N° 54

Séminaire de Structures Algébriques Ordonnées

1993-1994

F. Delon, M.A. Dickmann. D. Gondard

Février 1995

Séminaire de Structures Algébriques Ordonnées

Delon - Dickmann-Gondard

1993 - 1994

Liste des exposés.

9.11.93 - **P. Simonetta** (Univ. Paris VII).
Produits en couronne de groupes et de groupes ordonnés.

16.11.93 - **Z. Chatzidakis** (Univ. Paris VII).
Le modèle-compagnon des corps de différence.

23.11.93 - **F. Cucker** (Univ. Pompeu Fabra, Barcelone, Espagne).
Classes de complexité dans le modèle de Koiran.

30.11.93 - **D. Lascar** (Univ. Paris VII).
Le groupe des automorphismes de $\mathbb{C}$ laissant fixe les nombres algébriques est simple.

7.12.93 - **P. Jumpertz** (Univ. Paris VII).
Décomposition cylindrique dans un corps réel clos et vérification de formules.

11.01.94 - **R. Cignoli** (Univ. de Buenos-Aires, Argentine).
Dualité de Priestley pour les treillis distributifs (en anglais).

1.02.94 - **F. Miraglia** (Univ. de Sào Paulo (Brésil) et Univ. de Paris VII).
Faisceaux de structures du premier ordre (en anglais).

8.02.94 - **F. Miraglia** - suite.

15.02.94 - **G. Martinez** (Univ. d'Oxford, Grande-Bretagne).
Topological duality for lattice-ordered groups (en anglais).

8.03.94 - **Ch. Michaux** (Univ. de Mons, Belgique).
Critères de définissabilité dans l'arithmétique de Presburger.

3.05.94 - **I. Efrat** (Univ. Konstanz, Allemagne et Jérusalem, Israël).
Orderings, valuations and free products of Galois groups.

10.05.94 - **B. Kahn** (Univ. Paris VII).
Dimension diophantienne des corps.

24.05.94 - **J. Koenigsmann** (Univ. Konstanz, Allemagne).
Definable valuations.

7.06.94 - **C. Wood** (Wesleyan Univ., Conn, E.U.).
Separably closed fields and higher derivations.

14.06.94 - **B. Kahn** (Univ. Paris VII).
Hauteur et degré des formes quadratiques.

Séminaire de Structures Algébriques Ordonnées

Delon - Dickmann-Gondard

1993 - 1994

Liste des contributions.

P. Simonetta (Univ. Paris VII).
Produits en couronne de groupes et de groupes ordonnés.

Z. Chatzidakis (Univ. Paris VII).
Le modèle-compagnon de la théorie des corps de différence.

D. Lascar (Univ. Paris VII).
Le groupe des automorphismes du corps des complexes laissant les nombres algébriques fixes est simple.

P. Jumpertz (Univ. Paris VII).
Présentation de la méthode de décomposition cylindrique de Collins.

R. Cignoli (Buenos-Aires, Argentine).
Priestley duality and distributive lattices with operators.

N. Martinez (Buenos-Aires, Argentine et Oxford, Grande-Bretagne).
A simplified duality for implicative lattices and ℓ-groups.

Ch. Michaux (Univ. de Mons, Belgique) et
R. Villemaire (Univ. de Québec à Montréal, Canada).
Open questions around Büchi and Presburger arithmetics.

I. Efrat (Univ. de Konstanz, Allemagne, et Univ. de Jérusalem, Israël).
Orderings, valuations and free products of Galois groups.

J. Koenigsmann (Univ. Konstanz, Allemagne).
Definable valuations.

M. Messmer et **C. Wood** (Wesleyan University, Connecticut, Etats-Unis).
Separably closed fields with higher derivations I.

Produits en couronne de groupes et de groupes ordonnés

par Patrick SIMONETTA
(Université de Paris VII)

Introduction

Les produits en couronne ont de très nombreuses applications dans l'étude des groupes et des groupes de permutations. D'une part ils servent à construire des exemples de groupes ayant des propriétés particulières. D'autre part, ils ont parmi les groupes de permutations un certain caractère universel comparable à celui des produits de Hahn pour les groupes ordonnés. Nous n'exposerons pas ici ces applications, bien que nous en citions quelques unes, et nous nous permettrons de renvoyer le lecteur à la bibliographie pour plus d'informations. Après avoir rappelé quelques définitions générales, nous montrerons que certains types de produits en couronne permettent de construire de nouveaux exemples de groupes non abéliens décidables. Pour terminer nous complèterons ces résultats par la preuve de l'indécidabilité des produits en couronne classiques (restreint et complet) d'un groupe par un groupe contenant un élément d'ordre infini.

Notations et définitions:

Soit A un groupe, et E et F deux ensembles.

$.$, e_A, x^{-1}, désigneront respectivement la loi de A, son élément neutre, et l'inverse d'un élément $x \in A$.

Si $x,y \in A$, $x^y = y^{-1}xy$ et $[x;y] = x^{-1}y^{-1}xy$ sont respectivement le conjugué de x par y et le commutateur de x et de y.

Si H est un sous-groupe de A, $C_A(H) = \{a \in A \mid \forall h \in H \ h.a = a.h\}$ est le centralisateur de H dans A.

Si $x \in A$, $<x>_A$ et $C_A(x) = \{a \in A \mid x.a = a.x\}$ sont respectivement le sous-groupe de A engendré par x et le centralisateur de x dans A.

A^E désigne le groupe des applications de E dans A; si $f \in A^E$, le support de f est l'ensemble $\mathbf{supp(f)} = \{ x \in E \mid f(x) \neq e_A \}$;

$\overline{A^E}$ est le sous-groupe de A^E, formé par les applications de E dans A à support fini.

Dans le cas où E est un ensemble totalement ordonné, on peut considérer le sous-groupe $\overline{\overline{A^E}}$ de A^E, formé des applications de E dans A à support bien ordonné.

Si E et F sont des ensembles totalement ordonnés, nous noterons $E \overleftarrow{\times} F$ le produit $E \times F$ muni de l'ordre antilexicographique:

pour (x,y) et (z,t) dans $E \times F$, $(x,y) \geq (z,t)$ si $y \geq t$ ou $(y = t$ et $x \geq z)$.

I/ Produits en couronne de groupes de permutations

Un groupe de permutations est un couple (A,Ω), où Ω est un ensemble et A est un groupe agissant fidèlement sur Ω (i.e. la seule action triviale est celle de l'élément neutre).
Soient (A,Ω) et (B,T) deux groupes de permutations. Si $f\in A^T$ et $b\in B$, l'application $\theta(f,b)$ de $\Omega\times T$ dans lui-même définie par:

$$\forall(\alpha,\beta)\in\Omega\times T \quad (\alpha,\beta).\theta(f,b)=(\alpha.f(\beta),\beta.b),$$

est une permutation de $\Omega\times T$. Il est aisé de vérifier que nous obtenons ainsi un groupe de permutations sur cet ensemble. Ce groupe, noté $(A,\Omega)\wr(B,T)$, est appelé **produit en couronne** de (A,Ω) par (B,T).

Un exemple important d'application de ces produits en couronne, est leur utilisation pour la construction de sous-groupes de Sylow des groupes de permutations sur un ensemble fini et pour en déterminer des générateurs (voir par exemple [H1] § 5.9).

Remarques: Les $\theta(e_{A^T},b)$ où $b\in B$ forment un sous-groupe de $(A,\Omega)\wr(B,T)$ isomorphe à B. Les $\theta(f,e_B)$ où $f\in A^T$ forment un sous-groupe normal de $(A,\Omega)\wr(B,T)$ isomorphe à A^T, et le quotient de $(A,\Omega)\wr(B,T)$ par ce sous-groupe est isomorphe à B. Les $\theta(e_{A^T},b)$ où $b\in B$ forment un sous-groupe de $(A,\Omega)\wr(B,T)$ isomorphe à B. B se plonge ainsi naturellement dans $(A,\Omega)\wr(B,T)$, qui est donc le produit semi-direct de A^T par B, l'action d'un élément $b\in B$ sur $f\in A^T$ étant définie par: $\forall x\in T \quad f^b(x)=f(x.b^{-1})$.

Pour $a\in A$ et $\tau\in T$, on note $\overline{a}_\tau$ l'élément de A^T défini par:

$\overline{a}_\tau(t)=e_A$ si $t\neq\tau$,

$\overline{a}_\tau(\tau)=a$.

Pour chaque $\tau\in T$, l'application qui à $a\in A$ associe $\overline{a}_\tau$ plonge A dans A^T et donc dans $(A,\Omega)\wr(B,T)$ (mais il existe bien sûr beaucoup d'autres plongements).

Le **produit en couronne restreint** de (A,Ω) par (B,T), noté $(A,\Omega)\bar{\wr}(B,T)$, est le sous-groupe de $(A,\Omega)\wr(B,T)$ dont les éléments sont les $\theta(f,b)$ où $f\in\overline{A}^T$ et $b\in B$. Lorsque (B,T) est transitif (i.e. $\forall t_1,t_2\in T\ \exists b\in B$ tel que $t_1.b=t_2$), $(A,\Omega)\bar{\wr}(B,T)$ peut aussi être vu comme le sous-groupe de $(A,\Omega)\wr(B,T)$ engendré par B et les $\overline{a}_\tau$ où τ est fixé et $a\in A$, (ce groupe ne dépend pas alors de $\tau\in T$).
$(A,\Omega)\bar{\wr}(B,T)$ est le produit semi-direct de $\overline{A}^T$ par B.

Les produits en couronne (restreints ou non) de groupes de permutations sont associatifs: si (A,Ω), (B,T) et (C,U) sont trois groupes de permutations, et si l'on identifie $(\Omega\times T)\times U$ avec $\Omega\times(T\times U)$, alors $((A,\Omega)\wr(B,T))\wr(C,U)$ et $(A,\Omega)\wr((B,T)\wr(C,U))$ sont isomorphes (même chose pour les produits en couronne restreints). On peut donc, pour tout entier n, définir sans ambiguïté le produit en couronne de n groupes de permutations. En fait, les produits en couronnes peuvent se généraliser à des familles quelconques de groupes de permutations. Nous ne rappellerons pas ici ces constructions et leurs nombreuses applications à l'étude des groupes de permutations transitifs; nous renvoyons à [H1], [H2] et [Ho].

Le produit en couronne est également un outil important dans l'étude des groupes de permutations de chaîne. Il s'agit des groupes de permutations (A,Ω) où Ω est une chaîne, c'est à dire un ensemble totalement ordonné, et où l'action de A préserve l'ordre de Ω. (A,Ω) admet un ordre défini par les images des éléments de Ω:

pour $a_1,a_2 \in A$, $a_1 \leq a_2$ si pour tout $\alpha \in \Omega$, $\alpha.a_1 \leq \alpha.a_2$.

Cet ordre n'est pas en général un ordre total; il est compatible avec la loi du groupe A: pour $x,y,z \in A$, $x \leq y$ implique $x.z \leq y.z$ et $z.x \leq z.y$.

Si (A,Ω) et (B,T) sont des groupes de permutations de chaînes, les produits en couronne $(A,\Omega)\wr(B,T)$ et $(A,\Omega)\tilde{\wr}(B,T)$ sont alors des groupes de permutations préservant l'ordre de $\overleftarrow{\Omega \times T}$. Nous renvoyons par exemple à [G] ch. 5 pour l'utilisation des produits en couronne dans ce contexte.

Si (B,T) est un groupe de permutation de chaîne, il n'est pas trop difficile de voir que les $\theta(f,b)$ où $f \in \overrightarrow{A^T}$ et $b \in B$ forment un sous-groupe de $(A,\Omega)\wr(B,T)$. Nous appelons ce groupe le **produit en couronne "bien ordonné"** de (A,Ω) par (B,T), et nous le notons $((A,\Omega)\wr(B,T))^*$; il dépend de l'ordre fixé sur T.

II/ Produits en couronne de deux groupes.

Nous donnons maintenant une autre version des produit en couronne, qui est en fait un cas particulier de la précédente, mais qui est celle qui nous intéresse spécialement. Tout groupe A agit sur lui même par translation à droite, et peut donc être vu comme un groupe de permutations transitif que nous noterons (A,A). Si A et B sont deux groupes, le **produit en couronne de A par B** est le groupe $AWB=(A,A)\wr(B,B)$. C'est le produit semi-direct de A^B par B, l'action d'un élément $b \in B$ sur $f \in A^B$ étant définie par:

$\forall x \in B \quad f^b(x)=f(xb^{-1})$.

Les éléments de AWB s'écrivent donc sous la forme b.f où $b \in B$ et $f \in A^B$.

On définit également les sous-groupes suivants de AWB:

- le **produit en couronne restreint de A par B**: $AwB=(A,A)\tilde{\wr}(B,B)$, qui est le produit semi-direct de $\overrightarrow{A^B}$ par B, et,

lorsque B est un groupe totalement ordonné, c'est à dire un groupe muni d'un ordre total compatible avec la structure de groupe,

-le **produit en couronne "bien ordonné"** de A par B: $(AWB)^*=((A,A)\wr(B,B))^*$ qui est le produit semi-direct de $\overrightarrow{\overrightarrow{A^B}}$ par B.

Chacun de ces groupes peut être considéré comme un groupe de permutations de l'ensemble $A \times B$. Il faut bien faire attention cependant, au fait que les produits en couronne de groupes que nous venons de définir ne se manipulent pas comme les produits en couronne de groupes de permutations, et ils n'ont pas les mêmes propriétés. En particulier, ils ne sont pas associatifs: si A, B et C sont trois groupes, alors (AWB)WC et AW(BWC) sont en général trivialement différents, ne serait-ce que pour des raisons de

cardinalité. Il faut comprendre que dans le produit $(A,A)\wr((B,B)\wr(C,C))$, $(B,B)\wr(C,C)$ est considéré comme un groupe de permutations sur $B\times C$ alors que dans la définition de AW(BWC), BWC est considéré comme un groupe de permutations agissant sur lui-même.

L'une des principales propriétés du groupe AWB est celle de contenir toutes les extensions du groupe A par le groupe B, comme le précise le théorème suivant du à L. Kaloujnine et M. Krasner (voir par exemple [Sc] th. III.5.k)

Théorème: Si G est une extension du groupe A par le groupe B, alors il existe un plongement $\pi:A \longrightarrow AWB$ tel que $\pi(A)\subseteq A^B$ et $(\pi(G).A^B)/A^B=B$.

Les produits en couronne de deux groupes A et B conservent certaines des propriétés des groupes A et B: il n'est pas trop difficile de voir, par exemple, que si A et B sont des groupes résolubles, alors AWB est lui même résoluble; si p est un nombre premier et si A et B sont des p-groupes, alors le produit en couronne restreint AwB est également un p-groupe; si A et B sont des groupes de torsion, alors AwB est lui aussi un groupe de torsion.

Toutes ces propriétés font des produits en couronne un outil très utile comme source d'exemples et à l'heure d'étudier certaines classes de groupes. Ils peuvent suppléer, par exemple dans l'étude de modèles existentiellement clos ou dans des problèmes de plongement, à l'usage du produit libre avec amalgamation ou des extensions H.N.N. lorsque ceux-ci ne peuvent servir. Le produit en couronne est l'outil essentiel qui a permis à D. Saracino de montrer que la théorie des groupes résolubles de classe de résolubilité au plus n, n étant un nombre entier donné, n'a pas de modèle-compagne (voir [S] th. 1). G. Baumslag a redémontré, en utilisant le produit en couronne restreint, que tout groupe se plonge dans un groupe divisible. La preuve originale de ce résultat, due à B.H. Neumann utilise le produit libre avec amalgamation. Mais la preuve de G. Baumslag a l'avantage de pouvoir s'adapter pour montrer que tout p-groupe se plonge dans un p-groupe divisible et que tout groupe de torsion se plonge dans un groupe de torsion divisible (voir [B] th. 4.3, 4.4 et 4.5).

Supposons maintenant que A et B sont des groupes totalement ordonnés. On peut alors munir les produits en couronne AwB et $(AWB)^*$ (défini pour l'ordre de B) d'une structure de groupe totalement ordonné en les munissant de l'ordre défini par: pour $b\in B$ et $f\in A^B$ à support fini (resp. à support bien ordonné),

$$b.f\geq e \text{ ssi } b>e_B \text{ ou } (b=e_B \text{ et } f(\min(\mathrm{supp}(f)))\geq e_A)$$

où e désigne l'élément neutre de AwB (resp. de $(AWB)^*$). Nous noterons respectivement $\overleftarrow{AwB}$ et $(AWB)^{\leftarrow}$ les groupes ordonnés ainsi définis. Remarquons que le produit en couronne CWD de deux groupes C et D ne peut être muni d'un ordre total compatible avec la structure de groupe que si C ou D est réduit à son élément neutre (voir [N] lemma 2.1).

Nous nous sommes intéressés aux produits en couronne parce qu'ils semblaient aussi pouvoir fournir de nouveaux exemples de groupes et de groupes ordonnés décidables. Sans trop entrer dans les détails, disons que l'idée de départ était l'analogie entre les

produits en couronne bien ordonnés et les corps de séries formelles k((B)) à exposants dans un groupe ordonné B et à coefficients dans un corps k. Les éléments de k((B)) ne sont rien d'autre que des applications de B vers k dont le support, c'est à dire l'ensemble des éléments de B dont l'image est non nulle, est bien ordonné; la multiplication dans le corps k((B)) induit une action du groupe B sur le groupe additif $k((B))_+$, et le produit semi-direct correspondant n'est autre que le produit en couronne bien ordonné $(k_+WB)^*$. Les théorèmes d'Ax-Kochen et Ershov sur les corps valués, permettent dans certains cas de déduire la théorie d'un corps de séries formelles k((B)) de la théorie du groupe ordonné B et de celle du corps k, de sorte que k((B)) est décidable lorsque k et B le sont. Nous nous sommes posé les questions analogues pour les produits en couronne bien ordonnés et avons trouvé les résultats suivants:

Proposition 1: *Si A est un groupe abélien qui est somme directe d'un groupe divisible et sans torsion et d'un nombre fini de groupes d'exposant premier et si B est un groupe totalement ordonné résoluble alors*
1) pour tout groupe A' et tout groupe totalement ordonné B':
a. $A \equiv A'$ *et* $B \equiv B'$ *implique* $(AWB)^* \equiv (A'WB')^*$,
b. $A \preceq A'$ *et* $B \preceq B'$ *implique* $(AWB)^* \preceq (A'WB')^*$ *pour le plongement naturel.*
2) Si B est en plus décidable, alors le groupe $(AWB)^*$ *est décidable.*

Si $A \subseteq A'$ et $B \subseteq B'$, le plongement naturel de $(AWB)^*$ dans $(A'WB')^*$ est celui qui identifie $(AWB)^*$ avec le sous-groupe de $(A'WB')^*$ dont les éléments s'écrivent sous la forme b.f où $b \in B$ et $f \in A'^{B'}$ avec $f(B') \subseteq A$ et $supp(f) \subseteq B$.

Proposition 2: *Si A est un groupe abélien totalement ordonné divisible, et B est un groupe totalement ordonné résoluble alors*
1) Pour tout groupe totalement ordonné divisible A' et tout groupe totalement ordonné B',
a) $B \equiv B'$ *ssi* $(AWB)^{\leftarrow} \equiv (A'WB')^{\leftarrow}$
b) $A \subseteq A'$ *et* $B \preceq B'$ *ssi* $(AWB)^{\leftarrow} \preceq (A'WB')^{\leftarrow}$.
2) B est décidable ssi $(AWB)^{\leftarrow}$ *est décidable.*

Les preuves de ces deux propositions, que nous ne donnons pas ici, se trouvent dans [Si] ch. IV prop. 7.1.7 et 7.1.19. Elles sont l'une des applications d'une étude plus générale, que nous avons conduite avec Françoise Delon, concernant des structures constituées par un groupe totalement ordonné B agissant sur un groupe abélien G avec une valuation de G dans B. Nous avons montré pour certaines de ces structures un principe d'Ax-Kochen-Ershov, analogue à celui qui concerne les corps valués.

Si A est un groupe totalement ordonné abélien non trivial et B est un groupe totalement ordonné résoluble de classe n, nous pouvons voir que le produit en couronne $(AWB)^{\leftarrow}$ est résoluble de classe n+1. La proposition 2 nous donne la possibilité de construire des groupes totalement ordonnés résolubles décidables, de classe de résolubilité arbitrairement grande. Si par exemple A est un groupe abélien ordonné divisible, et C_n est le groupe ordonné défini par récurrence: $C_1 = A$, et pour $n > 1$ $C_n = (AWC_{n-1})^{\leftarrow}$, alors chaque C_n est résoluble de classe n, et décidable grâce à la proposition 2. Pour $n > 2$, les C_n ne sont pas des groupes linéaires sur un corps commutatif (voir par exemple

[W] th. 10.21) et ne font donc pas partie des exemples classiques de groupes non abéliens décidables.

Les produits en couronne AWB et AwB d'un groupe A par un groupe ordonnable B sont en revanche toujours indécidables lorsque A et B ne sont pas réduits à leur élément neutre. Nous avons en effet montré dans [Si] ch. 4 section 8, la proposition suivante:

Proposition 3: *Si A et B sont deux groupes, si $A \neq \{e_A\}$, et si B contient un élément d'ordre infini, alors les produits en couronne AWB et AwB sont indécidables.*

La preuve de cette proposition, que nous donnons ci-dessous, consiste à interpréter la structure $\langle \mathbf{Z},0,1,+,-,| \rangle$ des entiers relatifs avec l'addition, l'opposé et la relation de divisibilité, dans les groupes AWB et AwB, ce qui suffit à en démontrer l'indécidabilité (voir [T]). L'indécidabilité des produits en couronne restreints, sous les hypothèses de la proposition 3, n'est pas surprenante: si les produits en couronne bien ordonnés présentent certaines analogies avec les corps de séries formelles, les produits en couronne restreints ressemblent d'une certaine façon aux anneaux de polynômes; or il s'avère que ces dernières structures sont en général indécidables (voir [R] et [D] cor. 1.63)

Dans la preuve de la proposition 3 nous emploierons les notations suivantes:

Nous notons e_A, e_B et e les éléments neutres respectivement de A, B et AWB.
Si $f \in A^B$, soit $|\ \mathbf{supp(f)}\ | \in \mathbf{N} \cup \{\infty\}$ le cardinal de son support.
Si $b \in B$, soit $\mathbf{ord(b)} \in \mathbf{N} \cup \{\infty\}$ l'ordre de b.
Soit $\Phi_b = \{\ f \in A^B\ |$ pour tout $x \in B$, $f(xb)=f(x)\ \}$; il s'agit de l'ensemble des fonctions périodiques de période b. On voit que $\Phi_b = C_{AWB}(b) \cap A^B$, et est donc un sous-groupe de A^B. Si $f \in \Phi_b$, supp(f) est stable par translation à droite par b; la réciproque est évidemment fausse.
Soient $a \in A$ et $b \in B$. Nous définissons les éléments $\bar{a}$, â et $f_{a,b}$ de A^B par:

- $\bar{a}(e_B)=a$ et $\bar{a}(x)=e_A$ pour $x \neq e_B$,
- $\hat{a}(x)=a$ pour tout $x \in B$,
- $f_{a,b}(x)=a$ si $x \in \langle b \rangle$ et $f_{a,b}(x)=e_A$ sinon.

On vérifie que â et $f_{a,b}$ appartiennent à Φ_b; d'autre part,

Lemme 1: *1) Si $f \in \Phi_b$, alors ord(b) divise $|\ supp(f)\ |$. En particulier, si $b \neq e_B$ alors $|\ supp(f)\ | \neq 1$, et si $ord(b)=\infty$, alors soit $f=e$ soit supp(f) est infini.*
2) Pour tout f et tout f' de A^B, $supp(f'^{-1}ff')=supp(f)$.
3) Si $|\ supp(f)\ |=1$, alors $C_{AWB}(f) \subseteq A^B$. En particulier, si $a \in C_A(A) \setminus \{e_A\}$, alors $C_{AWB}(\bar{a})=A^B$.
4) Soient $a \in A \setminus \{e_A\}$, $b,b' \in B$ et $f \in A^B$. $[f_{a,b};b'f]=e$ ssi $b' \in \langle b \rangle$ et $[f_{a,b};f]=e$.

Preuve: 1) Si $f \in \Phi_b$, $\langle b \rangle$ opère simplement sur supp(f) par translation à droite; il s'agit donc d'un résultat classique en théorie des groupes.
2) Pour $b \in B$, $f'^{-1}ff'(b)=f'^{-1}(b)f(b)f'(b)=e_A$ ssi $f(b)=e_A$.
3) Soit $b.f' \in AWB$, où $b \in B$ et $f' \in A^B$; b.f' commute avec f ssi $b^{-1}fb=f'ff'^{-1}$, ce qui implique, d'après 2), $supp(f)=supp(b^{-1}fb)=supp(f).b$; ceci n'est possible que si $b=e$.

En particulier, comme il est clair que $\bar{a}$ commute avec tout élément de A^B et $supp(\bar{a})=\{e_B\}$ on obtient $C_{AWB}(\bar{a})=A^B$.

4) $[f_{a,b};b'f]=e$ ssi $ff_{a,b}f^{-1}=b'^{-1}f_{a,b}b'$. Si $b'\notin<b>$, $(ff_{a,b}f^{-1})(b')=e_A$ et $(b'^{-1}f_{a,b}b')(b')=f_{a,b}(e_B)=a\neq e_A$. D'autre part, si $b'\in<b>$, $f_{a,b}$ commute avec b'. Nous voyons donc que si $[f_{a,b};b'f]=e$ alors $b'\in<b>$ et $[f_{a,b};f]=e$. La réciproque est triviale. □

Lemme 2: *Soient $b,c\in B$ et $f\in A^B$. Alors*

1) $cf\in C_{AWB}(b)$ ssi $c\in C_B(b)$ et $f\in\Phi_b$.

2) $cf\in C_{AWB}(C_{AWB}(b))$ ssi $c\in<b>$ et $f\in(C_{A^B}(A^B)\cap\bigcap_{x\in C_B(b)}\Phi_x)$. En particulier, si $C_A(A)=\{e_A\}$, alors pour tout $b\in B$, $C_{AWB}(C_{AWB}(b))=<b>$.

Preuve: 1) Pour tout $c\in B$ et $f\in A^B$, $b^{-1}cfb=cf$ ssi $b^{-1}cb=c$ et $b^{-1}fb=f$, puisque $B\cap A^B=\{e\}$. b commute donc avec cf ssi $c\in C_B(b)$ et $f\in C_{AWB}(b)\cap A^B=\Phi_b$.

2)Soit $g\in C_{AWB}(C_{AWB}(b))$; g s'écrit $g=cf$ avec $c\in B$ et $f\in A^B$. On a $C_{AWB}(b)\subseteq C_{AWB}(g)$.

- Pour tout $a\in A$, $\hat{a}\in C_{AWB}(b)\cap C_{AWB}(c)$, et donc â commute avec f. Par conséquent, pour tout $x\in B$, et tout $a\in A$, $f(x)a=af(x)$ et $f\in C_A(A)^B=C_{A^B}(A^B)$.

- Pour tout $a\in A$, $f_{a,b}$ commute avec b et donc avec g. Nous en déduisons grâce au lemme 1 4), que $c\in<b>$, et il existe un entier relatif n tel que $c=b^n$.

- Comme c et g commutent avec tous les éléments de $C_{AWB}(b)$, f fait de même, et par conséquent $f\in\Phi_x$ pour tout $x\in C_B(b)$.

Réciproquement, si $n\in\mathbf{Z}$ et $f\in(C_{A^B}(A^B)\cap\bigcap_{x\in C_B(b)}\Phi_x)$, on vérifie aisément que b^nf commute avec tous les éléments de $C_{AWB}(b)$. □

Lemme 3: *Supposons $C_A(A)\neq\{e_A\}$. Soit Div(x,y) la relation binaire sur AWB, définie par:*

Div(g,g') ssi il existe $h\in A^B$ tel que $C_{AWB}(g)\subseteq C_{AWB}(g'h)$.

