F_1,\dots,F_s$ un polynôme P de $k[Y_1,\dots,Y_s]$, où les Y_i sont de variables auxiliaires, tel que :

$$P(0,\dots,0) = 1 \quad \text{et} \quad P(F_1(X_1,\dots,X_n),\dots,F_s(X_1,\dots,X_n)) = 0.$$

Lemme 11: ([28],6.4) Il existe une syzygie finale pour la famille de polynômes $F_1,\dots,F_s$ ssi elle est stablement inconsistente.

Nous allons à présent retourner à la situation du théorème 1 , c'est à dire $1 \in (F_1,\dots,F_s)$ avec les hypothèses supplémentaires suivantes :

$$\deg(F_1) = \dots = \deg(F_s) = d;$$

$$\operatorname{trdeg}_k\, k[\overline{F}_1,\dots,\overline{F}_s] = n+1, \text{ où } \overline{F}_i \text{ est l'homogénéisé de } F_i \text{ pour } 1 \leqslant i \leqslant s.$$

Soient $G_1,\dots,G_{n+1}$ des combinaisons linéaires de $\overline{F}_1,\dots,\overline{F}_s$ qui forment une suite régulière à distance finie et telles que $k[G_1,\dots,G_{n+1}] \subset k[F_1,\dots,F_s]$ soit une extension entière. On a $X_0 \in \operatorname{rad}(G_1,\dots,G_{n+1})$ et d'après l'inégalité de Bézout ([4], Proposition 5) on a $[\, k(X_0,\dots,X_n) : k(G_1,\dots,G_{n+1}) \,] \leqslant d^{n+1}$.

Proposition 12 : Avec les notations et hypothèses précédentes:
X_0 est entier sur $k[G_1,\dots,G_{n+1}]$ ssi la famille $F_1,\dots,F_s$ est stablement

inconsistante.

Preuve : Supposons que X_0 est entier sur $k[G_1,\dots,G_{n+1}]$.

Comme $k[G_1,\dots,G_{n+1}]$ est intégralement clos, le polynôme minimal de X_0 sur $k(G_1,\dots,G_{n+1})$ est une relation de dépendance intégrale de degré égal à :

$$[\,k(G_1,\dots,G_{n+1},X_0) : k(G_1,\dots,G_{n+1})\,] \leqslant [\,k(X_0,\dots,X_n) : k(G_1,\dots,G_{n+1})\,] \leqslant d^{n+1}.$$

Ceci signifie qu'il existe un entier r, $1 \leqslant r \leqslant d^{n+1}$ et r polynômes homogènes $A_0,\dots,A_{r-1}$ dans $k[G_1,\dots,G_{n+1}]$ tels que :

$$X_0^{\,r} + A_{r-1}X_0^{\,r-1} + \dots + A_0 = 0.$$

et $\deg(A_i) = r-i$ ou $A_i = 0$ pour $0 \leqslant i \leqslant r-1$.

Remarquons que A_i est à priori polynôme de $k[G_1,\dots,G_{n+1}]$, homogène en $X_0,\dots,X_n$; mais comme les $G_1,\dots,G_{n+1}$ sont homogènes de degré d et algébriquement indépendants sur k, on déduit que A_i est aussi homogène de degré $\leqslant d^{n+1}$ dans $k[G_1,\dots,G_{n+1}]$. En particulier $A_i \in (\overline{F}_1,\dots,\overline{F}_s)$.

Spécialisons X_0 en $1 \in k$. Les $\overline{F}_j$ se spécialisent en F_j, les A_i en certains A'_i de $k[X_1,\dots,X_n]$ qui on une représentation (non nécessairement unique) comme polynômes en $F_1,\dots F_s$ "sans terme constant" et de degré $\leqslant d^{n+1}$:

$$1 + A'_{r-1} + \dots + A'_0 = 0.$$

Autrement dit, on obtient une syzygie finale de degré $\leqslant d^{n+1}$ de la famille $F_1,\dots,F_s$.

Réciproquement s'il existe une syzygie finale P pour la famille $F_1,\dots,F_s$ en homogénéisant la relation correspondante, on voit facilement que X_0 est entier sur $k[\overline{F}_1,\dots,\overline{F}_s]$. Comme $k[G_1,\dots,G_{n+1}] \subset k[\overline{F}_1,\dots,\overline{F}_s]$ est une extension entière, on en déduit que X_0 est entier sur $k[G_1,\dots,G_{n+1}]$. ♦

Remarque : La proposition précédente pose donc la question de déterminer si X_0 est entier sur $k[G_1,\ldots,G_{n+1}]$. Nous n'avons qu'une réponse partielle qui découle de ([4], Remark 9) :

$k[G_1,\ldots,G_{n+1}] \subset k[X_0,\ldots,X_n]$ est une extension entière ssi $\{ \overline{F}_1=0,\ldots,\overline{F}_s=0 \} = \varnothing$.

Donc si $F_1,\ldots,F_s$ n'ont pas de zéros communs même à l'infini, on peut conclure que cette famille est stablement inconsistante. (Voir aussi [21].)

Remarque Dans le cas général, il est clair que l'on doit multiplier $F_1,\ldots,F_s$ par des monômes en $X_1,\ldots,X_n$ pour obtenir une syzygie finale. Si on savait borner le degré de ces monômes, on obtiendrait une démonstration vraiment élémentaire d'un Nullstellensatz effectif basée uniquement sur l'inégalité de Bézout.

4. La conjecture de Serre : point de vue quantitatif et effectif

Nous allons appliquer notre Nullstellensatz effectif, Théorème 1, dans le contexte de l'ex-Conjecture de Serre.
Cette conjecture a été résolue en plusieures étapes. Nous nous occupons seulement de la dernière où on démontre que les anneaux polynomiaux sur un corps sont hermitiens. Les premières démonstrations de ce fait ont été données par Suslin et Quillen indépendemment. Notre point de départ sera la démonstration de Suslin (voir [20]).

Dans ce paragraphe nous supposons que k est infini. (Ce sera l'unique hypothèse sur k. En particulier la caractéristique de k peut être arbitraire.)

Notons $R = k[X_1,\dots,X_n]$.

Soit $F = (F_{ij})_{1\le i\le r,1\le j\le s} \in R^{r\times s}$ une $r\times s$-matrice polynomiale avec $F_{ij} \in R$ pour $1 \le i \le r$, $1 \le j \le s$. Notons

$\deg F = \max_{1\le i\le r,1\le j\le s} \deg F_{ij}$ le degré de F.