Alors Div est définissable dans AWB (avec un paramètre) et pour tout $b,b'\in B$, $f,f'\in A^B$,

Div(bf,b'f') ssi il existe $n\in\mathbf{Z}$ tel que $b'=b^n$.

Preuve: Pour voir que Div est définissable il suffit de vérifier que A^B l'est; si $a\in C_A(A)\setminus\{e_A\}$, le centralisateur de $\bar{a}$ dans AWB est A^B d'après le lemme 1 3), ce qui prouve que

$$Div(g,g')\longleftrightarrow\exists u\,([u;\bar{a}]=e\wedge(\forall v\,[v;g]=e\longrightarrow[v;g'u]=e)).$$

Si $a\in C_A(A)\setminus\{e_A\}$ alors $f_{a,b}\in C_{A^B}(A^B)$; d'après le lemme 1 4), $f_{a,b}\in C_{AWB}(bf)$, et s'il existe $h\in A^B$ tel que $C_{AWB}(bf)\subseteq C_{AWB}(b'f'h)$, alors $f_{a,b}\in C_{AWB}(b'f'h)$. Ceci implique $b'\in<b>$, toujours d'après le lemme 1 4).

Réciproquement, si $n\in\mathbf{Z}$, $f,f'\in A^B$, et $h'=(bf)^{-m}b^n$ alors $h'=\prod_{i=0}^{n-1}(f^{-1})^{b^i}\in A^B$, et, $b^nf'=(bf)^mh'f'$; si on pose $h=(h'f')^{-1}$, alors $h\in A^B$ et $b^nf'h=(bf)^n$. Il est clair que $C_{AWB}(bf)\subseteq C_{AWB}((bf)^n)$. □

Preuve de l'indécidabilité de AWB:

Soit b un élément d'ordre infini de B. Nous distinguerons deux cas:

Cas 1: $C_A(A)=\{e_A\}$. Soit div(x,y) la relation binaire

$$\text{div}(x,y) \longleftrightarrow \forall z \ (\ xz=zx \longrightarrow yz=zy\ )\ .$$

$<b>$ est définissable: d'après le lemme 2 2), pour tout $g\in AWB$, $g\in <b>$ ssi $AWB \models \text{div}(b,g)$.

Si $n,m\in\mathbf{Z}$, $AWB \models \text{div}(b^m, b^n)$ ssi $m \mid n$. Nous en déduisons que $\langle <b>,e,b,.,^{-1},\text{div}\rangle$ est isomorphe à $\langle \mathbf{Z},0,1,+,-,\mid\rangle$, cette structure est définissable dans $\langle AWB,b\rangle$, et la théorie de AWB est donc indécidable.

Cas 2: $C_A(A)\neq\{e_A\}$. Soit $a\in C_A(A)\backslash\{e_A\}$. D'après le lemme 3, A^B et Div sont définissables dans $\langle AWB, \bar{a}\rangle$ et Div est compatible avec la relation d'équivalence associée au sous-groupe normal A^B. Soit div la relation quotient de Div définie sur $(AWB)/A^B$, et $\tilde{g}$ la classe d'un élément $g\in AWB$ dans ce groupe. $(AWB)/A^B \models \text{div}(\tilde{g},\tilde{g}')$ ssi $\tilde{g}'\in <\tilde{g}>$. $\tilde{b}$ est d'ordre infini, et comme dans le premier cas, on montre que $\langle <\tilde{b}>,e,b,.,^{-1},\text{div}\rangle$ est isomorphe à $\langle \mathbf{Z},0,1,+,-,\mid\rangle$, et cette structure est interprétable dans $\langle AWB,\bar{a},b\rangle$. La théorie de AWB est donc indécidable. □

Lemme 4: *Si $b\in B$ est d'ordre infini, alors $C_{AwB}(b)=C_B(b)$.*

Preuve: Il suffit de remarquer que, d'après le lemme 1 1), $\Phi_b\cap \overline{A^B}=\{e\}$; le résultat découle alors immédiatement du lemme 2. □

Lemme 5: *Soit $\varphi(x,y,z)$ la formule*

$\varphi(x,y,z)$: $\quad [y;z]=e \ \wedge\ (\exists u\ [x;u]=e \ \wedge\ [x;z]=[u;y])$.

Soient $a\in A\backslash\{e_A\}$ et $b\in B$ d'ordre infini. Pour tout $g\in AwB$, $AwB \models \varphi(\bar{a},b,g)$ ssi $g\in <b>$.

Preuve: Soit $n\in\mathbf{Z}$ et $g=b^n$. $[g;b]=e$, et il nous faut trouver $u_n\in \overline{A^B}$ tel que $[\bar{a};g]=[u_n;b]$. Si $n=0$, il suffit de prendre $u_0=e$.

Si $n>0$, définissons u_n par: $\quad u_n(b^i)=a$ si $i\in\{0,..,n-1\}$

$\qquad\qquad\qquad\qquad\quad u_n(x)=e_A$ sinon.

Si $n<0$. $\qquad\qquad\quad u_n(b^i)=a^{-1}$ si $i\in\{n,..,-1\}$

$\qquad\qquad\qquad\qquad\quad u_n(x)=e_A$ sinon.

Dans tous les cas, u_n est un élément de $\overline{A^B}$ et $[u;\bar{a}]=e$.

Si $n\neq 0$, pour tout $x\in B$, $[u_n;b](x)=u_n^{-1}(x).u_n(xb^{-1})$

$\qquad\qquad\qquad\qquad\qquad\qquad\quad =a^{-1}$ si $x=e$,

$\qquad\qquad\qquad\qquad\qquad\qquad\quad =a$ si $x=b^n=g$

On a donc $[u_n;b]=\bar{a}^{-1}b^{-n}\bar{a}\,b^n=[\bar{a};g]$.

Réciproquement, soit g tel que $AwB \models \varphi(\bar{a},b,g)$. $[b;g]=e$, et donc $g\in B$ d'après le lemme 4. Nous pouvons supposer que $g\neq e$. Soit $u\in AwB$ tel que $[\bar{a};u]=e$ et $[\bar{a};g]=[u;b]$. $u\in \overline{A^B}$ d'après le lemme 1 3), et pour tout $x\in B$, $[u;b](x)=(u(x))^{-1}u(xb^{-1})$; d'autre part,

$[\bar{a};g](x)=a^{-1}$ si $x=e_B$
$=a$ si $x=g$
$=e_A$ sinon.

Nous en déduisons:

$u(b^{-1})=u(e_B)a^{-1}$ (1)
$u(gb^{-1})=u(g)a$ (2)
$u(x)=u(xb^{-1})$ pour $x\notin\{e_B,g\}$ (3)

Si $g\notin<b>$, alors pour tout entier n non nul, $b^n\notin\{e_B,g\}$, et (3) implique $u(b^n)=u(b^{n-1})$. On en déduit par récurrence que, si $n>0$, $u(b^n)=u(e_B)$, et si $n<0$, $u(b^n)=u(b^{-1})$. b étant d'ordre infini et u ayant un support fini, il est nécessaire que $u(e_B)=u(b^{-1})=e_A$. (1) implique alors $a=e_A$, ce qui est contraire aux hypothèses. Nous avons donc $g\in<b>$. □

Preuve de l'indécidabilité de AwB:

D'après le lemme 5, si b est un élément d'ordre infini de B et a un élément de $A\backslash\{e_A\}$, $<b>$ est définissable dans $\langle AwB,\bar{a},b\rangle$. Soit div la relation binaire définie par

$div(y,z) \longleftrightarrow \varphi(\bar{a},y,z)$.

On constate que $\langle<b>,e,b,.,^{-1},div\rangle$ est isomorphe à $\langle\mathbf{Z},0,1,+,-,|\ \rangle$, et cette structure est interprétable dans $\langle AwB,\bar{a},b\rangle$. La théorie de AwB est donc indécidable. □

Corollaire : *Pour tout groupe A non trivial, et tout groupe ordonnable B non trivial, les théories des groupes AWB et AwB sont indécidables.*

Preuve: Un groupe ordonnable n'a, à part l'élément neutre, que des éléments d'ordre infini. □

Références

[B] G. Baumslag. *Wreath products and p-groups*. Proc. Cam. Philos. Soc. 55 (1959), pp 224-231.

[D] F. Delon. *Quelques propriétés des corps valués en Théorie des Modèles*. Thèse d'Etat, Université de Paris VII, Paris, 1982.

[G] A.M.N. Glass. *Ordered Permutation Groups*. London Math. Soc. Lecture Note Series 55.

[H1] M. Hall. *The Theory of Groups*.The Macmillan Company, New York 1959.

[H2] P. Hall. *Wreath powers and characteristically simple groups*. Proc. Camb. Philos. Soc. 58 (1962), pp 170-184.

[H3] P. Hall. *On non strictly simple groups*. Proc. Camb. Philos. Soc. 59 (1963), pp 531-553.

[Ho] W. Holland. *The Characterization Generalized Wreath Products*. Journal of Algebra 13 (1969) pp. 152-169.

[N] B.H. Neumann. *Embedding theorems for ordered groups*. Journal Lon. Math. Soc. 35 (1960), pp 503-512.

[R] R. Robinson. *Undecidable rings*. Trans. Amer. Math. Soc. 70 (1951), pp 137-159.

[S] D. Saracino. *Wreath products and existentially complete solvable groups*. Trans. Amer. Math. Soc. 197 (1974), pp 327-339.[Sc] E. Schenkman. *Group Theory*. Van Nostran, Princeton, New Jersey, 1965.

[Sc] E. Schenkman. *Group Theory*. Van Nostran, Princeton, New Jersey, 1965.

[Si] P. Simonetta. *Décidabilité et interprétabilité dans les corps et les groupes non commutatifs*. Thèse de Doctorat, Université de Paris VII, Paris 1994.

[T2] A Tarski. *Undecidability of group theory* (abstract). Jour. Symbolic Logic 14 (1949) p 76-77.

[W] B.A.F. Wehrfritz. *Infinite Linear Groups*. Springer-Verlag, Berlin Heidelberg New York 1973.

CNRS, URA 753
Université de Paris 7
2, Place Jussieu, Case 7012
75251 Paris Cedex 05

Adresse électronique : simbaud@logique.jussieu.fr

Le model-compagnon de la théorie des corps de différence

Zoé Chatzidakis, CNRS/Paris 7

Résultats algébriques

Rappelons qu'un anneau de différence est un anneau A, muni d'un monomorphisme $\sigma : A \to A$. Le langage dans lequel nous travaillons est celui des anneaux, augmenté d'un prédicat de fonction unaire pour σ. Les résultats que nous citons dans ce chapitre peuvent être trouvés dans le livre de Richard Cohn [C].

Si l'anneau A est intègre, σ se prolonge de façon unique au corps des fractions de A. Si A est un corps on parle de corps de différence.

Le monomorphisme σ n'est pas nécéssairement surjectif; cependant, tout anneau de différence a une extension dans laquelle σ est un automorphisme; de plus il y a une plus petite telle extension, dont nous donnons maintenant la construction.

Soit $A_{-1} = \{\tilde{a} \mid a \in A\}$ une copie isomorphe de (A, σ); on plonge A dans A_{-1} par $a \mapsto \widetilde{\sigma(a)}$; alors $(A, \sigma(A), \sigma) \simeq (A_{-1}, A, \sigma)$. De cette façon on construit un système inductif $(A_{-n}, \sigma))_{n \in \mathbb{N}}$ d'anneaux de différence avec $A_{-n+1} = \sigma(A_{-n})$. Si B est la limite inductive des A_{-n}, alors σ est un automorphisme de B.

A partir de maintenant, dans tous les corps de différence, σ est un automorphisme.

Soit K un corps de différence. On définit l'anneau de polynômes de différence sur K dans les variables $X_1, \ldots, X_n$, comme étant l'anneau de polynômes $K[X_1, \ldots, X_n, \sigma(X_1), \ldots, \sigma(X_n), \sigma^2(X_1), \ldots]$; l'action de σ étend celle sur K et envoie $\sigma^n(X_i)$ sur $\sigma^{i+1}(X_i)$. On dénote cet anneau de polynômes par $K\langle \bar{X} \rangle$.

Il y a une notion naturelle de σ-idéal: $I \subset K\langle \bar{X} \rangle$ est un σ-idéal si c'est un idéal clos par σ et σ^{-1}. Un σ-idéal correspond au noyau d'un homomorphisme de $K\langle \bar{X} \rangle$ dans un anneau de différence.

Attention: $K\langle \bar{X} \rangle$ n'est pas noethérien: soit I le σ-idéal engendré par $X\sigma(X), X\sigma^2(X), \ldots, X\sigma^n(X), \ldots$. Un σ-idéal I est parfait si tout élément a dont un produit de transformés est dans I, appartient lui-même à I; notons qu'un tel idéal est en particulier radiciel. Nous avons alors la condition de chaîne ascendante pour les σ-ideaux parfaits. Notons aussi que tout σ-idéal premier est parfait. Nous avons aussi que tout σ-idéal parfait est l'intersection des σ-idéaux premiers le contenant.

Soient $(F, \sigma) \subset (K, \sigma)$ des corps de différence, et a un uplet d'éléments de K. On dénote par $F(a)_\sigma$ le plus petit corps de différence contenant a, c'est à dire le coprs $F(\ldots, \sigma^{-1}(a), a, \sigma(a), \ldots)$. A a nous associons un σ-idéal $I(a/F) \subset F\langle \bar{X} \rangle$ de la manière naturelle, en définissant

$$I(a/F) = \{f \in F\langle \bar{X} \rangle \mid f(a) = 0\}.$$

Clairement, $I(a/F)$ est un σ-idéal premier.

Il se peut que $tr.deg(F(a)_\sigma/F)$ soit fini. Dans ce cas, pour n suffisamment grand, $F(a)_\sigma$ est une extension algébrique de $F(a, \sigma(a), \ldots, \sigma^n(a))$; pour $m \geq n$ les entiers $d_m =_{\text{df}} [F(a, \sigma(a), \ldots, \sigma^{m+1}(a)) : F(a, \sigma(a), \ldots, \sigma^m(a))]$ forment une suite décroissante, qui se

stabilise en un entier appelé le degré limite de $F(a)_\sigma$ sur F; ce degré limite est un invariant de l'extension $F(a)_\sigma/F$, i.e., il ne dépend pas des générateurs choisis.

De plus en caractéristique 0, une telle extension est en fait engendrée par un seul élément; en caractéristique positive, il faut faire attention aux extensions inséparables, cependant un résultat analogue existe.

Résultats de théorie des modèles

Les résultats de ce chapitre sont en partie dûs à L. van den Dries, A. Macintyre et C. Wood, mais n'ont jamais été publiés; les résultats concernant l'équivalence élémentaire et les types sont des traductions de démonstrations pour les corps PAC à notre contexte.

Nous voulons donner une axiomatisation de la théorie $ACFA$, modèle-compagnon de la théorie des corps de différence. Il s'agit d'exprimer que tout système d'équations et d'inéquations qui a une solution dans une extension a une solution.

Proposition 1. Soit $ACFA$ la théorie dont les modèles sont des structures (K, σ) satisfaisant:

(i) σ est un automorphisme de K.

(ii) K est algébriquement clos.

(iii) Si U est une varieté définie sur K, et $V \subset U \times \sigma(U)$ une varieté définie sur K telle que les projections de V sur U et $\sigma(U)$ sont denses dans U et $\sigma(U)$. Alors il existe $a \in U(K)$ tel que $(a, \sigma(a)) \in V$.

Alors $ACFA$ est le model-compagnon de la théorie des corps de différence.

Démonstration. Quelques mots d'abord sur les termes employés; une varieté est pour nous un ensemble algébrique (défini sur K) irréductible; la varieté $\sigma(U)$ est celle dont les points sont $\{\sigma(a) \mid a \in U\}$; $U(K)$ denote l'ensemble des points K-rationnels de U. Notons que ces proprietés sont expressibles dans notre langage, puisqu'elles sont essentiellement algébriques.

Nous allons d'abord montrer que les modèles de la théorie $ACFA$ sont existentiellement clos. Pour celà, notons d'abord que l'on peut éliminer les inéquations par l'astuce habituelle, et donc se ramener à la résolutions d'équations de la forme

$$f_1(x, \ldots, \sigma^k(x)) = \ldots = f_m(x, \ldots, \sigma^k(x)) = 0,$$

où $x = (x_1, \ldots, x_n)$, les polynômes f_i sont des polynômes à coefficients dans K, avec variables $x, \ldots, \sigma^k(x)$.

Soit L une extension de K dans laquelle ce système d'équations a une solution, a. Soient $U \subset \mathbf{A}^{kn}$ la varieté définie sur K dont $(a, \ldots, \sigma^{k-1}(a))$ est un point générique, et V celle dont $(a, \ldots, \sigma^{k-1}(a), \sigma(a), \ldots \sigma^k(a))$ est un point générique. Alors U et V satisfont les hypothèses de (iii), et donc il existe $b \in U(K)$ tel que $(b, \sigma(b)) \in V$: écrivons b comme $(c, \ldots, \sigma^{k-1}(c))$; alors c est l'élément cherché.

Montrons maintenant que tout corps de différence K se plonge dans un modèle de $ACFA$; les axiomes (i) et (ii) ne posent aucun problème, car tout automorphisme d'un corps s'étend en un automorphisme de sa clôture algébrique. Soient donc U et V comme dans (iii), avec K algébriquement clos, et a un point générique de U, b , et F la clôture algébrique de $K(a)$; puisque F est algébriquement clos et $tr.deg(F/K) = dim(U) =$

$dim(\sigma(U))$, nous pouvons trouver dans F un point b génerique de $\sigma(U)$ tel que $(a,b) \in V$; l'isomorphisme σ entre $K(a)$ et $K(b)$ (qui prolonge σ et envoie a sur b) s'étend alors à F.

Proposition 2. Soit $K \models ACFA$, F le sous-corps de K fixé par σ. Alors F est pseudo-fini.

Démonstration. Il est clair que F est parfait; de plus il est PAC: si la varieté U est définie sur F, alors $U = \sigma(U)$ et nous pouvons prendre pour V la varieté diagonale. Il reste maintenant à montrer que F a exactement une extension algébrique de chaque degré. Notons F^{alg} la clôture algébrique de F; alors $\sigma(F^{alg}) = F^{alg}$, et donc $Gal((F^{alg}/F)$ est engendré par σ; F a donc au plus une extension de chaque degré; pour montrer qu'il en a une, notons que le système

$$\sigma^n(x) = x,\ x \neq \sigma(x),\ \ldots\ , x \neq \sigma^{n-1}(x)$$

a une solution dans une extension de K, et donc dans K.

Proposition 3. Soient (K,σ_1), (L,σ_2) deux modèles de $ACFA$, contenant un sous-corps de différence (E,σ) qui est algébriquement clos. Alors

$$(K,\sigma_1) \equiv_E (L,\sigma_2).$$

Démonstration. On peut supposer K et L $|E|^+$-saturés de même cardinalité. Par un argument de va-et-vient il suffit de montrer que pour tout (élément) $a \in K$ il existe $b \in L$ et un E-isomorphisme $\varphi : E(a)^{alg}_{\sigma_1} \to E(b)^{alg}_{\sigma_2}$ qui envoie a sur b.

Soit Δ le diagramme sans quantificateurs de $E(a)^{alg}_{\sigma_1}$, avec les variables x_α, $\alpha \in E(a)^{alg}_{\sigma_1}$. Remplaçant L par une copie E-isomorphe s'il le faut, nous pouvons supposer que L et K sont linéairement disjoints au-dessus de E. Soit M le corps composite de L et $E(a)^{alg}_{\sigma_1}$: c'est le corps de fractions de $E(a)^{alg}_{\sigma_1} \bigotimes_E L$. Définissons τ sur L' en posant $\tau(c \otimes d) = \sigma_1(c) \otimes \sigma_2(d)$; τ prolonge σ_1, σ_2, et s'étend en un automorphisme de M^{alg}.

Puisque $ACFA$ est modèle complète, celà implique que $\mathrm{Th}(L,\sigma_2,c)_{c\in E} \cup \Delta$ est consistent; par saturation, Δ est réalisé dans L, par (b_α); définissons $\varphi : E(a)^{alg}_{\sigma_1}$ par $\alpha \mapsto b_\alpha$.

Ce résultat a bien sûr plusieurs corollaires:

Corollaire 1. Soient (K,σ_1), (L,σ_2) deux modèles de $ACFA$ de même caractéristique, et k la clôture algébrique du sous-corps premier. Alors

$$(K,\sigma_1) \equiv (L,\sigma_2) \quad \Longleftrightarrow \quad (k,\sigma_1|_k) \simeq (k,\sigma_2|_k).$$

Corollaire 2. Soit $K \models ACFA$, E un sous-corps de K et a, b des uplets. Alors $tp(a/E) = tp(b/E)$ si et seulement s'il existe un E-isomorphisme $\varphi : E(a)^{alg}_{\sigma} \to E(b)^{alg}_{\sigma}$ qui envoie a sur b.

Corollaire 3. Les notions algébrique et modèle-théorique de clôture algébrique d'un corps de différence coïncident.

Démonstration. Soit E un sous-corps de différence de $K \models ACFA$, et supposons le E algébriquement clos en tant que corps. Il nous faut montrer que si $a \in K \setminus E$ alors

$tp(a/E)$ a une infinité de réalisations. Soit $F = E(a)_\sigma^{alg}$, et soit (F', σ') une copie de (F, σ), linéairement disjointe de K au-dessus de E. Procédant de même que dans la démonstration de la Proposition 3, on étend σ et σ' en un automorphime τ de la clôture algébrique M du corps composite de K et F'. Puis l'on plonge M dans un modèle L de $ACFA$. On a alors $K \prec L$, et $L \setminus K$ contient une réalisation de $tp(a/E)$. Ce qui montre bien que $tp(a/E)$ peut être réalisé une infinité de fois dans un modèle suffisamment saturé.

Bibliographie

[C] R.M. Cohn, Difference algebra, Tracts in Mathematics 17, Interscience Pub. 1965.

CNRS, URA 753
Université de Paris 7
2, Place Jussieu, Case 7012
75251 Paris Cedex 05

Adresse électronique : zoe@logique.jussieu.fr

Le groupe des automorphismes du corps des complexes laissant les nombres algébriques fixes est simple.

Daniel Lascar

Janvier 1994

1 Introduction

Cet exposé reprend certains résultats de l'article "les automorphismes d'un ensemble fortement minimal" [1]. Dans cet article, on démontre, entre autres, que le groupe d'automorphismes d'une structure fortement minimale, saturée et dénombrable est "presque" simple (on verra plus loin le sens exact de ce "presque"). Le cas des corps algébriquement clos de caractéristique 0 est particulièrement intéressant. Le résultat peut se généraliser au cas non dénombrable, ce qui permet d'obtenir le théorème suivant :

Théorème 1 *Le groupe des automorphismes de $\mathbb{C}$ laissant fixes tous les nombres algébriques est simple.*

(Ici $\mathbb{C}$ désigne le corps des nombres complexes.)

Dans l'article mentionné plus haut, on annonce ce résultat à l'aide de l'hypothèse du continu. Un des buts de cet exposé est de montrer que, en fait, l'hypothèse du continu est inutile. Un autre but est d'en présenter la preuve sans jamais faire référence à des notions de théorie des modèles, afin qu'elle soit immédiatemnt compréhensible pour quiconque connaît un peu d'algèbre. Cependant, cette preuve sera écrite de façon à pouvoir aussi être lue comme une preuve du théorème 10 (voir plus loin) qui affirme que le groupe des automorphismes d'une structure fortement minimale et saturée (quelque soit sa cardinalité) est "presque simple".

On commence par introduire quelques notations :

- κ désigne la cardinalité de $\mathbb{C}$ ($\kappa = 2^{\aleph_0}$) ;
- G désigne le groupe des automorphismes de $\mathbb{C}$ laissant fixes les nombres algébriques ;
- Ω désigne l'ensemble des sous-corps algébriquement clos de $\mathbb{C}$ qui sont de cardinalité strictement inférieure à κ ;

• si $K \in \Omega$, G_K désigne le groupe des automorphismes de K laissant les nombres algébriques fixes, et $Aut_K(\mathbb{C})$ désigne le groupe des automorphismes de $\mathbb{C}$ laissant les points de K fixes.

Définition 2 *Soit $g \in G$. On dit que g est borné s'il existe $K \in \Omega$ tel que pour tout $a \in \mathbb{C}$, $g(a)$ est algébrique sur $K \cup \{a\}$.*

On remarque que les automorphismes bornés forment un sous-groupe normal de G, et si g est borné et que le corps K est comme dans la définition 2, alors le corps K est laissé globalement fixe par g ce qui s'écrit $g[K] = K$).

Le théorème 1 découle immédiatement des deux propositions suivantes :

Proposition 3 *Soit g un élément non borné dans G. Alors :*

$$G = g^G \circ (g^{-1})^G \circ (g^{-1}) \circ g^G.$$

(g^G désigne l'ensemble $\{h^{-1}gh \ ; \ h \in G\}$)

Proposition 4 *L'identité est le seul élément borné dans G.*

2 Preuve de la proposition 3

On va montrer la proposition 3. Pour toute cette preuve, on fixe un automorphisme g de G non borné. On a besoin maintenant de quelques notations supplémentaires.

• χ désigne l'application de $G \times G$ dans G qui à (h, k) fait correspondre $h^{-1} \circ g \circ k^{-1} \circ g^{-1} \circ k \circ h$. On voit que $\chi(h, g) \in g^G \circ (g^{-1})^G$.

• si $K \in \Omega$, χ_K désigne l'application de $G_K \times G_K$ qui à (h, k) fait correspondre $h^{-1} \circ g \circ k^{-1} \circ g^{-1} \circ k \circ h$ (autrement dit, χ_K est la restriction de χ à $G_K \times G_K$).

L'essentiel de la démonstration est contenu dans le lemme suivant :

Lemme 5 *Soit $K \in \Omega$, h, k appartenant à G_K , $K' \in \Omega$ et $f \in G_{K'}$. On suppose que $K \subset K'$ et que f prolonge $\chi_K(h, k)$. Alors il existe h' et k' dans G tel que $\chi(h', k')$ prolonge f.*

On aura besoin des deux sous-lemmes suivants. Ici et plus loin, indépendants veut dire algébriquement indépendants et la dimension est la cardinalité d'une base de transcendance.

Sous-lemme 6 *Supposons que K_0 , K_1 et K_2 soient trois éléments de Ω, que $K_0 \subset K_1$, que $K_0 \subset K_2$ et que K_1 et K_2 sont indépendants au dessus de K_0. On suppose de plus que $h_1 \in G_{K_1}$ que $h_2 \in G_{K_2}$, que $h_1 \mid K_0 = h_2 \mid K_0 = h$. Alors il existe un automorphisme h dans G prolongeant à la fois h_1 et h_2.*

Preuve : Soit K le corps engendré par $K_1 \cup K_2$. Considérons l'application h de K dans K définie de la façon suivante : tout élément b de K peut s'écrire $R(\overline{b_0}, \overline{b_1}, \overline{b_2})$, où R est une fraction rationnelle à coefficients entiers, $\overline{b_0}$ une suite d'éléments de K_0, $\overline{b_1}$ une suite d'éléments de $K_1 - K_0$, et $\overline{b_2}$ une suite d'éléments de $K_2 - K_0$. On pose : $h(b) = R(h_0(\overline{b_0}), h_1(\overline{b_1}), h_2(\overline{b_2}))$. On vérifie alors que l'application h est bien définie ($h(b)$ ne dépend pas de la représentation $R(\overline{b_0}, \overline{b_1}, \overline{b_2})$ choisie) et que c'est un automorphisme de K qui se laisse prolonger sans peine à $\mathbb{C}$ tout entier.
♡

Sous-lemme 7 *Soit $K \in \Omega$ tel que $g[K] = K$ et λ un cardinal inférieur ou égal à κ. Alors il existe $K_1 \in \Omega$, $K \subset K_1$ tel que K_1 et $g[K_1]$ soient indépendants au dessus de K et $\dim(K_1/K) = \lambda$.*

Preuve : On construit par induction une suite $(a_i \, ; \, i \in \lambda)$ de points de $\mathbb{C}$ de telle sorte que, pour tout $i \in \lambda$, $g(a_i)$ ne soit pas algébrique sur $K(\{g(a_j) \, ; \, j < i\} \cup \{a_j : j \leq i\})$. Ceci est possible parce que g n'est pas borné.
♡

Nous attaquons maintenant la démonstration du lemme 5.

Preuve : On peut trouver $h_1 \in G$ étendant h et laissant K' globalement fixe. Posons $h_2 = h_1 \mid K'$. Plutôt que de construire h' et k' prolongeant respectivement h et k et appartenant à G tels que :

(1) $\quad h'^{-1} \circ g \circ k'^{-1} \circ g^{-1} \circ k' \circ h'$ prolonge f

on construira $a \in Aut_K(\mathbb{C})$ et k' prolongeant k tels que :

(2) $\quad a^{-1} \circ g \circ k'^{-1} \circ g^{-1} \circ k' \circ a$ prolonge $h_2 \circ f \circ h_2^{-1}$.

(Il suffira alors de prendre $h' = a \circ h_1$). D'après le sous-lemme 7, il existe $K_0 \in \Omega$ tel que $\dim(K_0/K) = \dim(K'/K)$ et tel que K_0 et $K_1 = g[K_0]$ soient indépendants au dessus de K. On choisit $a \in Aut_K(\mathbb{C})$ de sorte que $a[K'] = K_1$. Soit $f_1 \in G_{K_1}$ l'application $a \circ h_2 \circ f \circ h_2^{-1} \circ a^{-1}$ (il faudrait plutôt écrire $f_1 = (a \mid K') \circ h_2 \circ f \circ h_2^{-1} \circ (a \mid K')^{-1}$).

Il nous faut donc maintenant trouver $k' \in G$ prolongeant k tel que

(3) $\quad g \circ k'^{-1} \circ g^{-1} \circ k'$ prolonge f_1.

Soit $k_1 \in G_{K_1}$ prolongeant k et $k_0 \in G_{K_0}$ prolongeant $g^{-1} \circ f_1 \circ k_1^{-1} \circ g$ (ou, plus exactement prolongeant $(g \mid K_0)^{-1} \circ f_1 \circ k_1^{-1} \circ (g \mid K_0)$), de sorte que $g \circ k_0 \circ g^{-1}$ est égal à $f_1 \circ k_1^{-1}$. On remarque alors que $k_0 \mid K = k$ (parce que f_1 prolonge $g \circ k^{-1} \circ g^{-1} \circ k$). On utilise alors le sous-lemme 6 qui nous dit qu'il existe $k' \in G$ prolongeant simultanément k_0 et k_1. Alors $g \circ k'^{-1} \circ g^{-1} \circ k'$ prolonge $g \circ k_0^{-1} \circ g^{-1} \circ k_1 = f_1$.
♡

Modifions légèrement le lemme 5

Lemme 8 *Soit $K \in \Omega$, h et k appartenant à G_K, $K' \in \Omega$, $f \in G$ et $b \in G_{K'}$. On suppose que $K \subset K'$ et que b prolonge $\wr_K(h, k)$. Alors il existe $K_1 \in \Omega$, h_1 et k_1 dans G_{K_1} tels que $K' \subset K_1$, $g[K_1] = K_1 = f[K_1]$, $card(K_1) = card(K')$ et $\wr_{K_1}(h_1, k_1)$ prolonge b.*

Preuve : On construit d'abord des automorphismes h' et k' comme dans le lemme précédent, puis, à l'aide d'un raisonnement du type Löwenheim-Skolem, on trouve un sous-corps K_1 de $\mathbb{C}$ tel que $K' \subset K_1$, $g[K_1] = K_1$, $f[K_1] = K_1$ et $card(K_1) = card(K')$ et il suffit alors de poser $h_1 = h' \mid K_1$ et $k_1 = k' \mid K_1$.
♡

Soit $f \in G$. On va montrer qu'il existe h_*, k_*, h'_*, et k'_* tels que $\chi(h_*, k_*) \circ (\chi(h'_*, k'_*))^{-1} = f$. Le lemme qui suit constitue un premier pas.

Lemme 9 *Soit $K \in \Omega$, h , k , h' , k' appartenant à G_K , $a \in \mathbb{C}$ et on suppose que f prolonge $\chi_K(h, k) \circ (\chi(h', k'))^{-1}$. Alors il existe $K_1 \in \Omega$ et h_1, k_1, h'_1, k'_1 appartenant à G_{K_1} prolongeant h, k, h', k' respectivement tels que $g[K_1] = K_1$, $card(K_1) = card(K)$ et f prolonge $\chi_{K_1}(h_1, k_1) \circ (\chi_{K_1}(h'_1, k'_1))^{-1}$.*

Preuve : On commence par choisir $K^1 \in \Omega$ tel que $card(K^1) = card(K)$, $a \in K^1$, $g[K^1] = K^1$ et $f[K^1] = K^1$. Soit h'^1 et k'^1 appartenant à G_{K^1} prolongeant respectivement h' et k'. On voit alors que $(f \mid K^1) \circ \chi_{K^1}(h'^1, k'^1)$ prolonge $\chi_K(h, k)$. Grâce au lemme 8, on trouve $K^2 \in \Omega$ tel que $card(K^2) = card(K)$, $g[K^2] = K^2$, $f[K^2] = K^2$ et h^2 et k^2 appartenant à G_{K^2} prolongeant respectivement h et k tels que $\chi_{K^2}(h^2, k^2)$ prolonge $(f \mid K^1) \circ \chi_{K^1}(h'^1, k'^1)$. Autrement dit $(f \mid K^2)^{-1} \circ \chi_{K^2}(h^2, k^2)$ prolonge $\chi_{K^1}(h'^1, k'^1)$. On utilise encore le lemme, et on trouve $K^3 \in \Omega$ tel que $card(K^3) = card(K)$, $g[K^3] = K^3$, $f[K^3] = K^3$ et h'^3 et k'^3 appartenant à G_{K^3} prolongeant respectivement h'^1 et k'^1 tels que $\chi_{K^3}(h'^3, k'^3)$ prolonge $(f \mid K^2) \circ \chi_{K^2}(h^2, k^2)$. Maintenant, c'est $(f \mid K^3) \circ \chi_{K^3}(h'^3, k'^3)$ qui prolonge $\chi_{K^2}(h^2, k^2)$ et on construit ainsi une suite croissante $(K^i \,;\, i \in \omega)$ d'éléments de Ω et des suites croissantes $(h^i \,;\, i \in \Omega, i \text{ pair})$, $(k^i \,;\, i \in \Omega, i \text{ pair})$, $(h^i \,;\, i \in \Omega, i \text{ impair})$, $(k'^i \,;\, i \in \Omega, i \text{ impair})$ de sorte qu'en posant $K_1 = \bigcup_{i \in \omega} K^i$, $h_1 = \bigcup_{i \in \omega} h^{2i}$, $k_1 = \bigcup_{i \in \omega} k^{2i}$, $h'_1 = \bigcup_{i \in \omega} h'^{2i+1}$, $k'_1 = \bigcup_{i \in \omega} k'^{2i+1}$, on obtienne bien ce que l'on voulait.
♡

On peut maintenant terminer la preuve de la proposition 3. On énumère $\mathbb{C}$: $\mathbb{C} = \{a_\alpha \,;\, \alpha \in \kappa\}$, on construit par induction des suites croissantes $(K_\alpha \,;\, \alpha \in \kappa)$ d'éléments de Ω, $(h_\alpha \,;\, \alpha \in \kappa)$, $(k_\alpha \,;\, \alpha \in \kappa)$, $(h'_\alpha \,;\, \alpha \in \kappa)$, $(k'_\alpha \,;\, \alpha \in \kappa)$ d'éléments de G_{K_α}, telles que, pour tout $\alpha \in \kappa$, $f[K_\alpha] = K_\alpha$, $g[K_\alpha] = K_\alpha$, $a_\alpha \in K_\alpha$ et f prolonge $\chi_{K_\alpha}(h_\alpha, k_\alpha) \circ (\chi(h'_\alpha, k'_\alpha))^{-1}$. On démarre avec K_0 égal au corps des nombres algébriques et h_0, k_0, h'_0, k'_0 égaux à l'identité sur K_0 ; les autres étapes sont résolues grâce au lemme 9, et il suffit de poser $h_* = \bigcup_{\alpha \in \kappa} h_\alpha$, $k_* = \bigcup_{\alpha \in \kappa} k_\alpha$, $h'_* = \bigcup_{\alpha \in \kappa} h'_\alpha$, $k'_* = \bigcup_{\alpha \in \kappa} k'_\alpha$.
♡

3 Preuve de la proposition 4

Une preuve de la proposition 4 est donnée dans [1]. M. Ziegler a en a donné une autre qui fonctionne aussi si la caractéristique n'est pas nulle. On va en

donner une troisième, complètement élémentaire et qui se généralise facilement à la caractéristique non nulle.

Soit g un automorphisme borné, soit K appartenant à Ω tel que, pour tout $a \in \mathbb{C}$, $g(a)$ est algébrique sur $K(a)$.

Supposons momentanément que, pour un point $a \in \mathbb{C} - K$, $g(a) = a$. On va montrer que cela entraîne que g est l'identité. Soit b un autre point de $\mathbb{C}$ non algébrique sur $K(a)$. Alors $g(b)$ est algébrique sur $K(b)$, et il en est de même de $g(b) - b$. Par ailleurs, $g(a + b) = a + g(b)$, et donc, $a + g(b)$ est algébrique sur $K(a+b)$, de même que $a+g(b)-(a+b) = g(b)-b$. On voit donc que $g(b)-b$ doit être algébrique sur $K(b)$ et sur $K(a + b)$, donc doit appartenir à K, puisque b et $a+b$ sont algébriquement indépendants au dessus de K. Posons $c = g(b)-b$. Pour la même raison, $g(ab) - ab$ doit appartenir à K. Or $g(ab) = g(a)g(b) = ab + ac$. On en déduit que ac appartient à K, ce qui n'est possible que si $c = 0$. Il en découle que g est égal à l'identité sur le complémentaire de K, donc sur $\mathbb{C}$ tout entier.

Revenons au cas général. Soit a n'appartenant pas à K. Posons $a' = g(a)$, Soit $P(X, X')$ un polynôme à coefficients dans K tel que $P(a, a') = 0$ et de degré minimum; on voit aussi que $P(a, X')$ est le polynôme à coefficient dans $K(a)$ de degré minimum annulé par a'. On remarque que si c n'appartient pas à K et si c' est tel que $P(c, c') = 0$, alors il existe un K-automorphisme de $\mathbb{C}$ qui envoie a en c et a' en c'. Nous allons montrer que $P(a, X') = 0$ n'a qu'une seule solution dans $\mathbb{C}$.

En effet, soit b un autre point de $\mathbb{C}$, non algébrique sur $K(a)$ et K_1 la clôture algébrique de $K(b)$. Le polynôme $P(a, X')$ reste de degré minimum parmi tous les polynômes à coefficients dans K_1 qui sont annulés par a'. Donc si pour $a'' \in \mathbb{C}$, on a aussi $P(a, a'') = 0$, alors il existe un K_1−automorphisme f de $\mathbb{C}$ laissant a fixe et envoyant a' en a''. On voit alors que l'automorphisme $h = g^{-1} \circ f \circ g \circ f^{-1}$ laisse b fixe et envoie a' en a'' et est tel que, pour tout $c \in \mathbb{C}$, $h(c)$ est algébrique sur $K(c)$, ce qui n'est possible, d'après ce qui vient d'être dit, que si $a' = a''$.

Cela montre que le degré de P en X' est égal à 1 (en caractéristique non nulle, il faudrait faire preuve d'un peu plus de finesse). Pour la même raison, son degré en X doit être aussi 1. Autrement dit, $g(a) = \alpha a + \beta$, pour des points α et β de K. En appliquant le même raisonnement à a^2 et à $a + 1$, on voit qu'il existe γ, δ et ϵ dans K tels que $g(a^2) = \gamma a^2 + \delta = \alpha^2 a^2 + 2\alpha a\beta + \beta^2$ et $g(a + 1) = \alpha a + 1 = \epsilon(a + 1)$; ceci n'est possible que si $\alpha = 1$ et $\beta = 0$. Il en découle facilement que g est l'identité.

♡

4 Le coin des théoriciens des modèles.

La proposition que l'on vient de montrer n'est qu'un cas particulier d'un théorème plus général portant sur le groupe d'automorphismes d'une structure fortement

minimale non dénombrable. Le cas dénombrable est traité dans [1]. Supposons maintenant que C soit une structure fortement minimale de cardinalité κ non dénombrable. Soit Ω la classe des sous-ensembles de C^{eq}, algébriquement clos et de cardinalité inférieure à κ. Pour ces structures, il existe des notions d'algébricité, d'indépendance et de dimension. La définition 2 a donc un sens. On notera G le groupe des automorphismes forts de C. La proposition 4 n'est plus vraie en général ; appelons B le sous-groupe normal de G constitué des automorphismes forts et bornés de C (en fait, si C est localement modulaire, B n'est pas trivial, voir [1]). La proposition 3 donne :

Théorème 10 : *Le groupe quotient G/B est simple.*

Il ne faut que peu de changements à la démonstration que nous avons donnée de la proposition 3 pour en faire une démonstration du théorème 10. Posons encore $\kappa = card(C)$. Le seul point qu'il faille modifier est la preuve du sous-lemme 6. Mais ce lemme est précisément la propriété d'amalgamation pour les automorphismes qui est démontrée pour les structures stables dans [2].

References

[1] DANIEL LASCAR, *Les automorphismes d'un ensemble fortement minimal*, **JSL** Vol.57, Number 1, March 1992, pp 238-251.

[2] DANIEL LASCAR, *Autour de la propriété du petit indice*, **Proceedings of the London Mathematical Society,** Ser. 3 Vol. 62.(1991), pp 25-53.

Daniel Lascar, CNRS, URA 753
Université Paris 7
2 Place Jussieu, Tour 45-55, 5ème étage
75 251 Paris Cedex 05
Adresse électronique : lascar@logique.jussieu.fr

Présentation de la Méthode de Décomposition Cylindrique de Collins

Pierre Jumpertz

La méthode de Collins [Col] a ouvert la voie à l'étude calculatoire des corps réels clos. De nombreuses méthodes de calculs effectifs ont été proposées, arrivant aux bornes de la complexité théorique, mais qui ne changent pas la structure de décision des formules qui reste celle de Collins. Cet article se propose d'analyser la méthode de Collins plutôt d'un point de vue logique, en montrant l'utilisation d'ensembles, définissables dans la théorie, qui ont vis-à-vis d'une classe de formules un comportement "uniforme", et en analysant l'aspect cylindrique de la décomposition.

1. langage et formule

Soit L le langage des anneaux ordonnés : $L = \{1, 0, +, -, \cdot, <, =\}$
Les formules sans quantificateur sont des combinaisons booléennes d'équations ou d'inéquations polynômiales dans $Z[\overline{X}]$ (ou $\overline{X}=(X_1,\ldots,X_n)$).
On considère la théorie $\mathcal{T}$ des corps réels clos, corps commutatifs, ordonnés, avec le schéma d'axiome de la valeur intermédiaire :

pour chaque polynôme P de $Z[X]$, on a $\forall a\, \forall b\, \exists c \left[\begin{array}{c}(P(a)<0)\wedge(0<P(b))\\ \wedge\,(a<b)\end{array}\right] \rightarrow \left[\begin{array}{c}(P(c)=0)\\ \wedge\,(a<c)\wedge(c<b)\end{array}\right]$

$\mathbb{R}$ est un modèle de cette théorie...De nombreuses situations géométriques sont exprimables et des problèmes de nature topologique peuvent être traités [S&S], [BCR].

Cette théorie $\mathcal{T}$ est complète (pour chaque formule close, soit elle-même, soit sa négation est prouvable). La théorie $\mathcal{T}$ est décidable (il existe des méthodes effectives pour déterminer si une formule close est vraie ou non) : elle admet une élimination effective des quantificateurs, c'est-à-dire que toute formule est équivalente modulo $\mathcal{T}$ à une formule sans quantificateur avec les mêmes variables libres [Tar], [Col].

définition : un ensemble semi-algébrique est un ensemble S (de $\mathbb{R}^n$) défini par une formule Φ de L.

ex : "$X^2+Y^2<1$" définit le disque de centre 0 et rayon 1
"$\exists$ X tq $XY-1=0$" définit la projection des branches d'hyperbole...

Le semi-algébrique associé à une équation est l'ensemble de ses solutions, à une inéquation, l'ensemble de ses solutions dans $\mathbb{R}^n$. Les ensembles semi-algébriques sont liés par les opérations ensemblistes

usuelles qui correspondent aux connecteurs, ainsi $\wedge$ et $\cap$, $\vee$ et $\cup$, $\neg$ et comp. (le complémentaire), se correspondent-ils. On obtient, dans les semi-algébriques, une structure d'algèbre de Boole qui correspond à la structure des formules.

Les quantificateurs sont liés à des opérations de projection. La quantification existentielle est une projection ($\exists x : pr_x$), on obtient la quantification universelle d'une formule Φ par complémentaire de la projection de la négation de Φ.

définition : une cellule est un ensemble semi-algébrique non vide et connexe[1].

2. décisions de formules et décompositions

On veut pouvoir décider si des formules sont prouvables dans la théorie, ou trouver des expressions sans quantificateur équivalentes à ces formules.

définition : une decomposition d'un espace[2] $\mathbb{R}^n$ pour un ensemble S de formules de L (ayant au plus n variables libres) est un ensemble de formules Δ de L :

- sans quantificateur, avec comme variables libres uniquement celles qui apparaissent dans S,
- qui définissent des semi-algébriques non vides,
- telles que pour toute formule Φ de S , si Φ est satisfaisable modulo $\mathcal{T}$ alors il existe une formule δ de la décomposition Δ telle qu'un point satisfaisant cette formule δ satisfasse[3] aussi Φ,
- qui sont "uniformes" : tous les points qui satisfont une même formule de Δ satisfont[4] les mêmes formules de S.

On dira, de plus, que la decomposition est cylindrique pour un certain ordre des variables $x_0 \ldots x_n$ si :

- elle induit une suite de décompositions Δ_0 de $\mathbb{R}, \ldots, \Delta_n$ de $\mathbb{R}^{n+1}$ telle que :

pour chaque $j \geq 1$ et pour chaque ensemble semi-algébrique D de la décomposition Δ_j de $\mathbb{R}^{j+1}$, l'ensemble $pr_{x_j}(D)$ et $pr_{x_j}(\text{comp.}D)$ soient des ensembles de la décomposition Δ_{j-1} de $\mathbb{R}^j$.

remarque : une décomposition de $\mathbb{R}$ est cylindrique.

exemple 1 : une decomposition de $\mathbb{R}$ pour $S=\{x^2-1>0; (x-1)(x-3)=0\}$ est $\Delta=\{-1<x ; x=-1 ; -1<x \wedge x<1 ; x=1 ; 1<x \wedge x<3 ; x=3 ; 3<x\}$

On sait établir une decomposition pour un ensemble d'equations ou d'inequations polynômiales en une seule variable, si l'on sait établir une décomposition pour chacun des polynômes, et si l'on sait déterminer les racines communes (par le calcul du pgcd) de tout couple de polynômes.

---

[1] La définition diffère de celle de Collins pour s'attacher à ce qui fonde les résultats (en particulier pour la détermination des signes)

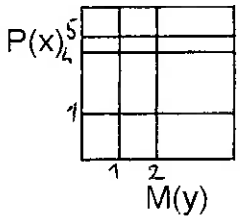
[2] On se place dans le cas le plus simple, mais bien sûr on peut ne décomposer qu'une partie semi-algébrique de l'espace $\mathbb{R}^n$ (les formules de S sont alors interprétées d'une façon restrictive)

[3] On peut dire que la décomposition "couvre toutes les situations". Ce qui peut se faire par partition de l'espace [Col] ou par le choix judicieux de points algébriques [BKR] ou par la projection des points extrêmes de toutes les composantes connexes [HRS],[Ren]

[4] Pour toute formule δ de la décomposition Δ, δ définissant un ensemble semi algébrique D, et pour toute formule Φ de S, on a : tous les points de D satisfont Φ ou tous les points de D satisfont $\neg\Phi$

exemple 2 : une décomposition de $\mathbb{R}^2$ pour $S=\{x=y^2\}$ est $\Delta=\{ x<y^2 , x=y^2 , x>y^2 \}$

exemple 3 : une décomposition de $\mathbb{R}^2$ pour $S=\{(x-1)(x-4)(x-5)=0 ; (y-1)(y-2)=0\}$ est obtenue par produit cartesien des deux décompositions de $\mathbb{R}$ $\{ x<1 ; x=1 ; 1<x \wedge x<4 ; x=4 ; 4<x \wedge x<5 ; x=5 ; 5<x \}$ et $\{ y<1 ; y=1 ; 1<y \wedge y<2 ; y=2 ; 2<y \}$:



$\Delta=\{ x<1 \wedge y<1, x=1 \wedge y<1, 1<x \wedge x<4 \wedge y<1, x=4 \wedge y<1, 4<x \wedge x<5 \wedge y<1, x=5 \wedge y<1, 5<x \wedge y<1 ,$
$x<1 \wedge y=1, x=1 \wedge y=1, 1<x \wedge x<4 \wedge y=1, x=4 \wedge y=1, 4<x \wedge x<5 \wedge y=1, x=5 \wedge y=1, 5<x \wedge y=1 ,$
$x<1 \wedge 1<y \wedge y<2, x=1 \wedge 1<y \wedge y<2, 1<x \wedge x<4 \wedge 1<y \wedge y<2, x=4 \wedge 1<y \wedge y<2, 4<x \wedge x<5 \wedge 1<y \wedge y<2,$
$x=5 \wedge 1<y \wedge y<2, 5<x \wedge 1<y \wedge y<2.$
$x<1 \wedge y=2, x=1 \wedge y<2, 1<x \wedge x<4 \wedge y=2, x=4 \wedge y=2, 4<x \wedge x<5 \wedge y=2, x=5 \wedge y=2, 5<x \wedge y=2 ,$
$x<1 \wedge 2<y, x=1 \wedge 2<y, 1<x \wedge x<4 \wedge 2<y, x=4 \wedge 2<y, 4<x \wedge x<5 \wedge 2<y, x=5 \wedge 2<y, 5<x \wedge 2<y \}$

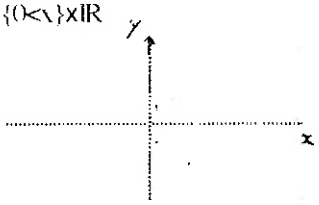
Cette décomposition est cylindrique quelque soit l'ordre sur $\{x,y\}$.

Si l'on a deux décompositions pour deux ensembles de formules $\mathcal{A}$ et $\mathcal{B}$ qui définissent deux ensembles de polynômes qui n'ont pas de variables communes, on obtient une décomposition pour $\mathcal{A} \cup \mathcal{B}$ par le produit cartesien des deux décompositions.

exemple 4 : une décomposition cylindrique de $\mathbb{R}^2$ pour $S=\{x=y^2\}$ selon l'ordre des variables x,y est :

$\Delta=\{ x<0 , (x=0) \wedge (0<y), (x=0) \wedge (0=y), (x=0) \wedge (0<y), (0<x) \wedge (0<y) \wedge (x<y^2),$
$(0<x) \wedge (0<y) \wedge (x=y^2), (0<x) \wedge (x>y^2), (0<x) \wedge (y<0) \wedge (x<y^2), (0<x) \wedge (y<0) \wedge (x<y^2) \}$

la décomposition de $\mathbb{R}$ pour $\{x<0; x=0; 0<x\}$ définit des "cylindres" de $\mathbb{R}^2$: $\{x<0\}x\mathbb{R}$; $\{x=0\}x\mathbb{R}$; $\{0<x\}x\mathbb{R}$



Pour faire une décomposition cylindrique pour S, un ensemble de formules, il suffit de pouvoir définir des cylindres où le nombre de racines est constant pour chaque polynôme apparaissant dans S, et où le nombre de racines communes pour chaque couple de polynômes est aussi constant. On se ramène à une situation "analogue" au produit cartesien, mais la decomposition dépend du cylindre et les fonctions qui définissent les "tranches" ne sont plus constantes.

Une décomposition est interessante pour décider simultanement tout un ensemble de formules.

Pour S un ensemble fini de formules de L_r sans quantificateur, on cherche une décomposition pour S_0 l'ensemble des formules obtenues de la façon suivante : $\bigcap_{\Phi_i \in I} \Phi_i \cap \bigcap_{\Phi_i \notin I} \neg\Phi_i$, pour chaque partition en deux

classes (1, 1') de l'ensemble de formule S.

proposition :
si Δ est une décomposition pour (S_0) alors Δ est une décomposition pour (S) et même une décomposition de (S'), l'ensemble de toutes les combinaisons booléennes des formules de S.
De plus si l'on fixe un certain ordre des variables et que la décomposition pour (S_0) est cylindrique alors on obtient une décomposition cylindrique selon le même ordre des variables pour S et S'.

Une décomposition permet de déterminer l'ensemble des formules satisfaites (qui sont satisfaites pour tous les ensembles semi-algébriques définis par la décomposition) ou de déterminer les ensembles semi-algébriques où les formules sont vraies. Si la décomposition est cylindrique, on vérifie la validité des quantifications d'une formule, en regardant l'agencement cylindrique des semi-algébriques où cette formule est vraie. On peut ainsi trouver une expression sans quantificateur équivalente à la formule de départ.
exemple : "$\exists x\ x^2+bx+c=0$" équivaut à "$b^2-4c\geq 0$".

La complexité effective de la méthode de Collins est doublement exponentielle dans le nombre des variables puisqu'on calcule une décomposition valable pour un ensemble de formules qui peuvent avoir une alternance[5] quelconque des quantificateurs existentiel et universel (l'ordre des variables restant fixé)...

3. cylindre et projection

Dans la méthode de Collins, pour trouver une formule sans quantificateur équivalente à une formule Φ, on cherche une décomposition cellulaire telle que chaque polynôme qui apparaît dans Φ ait un signe déterminé sur chaque cellule : on dit qu'une telle décomposition est "signe-invariante". On prend donc comme ensemble des formules pour lesquelles on cherche la décomposition, l'ensemble des distributions de signes sur l'ensemble τ_0 des polynômes apparaissant dans Φ :

$$C_0 = \bigcup_{P\in\tau_0} \{P(\overline{x}) = 0,\ P(\overline{x}) > 0,\ P(\overline{x}) < 0\}$$

3.1 suite de projections :

On construit la décomposition en deux phases :
1) On recherche par récurrence un ensemble de conditions qui assurent que la décomposition est cylindrique.

---

[5] Comme cette formule Φ_n de taille polynomiale en n, avec deux n alternances des quantificateurs, définie par récurrence $\Phi_0(x,y) :=$ "$x^1 = y$", puis $\Phi_{n+1}(x,y) :=$"$\exists y\ \forall u \forall v \left[(u=x \wedge v=y) \vee (u=y \wedge v=y)\right] \rightarrow \Phi_n(u,v)$" en l'appliquant à x et 1 en Φ_n on trouve $x^{2^n} = 1$. En identifiant l'ensemble des nombres complexes à $\mathbb{R}^2$, on trouve les racines de l'unité. Or l'obtention de toutes les racines de l'unité donne une expression sans quantificateur dont la taille est proportionnelle au nombre de racines

Si des polynômes $P(x_0,x_1,\ldots,x_n)$, incluent dans τ_0 ,vérifient l'ensemble, noté $C(\tau_0)$, des conditions suivantes sur un ensemble $\mathcal{C}$ dans $\mathbb{R}^n$, alors on peut retrouver une décomposition de Collins de $\mathbb{R}^{n+1}$ pour $C_0 = \bigcup_{P\in\tau_0} \{P(\overline{x}) = 0,\ P(\overline{x}) > 0,\ P(\overline{x}) < 0\}$ sur chacune des parties connexes de $\mathcal{C}$.