Si les $r\times r$-mineurs de F engendrent l'idéal trivial R nous di ons que F est unimodulaire. Considérons les deux cas particuliers $r=1$ et $r=s$.
Si $r=1$ et $F = (F_1,\dots,F_s)$, la condition F unimodulaire signifie $RF_1 + \dots + RF_s = R$.
Si $r=s$ la condition F unimodulaire signifie $\det F \in k \setminus \{0\}$ ($\det F$ est le déterminant de F).

F unimodulaire signifie que l'application k-linéaire induite par F

$$R^s \xrightarrow{F} R^r$$

est surjective.

Le Nullstellensatz effectif entraîne

Théorème 13 ([9], [4]): Soit k un corps infini, $R = k[X_1, \ldots, X_n]$ et $F \in R^{r \times s}$ une matrice unimodulaire avec $d := \deg F$.
Alors il existe une matrice unimodulaire $M \in R^{s \times s}$ avec les propriétés suivantes :

(i) $F \cdot M = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ (s colonnes, r lignes)

(ii) $\deg M = (rd)^{O(n)}$

(iii) M a une représentation $M = N_1 \cdot \ldots \cdot N_p$ comme produit de $p \leq ns\,(rd)^{2n}$ matrices $N_k \in R^{s \times s}$ telles que pour $1 \leq k \leq p$: $\deg N_k = (rd)^{O(n)}$

N_k est élémentaire ou de la forme

$$N_k = \begin{pmatrix} N'_k & \\ - & - \\ & \end{pmatrix} \quad (r+1 \text{ lignes}, s \text{ colonnes}) \qquad \text{avec } N'_k \in SL_{r+1}(R) .$$

(iv) On peut calculer M par un réseau arithmétique [8] en temps séquentiel $r^{O(n^2)}\, s^{O(r^2)}\, d^{O(n^2 + r^2)}$ et en temps parallèle $O(n^6\, r^4 \log^4 rd \log^2 sd)$.

Le fait que R est hermitien signifie, dans les hypothèses du Théorème 13, qu'il existe une matrice unimodulaire $M \in R^{s \times s}$ qui satisfait (i).

Les bornes du Théorème 13 (ii) et (iii) représentent le (nouvel) aspect quantitatif et les complexités dans (iv) l'aspect algorithmique du résultat qui est par ailleurs classique. Ce résultat dont les démonstrations classiques ne sont pas constructives implique la résolution de la Conjecture de Serre (voir [20]).

On peut se limiter au cas $r \leq \min\{n, s\}$. De ce point de vue Théorème 13 (iv) représente une solution algorithmique de la Conjecture de Serre simplement exponentielle en temps séquentiel et (simultanément) polynomial en temps parallèle.

Les propriétés Théorème 13 (i) et (ii) impliquent un Nullstellensatz effectif (poser $r=1$ et considérer la première ligne de M).

On déduit de l'exemple cité de Masser et Philippon ([3]) que toute borne pour $\deg M$ est intrinsequement exponentielle en n.

Corollaire 14 : Soient R et F comme dans le Théorème 13. Considérons la suite exacte courte de R-modules induite par F :

$$0 \longrightarrow P \longrightarrow R^s \xrightarrow{F} R^r \longrightarrow 0 \ ,$$

où P est un sous-module de R^s.
Alors P est un R-module libre de rang $s-r$ et on peut trouver en temps séquentiel $r^{O(s^2)}\, s^{O(r^2)}\, d^{O(n^2+r^2)}$ et en temps parallèle $O(n^6\, r^4 \log^4 rd \log^2 sd)$ une base de P décrite par une matrice $N \in R^{(s-r)\times s}$ de degré $\deg N = (rd)^{O(n)}$.

Démonstration : Soit R,F et M comme dans le Théorème 13. Considérons le diagramme commutatif

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P & \longrightarrow & R^s & \xrightarrow{\quad F \quad} & R^r & \longrightarrow & 0 \\ & & \wr\uparrow & & \wr\uparrow M & & \| & & \\ 0 & \longrightarrow & R^{s-r} & \longrightarrow & R^s & \xrightarrow{\quad r \quad} & R^r & & \end{array}$$

où M est la matrice $\begin{pmatrix} 1 & 0 & \\ & \ddots & \\ 0 & 1 & 0 \end{pmatrix}$ (1 sur la diagonale, 0 ailleurs, s colonnes, r lignes).

On en déduit que les $s-r$ dernières colonnes de M forment une base de P.

Pour la démonstration du Théorème 13 nous référons le lecteur à [9].

Nous allons ici considérer le cas $r=1$. Voici une version quantitative et effective du Théorème de Suslin ([20]) :

Théorème 15 ([4],[9]): Soit k infini et $R = k[X_1,\ldots,X_n]$. Soit $F = (F_1,\ldots,F_s) \in R^s$ un vecteur unimodulaire.
Alors il existe une matrice unimodulaire $M \in R^{s\times s}$ avec les propriétés suivantes

(i) $F \cdot M = (1, 0, \ldots, 0)$

(ii) $\deg M \leq s\, d^{O(n)}$

(iii) M a une représentation $M = N_1 \cdot \ldots \cdot N_p$ comme produit de $p \leq 2\, n\, s^2 d$ matrices $N_k \in R^{s\times s}$ telles que pour tout $1 \leq k \leq p$:

$$\deg N_k = s\, d^{O(n)}$$

N_k est élémentaire ou de la forme

$$N_k = \begin{matrix} \\ \\ 2 \end{matrix}\left\{\left[\begin{array}{c|ccc} \widetilde{N'_k} & & 0 & \\ \hline & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{array}\right]\right. \quad \text{avec} \quad N'_k \in SL_2(R)\,.$$

(iv) On peut calculer M en temps séquentiel $s^4\, d^{O(n^2)}$ et en temps parallèle $O(n^6 \log^3 sd)$.

Pour la démonstration du Théorème 15 nous avons besoin de quelques préparations.
Soit $A := k[X_1,\ldots,X_{n-1}]$ et $X := X_n$. Nous considérons les $G \in R = A[X]$ comme polynômes en X à coéfficients dans A. Dans ce sens on peut substituer des éléments $B \in R$ dans G. Nous écrivons $G(B)$ le résultat de la substitution. Evidemment $G(B) \in R$ en général, et $G(B) \in A$ si $B \in A$.
Pour un vecteur $F = (F_1,\ldots,F_s) \in R^s$ et $B \in R$ nous écrivons $F(B) = (F_1(B),\ldots,F_s(B)) \in R^s$.

Pour ce qui suit, soitent $s \geq 2$, $F = (F_1,\ldots,F_s) \in R^s$ un vecteur unimodulaire et $d := \deg F$.

<u>Lemme 16</u> : Soit $c := \mathrm{Res}_X(F_1, F_2)$ le résultant de F_1 et F_2 comme polynômes en X. Etant donnés $B, B' \in R$ avec $D = \max\{\deg B, \deg B'\}$ et $B - B' \in Rc$.
Alors il existe une matrice unimodulaire $N \in R^{s\times s}$ avec

(i) $F(B)\, N = F(B')$

(ii) $\deg N \leq D\,(d + d^2)$

(iii) N a une représentation $N = E_1 \cdot \ldots \cdot E_{2(s-2)}\, S$, où $E_1,\ldots,E_{2(s-2)} \in R^{s\times s}$ sont des matrices élémentaires et $S \in R^{s\times s}$ est de la forme

$$S = \left[\begin{array}{c|ccc} S' & & 0 & \\ \hline & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{array}\right] \quad \text{où} \quad S' \in SL_2(R)\,.$$

Démonstration : Partant de la matrice de Sylvester correspondante à F_1 et F_2 on peut calculer deux polynômes $G_1, G_2 \in R$ tels que

(15) $\quad c = G_1 F_1 + G_2 F_2 \quad$ et $\quad \deg G_1 , \deg G_2 \leq d^2$.

On a — aussi $\deg c \leq d^2$. Comme $c \in A$ ne contient pas l'indéterminée X, on obtient de (15)

(16) $\quad c = G_1(B)\, F_1(B) + G_2(B)\, F_2(B)$.

Soit $3 \leq j \leq s$. On a $F_j(B) - F_j(B') \in R(B-B') \subset Rc$, donc pour $A_j := (1/c)(F_j(B) - F_j(B'))$ on a $A_j \in R$, $\deg A_j \leq D\,d$ et $F_j(B) - F_j(B') = A_j c = A_j G_1(B)\, F_1(B) + A_j G_2(B)\, F_2(B)$.

A $A_j G_1(B)$ et $A_j G_2(B)$ correspondent deux $s \times s$-matrices élémentaires à coéfficients dans R qui transforment $(F_1(B), F_2(B), \ldots, F_j(B), \ldots, F_s(B))$ en $(F_1(B), F_2(B), \ldots, F_j(B'), \ldots, F_s(B))$.

Avec $2(s-2)$ ——— matrices élémentaires $E_1, \ldots, E_{2(s-2)} \in R^{s\times s}$ on obtient $F(B)\, E_1 \cdot \ldots \cdot E_{2(s-2)} = (F_1(B), F_2(B), F_3(B'), \ldots, F_s(B'))$.

Considérons maintenant la matrice

$$S := \left[\begin{array}{c|ccc} S' & & & \\ \hline & 1 & & \\ & & \ddots & \\ & & & 1 \end{array}\right] \quad \text{avec} \quad S' := \frac{1}{c} \begin{bmatrix} G_1(B) & -F_2(B) \\ G_2(B) & F_1(B) \end{bmatrix} \begin{bmatrix} F_1(B') & F_2(B') \\ -G_2(B') & G_1(B') \end{bmatrix} .$$

On a $\det S' = 1$. A première vue S' est une matrice à coéfficients dans $cf(R) = k(X_1, \ldots, X_n)$.
D'autre part $B - B' \in Rc$ implique que tous les coéfficients du produit

$$\begin{bmatrix} G_1(B) & -F_2(B) \\ G_2(B) & F_1(B) \end{bmatrix} \begin{bmatrix} F_1(B') & F_2(B') \\ -G_2(B') & G_1(B') \end{bmatrix}$$

sont divisibles par c .
Donc $S' \in R^{2\times 2}$. Cela implique $S' \in SL_2(R)$.

On vérifie que ——— $(F_1(B), F_2(B))\, S' = (F_1(B'), F_2(B'))$ et $(F_1(B), F_2(B), F_3(B'), \ldots, F_s(B'))\, S = F(B')$.

Pour $N := E_1 \cdot \ldots \cdot E_{2(s-2)}\, S$ on a finalement $F(B)\, N = F(B')$, d'où (i) et (iii).

On a ——— $\deg S' \leq D(d + d^2)$ et, pour $3 \leq j \leq s$ et $1 \leq k \leq 2$, $\deg A_j G_k(B) \leq$ $\leq \deg A_j + \deg G_k(B) \leq D(d + d^2)$. Cela implique (ii). □

←——— La matrice $N \in R^{s \times s}$ de la démonstration du Lemme 16 est calculable en temps séquentiel $(Dd)^{O(n)}$ et en temps parallèle $O(n^2 \log^2 Dd)$.

Lemme 17 : Supposons $\deg_X F = \deg F_1$.
Soit $\ell := (s-2)d + 1$ et soient donnés $a_1, \ldots, a_\ell \in k$ tous distincts.
Pour $1 \leq i \leq \ell$ notons $F_{2,i} = F_2 + a_i F_3 + a_i^2 F_4 + \ldots + a_i^{s-2} F_s$ et

$$c_i = \mathrm{Res}_X(F_1, F_{2,i}) .$$

←——— Alors, on a $Ac_1 + \ldots + Ac_\ell = A$.

Démonstration : Il suffit — démontrer que $c_1, \ldots, c_\ell$ n'ont pas de zéro commun dans $\bar{k}^{n-1}$.
Supposons le contraire et soit $z \in \bar{k}^{n-1}$ tel que $c_1(z) = \ldots = c(z) = 0$.
Comme $\deg_X F_1 = \deg F_1$, cette condition implique qu'il existe des $\xi_1, \ldots, \xi_\ell \in \bar{k}$ tels que pour $1 \leq i \leq \ell$, $F_1(z, \xi_i) = F_{2,i}(z, \xi_i) = 0$.
L'égalité $\deg_X F_1 = \deg F_1 \leq d$ implique que le polynôme $F_1(z,X) \in \bar{k}[X]$ a au plus d zéros. Donc $\# \{\xi_1, \ldots, \xi_\ell\} \leq d$ (# désigne le cardinal).
Soit $L = \{1, \ldots, \ell\}$. ——— Considérons la partition P de L qui correspond à la relation d'équivalence sur L qui identifie $k_1, k_2 \in L$ si

$$\{i \in L ; F_{2,}(z, \xi_{k_1}) = 0\} = \{i \in L ; F_{2,}(z, \xi_{k_2}) = 0\} .$$

On voit que P a au plus d classes. Comme $\ell = (s-2)d + 1$ il existe d'après le principe des tiroirs une classe dans P qui contient au moins s-1 éléments de L. Cela signifie qu'il existe un $\xi \in \{\xi_1, \ldots, \xi_\ell\}$ qui annule s-1 des polynômes $F_{2,i}(z,X) \in k[X]$.
Sans restriction de généralité on peut supposer $F_{2,i}(z,\xi) = \ldots = F_{2,s-1}(z,\xi) = 0$. De plus, on a $F_1(z,\xi) = 0$.
Considérons $x := (z,\xi) \in \bar{k}^n$. x est contenu dans $\{F_1 = 0, F_{2,1} = 0, \ldots, F_{2,s-1} = 0\}$ qui est donc un ensemble non-vide.