Les conditions sont, en distinguant une variable x_0 et en travaillant dans $Z[x_1,\ldots,x_n][x_0]$:

- que le degré effectif (en x_0) de chaque P soit constant, ce qui peut s'exprimer en disant que le coefficient principal n'est pas nul :

si $P(x_0,x_1,\ldots,x_n)=\sum_{k=0}^{m} a_k(x_1,\ldots,x_n).x_0^k$ alors la formule "$\left(a_r(x_1,\ldots,x_n) \neq 0\right) \wedge \left(\bigwedge_{k=r+1}^{m} a_k(x_1,\ldots,x_n) = 0\right)$", qui indique que le degré effectif de P est r, est élément de $C(\tau_0)$,

- que le nombre de racines distinctes soit constant pour chaque polynôme : si pour tout P de τ_0, Q est la dérivée de P par rapport à x_0, et (pseudo-)pgcd(P,Q)$=\sum_{k=0}^{m} b_k(x_1,\ldots,x_n).x_0^k$,où les b_k s'obtiennent à l'aide des sous-résultantes[6], alors la formule "$\left(b_r(x_1,\ldots,x_n) \neq 0\right) \wedge \left(\bigwedge_{k=r+1}^{m} b_k(x_1,\ldots,x_n) = 0\right)$" , qui indique que le degré effectif du (pseudo-)pgcd(P,Q) est r, est élément de $C(\tau_0)$,

- que le nombre de racines communes de chaque couple de polynômes soit aussi constant, ce qui s'exprime sous la forme de conditions sur les sous-résultantes :

si pour tout couple P,Q de τ_0 (pseudo-)pgcd(P,Q)$=\sum_{k=0}^{m} b_k(x_1,\ldots,x_n).x_0^k$ alors la formule "$\left(b_r(x_1,\ldots,x_n) \neq 0\right) \wedge \left(\bigwedge_{k=r+1}^{m} b_k(x_1,\ldots,x_n) = 0\right)$" , qui indique que le degré effectif du (pseudo-)pgcd(P,Q) est r, est élément de $C(\tau_0)$.

L'ensemble, $C(\tau_0)$, de ces conditions ne dépend que de τ_0. Les formules de $C(\tau_0)$ sont des formules de L, où les termes sont des polynômes de $Z[x_1,\ldots,x_n]$. On appelle τ_1 l'ensemble des polynômes qui apparaissent dans les formules de $C(\tau_0)$. Puis on cherche les conditions d'une décomposition de Collins[7] pour $C_1 = \bigcup_{P\in\tau_1} \{P(\overline{x}) = 0,\ P(\overline{x}) > 0,\ P(\overline{x}) < 0\}$.

Ainsi, pour j un entier compris entre 0 et n-1, pour un ensemble de polynômes τ_j dans $Z[x_1,\ldots,x_n]$, on cherche les polynômes de τ_{j+1} (inclus dans $Z[x_{j+1},\ldots,x_n]$) intervenant dans $C(\tau_j)$. On note $C_{j+1} = \bigcup_{P\in\tau_{j+1}} \{P(\overline{x}) = 0,\ P(\overline{x}) > 0,\ P(\overline{x}) < 0\}$.

On obtient finalement C_n où les polynômes de τ_n sont dans $Z[x_n]$.

On a trouvé pour tout entier j compris entre 0 et n, des ensembles de formules $S_j=C_j\cup\ldots\cup C_n$.

On construit une décomposition Δ_{n-1} de l'espace $\mathbb{R}^{n+1-j}$ pour chaque S_j. La suite de décompositions Δ_0 de $\mathbb{R}$,..., Δ_n de $\mathbb{R}^{n+1}$ est une décomposition cylindrique selon l'ordre des variables $x_0,\ldots,x_n$.

2) On recompose la décomposition selon les variables récursivement.

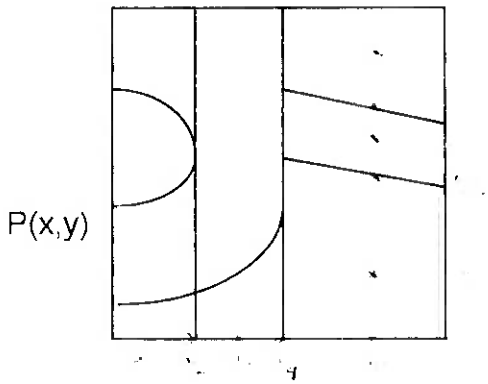
---

[6] Les sous résultantes donnent les coefficients des pseudo pgcd de deux polynômes P et Q, à l'aide de calculs de déterminants de matrices composées des coefficients de P et Q, voir [Col]

[7] Une décomposition pour C_1 sera une décomposition pour $C(\tau_0)$

On construit un ensemble "des points témoins" de tous les semi-algébriques d'une décomposition cylindrique. Chaque cellule est représentée par un point témoin[8]. On trouve des points témoins effectivement[9] (comme unique racine d'un polynôme dans un intervalle rationnel) grâce aux suites de Sturm.

Puis pour des polynômes P(x,y), ayant trouvé les points témoins $\{a_i\}$ des bases des cylindres, on calcule des suites de Sturm pour les polynômes $P(x,a_i)$, et on trouve les racines de ces polynômes $b_{i,j}$, on recompose les points témoins $(b_{i,j}, a_i)$ de cette décomposition (on a "relevé" la décomposition). On peut poursuivre le processus.



La décomposition finale satisfait toutes les distributions de signes. Les conjonctions non-satisfaisables sont éliminées au fur et à mesure que l'on calcule les suites de Sturm qui ne donnent que les formules satisfaisables.

3.2 cylindre et vérification de formules :

Une fois cet ensemble obtenu, on vérifie la satisfaction de la formule Φ sur l'ensemble des points témoins. On détermine l'ensemble des signes que chaque polynôme P de Φ prend sur chaque point témoin (et par suite, sur chaque cellule).

On vérifie si les conjonctions ou les disjonctions de conditions de signes de la formule Φ sont vérifiées sur chaque point témoin a_i, on obtient un ensemble de points témoins où Φ est vraie.

$$\mathbb{R}^n \longrightarrow \{Vrai, Faux\}$$

$$a_i \longmapsto \Phi(a_i)$$

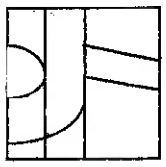
On cherche ensuite à savoir si une quantification est satisfaite en observant la disposition des points trouvés dans les cylindres de la décomposition. Par exemple si une variable est quantifiée universellement on vérifie sur la conjonction des points témoins dans le même cylindre, si elle est quantifiée existentiellement, sur la disjonction.

---

[8] La recherche des points témoins qui permettent la manipulation des cellules est la particularité de la méthode de Collins. Les cellules ne sont plus données explicitement par des formules

[9] S'il s'agit d'un point algébrique racine d'un polynôme, alors les calculs se feront modulo ce polynôme

P(x,y)



$\forall y \exists x\ P(x,y)>0$

La décomposition a la forme d'un arbre...on élimine les quantificateurs selon cette structure d'arbre.

4. développements : Méthodes en parallèle

La mise en œuvre de ces derniers calculs a un coût, et l'on peut souhaiter ne pas l'effectuer de façon aussi uniforme. On utilise conjointement aux calculs des "stacks" (arbres des points témoins) la forme des formules pour réduire le calcul [Hon]...

Une autre approche peut être de construire une représentation algébrique du problème [BKR]. On transforme la formule à prouver sous la forme d'une conjonction[10] d'une équation $P(x)=0$ et de plusieurs inéquations $R_j(x)>0$ dont les polynômes sont dans $Z[X]$ (une seule variable) et P et les R_j sont sans racine commune. On vérifiera, alors, la satisfaction de cette conjonction. On commence par trouver par un algorithme parallèle, P et les R_j, puis l'on calcule les distributions de signes des R_j sur les racines de P en résolvant des systèmes d'équations linéaires. On peut simplifier les matrices qui représentent les équations (si une formule est contradictoire) et combiner les matrices sous la forme d'un produit tensoriel.
On fixe a priori l'ensemble sur lequel on décide des formules, l'ensemble des racines du polynôme P, sans chercher les points témoins pour toutes les distributions de signes comme dans Collins.

Cette méthode a été étendue au cas de polynômes à plusieurs variables, par Renegar [Ren] et aussi par M.F. Roy [HRS]. On travaille par bloc de quantificateurs : après une transformation topologique du problème, on détermine l'ensemble "des points témoins", sur lequel on décide les formules, par projection orthogonale sur une droite des points extrêmes de chaque composante connexe des semi-algébriques définis par les formules. Dans la méthode [HRS], les suites de Sturm-Habicht permettent de calculer selon une forme indépendante des degrés effectifs des polynômes (les calculs par sous-résultantes de la méthode de Collins demandent à ce que le polynôme soit d'un degré effectif défini).

Mais ces améliorations des méthodes de calcul ne changent pas fondamentalement l'approche de la méthode de Collins telle qu'elle a été exposée ici. L'explicitation des formules permet de donner une forme où une décomposition pourrait être recomposée avec d'autres, et d'avoir moins une méthode de décision qu'un système de preuve [Jum], prenant en compte les connecteurs.

[10] Dans le cas d'une inégalité large $R_j(x)\geq 0$, on traite les cas selon la disjonction $R_j(x)=0 \vee R_j(x)>0$

bibliographie

[BCR] J. Bochnak, M. Coste & M.F. Roy : Géométrie algébrique réelle, Springer 1987.

[BKR] : M Ben-Or, D. Kozen & J. Reiff : The complexity of Elementary Algebra and Geometry, J. of Computer and System Science 32 (1986) 251-264.

[Col] G.E Collins: Quantifier Elimination for Real closed Fields by cylindrical algebraic decomposition, proc. 2nd GI Conference on Automata theory and Formal language, Lect. Notes in Computer Science 35 (1975) 134-183.

[Hon] H Hong: Improvement in CAD-based Quantifier Elimination, Ph D thesis, The Ohio State University, 1990 et pre-print conf Linz 1993.

[HRS] M F Roy : J. Heintz, M.F. Roy & P. Solerno : Sur la complexité du principe de Tarski-Seidenberg, Bulletin Soc. Math. de France, 118 (1990) 13-30.

[Jum] P. Jumpertz: Linear Logic And Real Closed Field : A Way To Handle Situations Dynamically, à paraître in Lec. Notes in Computer Science.

[Ren] J. Renegar : On the computational complexity and geometry of the first order theory of the reals, J. of Symbolic Computation 13 (1992) 255-352.

[S&S] Schwartz & Sharir : On The Piano Mover's problem 2, Adv. Appl. Math 4 (1983) 298-351.

[Tar] A.Tarski : The completness of elementary algebra and geometry, devant paraître à Paris en 1940, copies diffusées en (1967).

CNRS, URA 753
Université Paris 7
2, Place Jussieu, Tour 45-55, 5ème étage
75251 PARIS CEDEX 05

Adresse électronique : jumpertz@logique.jussieu.fr

Priestley duality and distributive lattices with operators

Roberto Cignoli

In this talk I will try to summarize some recent work done in Buenos Aires on Priestley duality for bounded distributive lattices. In the first part, I will recall the main facts about Priestley duality, and in the secon one I will concentrate on the ext ensions of this duality obtained in Buenos Aires.

1 Priestley duality

The letters L, M will always denote bounded distributive lattices, i.e., distributive lattices with smallest element 0 and greatest element 1. By a homomorphism I shall understand a lattice homomorphism that preserves 0 and 1. I will den ote by $\mathcal{D}$ the category of bounded distributive lattices and homomorphisms, and by $\mathcal{D}_{Fin}$ the full subcategory of $\mathcal{D}$ whose objects are the finite distributive lattices. Furthermore, the category $\mathcal{B}$ of Boolean algebras an d Boolean homomorphisms will be treated as a full subcategory of $\mathcal{D}$.

Recall that an element $p \in L$ is said to be *join irreducible* if $p \neq 0$ and whenever $p \leq a \vee b$, then $p \leq a$ or $p \leq b$. I denote the set of all join-irreducible elements of L, with the order inherited from L, by $J(L)$.

Let X be a poset (= partially ordered set) and $Y \subseteq X$. I shall denote by $(Y]$ the set of all x in X such that $x \leq y$ for some $y \in Y$. The set $[Y)$ is defined dually. Y is *increasing* (*decreasing*) if $Y = [Y)$ $(Y = (Y])$. For $x \in X$, I write $(x]$ and $[x)$ instead of $(\{x\}]$ and $[\{x\})$, respectively.

A *totally order-disconnected topological space* is a triple $\langle X, \leq, \tau \rangle$ such that $\langle X, \leq \rangle$ is a poset, $\langle X, \tau \rangle$ is a topological space, and given x, y in X such that $x \not\leq y$, there is a clopen (= closed and open) increasing set U such that $x \in U$ and $y \notin U$. A *Priestley space* is a compact totally order-disconnected

topological space. I denote by $\mathcal{P}$ the category of Priestley spaces and orde r-preserving continuous functions, and by $\mathcal{P}_{Fin}$ the full subcategory whose objects are the finite Priestley spaces.

For each Priestley space X, define $D(X)$ as the lattice of increasing open subsets of X, and for each order-preserving continuous function f from X into a Priestley space Y, define $D(f)\colon D(Y) \to D(X)$ by the prescription $D(h)(V) = h^{-1}(V)$, for each $V \in D(Y)$. It is easy to check that $\mathbf{D}$ is a contravariant functor from $\mathcal{P}$ into $\mathcal{D}$, i.e. a functor from $\mathcal{P}$ into $\mathcal{D}^{op}$, where $\mathcal{C}^{op}$ denotes the opposite of a category $\mathcal{C}$.

As a first example, note that the familiar totally disconected topological spaces are the totally order-disconnected spaces such that the order relation is the equality. Therefore the Stone spaces, i.e., the compact totally disconnected topological spa ces, are particular cases of Priestley spaces. If X is a Stone space, then $D(X)$ becomes the Boolean algebra of all clopen subsets of X. Therefore, by taking into account that all functions between Stone spaces are trivially order preserving, we have that *the category $\mathcal{S}$ of Stone spaces and continuous functions is a full subcategory of the category $\mathcal{P}$*, and the restriction of $\mathbf{D}$ to $\mathcal{S}$ gives the well known Stone functor from $\mathcal{S}$ into $\mathcal{B}^{op}$.

As a second example, suppose that X is a finite Priestley space. Since X is a Hausdorff space, all its points are closed, and then the topology is discrete. Hence $D(X)$ is the set of all increasing subsets of X. Therefore $\mathcal{P}_{Fin}$ is the category of finite posets and order-preserving functions, and the restriction of $\mathbf{D}$ to $\mathcal{P}_{Fin}$ is a functor from $\mathcal{P}_{Fin}$ into $\mathcal{D}_{Fin}^{op}$.

The most important examples of Priestley spaces are obtained as follows.

Let T denote the two-element chain $0 < 1$ endowed with the discrete topology. Then for each set $I \neq \emptyset$, the set T^I, equipped with the product topology and the pointwise order, is a Priestley space.

Since the set $X(L)$ of all homomorphisms from L into T is a closed subset of T^L, it is also a Priestley space, that is called *the Priestley space of* L. Alternatively, $X(L)$ can be described as the set of all prime filters of L, ordered by inclusion and with the topology having as a sub-basis the sets of the form $\sigma_L(a) = \{P \in X(L) \mid a \in P\}$ and $X(L) \setminus \sigma_L(a)$, for each $a \in L$.

For each homomorphism $h\colon L \to M$, define $X(h)\colon X(M) \to X(L)$ as the composition $X(h)(\varphi) = \varphi \circ h$, for each homomorphism $\varphi\colon M \to T$. Alternatively, we can define $X(h)(Q) = h^{-1}(Q)$ for each prime filter Q of the lattice M.

It is easy to check that $\mathbf{X}$ defines a functor from the $\mathcal{D}$ into $\mathcal{P}^{op}$.

When L is a Boolean algebra, the prime filters of L coincide with the maximal filters (= ultrafilters), then it follows that the order relation in $X(L)$ reduces to the equality, and for each $a \in L$, $X(L) \setminus \sigma_L(a) = \sigma_L(\neg a)$, where $\neg a$ denotes the complement of a. Therefore $X(L)$ becomes the set of ultrafilters of L, with the topology having as basis the sets of the form $\sigma_L(a)$, for $a \in L$. Consequently, $\mathbf{X}$ restr icted to $\mathcal{B}$ gives the familiar functor from $\mathcal{B}$ into $\mathcal{S}^{op}$ defined by Stone in 1936 [42].

If L is a finite distributive lattice, then the prime ideals of L are of the form $[p)$, for $p \in J(L)$. Therefore $X(L)$ can be identified with the order dual of the poset $J(L)$, and then $D(X(L))$ can in tu rn be identified with the lattice of all decreasing subsets of the poset of join-irreducible elements in L. Moreover, it is plain that the restriction of $\mathbf{X}$ to $\mathcal{D}_{Fin}$ is a contravariant functor into $\mathcal{P}_{Fin}$.

It was proved by Priestley [33, 34](see also [37, 19] that $\sigma_L: L \to D(X(L))$ is an isomorphism, and that $\varepsilon_X: X \to X(D(X))$, defined by the prescription $\varepsilon_X(x) = \{U \ in D(X) \mid x \in U\}$ is both a homeomorphism and an order isomorphism for each Priestley space X. In other words, she proved the following:

Theorem 1 (Priestley [33]) *The functors $D: \mathcal{P} \to \mathcal{D}^{op}$ and $X: \mathcal{D} \to \mathcal{P}^{op}$ define a natural duality between the categories $\mathcal{D}$ and $\mathcal{P}$. The unit and counit of the corresponding adjunction are ε and σ respectively.*

At the light of the above remarks on Boolean algebras and finite distributive lattices, we see that as particular cases of Priestley's results we obtain the well known duality between Boolean algebras and Stone spaces developed by Stone in 1936 [?], as well as a celebrated theorem of Birkhoff, first published in 1933 [2, 3], asserting that each finite distributive lattice L is isomorphic to the lattice of all decreasing subsets of $J(L)$. As a matter of fact, the restri ctions of the functors $\mathbf{D}$ and $\mathbf{X}$ establish a duality between the categories $\mathcal{D}_{Fin}$ and $\mathcal{P}_{Fin}$.

A closed subset F of a topological space X is called *irreducible* if it is a join-irreducible element in the lattice of closed subsets of X. A *spectral space* is a compact T_0 topological space such that its compact open subs ets form a multiplicative basis and each irreducible closed set is the closure of a point.

Every spectral space X becomes a Priestley space $P(X)$ when equipped with the *specialization order*: $x \leq y$ if and only if $y \in \overline{\{x\}}$ and the *patch*

topology, i.e., the topology generated by the compact open subse ts of X and their complements. Moreover $U \subseteq X$ is compact open if and only if $U \in D(P(X))$. Conversely, every Priestley space X becomes a spectral space $S(X)$ if one forgets the order relation and considers the topology generated by the compact open subsets of X. Furthermore, for each spectral space X, $S(P(X)) = X$ and for each Priestley space X, $P(S(X)) = X$ (see, for instance [13]).

Consequently Priestley's theorem is a reformulation of a classical theorem of Stone [43], asserting that each bounded distributive lattice is isomorphic to the lattice of compact open subsets of a spectral space.

One advantage of Priestley spaces over spectral spaces is that the natural morphisms are the order preserving continuous functions, instead of the awkward "continuous functions such that the inverse image of each compact open subset is compact open." How ever, the main advantage of shifting from spectral to Priestley spaces is that one obtains a very nice characterization of the congruences of bounded distributive lattices.

Recall that a *congruence* Θ on L is an equivalence relation such that $(a, b) \in \Theta$ and $(c, d) \in \Theta$ imply that $(a \vee c, b \vee d) \in \Theta$ and $(a \wedge c, b \wedge d) \in \Theta$. The congruences on L, orde red by inclusion, forms a complete lattice, that is denoted by $Con(L)$. Given a, b in L, $\Theta(a, b)$ denotes the *principal congruence generated by a and b*, i.e., the intersection of all congruences containing the pair (a, b).

A. Monteiro [31] observed that for each set Y of prime filters of L, the relation

$$\Theta(Y) = \{(a, b) \in L \times L \mid \forall P \in Y, a \in P \leftrightarrow b \in P\}$$

is a congruence on L. Moreover, given $\Theta \in Con(L)$, if X denotes the set of prime filters of the quotient lattice L/Θ, $h\colon L \to L/\Theta$ is the natural projection and $Z = \{h^{-1}(P) \mid P \in X\}$, then $\Theta = Theta(Z)$.

The correspondence $Y \mapsto \Theta(Y)$ is not one-to-one. Indeed, one can characterize the congruence $\Theta(Y)$ in terms of the Priestley space of L as follows:

$$\Theta(Y) = \{(a, b) \in L \times L \mid \sigma_L(a) \cap Y = \sigma_L(b) \cap Y\}.$$

and it follows that for each $Y, Z \subseteq X(L)$, $\Theta(Y) = \Theta(\overline{Y})$, and that $\Theta(Y) = \Theta(Z)$ if and only if $\overline{Y} = \overline{Z}$ (see [9]). From these results one can easily derive the follow ing:

Theorem 2 (Priestley [36, 37]) *Let L be a bounded distributive lattice and $X = X(L)$. Then the correspondence $V \mapsto \varphi_L(V) = \Theta(X \setminus V)$ defines an isomorphism φ_L from $Con(L)$ onto the lattice $Op(X)$ of all open subs ets of X.*

Corollary 1 *For each finite distributive lattice L, $Con(L)$ is isomorphic to the Boolean algebra of all subsets of $J(L)$.*

The following characterization of principal congruences is an interesting consequence of the above theorem.

Corollary 2 *For $a, b \in L$, $\varphi_L(\Theta(a,b)) = \sigma_L(a)\Delta\sigma_L(b)$, where Δ means symmetric difference.*

For instance, from the above corollaries one can infer that the number of congruences of an n-element chain is 2^{n-1}, while the number of principal congruences is $n + \frac{(n-2)(n-1)}{2}$.

Priestley's theorems 1 and 2 have been applied by several authors to develop dualities for several classes of algebras having a bounded distributive lattice reduct and to characterize the corresponding subdirectly irreducibl e algebras. See, for instance, [6, 7, 8, 11, 14, 15, 16, 17, 21, 28, 29, 30, 35, 36, 40, 41, 44, 45] as well as the books [4] and [5]. For further developments on this line, consult the excellent surveys [38] and [18].

2 Distributive lattices with operators

In a classical paper, Jónsson and Tarski [26] showed that a Boolean algebra endowed with a family of join-preserving operations can be represented as a subalgebra of the Boolean algebra of all subsets of a set X, in such a way that the oper ations are in correspondence with certain relations defined on the set X. Later on, Halmos [22, 24] characterized the relations between Stone spaces which correspond to 0-preserving join-homomorphisms between the corresponding Boolean alg ebras of clopen sets. These relation were called *Boolean relations*. Wright [46] completed these results by showing that the classical Stone duality between the categories $\mathcal{B}$ and $\mathcal{S}$ can be extended to a duality between the categories of Boolean algebras and 0-preserving join-homomorphisms and Stone sp aces and Boolean relations.

On the other hand, there is a duality between the subalgebras of a Boolean algebra B and certain equivalence relations on the Stone space $X(B)$ (see, for instance, [27]).

The connection between the duality for join-homomorphisms and that for subalgebras is given by the *quantifiers*. A *quantifier* on a Boolean algebra B is a closure operator on B such that its range is a subalgebra of B. The dual of a quantifier Q considered as a 0-preserving join-homomorphism is an equivalence relation which is also the dual of the range of Q.

In the last few years, with my students at Buenos Aires, we extended the Halmos-Wright duality to distributive lattices [8, 10, 12, 32].

In this section L, M will continue to denote bounded distributive lattices. By a join-homomorphism from L into M we understand a mapping $j: L \to M$ such that $j(0) = 0$ and $j(a \vee b) = j(a) \vee j(b)$. The meet-homomorphisms are defined dually. Note that a mapping $h: L \to M$ is a homomorphism if and only if it is both a join-homomorphism and a meet-homomorphism. The category of bounded distributive lattices and join-(meet-)homomorphisms will be denoted by $\mathcal{J}$ ($\mathcal{M}$). Obviously, $\mathcal{D}$ is a subcategory of both $\mathcal{J}$ and $\mathcal{M}$. Note that the isomorphisms in these three categories are the same: the one-to-one and onto homomorphisms.

Given a relation $R \subseteq X \times Y$, for each $Z \subseteq X$, $R(Z)$ will denote the image of Z by R, i.e.,

$$R(Z) = \{y \in Y \mid \exists x \in Z \ (x, y) \in R\}$$

and for each $Z \subseteq Y$, $R^{-1}(Z)$ will denote the inverse image of Z by R, i.e.,

$$R^{-1}(Z) = \{x \in X \mid R(\{x\}) \cap Z \neq \emptyset\}$$

Note that the domain of R is $R^{-1}(Y)$, in symbols, $dom(R) = R^{-1}(Y)$. When $x \in X$ ($y \in Y$), I write $R(x)$ ($R^{-1}(y)$) instead of $R(\{x\})$ ($R^{-1}(\{y\})$).

Let X and Y be Priestley spaces. A relation $R \subseteq X \times Y$ is said to be a *Priestley relation* provided the following conditions are satisfied:

i) For each $x \in X$, $R(x)$ is a closed and decreasing subset of Y, and

ii) For each $V \in D(Y)$, $R^{-1}(V) \in D(X)$.

A Priestley relation is said to be *functional* in case $dom(R) = X$ and $R(x)$ has a greatest element for each $x \in X$.

For Priestley spaces X and Y, $\mathcal{P}R(X,Y)$ will denote the set of all Priestley relations $R \subseteq X \times Y$, and $\mathcal{P}F(X,Y)$, the subset of functional Priestley relations.

When X and Y are Stone spaces, Priestley relations coincide with the Boolean relations defined by Halmos [22]. A Boolean relation is functional if and only if $R(x)$ is a singleton for each $x \in X$, i.e., if and only if R is a function from X into Y.

In what follow, X, Y will denote Priestley spaces.

Since the composition of Priestley relations is a Priestley relation (see [12]), one can define the category $\mathcal{P}R$ whose objects are the Priestley spaces and the morphisms are the Priestley relations.

It is proved in [12] that for each continuous and monotonic function $f: X \to Y$, $R_f = \{(x,y) \in X \times Y \mid y \leq f(x)\} \in \mathcal{P}F(X,Y)$. Conversely, if $R \in \mathcal{P}F(X,Y)$ then the function $f_R: X \to Y$ obtained by defining $f_R(x)$ as the greatest element of $R(x)$, is continuous and monotonic. It is plain that $R = R_{f_R}$ and $f = f_{R_f}$. In particular, the dual order $\geq \subseteq X \times X$ is the functional Priestley relation associated with the identity function on X. Therefore, one can identify $\mathcal{P}$ with the subcategory of $\mathcal{P}R$ having the same objects but having the functional Priestley relations as morphisms.

For each $j \in \mathcal{J}(L,M)$, $j^* = \{(Q,P) \in X(M) \times X(L) \mid P \subseteq j^{-1}Q)\}$ is a Priestley relation, and $dom(j^*) = \{Q \in X(M) \mid j(1) \in Q\}$. Moreover, $j \in \mathcal{J}(L,M)$ is a homomorphism if and only if $j^* \in \mathcal{P}F(X(M),X(L))$.

Therefore one can consider the functor $\mathbf{X}$ as a functor from $\mathcal{P}R$ into $\mathcal{J}^{op}$ by defining $X(j) = j^*$ for each join-homomorphism j (see [12] for details).