Or, on obtient le vecteur $(F_{2,1}, \ldots, F_{2,s-1}) \in R^{s-1}$ en multipliant le vecteur $(F_1, \ldots, F_s) \in R^{s-1}$ par la matrice de Vandermonde inversible :

$$\begin{bmatrix} 1 & \cdot & \cdot & \cdot & 1 \\ a_1 & \cdot & \cdot & \cdot & a_{s-1} \\ \vdots & & & & \vdots \\ a_1^{s-2} & \cdot & \cdot & \cdot & a_{s-1}^{s-2} \end{bmatrix} .$$

Cela implique $\emptyset \neq \{F_1 = 0 , F_{2,1} = 0 , \ldots , F_{2,s-1} = 0\} = \{F_1 = 0 , F_2 = 0 , \ldots , F_s = 0\}$. On obtient donc une contradiction avec l'hypothèse que $F = (F_1, \ldots, F_s)$ est unimodulaire.

Remarque 18 : Puisque $\deg c_1, \ldots, \deg c_\ell \leq d^2$ notre Nullstellensatz et le Lemme 17 impliquent qu'il existe des $q_1, \ldots, q_\ell \in A$ avec $\deg q_i \leq 3\, d^{2(n-1)}$ ——————— pour $1 \leq i \leq \ell$, tels que $1 = \sum_{1 \leq i \leq \ell} q_i c_i$.

←——— On peut calculer $q_1, \ldots, q_\ell$ en temps séquentiel $\ell^4\, d^{O(n^2)}$ et en temps parallèle $O(n^4 \log^2 \ell d)$.

Fin de la démonstration du Théorème 15

Comme k est infini nous pouvons supposer qu'après un eventuel changement linéaire des variables $X_1, \ldots, X_n$ la condition $\deg_{X_j} F_1 = \deg F_1$ est satisfaite pour tout $1 \leq j \leq n$.

Dans une première étape nous construisons une matrice unimodulaire $M_n \in R^{s \times s}$ telle que $F \cdot M_n = F(0)$, $\deg M_n = s\, d^{O(n)}$ et M_n a une représentation $M_n = N_1 \cdot \ldots \cdot N_p$ comme produit de $p = 2\, d\, s^2$ matrices $N_k \in R^{s \times s}$, $1 \leq k \leq p$, N_k étant une matrice élémentaire ou de la forme

$$N_k = \left[\begin{array}{c|ccc} N_k' & & 0 & \\ \hline & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{array}\right] \quad \text{avec} \quad N_k' \in SL_2(R) .$$

En plus on a $\deg N_k = s\, d^{O(n)}$.

On peut calculer M_n en temps séquentiel $s^4\, d^{O(n^2)}$ et en temps parallèle $O(n^6 \log^2 (sd))$.

←——— On a $\deg_{X_j} F_1(0) = \deg F_1(0) = \deg F_1$ pour $1 \leq j \leq n-1$

←——— et $\deg F(0) \leq d$.

F unimodulaire implique $F(0)$ unimodulaire. Comme au paravant on trouve maintenant une $s\times s$-matrice unimodulaire M_{n-1} qui transforme $F(0)$ en $F(0,0) := (F_1(X_1,\ldots,X_{n-2},0,0),\ldots,F_s(X_1,\ldots,X_{n-2},0,0))$.
Donc $F\ M_n\ M_{n-1} = F(0,0)$.

Continuant ainsi on arrive finalement à une matrice unimodulaire $M' \in R^{s\times s}$ qui transforme F en $F(0,\ldots,0) := (F_1(0,\ldots,0),\ldots, F_s(0,\ldots,0)) \in k^s$.

Comme $F(0,\ldots,0)$ est unimodulaire, c'est-à-dire $F(0,\ldots,0)\neq(0,\ldots,0)$ on peut mettre $F(0,\ldots,0)$ sous forme $(1,0,\ldots,0)$ par une transformation unimodulaire. En composant cette dernière transformation avec M' on obtient une matrice unimodulaire $M\in R^{s\times s}$ qui satisfait les exigences du Théorèmes 15.

Construisons maintenant M_n .
Choisissons des éléments distincts $a_1,\ldots,a_\ell \in k$ (k est infini).
Soient $c_1,\ldots,c_\ell \in A$ comme dans Lemma 17.
Choisissons maintenant $q_1,\ldots,q_\ell \in A$ d'après la Remarque 18.
Soient $P_1 := X\ q_1\ ,\ldots,\ P_\ell := X\ q_\ell$. On a $X = \sum_{1\leq i\leq \ell} P_i\ c_i$.

Pour chaque $1 \leq i \leq \ell$ appliquons le Lemme 16 avec $c := c_i$, $B := \sum_{1\leq k\leq i} P_k c_k$, $B' := \sum_{1\leq k'\leq i-1} P_{k'} c_{k'}$ pour transformer

$(F_1(B), F_{2,i}(B), F_3(B),\ldots,F_s(B))$ en $(F_1(B'), F_{2,i}(B'), F_3(B'),\ldots, F_s(B'))$.

Maintenant on transforme par des $s\times s$-matrices unimodulaires $F(B)$ en $(F_1(B), F_{2,i}(B), F_3(B),\ldots, F_s(B))$, puis en $(F_1(B'), F_{2,i}(B'), F_3(B'),\ldots, F_s(B')$ puis en $F(B')$.

Grâce au Lemme 17 on obtient une chaine de $s\times s$-matrices unimodulaires qui transforment

F en $F(\sum_{1\leq k\leq \ell-1} P_k c_k)$, puis en $F(\sum_{1\leq k'\leq \ell-2} P_{k'} c_{k'})$,...
... et finalement $F(P_1 c_1)$ en $F(0)$.

Les propriétés (ii) et (iii) se déduisent maintenant par application itérée des bornes des Lemme 16 et Remarque 18.
Similairement on verifie la propriété (iv) .

Observons que notre preuve du Théorème 15 constitue une démonstration nouvelle, élémentaire et constructive du Théorème de Suslin.