For each $R \in \mathcal{P}R(X,Y)$, the correspondence $U \mapsto R^{-1}(U)$ defines a join-homomorphism $R^*: D(Y) \to D(X)$, and $R^*(Y) = dom(R)$. Moreover, if $R \in \mathcal{P}R(X,Y)$, then for each $x \in X$ a nd each $y \in Y$, $(x,y) \in R$ if and only if $(\varepsilon_X(x), \varepsilon_Y(y) \in R^{**}$. Therefore one can also consider the functor $\mathbf{D}$ as a functor from $\mathcal{J}$ into $\mathcal{P}R^{op}$, by defining $D(R) = R^*$ fo r each Priestley relation R. Since $\varepsilon_X: X \to X(D(X))$ is both a homeomorphism and an order isomorphism, $\rho_X = R_{\varepsilon_X}$ is an isomorphism in $\mathcal{P}R$.

The following theorem, established in [12], generalizes Priestley duality as well as Halmos-Wright duality.

Theorem 3 *(The functors $D: \mathcal{P}R \to \mathcal{J}^{op}$ and $X: \mathcal{J} \to \mathcal{P}R^{op}$ define a natural duality between the categories $\mathcal{J}$ and $\mathcal{P}R$. The unit and counit of the corresponding adjunction ar e ρ and σ respectively.*

For each $C \subset L$ define $M^{\#} = \{(P,Q) \in X(L) \times X(L) \mid P \cap C \subseteq Q\}$, and for each $R \subseteq X \times X$ define $R^{\#} = \{U \in D(X) \mid R^{-1}(U) = U\}$. A *lattice preorder* on a Priestley space X is a reflexive and transitive relation R that satisfies the condition:

(ℓ) *Given x,y in X such that $(x,y) \notin R$, there is $U \in R^{\#}$ such that $x \in U$ and $y \notin U$.*

The next theorem, also proved in [12], establish a duality between 0-1-sublattices of L and lattice preorders on $X(L)$.

Theorem 4 *The correspondence $M \mapsto M^{\#}$ defines an antiisomorphism from the lattice of all 0-1-sublattices of L onto the lattice of all lattice preorders defined on $X(L)$.*

As particular cases of lattice preorders one can consider *lattice orders* and *lattice equivalences.*

Theorem 5 ([12]) *The following propositions hold true for each 0-1-sublattice M of L:*

i) $M^{\#}$ is an order iff for each prime filter P of M there is exactly one prime filter Q of L such that $P = Q \cap M$.

ii) $M^{\#}$ is an equivalence if and only if all the elements of M are complemented.

From (ii) in the above theorem, one obtains the well-known correspondence between subalgebras of a Boolean algebra B and equivalences on the Stone space $X(B)$ satisfying condition (ℓ) (see [27, §8.2]).

For each join-homomorphism $j\colon L \to L$, let $M_j = \{a \in L \mid a \leq j(a)\}$. It is easy to check that M_j is a 0-1-sublattice of L, and then $j^{\#} = M_j^{\#}$ is a lattice preorder associated with j. It follows that $j^{\star} \subseteq j^{\#}$.

Recall that an *additive closure* on L is a join-homomorphism such that $a \leq j(a)$ and $j(j(a)) = a$ for each $a \in L$. The image of j, $j(L)$ is a 0-1-sublattice of L, and for each $a \in L$, $j(a)$ is the smallest element in the se t $(a] \cap j(L)$ (see [1, II.4, Theorem 11]). Let $C(L)$ denote the set of all additive closure operators on L. A *quantifier* on L is a $j \in \cap j(L)$ such that $j(j(a) \wedge b) = j(a) \wedge j(b)$ for all a, b in L.

One have the following characterization of closure operators among join-homomorphisms: $j^* = j^\#$ iff $j \in \mathcal{C}(L)$ iff j^* is a preorder. Analogously, a 0-1-sublattice M of L is the range of a closure operator iff $M^\#$ is a Priestley relation (see [12]).

A J-distributive lattice is an algebra $\langle L, \vee, \wedge, j, 0, 1\rangle$ such that $\langle L, \vee, \wedge, 0, 1\rangle$ is a bounded distributive lattice and $j\colon L \to L$ is a join-homomorphism. The particular case when j is a quantifier is consider in [8] under the name of Q-distributive lattices.

A J-Priestley space is a Priestley space X endowed with a Priestley relation R. If (X, R) and (Y, S) are J-Priestley spaces, a J-function from (X, R) into (Y, S) is an order preserving continuous function $f\colon X \to Y$ such that $f^{-1}(S^{-1}(V)) = R^{-1}(f^{-1}(V))$ for each $V \in D(Y)$.

¿From Theorem 3 Petrovich [32] derived a duality between the categories of J-distributive lattices and homomorphisms and J-Priestley spaces and J-functions.

Let (X, R) be a J-Priestley space. A subset $Z \subseteq X$ is called R-saturated provided $x \in Z$ implies $\max R(x) \subseteq Z$ for each $x \in X$. The set of all R-saturated subsets of X is denoted by $Sat_R(X)$.

Petrovich [32] proved the following generalization of Theorem 2:

Theorem 6 (Petrovich) *The congruence lattice of a J-distributive lattice (L, j) is antiisomorphic to the lattice of all closed j^*-saturated subsets of $X(L)$.*

¿From this theorem Petrovich obtained characterizations of the simple and the subdirectly irreducible J-distributive lattices.

References

[1] R. Balbes and P. Dwinger, **Distributive lattices**, University of Missouri Press, Columbia, Missouri, 1974.

[2] G. Birkhoff, *On the combination of subalgebras*, Proc. Cambridge Phil. Soc. **29** (1933), 441–464.

[3] G. Birkhoff, **Lattice Theory** (Third Edition), Amer. Math. Soc., Providence, Rhode Island, 1967.

[4] V. Boicescu, A. Filipoiu, G. Georgescu and S. Rudeanu., **Lukasiewicz -Moisil algebras**, North Holland, Amsterdam, 1991.

[5] T.S. Blyth and J.C. Varlet, **Ockham algebras**, Oxford University Press, Oxford, 1994.

[6] R. Cignoli, *Coproducts in the categories of Kleene and three-valued Lukasiewicz algebras*, Studia Logica **38** (1979), 237–245.

[7] R. Cignoli, *The class of Kleene algebras satisfying an interpolation property and Nelson algebras*, Algebra Universalis, **23** (1986), 262–292.

[8] R. Cignoli, *Quantifiers on distributive lattices*, Discrete Math., **96** (1991). 183–197.

[9] R.Cignoli, *Distributive lattice congruences and Priestley spaces*, Proceedings of the First "Dr. Antonio A. R. Monteiro" Congress on Mathematics (Spanish) (Bahía Blanca, 1991), Univ. Nac. del Sur, Bahía Blanca, 1991, pp. 81–84.

[10] R. Cignoli, *Free Q-Distributive Lattices*, Studia Logica, to appear.

[11] R. Cignoli and M.S. de Gallego, *Dualities for some de Morgan algebras with operators and Lukasiewicz algebras*, J. Austral. Math. Soc. (A) **34** (1983), 377–393.

[12] R. Cignoli, S. LaFalce and A. Petrovich, *Remarks on Priestley duality for distributive lattices*, Order, **8** (1991), 299–315.

[13] W.H. Cornish, *On H.Priestley's dual of the category of bounded distributive lattices*, Mat. Vesnik **12** (27) (1975), 329–332.

[14] W.H. Cornish and P.R. Fowler, *Coproducts of de Morgan algebras*, Bull. Austral. Math. Soc. **16** (1977), 1–13.

[15] W.H. Cornish and P.R. Fowler, *Coproducts of Kleene algebras*, J. Austral. Math. Soc. (A) **27** (1979), 209-220.

[16] B.A. Davey, *Subdirectly irreducible distributive double p-algebras*, Algebra Universalis **8** (1978), 73–88.

[17] B.A. Davey, *Dualities for Stone algebras, double Stone algebras, and relative Stone algebras*, Colloq. Math. **46** (1982), 1–14.

[18] B.A. Davey, *Duality Theory on Ten Dollars a Day*, *in***Algebras and Orders** (I.G. Rosenberg and G. Sabidussi, eds.), NATO Advanced Study Institute Series, Series C, Vol. **389**, Kluwer , Dordrecht, 1993, pp. 71–111.

[19] B.A. Davey and H.A. Priestley, **Introduction to Lattices and Order**, Cambridge University Press, Cambridge, 1990.

[20] B.A. Davey and H.A. Priestley, *Optimal natural dualities*, Trans. Amer. Math. Soc. **338** (1993), 655–677

[21] M. Goldberg, *Topological duality for distributive Ockham algebras*, Studia Logica **42** (1983), 23–31.

[22] P.R. Halmos, *Algebraic logic. I. Monadic Boolean algebras.*, Compositio Math. **12** (1955), 217–249. Reproduced in [24, Chapter II].

[23] P.R. Halmos, *Free monadic algebras*, Proc. Amer. Math. Soc., **10** (1959), 219–227. Reproduced in [24, Chapter V].

[24] P.R. Halmos, **Algebraic logic**, Chelsea, New York, 1962.

[25] L. Henkin, J.D. Monk and A. Tarski, **Cylindric Algebras. Part II**, North-Holland, Amsterdam, 1985.

[26] B. Jónnsson and A. Tarski, *Boolean algebras with operators.I*, Amer. J. Math. **73** (1951), 891–938.

[27] S. Kippelberg, *Topological duality*, *in* **Handbook of Boolean Algebras** Vol. I (J.D. Monk and R. Bonnet, eds.), North-Holland, Amsterdam, 1989, pp. 95–126.

[28] N.G. Martínez, *The Priestley duality for Wajsberg algebras*, Studia Logica **49** (1990), 31–46.

[29] N.G. Martínez, *A topological duality for some ordered algebraic structures including ℓ-groups*, Algebra Universalis, **31** (1994), 516–541.

[30] N.G. Martínez, *A simplified duality for implicative lattices and ℓ-groups*, Studia Logica, to appear.

[31] A. Monteiro, *De Morgan algebras*, unpublished lectures given at the Universidad Nacional del Sur, Baía Blanca, 1962.

[32] A. Petrovich, *Distributive lattices with an operator*, Studia Logica, to appear.

[33] H.A. Priestley, *Representation of distributive lattices by means of ordered Stone spaces*, Bull. London Math. Soc., **2** (1970), 186–190.

[34] H.A. Priestley, *Ordered topological spaces and the representation of distributive lattices*, Proc. London Math. Soc., **4** (3) (1972), 507–530.

[35] H.A. Priestley, *Stone lattices: a topological approach*, Fund. Math. **84** (1974), 127–143.

[36] H.A.Priestley, *The construction of spaces dual to pseudocomplemented distributive lattices*, Quart. J. Math. Oxford (2) **26** (1975), 215–228.

[37] H.A. Priestley, *Ordered sets and duality for distributive lattices*, in **Orders, Descriptions and Roles**, (M. Pouzet and D. Richards, eds), Ann. Discrete Math., **23** (North-Holland, Amsterdam, New York, 1984), 39–60.

[38] H.A. Priestley, *Natural dualities, in* Proceedings of the Birkhoff Symposium, Darmstadt, 1991 (K.A. Barker and R. Wille, eds), to appear.

[39] H.A. Priestley, *Natural dualities for varieties of distributive lattices with a quantifier*, preprint.

[40] A. Sendlewski, *Nelson algebras through Heyting ones.* I, Studia Logica, **49** (1990), 105–126.

[41] A. Sendlewski, *Topologicality of Kleene algebras with a weak pseudocomplementation over distributive p-algebras*, Rep. Math. Logic **25** (1991), 13–56.

[42] M.H. Stone, *The theory of representation of Boolean algebras*, Trans. Amer. Math. Soc. **40** (1936), 37–111.

[43] M.H. Stone, *Topological representation of distributive lattices and Brouwerian logics*, Časopis Pěst. Mat. Fys. **67** (1937), 1–25.

[44] A. Urquhart, *Distributive lattices with a dual homomorphic operation*, Studia Logica **38** (1979), 201–209.

[45] D. Vaggione, *Sheaf representation of lattice-ordered structures*, *in* Proceedings of the First "Dr. Antonio A. R. Monteiro" Congress on Mathematics (Spanish) (Bahía Blanca, 1991), Univ. Nac. del Sur, Bahía Blanca, 1991, pp. 185–196.

[46] F.B. Wright, *Some remarks on Boolean duality*, Portug. Math., **16** (1957), 109–117.

Departamento de Matemática,
Facultad de Ciencias Exactas y Naturales,
Universidad de Buenos Aires.
Ciudad Universitaria
1428 Buenos Aires -- Argentina
e-mail: postmaster@cignol.uba.ar

A SIMPLIFIED DUALITY FOR IMPLICATIVE LATTICES AND l-GROUPS.

NESTOR G. MARTINEZ.

ABSTRACT. A topological duality is presented for a wide class of lattice-ordered structures including lattice-ordered groups. In this new approach, which simplifies considerably previous results of the author, the dual space is obtained by endowing the Priestley space of the underlying lattice with two binary functions, linked by set-theoretical complement and acting as symmetrical partners. In the particular case of l-groups, one of these functions is the usual product of sets and the axiomatization of the dual space is given by very simple first-order sentences, saying essentially that both functions are associative and that the space is a residuated semigroup with respect to each of them.

This talk summarizes the main results of a paper with the same title that will appear in a special issue of Studia Logica devoted to the Priestley duality.

Introduction.

This work can be seen as a refinement and a simplification of our previous duality developed in [11]. In that first approach, having in mind the topological representation of M. H. Stone for distributive lattices [16] and the duality theory of H. Priestley [14], [15], we developed a topological duality for a wide class of lattice-ordered algebraic structures, which we called implicative lattices. Also, we showed that lattice-ordered groups can be characterized as implicative lattices with some extra conditions, and we could derive a topological duality for these groups.

The main idea in that approach was to introduce in the dual space of the underlying lattice one suitable binary and continuous function, as the translation of the binary operation of the algebraic structure. However, when trying to axiomatize the properties of this function in the dual space, some of the conditions we got were quite complicated and obscure. Also, the morphisms of the dual space were rather unnatural and difficult to describe.

The key idea in this new approach is to consider a second binary function in the dual space, which is naturally defined from the first one by using set-theoretical complement and which acts as a symmetrical partner, simplifying all the proofs.

1991 *Mathematics Subject Classification.* AMS Math. Subject Classification: 06D05, 06E15, 06F15, 20F60.

Key words and phrases. duality, Priestley spaces, lattice-ordered groups, implicative lattices.

The author is supported at the Mathematical Institute of Oxford by a grant of the Argentinian *Consejo de Investigaciones Cientificas y Tecnicas* (CONICET). The author wishes to acknowledge the CONICET and the kind hospitality of the Mathematical Institute.

The conditions we get to axiomatize the dual space are now all simple and natural; the morphisms are also described in a nice way. Moreover, when applying the general schema to the case of lattice-ordered groups, we obtain very simple first-order conditions for the dual space, improving considerably our first version.

§1. The general setting: implicative lattices.

1.1. DEFINITION. $\mathbf{A} = (A; \vee, \wedge, \to)$ *is an implicative lattice iff* $(A; \vee, \wedge)$ *is a distributive lattice and* $\to$ *is a binary operation (called the implication of* $\mathbf{A}$*) satisfying the following equations:*

IL1) $x \to (y \wedge y') = (x \to y) \wedge (x \to y')$;
IL2) $(x \vee x') \to y = (x \to y) \wedge (x' \to y)$;
IL3) $x \to (y \vee y') = (x \to y) \vee (x \to y')$;
IL4) $(x \wedge x') \to y = (x \to y) \vee (x' \to y)$.

Implicative lattices provide the most general setting in which our duality can be carried on. Well-known algebras coming from Logic, such as Boolean algebras, de Morgan algebras, MV-algebras, ([7], [13]), or linear Heyting algebras [12], can be characterized as implicative lattices with additional operations and thus, fall within the scope of our approach (see the examples of [11] and also [10], as the first source of the theory).

Implicative lattices are also closely related with lattice-ordered groups, as we now show:

1.2. Example: Recall that a *lattice-ordered group* (l-group, for short) is a partially ordered group such that the underlying order is a lattice. Alternatively, an l-group $\mathbf{G}$ can be defined as an structure $\mathbf{G} = (G; \vee, \wedge, \cdot, ^{-1}, e)$ such that $(G; \cdot, ^{-1}, e)$ is a group, $(G; \vee, \wedge)$ is a lattice and the following equations are satisfied for all $a, b, c \in G$:

1) $a(b \wedge c) = ab \wedge ac$; 3) $a(b \vee c) = ac \vee ac$;
2) $(a \wedge b)c = ac \wedge bc$; 4) $(a \vee b)c = ac \vee bc$.

Two elementary facts about l-groups that will be important in the sequel are:

- The underlying (unbounded) lattice of an l-group is distributive.
- The inverse operation $^{-1}$ is a *Kleene negation*, which means that:
  $(a^{-1})^{-1} = a$; $(a \wedge b)^{-1} = a^{-1} \vee b^{-1}$ and $a \wedge a^{-1} \leq b \vee b^{-1}$ for all $a, b \in G$.
  (For the last condition, see, for example, [3], Chapter III, §4.)

From these facts and the equations 1)–4) above, it can be easily checked that if $\mathbf{G} = (G; \vee, \wedge, \cdot, ^{-1}, e)$ is an l-group and we define $a \to b = a^{-1}b$, then $(G; \vee, \wedge, \to)$ is an implicative lattice, which we call the *implicative lattice of* $\mathbf{G}$.

We will prove that in fact l-groups can be characterized as implicative lattices with a Kleene negation and an additional constant and that the general theory developed below, strengthened in a very simple way, yields a duality theory for these groups.

Given an implicative lattice $\mathbf{A}$, our starting point is to introduce two binary functions on the set of prime lattice filters of $\mathbf{A}$. To ensure good definition in every pair of points, we consider a slight variant of this spectrum, allowing $\varnothing$ and A to be admissible points.

Let's define then $S(A) := \{P \subseteq A : P \text{ is a prime lattice filter of } A\} \cup \{\varnothing, A\}$. Our first binary function is given by the formula

$$PQ = \bigcup_{x \in P} \{y : x \to y \in Q\} \quad \text{for all } P, Q \in S(A).$$

An easy computation, using only the rules IL1)-IL3) shows that effectively $PQ \in S(A)$ provided $P, Q \in S(A)$.

Consider now the family

$$S(A)^c = \{P \subseteq A : P \text{ is a prime lattice ideal of } A\} \cup \{\varnothing, A\}.$$

It is equally easy to show that if $P, Q \in S(A)^c$ and (with a little abuse of notation) we denote again by $PQ = \bigcup_{x \in P} \{y : x \to y \in Q\}$, then $PQ \in S(A)^c$.

Since $P \in S(A)^c$ if and only if its complement P^c belongs to $S(A)$, we can define a second binary function $*$ in $S(A)$ by the formula:

$$P*Q = (P^c Q^c)^c \quad \text{for all } P, Q \in S(A).$$

1.3. Observation. Coming back to Example 1.2. note that if $\mathbf{A}$ is the implicative lattice of an l-group $\mathbf{G}$, $PQ = \{xy : x \in P \text{ and } y \in Q\}$, (i.e., the usual product of sets). In a similar way, $P*Q$ is the complement of the usual product of sets P^c, Q^c.

Since implicative lattices are a juxtaposition of an algebraic structure and an order structure, it is natural to expect that the algebraic structure given by the implication yields some special features in the underlying lattice of $\mathbf{A}$, and thus in $S(A)$. A crucial fact about $S(A)$ is the existence of some distinguished elements, which we introduce in the following:

1.4. Lemma. *For each $P \in S(A)$ and for each $a \in A$, let's define the set $P_a := \{x \in A : x \to a \notin P\}$. Then:*

a) $P_a \in S(A)$.
b) P_a *is the greatest* $Q \in S(A)$ *such that* $a \notin QP$.
c) P_a *is the smallest* $Q \in S(A)$ *such that* $a \in Q*P$.
d) *For all* $a, b \in A$, $P_a \subseteq P_b$ *or* $P_b \subseteq P_a$.

Our next task is to prove that the implication of an implicative lattice $\mathbf{A}$ can be reconstructed from the spectrum $S(A)$ by using either one of the binary functions defined before plus set-theoretical operations.

1.5. Lemma. *Let $\mathbf{A}$ be an implicative lattice and let $\cdot$ and $*$ be the binary functions on $S(A)$ defined above. For each $a \in A$ let's denote by $\sigma(a) = \{P \in S(A) : a \in P\}$. Then:*

i) $\sigma(a \to b)$ *can be obtained from* $\sigma(a)$, $\sigma(b)$, *and* $\cdot$ *by the formula*

$$(\star) \quad \sigma(a \to b) = \bigcap_{P \in \sigma(a)} \{Q : PQ \in \sigma(b)\};$$

ii) $\sigma(a \to b)$ *can be also obtained from* $\sigma(a)$, $\sigma(b)$ *and* $*$ *by the formula*

$$(\star\star) \quad \sigma(a \to b) = \bigcup_{P \in \sigma(a)^c} \{Q : P*Q \in \sigma(b)\}.$$

lattice $\mathbf{A}$, $S(\mathbf{A})$ *is the implicative space of* $\mathbf{A}$ *and for each homomorphism of implicative lattices* $h\colon \mathbf{A} \to \mathbf{A}'$, $S(h)\colon S(\mathbf{A}') \to S(\mathbf{A})$ *is defined by* $S(h)(P) = h^{-1}[P]$ *for all* $P \in S(\mathbf{A}')$.

Then S *is a contravariant functor establishing a duality between* $\mathcal{IL}$ *and* $\mathcal{IS}$.

§3. The duality for lattice-ordered groups.

In order to apply the general schema developed in the previous sections to the theory of lattice-ordered groups, our first step is to characterize l-groups in terms of implicative lattices. To do this, we consider implicative lattices with an additional Kleene negation (standing for the inverse operation) and a constant, standing for the unit of the group:

3.1. Proposition. *Let* $\mathbf{G} = (G; \vee, \wedge, \cdot, ^{-1}, e)$ *be an l-group and define* $a \to b = a^{-1}b$. *Then* $I(\mathbf{G}) := (G; \vee, \wedge, \to, ^{-1}, e)$ *is an implicative lattice with a distinguished element* e *and an unary operation* $\neg x = x^{-1}$ *satisfying:*

i) $\neg\neg a = a$;
ii) $a \to a = e$;
iii) $a \to e = \neg a$;
iv) $a \to (\neg b \to c) = \neg(a \to b) \to c$.

Conversely, let $\mathbf{A} = (A; \vee, \wedge, \to, \neg, e)$ *be an implicative lattice with a distinguished element* e *and an additional unary operation* $\neg$ *fulfilling conditions i)–iv) above. Then, defining* $xy = \neg x \to y$ *and* $x^{-1} = \neg x$, $G(\mathbf{A}) := (A; \vee, \wedge, \cdot, ^{-1}, e)$ *is an l-group such that* $I(G(\mathbf{A})) = A$.

Let's denote now by $\mathcal{IL}^*$ the category whose objects are implicative lattices with a distinguished element e and an additional unary operation $\neg$ satisfying the equations i)–iv) of Proposition 3.1. and whose morphisms are the homomorphisms of implicative lattices preserving e and $\neg$. Let's denote by $\mathcal{G}$ the category of lattice-ordered groups.

From Proposition 3.1, we have that for each object $\mathbf{A}$ of $\mathcal{IL}^*$ there is an l-group, (namely $G(\mathbf{A})$) such that $\mathbf{A} = I(G(\mathbf{A}))$. Note also that a function $h\colon \mathbf{G} \to \mathbf{G}'$ is an homomorphism of l-groups if and only if $h\colon I(\mathbf{G}) \to I(\mathbf{G}')$ is an homomorphism of implicative lattices preserving $\neg$ and e. Thus, $[\mathbf{G}, \mathbf{G}']_{\mathcal{G}} = [I(\mathbf{G}), I(\mathbf{G}')]_{\mathcal{IL}^*}$ and we have the following:

3.2. Theorem. *The map* I *from* $\mathcal{G}$ *to* $\mathcal{IL}^*$ *defined in each l-group* $\mathbf{G}$ *as* $I(\mathbf{G})$ *and in each l-groups homomorphism* h *simply as* h *establishes a categorical equivalence between the category of l-groups and the category* $\mathcal{IL}^*$.

At this point, we have converted l-groups into implicative lattices with an extra constant and an additional Kleene negation satisfying the four equations of Proposition 3.1. Our next step is to give appropriate translations in our topological spaces for the new operations and these four equations.

Recall first that a function g from an ordered topological space $(X; \tau, \leq)$ to $(X;\ \tau, \leq)$ is said an *involution* iff g is an homeomorphism, $g^2 = \mathrm{Id}$, and $x \leq y$ implies $g(y) \leq g(x)$ for all $x \in X$.

all the proper clopen and increasing subsets, with the lattice operations given by union and intersection.

In many of the examples coming from logic the underlying distributive lattice is bounded; as we pointed out before, even in this case we are not allowed to use the usual Priestley spaces, because our binary functions may be not defined in some pair of points (see [11], Observation 2.3). However, we can use the following spaces:

2.3. DEFINITION. Bounded Priestley spaces of type 01.

A bounded Priestley space $\mathbf{X}$ *is of type 01 iff* $\{p_0\}$ *and* $\{p_1\}$ *are open subsets.*

If $\mathbf{X}$ *and* $\mathbf{X}'$ *are bounded Priestley spaces of type 01,* $f\colon \mathbf{X} \to \mathbf{X}'$ *is a 01-morphism iff* f *is a morphism of bounded Priestley spaces satisfying:*

0) $f(p) = p_1'$ *implies* $p = p_1$;
1) $f(p) = p_0'$ *implies* $p = p_0$.

Since $\sigma(0) = \{A\}$ and $\sigma(1) = S(A) \setminus \{\varnothing\}$, from Theorem 2.1 the following can also be derived:

2.4. Theorem: Duality theorem for bounded distributive lattices.

The map F *of Theorem 2.1. establishes a duality between the category of bounded distributive lattices and the category of bounded Priestley spaces of type 01.*

We are ready now to introduce the dual spaces of implicative lattices (compare with our previous version [11], Definition 4.1).

2.5. DEFINITION. Implicative spaces.

i) $\mathbf{X} = (X; \tau, \leq, \cdot, *, p_0, p_1)$ *is an implicative space iff:*
   a) $(X; \tau, \leq, p_0, p_1)$ *is a bounded Priestley space.*
   b) $\cdot$ *and* $*$ *are binary functions, order-preserving in each variable and such that* $\cdot$ *is continuous in the upper topology* $\tau\uparrow$ *and* $*$ *is continuous in the lower topology* $\tau\downarrow$.
   c) $pp_1 = p_1$ *if* $p \neq p_0$; $p_0p_1 = p_1p_0 = p_0$.
   $p{*}p_0 = p_0$ *if* $p \neq p_1$; $p_0{*}p_1 = p_1{*}p_0 = p_1$.
   d) $p \not\leq p'$ *implies* $p'{*}q \leq pq$ *for all* $p, p', q \in X$.
   e) *If* U *is a proper clopen and increasing subset of* X *and* $q \in X$, *there exists an element* $p \in X$ *such that* $p{*}q \in U$ *and* $pq \notin U$.

ii) *If* $\mathbf{X}, \mathbf{X}'$ *are implicative spaces, then* $f\colon \mathbf{X} \to \mathbf{X}'$ *is a morphism of implicative spaces iff it is a morphism of bounded Priestley spaces which satisfies the following two conditions:*
   1) $f(p)f(q) \leq f(pq)$ *for all* $p, q \in X$;
   2) $f(p{*}q) \leq f(p){*}f(q)$ *for all* $p, q \in X$.