(Le Théorème de Suslin [20] correspond à notre Théorème 15 (i).)

Une autre démonstration constructive du Théorème de Suslin est donnée dans [27].

Remarquons que les propriétés (ii) et (iv) du Théorème 13 ne s'obtiennent pas par simple itération du Théorème 15 (la croissance des degrés et par conséquent la croissance de la complexité seraient trop grandes).

Références

[1] C.A. Berenstein, A. Yger: Effective Bezout Identities in $\mathbb{Q}[z_1,\ldots,z_n]$.
Preprint University of Maryland 1987.

[2] J. Briançon : Sur le degré des relations entre polynômes.
C.R.Acad.Sci. Paris t.297 (1983) 553-556.

[3] W.D. Brownawell : Bounds for the degrees in the Nullstellensatz.
Ann.math. Second Series, Vol.126 No 3 (1987) 287-290.

[4] L. Caniglia, A. Galligo, J. Heintz: Some new effectivity bounds in computational geometry. - Best paper award.
à apparaître dans: Proc. Int. Conf. AAECC-6 Rome 1988.

[5] L. Caniglia, A. Galligo, J. Heintz: Borne simple exponentielle pour les degrées dans le théorème des zéros sur un corps de caractéristic quelconque.
C.R.Acad.Sci. Paris, t.307 Série I (1988) 255-258.

[6] M. Chardin : Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique.
Manuscript Ecole Polytéchnique 1988.

[7] A. Dickenstein, C. Sessa: An effective residual criterion for the membership problem in $\mathbb{C}[z_1,\ldots,z_n]$.
to appear in: Proc. IX Escuela Latinoamericano de Matemática (IX ELAM), Santiago de Chile 1988.

[8] N. Fitchas, A. Galligo, J. Morgenstern: Algorithmes rapides en séquentiel et en parallèle pour l'élimination de quantificateurs en géométrie élémentaire.
à apparaître dans: Séminaire Structures Algébriques Ordonnées, UER de Math., Université Paris VII (1988).

[9] N. Fitchas: Aspectos algoritmicos de la conjetura de Serre.
Manuscript Instituto Argentino de Matemática, Buenos Aires, 1988.

[10] W. Fulton: Intersection Theory.
Erg.Math. 3.Folge 2.Bd, Springer Verlag, Berlin 1984.

[11] A. Galligo, J. Heintz, J. Morgenstern: Parallelism and fast quantifier elimination over algebraically (and real) closed fields.
Invited lecture Int.Conf. FCT'87 Kazan; à apparaître dans Springer LN Comput.Sci.

[12] J. Heintz : Definability and fast quantifier elimination in algebraically closed fields.
Theoret.Comput.Sci. 24 (1983) 239-277; Traduction en russe: Kyberneticeskij Sbornik, Novaja Serija Vyp.22, Mir Moscow (1985) 113-158.

[13] J. Heintz, C.P. Schnorr: Testing polynomials which are easy to compute.
12th Ann.Symp. ACM Comput. 1980, 262-280; et aussi dans: Logic and Algorithmic. An international Symposium held in honour of Ernst Specker, Monographie No 30 de L'Enseignement Mathématique, Genève 1982, 237-254.

[14] J. Heintz, M. Sieveking: Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables.
8th Int.Coll. Automata, Languages and Programming ICALP 81, Springer LN Comput.Sci. 115 (1981) 16-28.

[15] J. Heintz, M.F. Roy, P. Solernó: On the complexity of semialgebraic sets.
soumis à: IFIP Congress'89 (1988).

[16] G. Hermann: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.
Math.Ann. 95 (1926) 736-788.

[17] J.P.Jouanolou: Théorèmes de Bertini et applications.
Birkhäuser PM 42 (1983).

[18] E. Kaltofen: Computing with polynomials given by straight-line programs II: sparse factorization.
Proc. 26th IEEE Symp. Foundations Comp.Sci. 1985, 451-458.

[19] J. Kollár: Sharp effective Nullstellensatz.
Manuscript 1988.

[20] T.Y. Lam: Serre's Conjecture.
Springer LN Math. 635 (1978).

[21] D. Lazard: Algèbre linéaire sur $K[X_1,\ldots,X_n]$ et élimination.
Bull.Soc.Math. France 105 (1977) 165-190.

[22] D. Lazard: Résolution des systèmes d'équations algébriques.
Theoret.Comput.Sci. 15 (1981) 77-110.

[23] F.S. Macaulay: Algebraic Theory of Modular Systems.
Cambridge Tracts in Math. 19, Cambridge Univ. Press 1916.

[24] H. Matsumura: Commutative algebra. (Second edition)
Benjamin/Cummings, Reading Mass. 1980.

[25] Ju.V. Nesterenko: Bounds for the characteristic function of a prime ideal.
Mat.Sbornik 123 No 1 (1984) 11-34 = Math. USSR Sbornik 51 (1985) 9-32.

[26] B. Shiffman: Degree bounds for the Nullstellensatz and Bezout equation in arbitrary characteristic.
Manuscript John Hopkins University 1988.

[27] B. Sturmfels: An algorithmic proof of the Quillen - Suslin Theorem.
Manuscript IMA, April 1988.

[28] B. Sturmfels: Computational Algebraic Geometry of Projective Configurations.
IMA Preprint Series # 389, Janvier 1988.

La théorie élémentaire d'un corps ordonné ne détermine pas la théorie de son plongement dans sa clôture réelle

Françoise Delon

Pour un corps K, K^a désigne sa clôture algébrique. Jerome Keisler a prouvé que si deux corps K et L sont élémentairement équivalents, alors les paires $(K \subseteq K^a)$ et $(L \subseteq L^a)$ sont équivalentes dans le langage $\{0, 1, +, -, ., E\}$ où E est un prédicat unaire représentant l'appartenance au petit corps. Si K^s est la clôture algébrique séparable d'un corps K, on a de la même façon: $K \equiv L \Rightarrow (K \subseteq K^s) \equiv (L \subseteq L^s)$ (c'est une conséquence de [D2]). Que se passe–t–il pour d'autres notions de clôture? Il convient bien sûr d'être prudent; prenons par exemple le cas de la clôture parfaite: il existe des corps $K \equiv L$ avec $K^{p^{-\infty}} \not\equiv L^{p^{-\infty}}$, voir [V]. On doit ne considérer que des notions de clôture pour lesquelles les clôtures de deux corps équivalents sont équivalentes. En particulier la question se pose de façon naturelle pour les corps ordonnés:

$$(K,<) \equiv (L,<) \overset{?}{\Rightarrow} (K \subseteq K^r) \equiv (L \subseteq L^r),$$

où K^r est la clôture réelle. La réponse est négative, et le contre–exemple que nous allons décrire prouve aussi

$$(K,v) \equiv (L,v) \not\Rightarrow (K \subseteq K^v) \equiv (L \subseteq L^v),$$

où v est une valuation et K^v la clôture henselienne de K pour v.