The main and last result of this section establishes the categorical duality between implicative lattices and implicative spaces:

2.6. Theorem. Duality theorem for implicative lattices.

Let's denote by $\mathcal{IL}$ *the category of implicative lattices and by* $\mathcal{IS}$ *the category of implicative spaces. Consider the map* $S\colon \mathcal{IL} \to \mathcal{IS}$ *such that for each implicative*

1.6. Corollary: Representation theorem for implicative lattices.
Let $\mathbf{A}$ *be an implicative lattice and consider the family of sets* $\Sigma(S(A)) = \{\sigma(a) : a \in A\}$, *equipped with union, intersection, and with the binary operation* $\sigma(a) \Rightarrow \sigma(b)$ *given by any of the formulas* $(\star)$ *or* $(\star\star)$ *of Lemma 1.5 above.*

Then $(\Sigma(S(A)); \cup, \cap, \Rightarrow)$ *is an implicative lattice and the map* $a \mapsto \sigma(a)$ *is an isomorphism of implicative lattices.*

§2. The general setting: the duality for implicative lattices.

Recall that a contravariant functor F from a category $\mathcal{A}$ to a category $\mathcal{B}$ establishes a *categorical duality* between $\mathcal{A}$ and $\mathcal{B}$ provided:

i) For each object B of $\mathcal{B}$ there is an object A of $\mathcal{A}$ such that $F(A)$ and B are isomorphic.

ii) For each pair of objects A, A' of $\mathcal{A}$, the function from $[A, A']_{\mathcal{A}}$ to $[F(A'), F(A)]_{\mathcal{B}}$ induced by F is one-one and onto.

Also recall that an ordered topological space $(X; \tau, \leq)$ is a *Priestley space* iff it is compact and *totally order-disconnected* (which means that for $x \not\leq y \in X$, there exists a clopen and increasing subset of X containing x but not y)

In a Priestley space $(X; \tau, \leq)$, the family of all the clopen and increasing subsets is the basis of a topology $\tau\uparrow$, called the *upper topology.* (This topology coincides with the Stone topology that we used in [11]). Also, the family of clopen and decreasing subsets is the basis of a second topology $\tau\downarrow$, called the *lower* topology.

Priestley spaces are the dual spaces of bounded distributive lattices; but since we are dealing with distributive lattices not necessarily bounded, we have to consider a slight modification of the usual duality theory. Following Davey and Werner ([8]. Section 2.8) we will say that a Priestley space $(X; \tau, \leq)$ is *bounded* iff there are two points $p_0, p_1 \in X$ such that $p_0 \leq x \leq p_1$ for all $x \in X$.

Let's denote by $\mathcal{BP}$ the category whose objects are bounded Priestley spaces and whose morphisms are those continuous and monotone functions preserving both bounds. Let's denote by $\mathcal{D}$ the category of distributive lattices with all the lattice-homomorphisms. Imitating the usual Priestley duality the following can be derived:

2.1. Theorem. Duality theorem for (unbounded) distributive lattices.
Consider the map F *from* $\mathcal{D}$ *to* $\mathcal{BP}$ *such that:*

a) *For each distributive lattice* $\mathbf{A}$, $F(\mathbf{A}) = (S(A); \tau_A, \subseteq, \varnothing, A)$, *where* τ_A *is the topology having as a subbasis the family*

$$B = \{\sigma(a) : a \in A\} \cup \{\sigma(a)^c : a \in A\}.$$

b) *For each lattice-homomorphism* h *from* $\mathbf{A}$ *to* $\mathbf{A}'$, $F(h)\colon F(A') \to F(A)$ *is defined by* $F(h)(P) = h^{-1}[P]$ *for all* $P \in S(\mathbf{A}')$.

Then F *is a contravariant functor establishing a duality between* $\mathcal{D}$ *and* $\mathcal{BP}$.

2.2. Observation. In particular, by the isomorphism $a \mapsto \sigma(a)$ of Corollary 1.6, the lattice $\mathbf{A}$ can be recaptured from it's bounded Priestley space as the lattice of

3.3. Proposition. *Let* $\mathbf{A}$ *be an implicative lattice with a distinguished element* $e \in A$ *and an additional operation* $\neg$ *satisfying the equations i)–iv) of Proposition 3.1. Let* $S(\mathbf{A})$ *be the implicative space of* $\mathbf{A}$ *and let's define* $\mathbf{g}\colon S(\mathbf{A}) \to S(\mathbf{A})$ *by* $\mathbf{g}(P) = P_e = \{x : \neg x \notin P\}$. *Then:*

1) $\mathbf{g}$ *is an involution such that* $P \subset \mathbf{g}(P)$ *or* $\mathbf{g}(P) \subset P$ *for all* $P \in S(A)$ *(Kleene condition).*
2) $\sigma(e) = \{P \in S(A) : \mathbf{g}(P) \subset P\}$.
3) *The functions* $\cdot$ *and* $*$ *are both associative and satisfy:*
   $P\mathbf{g}(\mathbf{g}(Q)P) \subseteq Q$; $\quad Q \subseteq P{*}\mathbf{g}(\mathbf{g}(Q){*}P)$.
4) $\mathbf{g}(P)P \subset \mathbf{g}(\mathbf{g}(P)P)$; $\quad \mathbf{g}(\mathbf{g}(P){*}P) \subset \mathbf{g}(P){*}P$.
5) $\mathbf{g}(Q) \subset Q$ *implies* $P \subseteq PQ$ *for all* $P \in S(A)$;
   $Q \subset \mathbf{g}(Q)$ *implies* $P{*}Q \subseteq P$ *for all* $P \in S(A)$.

3.4. Observation: Recall that a partially ordered semigroup $\mathbf{H} = (H; \cdot, \leq)$ is *right-residuated* iff for all $a, b \in H$, there exists an element $(a/b) \in H$ such that $x \leq (a/b)$ iff $xb \leq a$. $\mathbf{H}$ is a *left-residuated* semigroup iff for all $a, b \in H$ there exists an element $(a\backslash b) \in H$ such that $x \leq (a\backslash b)$ iff $bx \leq a$. $\mathbf{H}$ is called *residuated* iff it is both right and left-residuated. Any partially ordered group is residuated, the residual being precisely $x \to y = x^{-1}y$.

It is not difficult to show that $(S(\mathbf{A}); \subseteq, \cdot)$ is a residuated semigroup, with right-residual $(Q/P) = \mathbf{g}(P\mathbf{g}(Q))$ and left-residual $(Q\backslash P) = \mathbf{g}(\mathbf{g}(Q)P)$. Also, $(S(\mathbf{A}); \supseteq, *)$ is residuated, with right-residual $(Q/P) = \mathbf{g}(P{*}\mathbf{g}(Q))$ and left-residual $(Q\backslash P) = \mathbf{g}(\mathbf{g}(Q){*}P)$.

Let's introduce now the dual spaces of l-groups (compare again with our previous version [11], Definition 5.7):

3.5. DEFINITION: Let $\mathbf{X}$ be an implicative space. We say that $\mathbf{X}$ is an *l-space* iff:

a) There is an involution $g\colon \mathbf{X} \to \mathbf{X}$ such that $g(p) < p$ or $p < g(p)$ for all $p \in X$.
b) The set $U_e := \{p \in X : g(p) < p\}$ is a closed subset.
c) $\cdot$ and $*$ are both associative and satisfy:
   $pg(g(q)p) \leq q$; $\quad q \leq p{*}g(g(q){*}p)$.
d) $g(p)p < g(g(p)p)$ and $g(g(p){*}p) < g(p){*}p$ for all $p \in X$.
e) $g(q) < q$ implies $p \leq pq$ for all $p \in X$;
   $q < g(q)$ implies $p{*}q \leq p$ for all $p \in X$.

Condition a) says that $(X; \tau, \leq, g)$ is a *Kleene space*; condition b) stands for the existence of the unit. Note that all the remaining conditions are first-order sentences of the language $\mathcal{L} = \{\leq, \cdot, *, g\}$.

If $(\mathbf{X};\ g)$ and $(\mathbf{X};\ g')$ are l-spaces, a function $f\colon X \to X'$ is a *morphism of l-spaces* iff f is a morphism of implicative spaces and $f(g(p)) = g'(f(p))$ for all $p \in X$.

We are ready to state the main theorem of the section:

3.6. Theorem. The duality theorem for l-groups. *Let* S *be the map sending each object* $\mathbf{A}$ *of* $\mathcal{IL}^*$ *to* $(S(\mathbf{A}); \mathbf{g})$ *and each morphism* $h\colon \mathbf{A} \to \mathbf{A}'$, *to* $S(h)\colon S(\mathbf{A}') \to S(\mathbf{A})$, *given as before by* $S(h)(P) = h^{-1}[P]$ *for all* $P \in S(\mathbf{A}')$.

Then S establishes a duality between the category $\mathcal{IL}^*$ and the category $\mathcal{IS}^*$ of l-spaces. Thus, by Theorem 3.2, the contravariant functor $I \circ S$ establishes a duality between the category of l-groups and the category of l-spaces.

Let's call *abelian l-spaces* those l-spaces in which $\cdot$ and $*$ are conmutative. From Observation 1.3 and Theorem 3.6 also the following can be derived:

3.7. Theorem. Duality for abelian l-groups. *The map S of Theorem 3.6 establishes a duality between the category of abelian l-groups and the (full) subcategory of abelian l-spaces.*

REFERENCES

[1] Balbes R. and Dwinger Ph., *Distributive lattices*, Univ. Miss. Press, 1975.

[2] Bigard A. et al., *Groupes et Anneaux Reticules*, Lecture Notes in Mathematics 608. Springer Verlag.

[3] Birkhoff G., *Lattice Theory*, Third Edition, American Mathematical Society Colloquium Publications, Vol.25, 1967.

[4] Cornish W. and Fowler P., *Coproducts of De Morgan algebras*, Bull. Austral. Math. Soc. 16 (1977), 1–13.

[5] Cornish W. and Fowler P., *Coproducts of Kleene algebras*, Bull. Austral. Math. Soc. Ser A 27 (1978), 209–220.

[6] Cornish W., *Lattice ordered groups and BCK-algebras*, Math.Japonica 25 4 (1980), 471–476.

[7] Chang C.C., *Algebraic Analysis of many valued logics*, Trans. Am. Math. Soc. 88 (1958), 467–490.

[8] Davey B. and Werner H., *Dualities and equivalences for varieties of algebras.*, Colloq. Math. Soc. Janos Bolyai 33, North-Holland, Amsterdam (1983), 101–275.

[9] Fuchs L., *Partially Ordered Algebraic Systems*, Pergamon, Oxford, 1963.

[10] Martinez N. G., *The Priestley duality for Wajsberg algebras*, Studia Logica XLIX I (1990), 31–46.

[11] Martinez N.G., *A topological duality for a class of lattice-ordered algebraic structures including l-groups*, To appear in Algebra Universalis.

[12] Monteiro A., *Sur les algebres de Heyting symetriques*, Portugaliae Mathematica, Fasc. 1–4 39 (1980).

[13] Mundici D., *Interpretation of $AF - C^*$-algebras in Lukasiewicz sentential Calculus*, Journal of Functional Analysis, 65, No. 1 (1986), 15–63.

[14] Priestley H. A., *Representation of distributive lattices by means of ordered Stone spaces*, Bull. London. Math. Soc. 2 (1972), 186–190.

[15] Priestley H. A., *Ordered topological spaces and the representation of distributive lattices*, Bull. London. Math.Soc. 3 (1975), 507–530.

[16] Stone M. H., *Topological representation of distributive lattices and Brouwerian logics*, Casopis [illegible] 67 (1937), 1–25.

Open Questions around Büchi and Presburger Arithmetics

Christian Michaux [1]
Faculté des Sciences
Université de Mons-Hainaut
Mons, Belgium
smichaux@vm1.umh.ac.be

Roger Villemaire[2]
Département de mathématiques et d'informatique
Université du Québec à Montréal
Montréal (Québec), Canada H3C 3P8
villem@math.uqam.ca

Abstract

During the last three years several researchs on Cobham's and Semenov's theorems lead to results about Büchi Arithmetics and Presburger Arithmetic. The reader will find some of these results in [Br,Han 94],[B,H,M,V 94],[Fab 92], [Mi,Vil 93], [Mi,Vil 94],[Much 91],[Po 94],[Vil 92a] [Vil 92b],[Vil 92c] ...
In this survey we investigate around two classes of questions related to these results. One is concerned with definability questions, the other one with decidability questions. At our knowledge, most of them are open.
We will also discuss extensions of Cobham's and Semenov's theorems to numeration systems associated with a θ-shift.

1. Preliminaries.

In this section we give some basic definitions about automata theory and k-recognizability of sets of natural numbers.
We will use them in the sequel without reference. The reader will find more informations in Eilenberg's book [Eil 74, chapter 5].

[1]The first author was partially supported by ESPRIT-BRA Working Group 6317 *ASMICS* and by HUMAN CAPITAL AND MOBILITY project *Model theory and applications*

[2]The second author was partially supported by La Fondation de l'UQAM. He would also like to thank the Institute of Mathematics and Computer Science of the University of Mons-Hainaut for its hospitality and the Fonds National de la Recherche Scientifique of Belgium for financial support.

Let Σ be an *alphabet*, i.e. a finite set. We denote by Σ^* the set of *words* of finite length on Σ containing the *empty* word λ formed of no symbol. Any subset L of Σ^* is called a *language* on the alphabet Σ.

Definition Let Σ be an alphabet. A Σ-*automaton* is a finite labelled directed graph $\mathcal{A}$ whose vertices are called *states* and which satisfies the following properties.

a) There is a distinguished state called the *initial state.*

b) Some of the states are said to be *final states.*

c) For any state q and any element σ of the alphabet Σ, there is one and only one arrow labelled by σ leaving q.

Furthermore we have the following definitions.

Definition A word $\alpha \in \Sigma^*$ is said to be *accepted* by the Σ-automaton $\mathcal{A}$ if starting at the initial state of $\mathcal{A}$ and reading α from left to right taking arrows labelled by the letters of α, one reaches a final state.

Definition A language L on Σ is said to be Σ-*recognizable* if there exists a Σ-automaton such that the set of words accepted by this automaton is exactly L.

Remark Our definition of automaton is what is usually called a *complete deterministic automaton.* A *non-deterministic* automaton is one in which there can be many arrows with the same label leaving some state. It is well-known (see [Eil 74]) that the sets recognizable by non-deterministic automata are the same as the ones recognizable by deterministic automata; so there is no restriction in considering deterministic automata.

We here choose to read words from left to right. Reading from right to left would not change the notion of recognizability, but it would be unnatural with our definition of recognizability for subsets of IN^n (see below).

Let Σ_k be the alphabet $\{0, 1, \ldots, k-1\}$. For n a positive integer, let $[n]_k$ be the word on Σ_k which is the inverse of the k-ary expansion of n, i.e. if $n = \Sigma_{i=0}^{s} \lambda_i k^i$ with $\lambda_i \in \{0, \ldots, k-1\}$, $\lambda_s \neq 0$, then $[n]_k = \lambda_0 \cdots \lambda_s$. By convention we define $[0]_k$ as the empty word.

Definition For $k \in IN$, we say that a subset L of IN is k-*recognizable* if $\{[n]_k; n \in L\}$ is Σ_k-recognizable.

It is quite useful to have a notion of k-recognizability for subsets of IN^n for all

positive natural number n. For this,we follow the approach of [Hod 83] which is different from the definition generally used in language theory (for instance in [Be,Re 88]). Nevertheless it is a natural point of view since it will allow Büchi's theorem to work in full generality (see section 2). It is also the point of view adopted by [Sal 87] and [Sem 77].

It is possible to represent tuples of natural numbers by words on $(\Sigma_k^n)^*$ in the following way. Let $(m_1, \ldots, m_n) \in IN^n$. Add on the right of each $[m_i]_k$ the minimal number of 0 in order to make them all of the same length and call these words ω_i. Let $\omega_i = \lambda_{i1} \cdots \lambda_{is}$ where $\lambda_{ij} \in \Sigma_k$. We represent $(m_1, \ldots, m_n)$ by $[(m_1, \ldots, m_n)]_k$ which is the word $(\lambda_{11}, \lambda_{21}, \ldots, \lambda_{n1})$ $(\lambda_{12}, \lambda_{22}, \ldots, \lambda_{n2}) \cdots$ $(\lambda_{1s}, \lambda_{2s}, \ldots, \lambda_{ns}) \in (\Sigma_k^n)^*$, i.e. the word formed of the tuples of first letters, second letters etc...

Definition We say that a subset L of IN^n is *k-recognizable* if $\{[(m_1, \ldots, m_n)]_k; (m_1, \ldots, m_n) \in L\}$ is Σ_k^n-recognizable.

Let us end this section with some notations. We will denote the set of nonnegative integers by $\mathbb{N}$, the set of integers by $\mathbb{Z}$ and the set of nonnegative reals by IR^+.

2. Definable sets in Büchi Arithmetics.

The structures $< IN, +, V_k >$ for $k = 2, 3, \ldots$ are central in all the paper. Here V_k is the function which sends a nonzero natural number to the greatest power of k dividing it[3]. The first-order structure $< IN, +, V_k >$ will be called *Büchi Arithmetic of base k*. The importance of Büchi Arithmetics come from the following first-order version of Büchi's theorem:

Theorem B A subset of IN^n is k-recognizable if and only if it is first-order definable in the structure $< IN, +, V_k >$.

It has an immediate corollary :

Corollary B $< IN, +, V_k >$ is decidable.

The reader will find a clear exposition of the method of proof of Corollary B in [Hod 83].

Büchi's theorem is originally stated in terms of definability in $WS1S$, the weak monadic second-order theory of one successor, but only in the case $k = 2$ (see also [McNa 63]). A general statement of Büchi's theorem in terms of definability

[3]For example $V_6(72) = 36$.

in $WS1S$ can be find in [Tho 90] and [Vil 92c] for example. However the first-order version presented here was already present in Büchi's paper [Bu 60] (but only in the case $k = 2$ and with some flaw). The reader will find informations and a proof of this version in [B,H,M,V 94, pages 202, 207-211].

In the sequel *definable* will be intended for *first-order definable*. We will also say *k-definable* instead of definable in the structure $< IN, +, V_k >$.

In the following lemma we summarize some basic features of $< IN, +, V_k >$ which are the keys for a proof of theorem B as in [B,H,M,V 94]: these facts allow to code the behaviour of an automaton by a first-order formula of the language $< +, V_k >$.
We include it here because it gives the flavour of the relationship between Σ_k-automata and Büchi Arithmetic of base k. It is also the prototype of the generalization investigated in section 6.

Lemma B
(1) The set of powers of k (denoted by P_k in the sequel) is k-definable (by the formula $V_k(x) = x$)

(2) Let be the relations $\in_{j,k}(x, y)$, for $0 \leq j < k$, meaning that y is a power of k, and the coefficient of y in the k-ary expansion of x is equal to j, i.e., $x = \sum_{\in_{j,k}(x,y)} j \cdot y$. For powers y strictly greater than x, we consider $\in_{0,k}(x, y)$ to be satisfied (leading zeros).

The relations $\in_{j,k}(x, y)$, $0 \leq j < k$, are definable in $< IN, +, V_k >$ by the formula

$$P_k(y) \ \wedge \ [\, (\exists z)(\exists t)(x = z + j \cdot y + t) \ \wedge \ (z < y) \ \wedge \ (\, (y < V_k(t)) \vee (t = 0)\,)\,]\ .$$

Roughly this formula says that the powers of k of the k-ary expansion of x are shared into three groups : one group consists of y only (or equivalently the integer $j \cdot y$), the powers less than y are the second group (the integer z) and the powers greater than y are the third group (the integer t). So, it is possible to express in $< IN, +, V_k >$ the different letters $\lambda_0, \ldots, \lambda_t$ of the k-ary expansion $[n]_k = \lambda_0 \ldots \lambda_t$ of any integer n, as well as leading zeros.

Proof of lemma B is easy (see [B,H,M,V 94]).

The other direction of theorem B (which claims that all k-definable relations is k-recognizable) is a consequence that addition (the ternary relation) is k-recognizable (see [Hod 83] and [B,H,M,V 94]).

Originally Cobham's and Semenov's theorems were stated in terms of k-recognizability of sets of natural numbers (see [Co 69] and [Sem 77]).

Using theorem B we can state them in an equivalent first-order version :

Theorem C (Cobham's Theorem) Let k and l be multiplicatively independent[4]. If $L \subseteq IN$ is k- and l-definable, then L is definable in Presburger Arithmetic (i.e. in the structure $< IN, + >$).

In the original version [Co 69],"definable in Presburger Arithmetic" was replaced by "ultimately periodic"[5].

Theorem S (Semenov's Theorem) Let k and l be multiplicatively independent. If $L \subseteq IN^n$ is k- and l-definable, then L is definable in Presburger Arithmetic[6].

Semenov's theorem is the natural generalization of Cobham's theorem to higher dimensions.
We will discuss around theorems C and S and their proofs in sections 3, 4, 5 and 6 of this survey.

Theorem S recently received a counterpart (see [Vil 92a],[Vil 92b],[Vil 92c]) :

Theorem V Let k and l be multiplicatively independent. The structures $< IN, +, V_k, V_l >$ and $< IN, +, \cdot >$ are interdefinable[7].

Corollary V $< IN, +, V_k, V_l >$ is undecidable.

Section 7 is concerned with some open questions related to theorem V.

[4]Two reals k and l are said multiplicatively independent if the only solution in integers of the equation $k^m = l^n$ is the trivial one $m = n = 0$.

[5]A subset X of the nonnegative integers is said ultimately periodic if there exist d and p in IN such that for all $x \geq d$, x belongs to X if and only if $x + p$ belongs to X. The equivalence between ultimately periodic and definable in Presburger Arithmetic goes back to [Presb 29](see [End 72, chapter 3] for a more accessible reference).

[6]Similarly to the case of subsets of $\mathbb{N}$, subsets of IN^n which are definable in $< IN, + >$ can be characterized in terms of some periodicity (see [G,S 66]).

[7]Two structures are said interdefinable if the classes of definable relations are the same in both structures.

The results S and V are summarized by the following picture (k and l multiplicatively independent)[8].

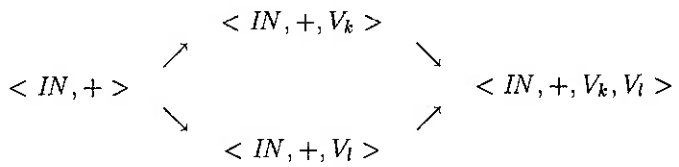


Figure 1. Theorems S and V

We can now end this section with our first question.
¿From a logical point of view Semenov's theorem says that : for k and l multiplicatively independent, let φ_k be a formula in the language $< +, V_k >$ and φ_l a formula in the language $< +, V_l >$, if $\varphi_k \leftrightarrow \varphi_l$ in the theory of $< IN, +, V_k, V_l >$ (which is the theory of $< IN, +, \cdot >$), then φ_k and φ_l are equivalent to a formula φ in the language $< + >=< +, V_k > \cap < +, V_l >$. This raises the following question :

Question 1 *Is it true that the following interpolation holds whenever k and l are multiplicatively independent?*

Let φ_k be a formula of $< +, V_k >$ and φ_l a formula of $< +, V_l >$, if $\varphi_k \rightarrow \varphi_l$ in the theory of $< IN, +, V_k, V_l >$, then there exists a formula φ in the language $< + >$ such that $\varphi_k \rightarrow \varphi \rightarrow \varphi_l$ (in the theory of $< IN, +, V_k, V_l >$ of course).

3. Around the proofs of Cobham's and Semenov's theorems.

In [Eil 74, page 118], S. Eilenberg challenged people to find a more reasonable proof of Cobham's theorem. The original proof was combinatorial and quite technical. In 1977 A. Semenov extended Cobham's theorem to higher dimensions (theorem S). The proof in [Sem 77] was complicated.
Eilenberg's challenge stimulated work about Cobham's theorem. In 1982 G. Hansel pointed out an intermediate result already present in Cobham's proof (called below theorem CH). By using it in a clever way (see [Han 82] and also [Per 90]), he succeeded in giving a more reasonable proof of Cobham's theorem. In 1991, A. Muchnik (see [Much 91]) gave a comprehensible proof of Cobham's

[8] It is easy to show (see for example [B,H,M,V 94, pages 213-214]) that $< IN, +, V_k >$ and $< IN, +, V_l >$ are interdefinable whenever k and l are multiplicatively dependent.

and Semenov's theorems. The proof is based on his powerful definability criterion (see section 5) and on a fine study of combinatorial properties of equivalence relations associated to Σ_k-automata (see also [B,H,M,V 94] for an exposition of this result). It is much simpler than Semenov's proof and also gives a new proof of Cobham's theorem. In [Mi,Vil 93] and [Mi,Vil 94] we formulate Cobham's and Semenov's theorems as stated in section 2 by using Buchi's theorem. Then we succeed to prove them as corollaries of new results on Presburger Arithmetic (theorem E and theorem MV below).
For additional details about the different proofs of Cobham's and Semenov's theorems, the reader can read the bibliographic notes of the survey [B,H,M,V 94, pages 219-220].

In the remaining of this section we give the architecture of our proof of Cobham's and Semenov's theorems as it appears in [Mi,Vil 94].

We need the next definitions.

Definition Let $L = \{l_n; n \in IN\}$ be a subset of IN listed in increasing order. Let D_L be the maximum of the set $\{l_{n+1} - l_n; n \in IN\}$ if it exists and infinity otherwise.

Definition We say that a subset L of IN is *expanding* if $D_L = \infty$.

Remark $D_L < \infty$ if and only if there is a bound on the distance between consecutive elements of L.

We first prove the next result about definability in Presburger Arithmetic :

Theorem E Let $L \subseteq IN$. If L is not definable in $< IN, + >$, then there is a $L' \subseteq IN$ definable in $< IN, +, L >$, which is expanding. (Actually we give two explicit sets one of which can be chosen to be L', see section 4).

We also use the following theorem due to Cobham and Hansel.

Theorem CH Let k and l be multiplicatively independent. If $L \subseteq IN$ is k- and l-definable, then it is non-expanding.

We can now give the proof of theorem C.

Theorem C (Cobham's Theorem) Let k and l be multiplicatively independent. If $L \subseteq IN$ is k- and l-definable, then L is definable in Presburger Arithmetic (i.e. in the structure $< IN, + >$).

Proof Let $L \subsetneq IN$ be k- and l-definable and not definable in $< IN, + >$. By **CH**, L is not expanding. Applying **E** we get an $L' \subseteq IN$ which is expanding. Still by **CH**, L' is definable in $< IN, +, L >$, so it is k- and l-definable. This contradicts **CH**.

Now we turn to our proof of Semenov's theorem. Let us recall it :

Theorem S (Semenov's Theorem) Let k and l be multiplicatively independent. If $L \subseteq IN^n$ is k- and l-definable, then L is definable in Presburger Arithmetic.

Proof Immediate from Cobham's theorem and from the following result on Presburger Arithmetic :

Theorem MV $L \subseteq IN^n$ is definable in $< IN, + >$ if and only if every subset of IN which is definable in $< IN, +, L >$ is definable in $< IN, + >$.

The proof of theorem MV uses Muchnik's definability criterion (see section 5). Theorem MV allows us to lift definability results from dimension 1 to higher dimensions.

Each of the next three sections is devoted to the discussion of a single step of our proof of Cobham's and Semenov's theorems: theorem E in section 4, theorem MV in section 5 and theorem CH in section 6.

4. Around Theorem E.

In this section we make the statement **E** more precise and formulate some open questions about it.
We will need the following notation.

Notation For $L \subseteq IN$ and $n, m \in IN$ let

$$L[n, m] = \{x \in IN; n + x \in L \text{ and } n + x \leq m\}.$$

We will say that $L[n, m]$ is a *factor* of L of length[9] $m - n$.

Remark Often in language theory one identifies $L \subseteq IN$ with the infinite word w_L on $\{0, 1\}$, having a 1 in position i if and only if $i \in L$. With this point of view $L[n, m]$ is the analog of the factor $w_L[n, m]$ (formed of the n-th to m-th

[9] it would be more natural to say of "length $m - n + 1$", by choosing "$m + n$" we avoid superfluous technicalities in the following computations.

symbol of w) of the infinite word w_L. Hence we have that $L[n,m] = L[n',m']$ if and only if $w_L[n,m] = w_L[n',m']$.

For n, m, $k \in IN$ such that $n < m$ and $m - n = k$, we have that $L[n,m] \subseteq \{0,1,\ldots,k\}$. Hence for a fixed k there are only finitely many possibilities for $L[n,m]$. Therefore for any k there is some factor of length k which is repeated. We will make use of this fact.

We will first define two functions $\tilde{d}_L$ and $\tilde{\alpha}_L$ and then modify them slightly in order to obtain two nondecreasing functions d_L and α_L.

Definition Let $L \subseteq IN$. Define $\tilde{d}_L : IN \to IN$ to be the function which sends $n \in IN$ to the smallest natural number $d \neq 0$ such that there exists an $a \in IN$ with

$$L[a, a+n] = L[a+d, a+d+n].$$

As said before, there are only finitely many factors of length n, hence there is at least one of them which is repeated. Therefore $\tilde{d}_L$ is defined over all of IN. Actually $\tilde{d}_L(n)$ is the smallest distance by which you can shift a factor of length n in order to recover another copy of it.
The following fact will be useful.

Proposition 4.1 $\tilde{d}_L$ is an nondecreasing function.

Proof Trivial, if one thinks in terms of factors (see the remark after the definition of $L[n,m]$).

Definition Let $L \subseteq IN$. Define $\tilde{\alpha}_L : IN \to IN$ to be the function which sends $n \in IN$ to the smallest natural number a such that

$$L[a, a+n] = L[a+\tilde{d}_L(n), a+\tilde{d}_L(n)+n].$$

Remark Hence $\tilde{\alpha}_L(n)$ is the smallest position at which starts a factor of length n repeating itself at distance $\tilde{d}_L(n)$.

It would be convenient (for technical reasons only apparent in the proofs) to have that $\tilde{\alpha}_L$ is nondecreasing. Since this is not always the case, we will need the following definitions.

Definition Let $U \subseteq IN$ be defined as follows. There are two cases.

1. If $Im\tilde{\alpha}_L$ is finite, then take $U = \tilde{\alpha}_L^{-1}(s)$, for the smallest $s \in Im\tilde{\alpha}_L$ such that $\tilde{\alpha}_L^{-1}(s)$ is infinite. (We denote by $Im\tilde{\alpha}$ the range of $\tilde{\alpha}$.)
2. If $Im\tilde{\alpha}_L$ is infinite, then let $U = \{x \in IN; \tilde{\alpha}_L(y) < \tilde{\alpha}_L(x), \text{ for all } y < x\}$.

In both cases U is infinite. Furthermore the restriction of $\tilde{\alpha}_L$ to U is nondecreasing.

Definition Define $d_L : IN \to IN$ to be the function which sends $n \in IN$ to $\tilde{d}_L(m)$, where m is the smallest element of U which is greater or equal to n.

Definition Define $\alpha_L : IN \to IN$ to be the function which sends $n \in IN$ to $\tilde{\alpha}_L(m)$, where m is the smallest element of U which is greater or equal to n.

Hence it is clear that

Proposition 4.2 The functions d_L and α_L are nondecreasing and also

$$L[\alpha_L(n), \alpha_L(n) + n] = L[\alpha_L(n) + d_L(n), \alpha_L(n) + d_L(n) + n].$$

Moreover we have:

Proposition 4.3 The functions d_L and α_L are definable in the structure $< IN, +, L >$.

The proof of proposition 4.3 is straightforward by tracing trough all the previous definitions.

We can now state a constructive[10] version of theorem E.

Theorem E Let $L \subseteq IN$. If L is not definable in $< IN, + >$, then either Imd_L or $Im\alpha_L$ is expanding.

The proof follows from the following combinatorial lemmas.

Lemma 4.4 If Imd_L and $Im\alpha_L$ are non-expanding, then d_L is eventually constant.

[10] in the sense that if L is Σ_k-recognizable, then Imd_L and $Im\alpha_L$ are Σ_k-recognizable.

Lemma 4.5 If $Im\alpha_L$ is non-expanding and d_L is eventually constant, then L is ultimately periodic, hence it is definable in $< IN, + >$.

The reader will find the proofs in [Mi,Vil 93] and [Mi,Vil 94, section 3].

In [Mi,Vil 94], we give two subsets L_1, L_2 of IN with the following properties.

1) Imd_{L_1} is non-expanding and $Im\alpha_{L_1}$ is expanding.

2) Imd_{L_2} is expanding and $Im\alpha_{L_2}$ is expanding.

L_1 is the set of powers of 2. One can easily show that $d_{L_1} = 1$ and $\alpha_{L_1}(0) = 1$ and $\alpha_{L_1}(n) = 2^{\lceil \log_2(n+3) \rceil}$ for $n > 0$.

L_2 is the Thue-Morse set, i.e. the set of natural numbers which have an even number of 1 in their representations in base 2.
In this case we have :

$d_{L_2}(0) = 1$, $\alpha_{L_2}(0) = 1$

$$d_{L_2}(n) = \begin{cases} 2^{\lfloor \log_2(n-1) \rfloor} \cdot 3 & \text{if } n \text{ is even and } n \neq 0 \\ 2^{\lfloor \log_2(n+1) \rfloor} & \text{if } n \text{ is odd} \end{cases}$$

$$\alpha_{L_2}(n) = \begin{cases} 2^{\lfloor \log_2(n-1) \rfloor} \cdot 11 & \text{if } n \text{ is even and } n \neq 0 \\ 2^{\lfloor \log_2(n+1) \rfloor} & \text{if } n \text{ is odd} \end{cases}$$

The reader will find all the details of the computation of d_L and α_L in both cases in [Mi,Vil 94].

There is now a natural question :

Question 2 *Does there exists a subset L of IN such that $Imd_L(n)$ is expanding and $Im\alpha_L$ is non-expanding ?*

Remark *Note that both of the sets L_1 and L_2 are 2-recognizable sets. These examples and the feeling that a set sastifying the conditions required in question 2 should be strange motivate the following conjecture by G. Hansel*

Question 3 *If L is k-recognizable for some k, then Imd_L is expanding implies that $Im\alpha_L$ is expanding.*

5. Around Theorem MV.

Up to now there is no good notion of expanding subsets of IN^n for $n \geq 2$, in the sense that we cannot extend theorem E and theorem CH to higher dimensions in a direct way.
This difficulty is turned by theorem MV which yields an extension of theorem E to higher dimensions.
In the sequel we will use the following definition and notation.

Definition Let $R \subseteq IN^n$. We say that R *does not extend* $< IN, + >$, if every subset of IN which is definable in $< IN, +, R >$ is definable in $< IN, + >$[11], i.e. is ultimately periodic.

Remark We consider functions as relations, so the above concept applies also to functions.

Notation Let $\bar{r} \in IN^n$, $\bar{r} = (r_1, \ldots, r_n)$. We will write $(\bar{r})_i$ for r_i.

Let us recall the nontrivial part of theorem MV.

Theorem MV Let L be a subset of IN^n. If L does not extend $< IN, + >$, then L is definable in $< IN, + >$.

In the remaining of the section we discuss it.
First we will give the proof of a very simple case of theorem MV which is appealing. Then the proof of the theorem consists in a reduction of the general case to this special one by using Muchnik's definability criterion. In the second half of this section we examine some conjectural extensions of theorem MV.

We begin by the simple case of theorem MV.

Proposition 5.1 Let f be a function from V to IN^n, where V is an infinite subset of IN. Let us assume that $(f)_i$ is nondecreasing for all $i = 1, \ldots, n$ and increasing for some $i \in \{1, \cdots, n\}$.
If f does not extend $< IN, + >$, then f is definable in $< IN, + >$.

Before to go through the proof we need some definitions.

Definition We will say that two sets v and w are *equal almost evrywhere* (notation $v =_{a.e.} w$) if the symmetric difference of v and w is finite.
In the sequel we will also write $v =_{a.e.} w$ for functions. In this case the notation is intended to mean that the graph of v and the graph of w are equal almost everywhere

[11] In the sequel we will consider this notion relatively to other structures on $\mathbb{N}$.

Definition Let $L \subseteq IN^n$ and $\bar{x} \in \mathbb{Z}^n$. We denote by $\bar{x} + L$ the set $\{\bar{x} + \bar{l} \in IN^n; \bar{l} \in L\}$.

Remark Remember that $L \subseteq IN$ is definable in $< IN, + >$ if and only if $L =_{a.e.} x + L$ for some non-zero $x \in IN$.

Definition We will call a subset L of IN^n a *line* if there exist two elements $\bar{a}$ and $\bar{b}$ in IN^n such that $L = \{\bar{a} + j \cdot \bar{b}; j \in IN\}$. The lines are ultimately periodic sets of IN^n.

Remark Note that for $\bar{b} \in IN^n$ the family of lines $F(\bar{x}) = \{\bar{x} + j \cdot \bar{b}; j \in IN\}$ is definable in $< IN, + >$, i.e. there is a formula $\varphi(\bar{x}, \bar{y})$ equivalent to $\bar{y} \in F(\bar{x})$.

Definition Let $W \subseteq U \times V$ and let $v : W \to W'$. For $x \in U$ we denote by $\mathrm{Im}v(x, \cdot)$ the set $\{v(x, y); y \in V\}$.
For $u : V \to W$, $\mathrm{Im}u(\cdot)$ denotes $\{u(y); y \in V\}$.

Let f be the function associated to the line $\{\bar{a} + j \cdot \bar{b}; j \in IN\}$, i.e. $f(j) = \bar{a} + j \cdot \bar{b}$, it is clear that f is definable in $< IN, + >$.
Moreover f satisfies the conclusions of the following lemma which is the key to a proof of proposition 5.1 .

Lemma 5.1 Let $f : V \to IN^n$. Under the assumptions of proposition 5.1 we have that

a) there exists $\bar{c} \in IN^n$, $\bar{c} \neq \bar{0}$, such that $\mathrm{Im}f(\cdot) =_{a.e.} \bar{c} + \mathrm{Im}f(\cdot)$.

b) $G = \{\bar{x} \in \mathbb{Z}^n; Imf(\cdot) =_{a.e.} \bar{x} + Imf(\cdot)\}$ is a non-trivial additive group generated by one element of IN^n.

Proof of lemma 5.1 and proposition 5.1
Since for all $i = 1, \cdots, n$ $(\mathrm{Im}f(\cdot))_i$ is a subset of IN definable in $< IN, +, f >$ it follows from the fact that f does not extend $< IN, + >$ that $(\mathrm{Im}f(\cdot))_i$ is ultimately periodic for all $i = 1, \cdots, n$. Therefore since $(f)_i$ is nondecreasing $(i = 1, \ldots, n)$ there exists a finite set $S \subseteq IN^n$ such that for all $v \in V$ $f(v^+) - f(v) \in S$, where v^+ is the successor of v in V. Let $A_{\bar{s}}$ be $\{v \in V; f(v^+) - f(v) = \bar{s}\}$, $\bar{s} \in S$. Note that $\bigcup_{\bar{s} \in S} A_{\bar{s}} = V$. Since the sets $A_{\bar{s}}$ are definable in $< IN, +, f >$ they are ultimately periodic ($A_{\bar{s}} \subseteq V \subseteq IN$), hence there exists $a_{\bar{s}} \neq 0$, $b_{\bar{s}} \in IN$ such that for $v \geq b_{\bar{s}}$, $v \in A_{\bar{s}}$ if and only if $v + a_{\bar{s}} \in A_{\bar{s}}$. Let b be the maximum of the $b_{\bar{s}}$ for $\bar{s} \in S$ and a be the l.c.m.[12] of the $a_{\bar{s}}$, $\bar{s} \in S$. Obviously we have that for all $\bar{s} \in S$ and for all $v \geq b$, $v \in A_{\bar{s}}$ if and only if $v + a \in A_{\bar{s}}$.

[12] l.c.m is a shorthand for least common multiple.

Let us now show by induction on v that $f(v+a) = f(v) + [f(b+a) - f(b)]$, for all $v \geq b$. Note that since $(Imf(\cdot))_i$ is increasing for at least one i, we have that $f(b+a) - f(b) \neq \bar{0}$. Taking $f(b+a) - f(b)$ as the value of $\bar{c}$, we will have that $\mathrm{Im}f(\cdot) = \bar{c} + \mathrm{Im}f(\cdot)$ (e.f.m.p). Let us remark that $\bar{c}$ is in IN^n since the $(f)_i$ $(i = 1, \cdots, n)$ are nondecreasing. For $v = b$ there is nothing to show. Suppose it holds for v. If $v \in A_{\bar{s}}$ we have that $v + a \in A_{\bar{s}}$ and $f((v+a)^+) = f(v+a) + \bar{s}$ and $f(v^+) = f(v) + \bar{s}$. But $(v+a)^+ = v^+ + a$. So we have that $f(v^+ + a) = f((v+a)^+) = f(v+a) + \bar{s}$ and using induction hypotheses we have that $f(v^+ + a) = f(v) + \bar{s} + [f(b+a) - f(b)] = f(v^+) + [f(b+a) - f(b)]$. So part (a) of the lemma is proved

Since every natural number $v \geq b$ can be written as $v_0 + j \cdot a$ with $b \leq v_0 < b + a$ and $j \in IN$ we have from the preceding paragraph that $f(v) = f(v_0) + j \cdot \bar{c}$ (for $v \geq b$ and $\bar{c} = f(b+a) - f(b)$).Thus the graph of f is an union of a finite set of points and of finitely many parallel lines (there is at least one line since V is infinite). From the remark about lines preceding the proof it is now clear that (b) holds and that f is definable in $< IN, + >$.

The next step towards a proof of theorem MV is a uniform version of part (b) of lemma 5.1 .

Lemma 5.2 Let $w : W \rightarrow IN^n$, where W is a subset of IN^2. Let $\tilde{W}$ be the set of u such that $w(u,x)$ is defined for an infinite number of x. Suppose that w does not extend $< IN, + >$ and that for all $u \in \tilde{W}$, $(w(u,\cdot))_i$ [13] satisfy the asumptions of proposition 5.1. Let $\bar{c}_u \in IN^n$ be the generator of $G(u) = \{\bar{x} \in \mathbb{Z}^n; Imw(u,\cdot) =_{a.e.} \bar{x} + Imw(u,\cdot)\}$ given by Lemma 5.1 applied to $w(u,\cdot)$ (for $u \in \tilde{W}$). Then there exists a bound $c \in IN$ such that $\| \bar{c}_u \| < c$ for all $u \in \tilde{W}$.[14]

Proof It is clear that $\tilde{W}$ is definable in $< IN, +, w >$. We want to show that there exists a bound $c \in IN$ such that for all $u \in \tilde{W}$ $\| \bar{c}_u \| < c$. Now in order to show this, it is sufficient to show that for all $i = 1, \cdots, n$ there exists a bound $c_i \in IN$ such that for all $u \in \tilde{W}$ $(\bar{c}_u)_i < c_i$. Let $I_u = \{u' \in \tilde{W}; u' < u\}$. Let $v_i : \tilde{W} \rightarrow IN$ be the function which sends u to the smallest non-zero element of $\bigcap_{u' \in I_u} (G(u'))_i$ (which clearly exists since it is well known that $\bigcap_{u' \in I_u} < (\bar{c}_u)_i > =$l.c.m.$(\{(\bar{c}_{u'})_i;\ u' \in I_u\})$. The function v_i is definable in $< IN, +, w >$, therefore $\mathrm{Im}v_i(\cdot)$ is ultimately periodic (note that $Imv_i \subseteq IN$). Now from the fact that $v_i(u)$ is given by the l.c.m.$(\{(\bar{c}_{u'})_i;\ u' \in I_u\})$ it is easy to see that there exists a bound to the set of $(\bar{c}_u)_i$ $(u \in \tilde{W})$. Indeed take $u_1,\ u_2 \in \tilde{W}$ with $u_1 < u_2$. Now $v_i(u_1) =$l.c.m.$(\{(\bar{c}_{u'})_i; u' \in I_{u_1}\})$ and

[13] $w(u,\cdot)$ denotes the function that sends j to $w(u,j)$.

[14] **Definition** Let $\bar{x} = (x_1, \ldots, x_n)$ be an element of IN^n. Here the *norm* $\|\bar{x}\|$ of $\bar{x}$ is the maximum of $\{x_i; i = 1, \ldots, n\}$. It is clear that for n fixed, the norm is definable in Presburger Arithmetic.

$v_i(u_2)$ =l.c.m.($\{(\bar{c}_{u'})_i; u' \in I_{u_2}\}$). Thus $v_i(u_2)$ is a multiple of $v_i(u_1)$ (at least $2v_i(u_1)$ if they are different). But this argument can be applied to any pair of consecutive elements of $\mathrm{Im}v_i(\cdot)$. So since there is a bound to the distance between consecutive elements of $\mathrm{Im}v_i(\cdot)$ ($Imv_i(\cdot)$ is ultimately periodic), we have that there exists a bound to the set of $(\bar{c}_u)_i$ ($u \in \tilde{W}$).

The last step of the proof of theorem MV uses Muchnik's definability criterion. This beautiful characterization of definable relations in Presburger Arithmetic generalizes in higher dimensions the fact that subsets of IN definable in $< IN, + >$ are ultimately periodic.
Before to state it we need some definitions.

Definition Let $L \subseteq IN^n$. A *section* of L is a set of the form $\{(r_1, \ldots r_i, r_{i+2}, \ldots, r_n); (r_1, \ldots r_i, x, r_{i+2}, \ldots, r_n) \in L\}$, for x some element of IN.

Remark If $L \subseteq IN^n$, then its sections are subsets of IN^{n-1}, which are definable in $< IN, +, L >$.

Definition Let $L \subseteq IN^n$, $\bar{x} \in IN^n$ and $m \in IN$. The *L-cube* at $\bar{x}$ of size m is the set $C_L(\bar{x}, m) = \{\bar{y} \in IN^n; \bar{x} + \bar{y} \in L \text{ and } ||\bar{y}|| \leq m\}$. Here $\bar{x} + \bar{y}$ represents the component-wise addition.

Remark $C_L(\bar{x}, m)$ is definable in $< IN, + >$.

Definition Let $L \subseteq IN^n$ and $\bar{r} \in IN^n$. If $C_L(\bar{x}, m) = C_L(\bar{x} + \bar{r}, m)$, we will say that $C_L(\bar{x}, m)$ can be *shifted* by $\bar{r}$.

Theorem M (Muchnik's definability criterion) A set $L \subseteq IN^n$ is definable in $< IN, + >$ if and only if the following conditions are satisfied.

M.1 Every section of L is definable in $< IN, + >$.

M.2 There exists an $s \in IN$ such that for any size k there is a bound l for which every L-cube of size k at some $\bar{x}$ with $|| \bar{x} ||> l$ can be shifted by $\bar{r}'$, for some $\bar{r}' \in IN^n$ of norm less than s.[15]

Our statement of Muchnik's definability criterion is slightly different from the original one but it is easily seen equivalent.

[15]This second condition is a first-order statement of $< IN, +, L >$. In fact the whole criterion can be expressed as a first-order statement of $< IN, +, L >$. This is trivial in dimension 1 since condition M.1 is empty and condition M.2 is equivalent to 'L is ultimately periodic'. The general case is proved in [Much 91] and [B,H,M,V 94, proposition 8.2].

The reader will find proofs of theorem M in [Much 91],[Mi,Vil 94, section 5] and [B,H,M,V 94, pages 221-222 and appendix].

Now the remaining of the proof of theorem MV is reminiscent of the proof of the constructive version of theorem E : we build two functions f_L and h_L which are definable in $< IN, +, L >$. And we prove that they have "*non expansion*" behaviour if and only if conditions M.2 is satisfied by L. Then we end by induction on n ($L \subseteq IN^n$) to show that condition M.1 holds.

In the next lines we give the flavour of this quite technical construction and of the final step in the proof of theorem MV without giving explicit definitions for the functions f_L and h_L. For a complete proof the reader is advised to look at [Mi,Vil 94, section 5].

Let us remark that the negation of Muchnik's second condition is :

For all s there exists a size k such that above any distance l of the origin there is a L-cube of size k which cannot be shifted by a vector of norm smaller than s.

sketch of the proof of theorem MV
Let us assume that L (a subset of IN^n) does not extend $< IN, + >$.
Let $M_L = \{s \in IN$; there exists a k for which above any distance l of the origin there is a L-cube of size k, which cannot be shifted by a vector of norm smaller than $s\}$.
The set M_L is definable in $< IN, +, L >$. Obviously Muchnik's second condition is equivalent to M_L being finite.
Then we build functions $h_L : W_L \to IN^n$ and $f_L : M_L \to IN$ where W_L is a infinite subset of $M_L \times IN$ such that each section $\{x; (s, x) \in W_L\}$ is infinite for all s in M_L. These functions are definable in $< IN, +, L >$ (hence their domains are also definable in $< IN, +, L >$) with the following properties.

C.1 $(h_L(s, \cdot))_i$ is nondecreasing for $i = 1, \cdots, n$ (as long as it is defined) and increasing for some i.

C.2 $C_L(h_L(s, x), f_L(s))$ cannot be shifted by a vector of norm smaller than s, for all $(s, x) \in W_L$.

C.3 $C_L(h_L(s, x), f_L(s)) = C_L(h_L(s, y), f_L(s))$ for all (s, x), $(s, y) \in W_L$.

Condition C.2 is clearly related to the negation of condition M.2 .
On the other hand L does not extend $< IN, + >$, so the function h_L does not too. Thus by condition C.1 the function h_L verifies all the assumptions of

lemma 5.2 and so there exists $\bar{b}_s \in IN^n$ and $b \in IN$ such that $Imh_L(s,\cdot) =_{a.e.} \bar{b}_s + Imh_L(s,\cdot)$ with $\| \bar{b}_s \| < b$. Let fix s, then for all but finitely many x in the domain of $h_L(s,\cdot)$ we can find y in this domain such that $||h_L(s,y) - h_L(s,x)|| = ||\bar{b}_s|| < b$. Now from condition C.3 we deduce that for such a x the L-cube $C_L(h_L(s,x), f_L(s))$ can be shifted by a vector of norm smaller than b. So by condition C.2, if $s > b$, (s,x) cannot be in W_L, except for finitely many x in IN. Hence s cannot be in M_L (since the sections of W_L above elements of M_L are infinite). Thus M_L contains only elements s smaller than b, i.e. M_L is finite and condition M.2 holds.
Now let us remark that the sections of L are subsets of IN^{n-1}, which are definable in $< IN, +, L >$. So they satisfy the assumption of theorem MV. By induction on n we can conclude that sections are definable in $< IN, + >$, so condition M.1 holds and finally L is definable in $< IN, + >$.

In the remaining of this section we explore possible extensions of theorem MV. Let us say that theorem MV holds for a structure $\mathcal{A} =< IN, \ldots >$ if every $R \subseteq IN^n$ which does not extend $\mathcal{A}$, is definable in $\mathcal{A}$.
First let us remark that theorem MV does not hold for Congruence Arithmetic, i.e. for the structure $< IN, \equiv (\text{mod } n) >_{n \in IN}$[16]. Indeed the ternary relation "$x + y = z$" does not extend $< IN, \equiv (\text{mod } n) >_{n \in IN}$ and *is not definable in* $< IN, \equiv (\text{mod } n) >_{n \in IN}$. The proof of this folk fact is left to the reader (see also [End 72, chapter 3]).
Theorem MV holds for Peano Arithmetic, i.e. for $< IN, +, \cdot >$ but for a somewhat trivial reason : it is a consequence of the existence of a definable (in $< IN, +, \cdot >$) pairing function.
It is also a folk fact that there is no pairing function which is definable in $< IN, + >$.
Up to now we cannot prove or disprove theorem MV for Büchi Arithmetics.

Question 4 *Does theorem MV hold for Büchi Arithmetics?*

In order to go further in our discussion, we look at the following binary predicate $div(x,y)$, meaning that x divides y. This example illuminates the scope of theorem MV and theorem M (in the case of $< IN, + >$).
First it is easy to show that condition M.1 of Muchnik's theorem holds, i.e. the sections of $div(x,y)$ are definable in $< IN, + >$. It is obvious that $div(x,y)$ is the union of all the lines[17] of equation $y = mx$, $m \in IN$. Hence the section above $x = t$ is here the union (for all m in $\mathbb{N}$) of the intersections of lines $y = mx$ and $x = t$, thus it is the set of multiples of t and so it is ultimately periodic. The section above $y = t$ is the union of the intersections of lines $y = mx$ and $y = t$.

[16] The symbol $\equiv (\text{mod } n)$ represents the binary relation modulo n.
[17] By the line of equation $y = ax + b$, we mean the set $\{(o,b) + j(1,a); j \in IN\}$. This definition agrees with the previous one for a line in the case of IN^2.

Since these intersections are empty except for finitely many m, the section is finite (it consists of the divisors of t). In fact the same argument shows that the intersection of a line $y = ax + b$ with $div(x, y)$ is always finite.
But condition M.2 does not hold for $L = div(x, y)$. Indeed when we look at an L-cube of size k, sufficiently far away of the origin $(0, 0)$, two cases happen : the L-cube is empty or it is a finite part of a line of slope m for some m (more precisely a set of the form $\{(x, y) \in IN^2; y = mx + b \text{ and } y \leq k\}$). In the first case there is no condition on the vectors by which the L-cube can be shifted; in the second one the L-cube can be shifted by only multiple of the vector $(1, m)$. It is clear that this prevents us to find a bound on the norm of the vectors by which the L-cube can be shifted, as required by condition M.2.
This shows that $div(x, y)$ is not definable in Presburger Arithmetic and answers by the negative the following natural question.

Question 5 *Let L be a subset of IN^2, of which all the intersections with lines of IN^2 are definable in $< IN, + >$. Is L definable in $< IN, + >$?*

By theorem MV, we have that $div(x, y)$ extend $< IN, + >$. This can be directly shown. Hereafter we sketch a folk argument which proves that $< IN, +, div >$ and $< IN, +, \cdot >$ are interdefinable.
It is obvious that the function $x^2 + x$ is definable in $< IN, +, div >$ by a formula which says "y is the smallest natural number divisible both by x and $x + 1$". So it is clear that the function x^2 and the set of squares are definable in $< IN, +, div >$. Thus $div(x, y)$ extend $< IN, + >$.
Now by using $(x + y)^2 = x^2 + 2xy + y^2$, it is easy to define multiplication in $< IN, +, div >$.
Conversely definability of div in $< IN, +, \cdot >$ is obvious.
By using $(x+1)^2 - x^2 = 2x$, it is easy to define the function x^2 in $< IN, +, SQ >$ where SQ is the set of squares. This finally shows that $< IN, +, div >$ and $< IN, +, SQ >$ are interdefinable.
This leads to the following question.

Question 6 *Is it true that for all $L \subsetneq IN^n, (n \geq 2)$, there exists $P \subseteq IN$ such that the structures $< IN, +, L >$ and $< IN, +, P >$ are interdefinable.*

There are some trivial results in this direction. We begin by a lemma.

Lemma 5.3 Let $L_1, \ldots, L_s$ be subsets of $\mathbb{N}$. Then there exists L a subset of IN such that $< IN, +, L_1, \ldots, L_s >$ and $< IN, +, L >$ are interdefinable.

Proof We give it for $s = 2$, but the generalization is easy. We define L as the union of $2L_1$ and $2L_2 + 1$. It is obvious that L is definable in $< IN, +, L_1, L_2 >$; conversely $x \in L_1$ (respectively $x \in L_2$) is definable in $< IN, +, L >$ by the formula $\exists z(z = x + x \wedge z \in L)$ (respectively $\exists z(z = x + x + 1 \wedge z \in L)$).

It is now trivial to show that question 6 has a positive answer for all $< IN, +, L >$ in which the multiplication is definable. In this case there is a pairing function which is definable in $< IN, +, L >$. So there exists L' such that $< IN, +, L >$ and $< IN, +, \cdot, L' >$ are interdefinable. Now we can replace $\cdot$ by SQ (see the argument above). We get the result by applying lemma 5.3.
An easy argument proves that question 6 has a positive answer when L is the graph of the function $f(x) = 2^x$. It suffices to remark that f is definable by adding the range of f and the set $\{x + f(x); x \in IN\}$ to Presburger Arithmetic.