Construction du contre–exemple

Soit k un corps de caractéristique nulle,

$(p_n)_{n\in\omega}$ la suite croissante des nombres premiers,

$K_o = k$, $K_n(X_n) \subsetneq K_{n+1} \subsetneq K_n(X_n)^{v_n}$,

où $\ldots^{v_n}$ désigne la clôture henselienne pour la valuation v_n associée à X_n ; précisément K_{n+1} est une clôture algébrique relative de $K_n(X_n)$ dans $K_n(X_n)^{v_n}$ pour les extensions de degré $\leq p_n$. Autre façon de dire la même chose: K_{n+1} n'admet pas d'extension v_n–immédiate de dimension $\leq p_n$. Sur K_{n+1} sont aussi définies les valuations composées (voir [R] §C) $v_n \times v_{n-1} \times \ldots v_i$ pour $n \leq i \leq 0$. Définissons

$$K = \bigcup_{n\in\omega} K_n ,$$

et sur K la valuation v d'anneau

$$A_v = \bigcup_{n\in\omega} A_{v_n \times \ldots \times v_0} ;$$

donc $vK = \mathbb{Z}^{(-\omega)}$ et a pour sous–groupes convexes $0 = H_0 \lhd H_1 \lhd \ldots \lhd H_n \lhd H_{n+1} \lhd \ldots vK$, où chaque H_n, $n \geq 1$, est le sous–groupe convexe principal engendré par $v(X_{n-1})$ et est isomorphe à $\mathbb{Z}^n$. On prolonge v_n de K_{n+1} à K en posant $v_n = \pi_n \circ v$, où π_n est la projection $vK \to vK/H_n$; on a $K/v_n = K_n$.

Lemme 1. Pour tout n, K n'admet pas d'extension v_n–immédiate propre de degré $\leq p_n$.

Démonstration. Soit x v_n–immédiat sur K (c'est–à–dire que l'extension $(K \subseteq K(x), v)$ est immédiate), et algébrique sur K, donc $x \in K^{v_n} = \bigcup_i K_{n+i}^{v_n}$, et il existe $i \in \mathbb{N}$ tel que $x \in K_{n+i}^{v_n}$. Chaque K_m est relativement algébriquement clos dans K_{m+1} donc dans K, donc x est de même degré sur K_{n+i} que sur K.

– Si x est algébrique sur K_n, comme $v_n \restriction K_n$ est triviale, on a $x \in K_n$.

– Montrons par induction sur i qu'on a pour tout (i,n) :

$$\left.\begin{array}{l} K_{n+i+1} \subseteq L \subseteq K_{n+i+1}^{v_n} \\ [\,L : K_{n+i+1}\,] \leq p_n \end{array}\right\} \Rightarrow L = K_{n+i+1} .$$

1) Pour $i = 0$, c'est vrai par définition de K_{n+1}.

2) Soit L comme ci–dessus avec $i \geq 1$. Alors

$$[\,L : K_{n+i+1}] \geq [\,L/v_{n+i} : K_{n+i+1}/v_{n+i}\,] ;$$

or $L/v_{n+i} \subseteq K_{n+i+1}^{v_n}/v_{n+i} = K_{n+i}^{v_n}$ (parce qu'une valuation composée est henselienne ssi chacun de ses facteurs l'est) et $K_{n+i+1}/v_{n+i} = K_{n+i}$, donc, en appliquant le résultat pour

$(i-1,n)$, $L/v_{n+i} = K_{n+i}$, ce qui montre que l'extension $(K \subsetneq L)$ reste v_{n+i}–immédiate. On achève en appliquant le résultat à $(0,n+i-1)$. ☺

Reformulons ce lemme en termes de "limites".

Définition. Soient des corps valués $(M \subsetneq N , v)$ et $x \in N$. On définit $I(x,M,v) = \{ g \in vM ; \exists m \in M , v(x-m) = g \}$, noté aussi $I(x,M)$, ou même $I(x)$, lorsqu'il n'y a pas ambiguïté; c'est un segment initial de vM ; $x \in N-M$ est dit limite sur M , lorsque $\forall m \in M \ \exists m' \in M$, $v(x-m') > v(x-m)$, ou, ce qui est équivalent, lorsque $I(x,M,v)$ coïncide avec $\{ v(x-m) ; m \in M \}$ et n'a pas d'élément maximal. Pour ces notions et celles de suite pseudo–Cauchy de type algébrique ou transcendant, nous renvoyons à [Ka].

Lemme 2. Il n'y a pas sur K de point v_n–limite, $\notin K$, et algébrique de degré $\leq p_n$.

Démonstration. Soit x contredisant l'énoncé. Une suite pseudo–Cauchy $(x_\alpha)_{\alpha<\alpha_0}$ de K maximale approchant x est de type algébrique, et un polynôme $Q \in K[X]$ de degré minimal pour lequel $v(Q(x_\alpha))$ n'est pas asymptotiquement constant a un degré $\leq$ celui du polynôme minimal de x sur $K \leq p_n$. On peut valuer $K[X]/Q$ de façon à en faire une extension immédiate de K , donc $K[X]/Q = K$ d'après le lemme précédent; alors Q est linéaire, et la suite x_α n'est pas maximale, contradiction. ☺

Notations. Soit (M,v) un corps valué arbitraire, A_v désigne son anneau de valuation.

– Pour $A \subsetneq vM$ et $g \in vM$, $\overline{A}$ est la clôture convexe de A dans vM ; $A + g = \{ a+g ; a \in A \}$; $-A = \{ -a ; a \in A \}$.

– Pour $P \in M[X]$, $J(P) = \{ v(P(x)) ; x \in M \}$, $H(P) = \overline{J(P)} \cap -\overline{J(P)}$; $H(P)$ est non vide dès que P a des coefficients entiers pour v ; $H(P)$ peut avoir ou non un élément maximal.

Lemme 3. Pour un corps valué (M,v) arbitraire et $x \in M^v$, il existe $H \lhd vM$, $H \neq 0$, et $g \in vM$ tels que $H + g$ est un segment final de $I(x,M)$.

Démonstration: voir [D3].

Lemme 4. Soit un corps valué (M,v) , P unitaire $\in A_v[X]$ tel que $H(P)$ soit un sous–groupe convexe non nul de vM . Alors $\overline{J(P)} = I(y,M)$ pour un $y \in M^v$ dont le degré sur M est $\leq$ degré de P .

Démonstration. Ecrivons J pour $J(P)$. Soit $P(X) = \Pi (X-x_i)$ où les x_i sont dans la clôture algébrique de M ; on a $v(x_i) \geq 0$. En décomposant M en

$\bigcup_i \{ x ; v(x-x_i) > v(x-x_j) , \forall j \neq i \} \cup \bigcup_{i,j} \{ x ; v(x-x_i) = v(x-x_j) > v(x-x_k) \ \forall k \neq i,j \} \cup \dots ,$

on voit que J est une union finie d'ensembles de la forme $\{ m.v(x-x_i) + g ; x \in M$, " x plus près de x_i que des autres racines" $\}$ pour un $m \in \mathbb{N}^*$ et un g dans la clôture divisible $D(vM)$ de vM , donc que l'un d'entre eux est cofinal dans J . Le x_i correspondant est limite d'une suite pseudo–convergente maximale de type algébrique de K . Prenons–en une limite algébrique y de degré minimal sur K ; alors $\overline{J} = \overline{m.I(y) + g}$. On sait par ailleurs qu' il existe $H' \lhd vM$ et $h' \in vM$ tels que $H' + g'$ soit cofinal dans $I(y)$; nécessairement $H = H'$, soit $\overline{J} = I(x_i) + h$, $h \in D(vM)$. Comme $\overline{J}$ contient $I(x_i)$, on peut prendre $h \geq 0$; comme $0 \in I(x_i)$, on a $h \in J$, d'où $\overline{J} = I(x_i) = I(y)$. ☺

Lemme 5. Soit (K,v) comme au début, $P \in A_v[X]$ unitaire de degré $\leq p_n$ et tel que $H(P)$ soit un sous–groupe convexe H non nul de vK . Alors H est H_1 ou H_2 , ... H_n .

Démonstration. Le y du lemme précédent est de degré $\leq p_n$ sur K et v–immédiat, ce qui signifie que $I(y,K,v)$ n'a pas d'élément maximal. $I(y,K,v_n)$ est la projection de $I(y,K,v)$ modulo H_n . Si $H \rhd H_{n+1}$, $I(y,K,v_n)$ n'a pas non plus d'élément maximal et y reste v_n–limite sur K , contradiction avec le lemme 2 . ☺

Lemme 6. Pour $P(T) = T^{p_{n+1}} - (1+X_i)$, i=1,...n , on a $H(P) = H_{i+1}$.

Corollaire. H_1 , ... H_n sont uniformément définissables dans (K,v) : ce sont des $H(P)$ pour P comme précédemment.

Démonstration. D'après les lemmes 5 et 6. ☺

Corollaire. Si $(L,w) \equiv (K,v)$ est ω–saturé, il existe $g \in wL$ vérifiant

$$(\forall P \in A_w[X] \text{ unitaire et tel que } 0 \neq H(P) \lhd wL)\ (\ H(P) < g\ )$$

Corollaire. Mêmes hypothèses. Alors $(L \subsetneq L^W)$ satisfait

$$(\exists g \in wL)\ (\forall x)\ [\ (\ 0 \neq [\ I(x,L) \cap -I(x,L)\ ] \lhd wL\ ) \dashrightarrow (\ I(x,L) < g\ )\ ] .$$

Corollaire. $(L \subsetneq L^W, w) \not\equiv (K \subsetneq K^V, v)$.

Si $k = \mathbb{C}$ ou $\mathbb{R}$, alors v est définissable dans K^V ([D1] proposition 9), donc

$(L \subsetneq L^W) \not\equiv (K \subsetneq K^V)$.

Cas des clôtures réelles

Lemme. Soit K construit comme précédemment à partir de $k = \mathbb{R}$ et sur K l'unique ordre pour lequel tous les X_i , $i \in \omega$, sont positifs. Alors v est définissable dans $(K,<)$.

Démonstration. A_v est la clôture convexe de $\mathbb{R}$ dans K . On va montrer $A_v = [-1,1] \cup C$, où $C = \{ x \in K ; |x| > 1 \wedge \forall y \exists z (|y| < 1 \rightarrow |1+y^3-z^3| < |x|^{-1}) \}$.
1. Soit $x \in \mathbb{R}$, $x \neq 0$, $y \in K$, $|y| < 1$; donc $v(y) \geq 0$ et $v(1+y^3) \geq 0$ et le polynôme $1+y^3-Z^3$ admet un zéro résiduel puisque $K/v = \mathbb{R}$ est réel clos, ce qui signifie: $\exists z \in K$, $v(1+y^3-z^3) > 0$, donc $1+y^3-z^3$ est infinitésimal, donc $< |x|^{-1}$. Cela montre $\mathbb{R} \subseteq [-1,1] \cup C$, et comme $[-1,1] \cup C$ est convexe, $A_v \subseteq [-1,1] \cup C$.
2. Réciproquement. L'ensemble $\{ aX_0^{-1} ; a \in \mathbb{R}^{*+} \}$ est co–initial dans $K^+ - \mathbb{R}$, il suffit donc de montrer que C ne contient aucun aX_0^{-1} ; pour $y = -1 + X_0.a^{-1}$, $v(1+y^3) = v(X_0)$ n'est pas divisible par 3 dans vK et est donc distinct de $v(z^3)$, $\forall z \in K$. Alors
– ou bien $1+y^3-z^3 \sim 1+y^3 \sim 3X_0a^{-1} > X_0a^{-1}$,
– ou bien $v(z) \leq 0$ et $1+y^3-z^3 \sim -z^3$ et $|z^3|$ > tout élément de valuation $v(X_0)$. ☺

Corollaire. Il existe $(K,<) \equiv (L,<)$ avec $(K \subsetneq K^r) \not\equiv (L \subsetneq L^r)$, où K^r est la clôture réelle de K .

Démonstration. Soit K et L définis comme précédemment avec $k = \mathbb{R}$. On a vu que v est définissable dans (K,v) . Continuons d'appeler v l'unique prolongement convexe de v sur K^r . Il est définissable dans $(K \subsetneq K^r)$, et la même formule que précédemment distingue $(L \subsetneq L^r)$ et $(K \subsetneq K^r)$ ($K^r \neq K^V$ mais exiger que $I(x,K) \cap -I(x,K)$ est un sous–groupe $\neq 0$ impose que x est limite et donc se comporte comme un point de K^V) . □

Bibliographie

[D1] Françoise Delon, Périodicité des théories élémentaires des corps de séries formelles itérées, J.S.L. 51 (1986), 334–351.

[D2] Françoise Delon, Idéaux et types sur les corps séparablement clos, Mémoires de la S.M.F., à paraître.

[D3] Françoise Delon, Indécidabilité de la théorie des paires immédiates de corps valués henseliens, manuscrit.

[Ka] Irving Kaplansky, Maximal fields with valuations, Duke math. J. 9 (1942), 303–321.

[Ke] Jerome Keisler, Complete theories of algebraically closed fields with distinguished subfields, Michigan Math. J. 11 (1964), 71–81.

[R] Paulo Ribenboim, Théorie des valuations, Les Presses de l'Université de Montréal, Montréal 1964.

[V] Carlos Videla, Elementary equivalent fields with inequivalent perfect closures, Proc. A.M.S. 99 (1987), 171–175.

On the Stability Index of Real Varieties

Claus Scheiderer (Regensburg)

Let R be a real closed field and V an affine algebraic variety over R. For polynomial functions $f_1, \ldots, f_r \in R[V] = \Gamma(V, \mathcal{O}_V)$ we put

$$S(f_1, \ldots, f_r) := \{x \in V(R) : f_1(x) > 0, \ldots, f_r(x) > 0\}. \qquad (\star)$$

Subsets of this form are called *basic open* (semi-algebraic) subsets of $V(R)$. Given a basic open $S \subset V(R)$, one denotes by $s(S)$ the minimal number r of inequalities needed to describe S as in $(\star)$. The supremum $\sup_S s(S)$ with S ranging over the non-empty basic open subsets of $V(R)$ is denoted by $s(V)$ and is well known to be finite. It has been called the *stability index* of the variety V.

It had been conjectured for some time that $s(V) = n$ holds for every n-dimensional real V $(n > 0)$. This conjecture has now been confirmed, and the aim of the talk is to present a sketch of the proof. The lower estimate $s(V) \geq n$ was already known before and is due to L. Bröcker [B1]. In the other direction he had given upper bounds for $s(V)$ growing quadratically with n and giving $s(V) = n$ for $n = 1, 2, 3$, see [B2].

One may ask a similar question concerning basic closed sets (replacing $>$ by $\geq$ in $(\star)$) and the corresponding invariant $\bar{s}(V)$. Also this had been an open problem which has now been solved, to the end that $\bar{s}(V) = \frac{n}{2}(n+1)$. Here the $\leq$-part is due to Bröcker [B3]. However we will only report on the basic open case here.

The main ingredients for the proof of $s(V) = n$ are the concept of the real spectrum on the one hand (see [CR], [BCR]) and reduced quadratic form theory over semilocal rings on the other. More specifically, one needs M. Marshall's theory of spaces of orderings, together with the fact that every semilocal ring gives rise to a space of orderings. For this, see e.g. [M] and [K].

If A is a semilocal ring, put $X_A := (\operatorname{Sper} A)^{\max}$ (the topological space of closed points in the real spectrum of A) and $G_A := A^*/\{u \in A^* : u > 0 \text{ on } \operatorname{Sper} A\}$. Then the pair (X_A, G_A) is a space of orderings.

Let $X = (X, G)$ be a space of orderings. A constructible subspace of X is a subset $Y \subset X$ of the form

$$Y = \{x \in X : x(f_1) = \cdots = x(f_m) = +1\} = X \cap \{f_1, \ldots, f_m\}^\perp$$

with $f_i \in G$. Each constructible subspace of X is a space of orderings by itself. The least possible $m \geq 0$ is denoted by $s_X(Y)$. The *stability index* $\operatorname{st}(X)$ of X can be described as

contains some f with $f|S > 0$. Since $f|S \geq 0$ for each $f \in L$, and moreover $L + L \subset L$ holds, it suffices to find for each $p \in S$ some $f \in L$ with $f(p) > 0$.

Fix $p \in S$ and put $C := \mathcal{O}_{V,p}$; one has to show $s_{\tilde{U} \cap X_C}(\tilde{S} \cap X_C) \leq m$. By the representation theorem for spaces of orderings this means

$$|\tilde{S} \cap G| \equiv 0 \bmod 2^{k-m}$$

for every fan G in $\tilde{U} \cap X_C$ with $|G| = 2^k > 2^m$. Let $Z \subset V$ be the support variety of such a fan G. Since $\mathcal{O}_{V,Z}$ is a regular local ring, there is a place $R(V) \to R(Z), \infty$ over R which coincides with the residue homomorphism $\mathcal{O}_{V,Z} \to R(Z)$ on $\mathcal{O}_{V,Z}$. Pulling back the fan G with respect to this place one arrives at a fan F in $\tilde{U} \cap X_{R(V)}$ together with a "specialization map" $s: F \to G$ satisfying $s(x) \in \overline{\{x\}}$ for $x \in F$ (the closure formed e.g. in $\operatorname{Sper} \mathcal{O}_{V,Z}$) and $|s^{-1}(y)| = 2^d$ for $y \in G$, independently from y, with some $d \geq 0$. Hence $|F| = 2^{k+d}$, and by $(\star\star)$ of the lemma this implies $|\tilde{S} \cap F| \equiv 0 \bmod 2^{k+d-m}$. From this congruence one concludes that $|\tilde{S} \cap G| \equiv 0 \bmod 2^{k-m}$, as desired.

It should be mentioned that this method of proof applies to a much more general situation. In fact, if A is any noetherian ring whose (real) singularities do not behave too bad (for example it suffices that $\operatorname{Sing}(A/p)$ is closed in $\operatorname{Spec}(A/p)$ for every real prime ideal $p \in \operatorname{Spec} A$), then one gets a result concerning the basic open constructible subsets of $\operatorname{Sper} A$ which is completely analogous to the theorem. For details see the author's forthcoming paper.

Bibliography

[BCR] J. Bochnak, M. Coste, M.-F. Roy, Géométrie Algébrique Réelle. Springer-Verlag, Berlin Heidelberg New York, 1987.

[B1] L. Bröcker, Zur Theorie der quadratischen Formen über formal reellen Körpern. Math. Ann. **210**, 233-256 (1974).

[B2] L. Bröcker, Description of semialgebraic sets by few polynomials. Lecture CIMPA, Nice, 1985.

[B3] L. Bröcker, Characterization of basic semialgebraic sets. Preprint 1987.

[CR] M. Coste, M.-F. Roy, La topologie du spectre réel. Contemporary Mathematics **8**, 27-59 (1982).

[K] M. Knebusch, On the local theory of signatures and reduced quadratic forms. Abh. Math. Sem. Univ. Hamburg **51**, 149-195 (1981).

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