A. Semenov gave a subset P of IN such that $< IN, +, V_2 >$ and $< IN, +, P >$ are interdefinable (see [Sem 84, page 173]).

We end this section with a remark by R. Solovay :

A positive answer to question 6 implies a positive answer to question 4.

In fact a positive answer to question 6 implies that theorem MV holds for any structure $< IN, +, V >$ $(V \subseteq IN^n)$. Indeed Let L be a subset of IN^r which does not extend $< IN, +, V >$. A positive answer to question 6 implies that there exists $P \subseteq IN$ such that $< IN, +, P >$ and $< IN, +, L >$ are interdefinable. So P is definable in $< IN, +, V >$ (since L does not extend $< IN, +, V >$) and thus L is definable in $< IN, +, V >$.

6. Theorem CH and Further results.

Clearly the statements of theorem C, theorem S, theorem E, theorem MV and theorem V as stated here are free of automata flavour. The same is true for their proofs. The link with automata theory is only via theorem B. Theorem CH has a particular status. Its statement is free of automata theory but the proofs of CH in [Co 69], [Han 82] and [Per 90] are combinatorial and use automata theory. Even our proof of it, although written in our logical framework, strongly uses theorem B and a basic fact of automata theory : the pumping lemma (see [Mi,Vil 94, section 4])[18]. Theorem CH has also a particular status with respect to the other ingredients of our proof of Cobham's and Semenov's theorems: it is the only ingredient which is specific to $< IN, +, V_k >$ and $< IN, +, V_l >$. All of the remaining of ingredients are about Presburger Arithmetic. So if we are able to prove a theorem CH about two extensions of Preburger Arithmetic, say $< IN, +, K >$ and $< IN, +, L >$, we immediately have a theorem S for $< IN, +, K >$ and $< IN, +, L >$, as the proofs in section 3 show it.

[18] And, as in all the proofs of CH, we use the following equivalent form of the essential assumption "k and l are multiplicatively independent" : $\{\frac{l^n}{k^m}; n, m \in IN\}$ is dense in $I\!R^+$.

In fact the proofs in section 3 show that for a pair of structures $< IN, +, K >$ and $< IN, +, L >$ the following three statements are equivalent :

Theorem CH holds $\Leftrightarrow$ Theorem C holds $\Leftrightarrow$ Theorem S holds

So we can ask the following :

Question 7 *For which pairs of extensions of Presburger Arithmetic,* $< IN, +, K >$ *and* $< IN, +, L >$ *, does theorem CH hold?*

Clearly Cobham's theorem gives a list of such pairs of extensions of Presburger Arithmetic. From some years, there are attempts to extend Cobham's theorem to Bertrand numeration systems (see [Fab 92], [Po 94]). These attempts extend the list of pairs of structures $< IN, +, K >$ and $< IN, +, L >$ for which theorem CH holds (and hence theorem C and theorem S too).
Fabre's thesis ([Fab 92]) is written on the viewpoint of automata theory. But again there is a "Büchi theorem" for these numeration system (see [Br,Han 94]). This result allows us to explain the state of the art in our logical frame.

We first give some definitions for an arbitrary numeration system.

Let $U = (U_n)_{n \in IN}$ be a strictly increasing sequence of integers with $U_0 = 1$. Any integer $x > 0$ has one and only one representation

$$x = a_0 U_0 + a_1 U_1 + \cdots + a_m U_m$$

with respect to U, using the so called *greedy algorithm* (see [Fra 85]) :
let m such that $U_m \leq x < U_{m+1}$ and $x_0 = x$. We compute by induction on i, $i = m, \ldots, 1, 0$,

$$a_i = x_i \text{ div } U_i, \quad x_{i+1} = x_i \bmod U_i.$$

We only consider sequences U where ratios U_{n+1}/U_n are uniformly bounded by an integer constant c (with c minimal). In this case we have $a_i < c$ for all i.

Definition With the previous notations, we say that U is a *numeration system* and $A = \{0, 1, \ldots, c-1\}$ is the *alphabet* associated with U. We call *U-representation* of x the word $a_0 a_1 \ldots a_m$ of A^* obtained by the above process. By definition, the U-representation of 0 is the empty word.
In the sequel we will denote the U-representation of x by $[x]_U$. Any word $u = 0^k[x]_U$, with $k \geq 0$, is called *normalized.* We denote by $\mathcal{N}$ the set of normalized words. Conversely, for any word $u = a_0 a_1 \ldots a_m \in A^*$, we call *value* of u the integer $\nu(u) = \sum_{i=0}^{m} a_i U_i$.

Let us remark that if $U = (k^n)_{n \in IN}$ with $k \geq 2$, the previous algorithm computes the usual k-ary representation of x.

Given a numeration system U, the set $\mathcal{N}$ may have an unexpected behaviour : for some $u, v \in A^*$ and $k > 0$, $u \in \mathcal{N}$ but $u0^k \notin \mathcal{N}$, $uv \in \mathcal{N}$ but $u \notin \mathcal{N}$. In [Bert 86], *Bertrand numeration systems* are characterized such that this behaviour is forbidden. They are related to θ-expansions of real numbers.

Let $\theta > 1$ be a real number. For any $x \in IR$, denote by $[x]$ its integer part and by $\{x\}$ its fractional part. Any real number $x \in [0, 1]$ satisfies the equality

$$x = \sum_{n \geq 1} a_n \theta^{-n} \qquad (\star)$$

where

$$a_n = [\theta x_n], \quad \textit{with } x_1 = x \textit{ and } x_{n+1} = \{\theta x_n\}, \textit{ for any } n \geq 1.$$

The infinite sequence $e(x) = (a_n)_{n \geq 1} = a_1 \cdots a_n \cdots$ is called the *θ-expansion* of x. A particular case is the θ-expansion $e(1)$ of the number 1. In the case it ends with an infinite sequence of 0's, i.e. $e(1) = a_1 \ldots a_{k-1} a_k 0^\omega$, $a_k > 0$, then we put instead

$$e(1) = (a_1 \ldots a_{k-1}(a_k - 1))^\omega.$$

This new sequence also satisfies equality $(\star)$.

With this convention, one can show that, for all $n \in IN \setminus \{0\}$, $a_n < \theta$. The *alphabet* Θ associated with θ is then defined as $\{0, 1, \ldots, [\theta]\}$ if $\theta \in IR \setminus IN$, and as $\{0, 1, \ldots, \theta - 1\}$ if $\theta \in IN$.

The set S_θ of θ-expansions of all $x \in [0, 1]$ is a subshift of A^{IN}, called the *θ-shift*. We denote by $L(\theta)$ the set of finite factors of the sequences in S_θ.
The form of $e(1)$ implies some properties for the θ-shift : for example,
$e(1)$ is ultimately periodic if and only if the language $L(\theta)$ is Θ-recognizable.

Examples
1) Let θ be the golden number $\phi = \frac{1+\sqrt{5}}{2}$. Then $e(1) = (10)^\omega$, the initial form of $e(1)$ being 110^ω.
2) Let $\theta = \phi^2 = \frac{3+\sqrt{5}}{2}$, then $e(1) = 21^\omega$.

Theorem 6.1 Let U be a numeration system and $\mathcal{N}$ its set of normalized words. The following are equivalent.

1) Let $u, v \in A^*$, let $k > 1$. If $u \in \mathcal{N}$, then $u0^k \in \mathcal{N}$; if $uv \in \mathcal{N}$, then $u, v \in \mathcal{N}$.

2) There exists a real number $\theta > 1$ such that $\mathcal{N} = L(\theta)$.

A numeration system which satisfies (2) will be called *Bertrand numeration system associated to the θ-shift.*

The reader will find more information on numeration systems and θ-expansions of reals in [Bert 86], [Bert 89], [Fra 85] and [Pa 60].

Assumption 1 *In the sequel we always assume that U is a Bertrand numeration system associated to a θ-shift such that $L(\theta)=\mathcal{N}$ is Θ-recognizable.*

In this case, one can show that the numeration system U is defined by a *linear recurrence* of *order* k, for some $k \geq 0$ (defined with respect to $e(1)$). More precisely, there exist integers $\gamma_1, \ldots, \gamma_k$, such that for any $n \geq k$,

$$U_n = \gamma_1 U_{n-1} + \gamma_2 U_{n-2} + \cdots + \gamma_k U_{n-k}.$$

Let $P(X) = X^k - \gamma_1 X^{k-1} - \cdots - \gamma_k$ be the *characteristic polynomial* of the linear recurrence. Then θ is root of $P(X)$ and the other roots have absolute value less than 2 (see [Pa 60]).

Here we will make an extra assumption :
Assumption 2 *the roots $\theta_2, \ldots, \theta_k$ of $P(X)$ not equal to θ, are simple and have absolute value less than* 1.

In particular, assumption (2) hold if $P(X)$ is the minimal polynomial of a Pisot[19] number θ.

Examples
1) If $\theta = k \in IN$, then $U_0 = 1$ and $U_n = kU_{n-1}$, $n \geq 1$.

2) If $\theta = \phi$, then $U_0 = 1$, $U_1 = 2$ and $U_n = U_{n-1} + U_{n-2}$ for all $n \geq 2$. This is the Fibonacci numeration system. In this case U will be denoted by Fib.

3) If $\theta = \phi^2$, then $U_0 = 1$, $U_1 = 3$ and $U_n = 3U_{n-1} - U_{n-2}$ for all $n \geq 2$.

Definition We will say that a subset X of IN is *U-recognizable* if $L = 0^* r(X)$ is Θ-recognizable.

Now we introduce the *structure* $< IN, +, V_U >$ where V_U is the function defined similarly to V_k by :
for all $x \neq 0$ with $[x]_U = a_0 \ldots a_m$, V_U is the smallest U_j such that $a_j \neq 0$.

[19] A Pisot number is an algebraic real θ whose all the conjugates different from θ have absolute value less than 1

Theorem 6.2 Under the assumptions (1) and (2) of this section, a set $X \subseteq IN^n$ is U-recognizable if and only if X is definable in $< IN, +, V_U >$.

This extension of Büchi's theorem is due to V. Bruyère and G. Hansel (see [Br,Han 94]). The proof follows the same way that the one given for theorem B in [B,H,M,V 94, p 207] for k-recognizable sets, but new difficulties appear: one is the use of normalized words, instead of any word of $\{0, \ldots, p-1\}^*$; another one is the U-recognizability of the addition which is no longer a trivial fact (in contrast with the proof of k-recognizability of the addition which is almost trivial).

Proposition 6.1 Under the assumptions (1) and (2) of this section, the set $X = \{(x, y, z) \in IN^3; x + y = z\}$ is U-recognizable.

Proposition 6.1 is proved in [Br,Han 94] in a simple way.
The U-recognizability of the addition is proved under the alone assumption that the numeration system U is given by a finite linear recurrence the polynomial of which is the minimal polynomial of a Pisot number[20] in the paper [Fr,So 94], but in a more complicated way.

An appropriate version of Lemma B (section 2) still holds for these numeration systems.

As in the case of theorem B, theorem 6.2 has an immediate corollary.

Corollary Under the assumptions (1) and (2) of this section, $< IN, +, V_U >$ is decidable.

In particular we get that $< IN, +, Fib >$ is decidable (since U is definable in $< IN, +, V_U >$), a result already proved by A. Semenov in [Sem 80].

S. Fabre (see [Fab 92]) shows that theorem C holds for $< IN, +, V_k >$ and $< IN, +, V_U >$ where k is an integer ≥ 2 and U is given by a finite linear recurrence the polynomial of which is the minimal polynomial of a Pisot number θ with an extra assumption. F. Point proves theorem S for $< IN, +, V_k >$ and $< IN, +, V_U >$ where U satisfies assumptions (1) and (2) and some extra conditions (different of Fabre's extra assumption). [21] Her proof follows the general scheme of Muchnik's proof of Cobham's and Semenov's theorems and uses U-recognizability of addition. Fabre's proof is based on the notion of U-substitution (the reader will find a clear exposition of the results on U-substitutions in [Br,Han 94]).

[20] There are numeration systems which satisfy this assumption but not asumption (1).

[21] In particular from Fabre's and Point's results, theorem S seems proved for $< IN, +, V_k >$ and $< IN, +, V_{Fib} >$.

We conjecture that theorem CH (and so theorems C and S) holds for pairs of structures $< IN, +, V_{U_1} >$ *and* $< IN, +, V_{U_2} >$ *where* U_1 *and* U_2 *are numeration systems respectively associated to a* θ_1*-shift and to a* θ_2*-shift with* θ_1 *and* θ_2 *two multiplicatively independent Pisot numbers.*

7. Around the indecidability of $< IN, +, V_k, V_l >$.

In [Vil 92a], [Vil 92b],[Vil 92c], the second author proves the following results.

Theorem V Let k and l be multiplicatively independent. The structures $< IN, +, V_k, V_l >$ and $< IN, +, \cdot >$ are interdefinable.

Corollary V $< IN, +, V_k, V_l >$ is undecidable.

These results answer by the negative a question by A. Joyal :
for k and l multiplicatively independent, does it exist some subclass of Turing machines which recognize exactly the sets which are in the smallest class containing all k-recognizable sets, all l-recognizable sets and closed under intersection, complementation, and projection? This is equivalent to ask for a type of machine which recognizes exactly the sets definable in $< IN, +, V_k, V_l >$.

The proof of theorem V is based on a first-order translation of the following theorem which is a slight generalization of a result by W. Thomas ([Tho 75, theorem 13]).

Theorem T Let $h^* : IN \rightarrow IN$ be a strictly increasing function such that $h^*(S(x)) > S(h^*(x))$[22] for infinitely many $x \in IN$. Suppose furthermore that there exists a $d \in IN$ such that for any consecutive natural numbers x, y satisfying the above inequality $x - y \leq d$. Then the addition of natural numbers is definable in $WS1S$.

The technique of proof of theorem T is essentially due to C.C. Elgot and M.O. Rabin (see [El,Ra 66]).

Theorem T has the following consequence.

Corollary T Let be a strictly increasing function $h : k^{IN} \rightarrow k^{IN}$ definable in $< IN, +, V_k, V_l >$ such that the following condition holds :
$(*)$ $h(k \cdot x) > k \cdot (h(x))$ *for infinitely many* $x \in k^{IN}$
and furthermore there exists a $d \in IN$ *such that for any consecutive power of* k, k^n,k^m *satisfying the above inequality we have* $m - n \leq d$.
Then the multiplication of powers of k is definable in $< IN, +, V_k, h >$.

[22]The symbol S denotes the function sucessor : $S(x) = x + 1$.

Lemma 7.1 Under the assumptions of corollary T, the concatenation in base k is definable in $< IN, +, V_k, h >$.

The proof is a easy consequence of corollary T.

By the following result of J.W. Thatcher (see [Tha 66]) it follows that any recursive function is definable in $< IN, +, V_k, V_l >$.

Lemma 7.2 Any recursive function is definable in $< IN, +, ^\wedge >$ where $^\wedge$ is the concatenation in base k.

The last step in the proof of V is the construction of a function h which verifies the assumptions of corollary T, whenever k and l are multiplicatively independent. This part of the proof is quite technical.
The reader will find complete proof of theorem V in [Vil 92b] and [Vil 92c]. A simple case is handled in [Vil 92a].

The proof of lemma 7.2 is by encoding Turing machines. This raises the following question.

Question 8 *Define multiplication in* $< IN, +, V_k, V_l >$ *without encoding a Turing machine (for* k, l *multiplicatively independent).*

Let us end this paper with a few additional questions. ¿From decidability of $< IN, +, V_k >$, we trivially get decidability of $< IN, +, P_2 >$ [23]. A few years ago, G. Cherlin asked about the decidability of $< IN, +, P_2, P_3 >$. This problem is still open. More generally we can ask :

Question 9 *For* k, l *multiplicatively independent is* $< IN, +, P_k, P_l >$ *decidable, decidable by automata or if it is undecidable, is multiplication definable in it ?*

In this direction we can easily show that $< IN, +, V_2, P_3 >$ is undecidable (multiplication can be defined in it). But we are not able to generalize the proof to solve the following questions?

Question 10 *Is* $< IN, +, V_k, P_l >$ *undecidable whenever* k *and* l *are multiplicatively independent?*

Question 11 *Is* $< IN, +, V_k, L >$ *undecidable for every* L *which is* l*-recognizable but not definable in* $< IN, + >$ *whenever* k *and* l *are multiplicatively independent?*

[23] Let us recall that P_k denotes the set of nonnegative powers of k.

Acknowledgement

We particulary want to thank M. Boffa, V. Bruyère, G. Hansel, F. Point and R. Solovay for helpful conversations and comments during the preparation of this paper. Finally, we wish to thank one of the referee of [Mi,Vil 94] who suggested to illustrate theorems M and MV with the predicate $div(x, y)$.

References

[Be,Re 88] J. Berstel, C. Reutenauer, Rational Series and their Languages, EATCS monographs on theoretical computer science, v. 12, Berlin, Springer 1988.

[Bert 86] A.Bertrand-Mathis, Développement en base θ, répartition modulo de la suite $(x\theta^n)_{n\geq 0}$, langages codés et θ-shift, Bull.Soc.Math.France 114(1986),271-323.

[Bert 89] A.Bertrand-Mathis, Comment écrire les nombres entiers dans une base qui n'est pas entière , Acta Math. Acad. Sci Hungar. 54 (1989), 237-241.

[Br,Han 94] V.Bruyère, G.Hansel, Recognizable sets of numbers in nonstandard bases, preprint 1994.

[B,H,M,V 94] V. Bruyère, C. Michaux, G. Hansel, R. Villemaire, Logic and p-recognizable Sets of Integers,Proceedings of the Congress Journées Montoises 1992, Bulletin of the Belgian Mathematical Society-Simon Stevin 1 (1994) no 2,191-238.

[Bu 60] J.R. Büchi, Weak second-order arithmetic and finite automata, Z. Math. Logik Grundlagen Math. 6 (1960),66-92.

[Co 69] A. Cobham, On the Base-Dependence of Sets of Numbers Recognizable by Finite-Automata, Math. Systems Theory 3, (1969)186-192.

[Eil 74] S. Eilenberg, Automata, Languages and Machines, Academic Press 1974.

[El,Ra 66] C.C. Elgot, M.O. Rabin, Decidability and undecidability of extensions of second (first) order theory of (generalized) successor, J.S.L. vol. 31 (1966) no 2,169-181.

[End 72] H.E. Enderton, An introduction to mathematical logic, Academic Press 1972.

[Fab 92] S.Fabre, Substitution et indépendance des systèmes de numération, *Thesis*, Université Aix-Marseille II,1992.

[Fra 85] A.S. Fraenkel, Systems of numeration, Amer. Math. Monthly 92 (1985),105–114.

[Fr,So 94] C.Frougny, B.Solomyak, On representation of integers in linear numeration systems, preprint 1994.

[G,S 66] S. Ginsburg, E. H. Spanier, Semigroups, Presburger formulas and languages, Pacific J. Math. 16 (1966),285–296.

[Han 82] G. Hansel, A propos d'un théorème de Cobham, in: D. Perrin, ed., Actes de la Fête des Mots, Greco de Programmation, CNRS, Rouen,1982.

[Ha,Wr 62] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., Oxford, Clarendon Press 1962.

[Hod 83] B. Hodgson, Décidabilité par automate fini, Ann. Sci. Math. Québec 7 (1983),39-57.

[McNa 63] R. McNaughton, Review of [4], J. Symbolic Logic 28 (1963),100-102.

[Mi,Vil 93] C. Michaux ,R Villemaire, Cobham's theorem seen trough Büchi theorem, Proc. Icalp'93, Springer Lecture Notes in Comput. Sci. 700 (1993),325-334.

[Mi,Vil 94] C. Michaux, R. Villemaire, Presburger arithmetic and recognizability of sets of natural numbers by automata : new proofs of Cobham's and Semenov's theorems, rapport de recherche no 229 (1994),Departement de mathematique et d'informatique ,Univ. du Québec à Montreal (35 pages).

[Much 91] A. Muchnik, Definable criterion for definability in Presburger Arithmetic and its applications, (preprint in Russian), Institut of new technologies, 1991.

[Pa 60] W. Parry, On the β-expansions of real numbers, Acta Math. Acad. Sci. Hungar. 11 (1960),401–416.

[Per 90] D. Perrin, Finite Automata, in: J. van Leeuwen, Handbook of Theoretical Computer Science, Elsevier 1990.

[Po 94] F.Point, sur le théorème de Cobham-Semenov, preprint, 1994 (12 pages).

[Presb 29] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, C. R. 1er congrès des Mathématiciens des pays slaves, Varsovie (1929),92–101.

[Sal 87] O. Salon, Suites automatiques à multi-indices, C. R. Acad. Sci. Paris 305 (1987),501-504.

[Sem 77] A. L. Semenov, The Presburger nature of predicates that are regular in two number systems, Siberian Math. J. 18 (1977),no 2, 289-299.

[Sem 80] A.L. Semenov, On certain extensions of the arithmetic of addition of natural numbers, Math. USSR. Izvestiya,15 (1980),no 2,401-418.

[Sem 84] A. L. Semenov, Decidability of monadic theories, Spinger Lecture Notes in Comput. Sci. 176 (1984),162-175.

[Tha 66] J.W. Thatcher, Decision Problems for multiple successor arithmetics, J.S.L. 11 (1966),182-190.

[Tho 75] W. Thomas, A note on undecidable extensions of monadic second order successor arithmetic, Arch. math. Logik 17 (1975),43-44.

[Tho 90] W. Thomas, Automata on infinite objects, in : Handbook of Theoretical Computer Science, vol. B, J. Van Leeuwen, Ed., Elsevier (1990),135–191.

[Vil 92a] R. Villemaire, $< IN, +, V_2, V_3 >$ est indecidable, C.R. Acad. Sc. Paris 314 (1992),no 10,775-777.

[Vil 92b] R. Villemaire, $< IN, +, V_k, V_l >$ is undecidable, Theoret. Comput. Sci. 106 (1992),337–349.

[Vil 92c] R. Villemaire, Joining k- and l-recognizable sets of natural numbers, Proc. Stacs'92, Springer Lecture Notes in Comput. Sci. 577 (1992),83–94.

ORDERINGS, VALUATIONS AND FREE PRODUCTS OF GALOIS GROUPS

Ido Efrat
The Institute of Mathematics
The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904
ISRAEL
e-mail: efrat@sunset.huji.ac.il

1. The p-Galois group of a field. Given a field K and a prime number p, let $K(p)$ be the compositum of all finite Galois extensions of K of pth power order and let $G_K(p) = \mathrm{Gal}(K(p)/K)$. We report here on some conjectures and results on the structure of $G_K(p)$ and its relation to the arithmetic of K.

When $\mathrm{char}\, K = p$ the structure of $G_K(p)$ is quite dull: it is a free pro-p group of rank $(K : \wp(K))$, where $\wp(X) = X^p - X$ [Se, II-5]. We therefore restrict ourselves to the case where $\mathrm{char}\, K \neq p$. We will henceforth also assume that K contains the roots of unity of order p. In this case, $K(p)$ is the closure of K with respect to repeatedly adjoining all possible pth roots, by Kummer theory.

It is often useful to consider $G_K(p)$ together with its natural action on the group μ_{p^∞} of all roots of unity of pth power order (over the prime field of K). Note that in our situation $\mu_{p^\infty} \subseteq K(p)$. Since $\mathbb{Z}_p^\times \cong \mathrm{Aut}(\mu_{p^\infty})$ (where $\alpha \in \mathbb{Z}_p^\times$ corresponds to the automorphism $\zeta \mapsto \zeta^\alpha$) the restriction $G_K(p) \to \mathrm{Aut}(\mu_{p^\infty})$ induces a continuous homomorphism $\chi_{K,p}: G_K(p) \to \mathbb{Z}_p^\times$. Since K contains by assumption the roots of unity of order p, one has in fact $\mathrm{Im}(\chi_{K,p}) \subseteq 1 + p\mathbb{Z}_p$.

2. Torsion in $G_K(p)$ and orderings. When p is odd, $G_K(p)$ is torsion-free [B]. As for $G_K(2)$, its torsion consists solely of involutions, and is closely related to the orderings on K. In fact, as proved by Becker [B], $G_K(2) \cong \mathbb{Z}/2\mathbb{Z}$ if and only if K is *euclidean* (i.e., it is an intersection of $K(2)$ with a real closed field; equivalently, K^2 is an ordering on K). Furthermore, for every ordering P on K we may associate a *euclidean closure*, i.e., a euclidean subextension $\hat{K}$ of $K(2)/K$ such that $P = \hat{K}^2 \cap K$; this closure is unique up to a unique K-isomorphism. Therefore the orderings on K may be identified with the conjugacy classes of the involutions in $G_K(2)$.

3. Valuations. Let v be a Krull valuation on K. A *p-henselization* of (K, v) is the decomposition field of an extension of v to $K(p)$. One says that (K, v) is *p-henselian* if it is a p-henselization of itself; equivalently, v has a unique prolongation $v(p)$ to $K(p)$.

Suppose that (K, v) is p-henselian, let k be its residue field and let T be the inertia group of $v(p)/v$ in $K(p)$. There is a split short exact sequence

$$1 \to T \to G_K(p) \to G_k(p) \to 1 \quad .$$

There are two essentially different cases:

CASE (I): $\operatorname{char} k \neq p$. Then $T \cong \mathbb{Z}_p^m$ where $m = \dim_{\mathbb{F}_p} v(K^\times)/p$. The action of $G_k(p)$ on T is given by $\tau^\sigma = \tau^{\chi_{K,p}(\sigma)}$ for $\sigma \in G_k(p)$ and $\tau \in T$. Furthermore, T acts trivially on μ_{p^∞}.

CASE (II): $\operatorname{char} k = p$. In this case T coincides with the ramification group of $v(p)/v$. When v is discrete and k is perfect, T is a free pro-p group.

In contrast to the case of euclidean fields, it is not clear to what extent is p-henselianity a Galois-theoretic property. For example, I do not know whether $G_K(p) \cong \mathbb{Z}_p^m$, with $m \geq 2$, implies that K is p-henselian with respect to a valuation whose inertia group in $K(p)$ is non-trivial.

4. Fields with finitely generated p-Galois groups. Suppose now that $G_K(p)$ is finitely generated (as a topological group); equivalently $(K^\times : (K^\times)^p) < \infty$. In this case it is conjectured that $G_K(p)$ decomposes as a free product in the category of pro-p groups

$$G_K(p) = G_{\hat{K}_1}(p) *_p \cdots *_p G_{\hat{K}_n}(p) \quad ,$$

where each $\hat{K}_i$ is a subextension of $K(p)/K$ of one of the following types:

(I) $\hat{K}_i$ is p-henselian with respect to a valuation with inertia group in $K(p)$;

(II) $p = 2$ and $\hat{K}_i$ is euclidean; or

(III) $G_{\hat{K}_i}(p) \cong \mathbb{Z}_p$.

Recall that a non-trivial valuation has *rank 1* if it has no non-trivial proper coarsenings. The following second conjecture may complement the picture: *Suppose that K is p-henselian with respect to a valuation of rank 1 with residue characteristic p, and suppose that* $\operatorname{rank} G_K(p) < \infty$. *Then either $G_K(p)$ is a free pro-p group or K is a finite extension of $\mathbb{Q}_p$.* In the latter case $G_K(p)$ is a Poincaré group of dimension 2 [Se, II-30, Th. 4].

Now let $\mathcal{C}_p$ be the class of all pairs (G, θ), where G is a pro-p group and $\theta: G \to 1 + p\mathbb{Z}_p$ is a continuous homomorphism. We will not distinguish between pairs that are isomorphic in the natural sense. Let $\mathcal{C}_p'$ be the subclass of $\mathcal{C}_p$ consisting of all pairs $(G_K(p), \chi_{K,p})$ where K is a field satisfying our constant assumptions and such that $\operatorname{rank} G_K(p) < \infty$. Let $\mathcal{C}_p''$ be the minimal subclass of $\mathcal{C}$ such that:

(a) $(1, 1) \in \mathcal{C}_p''$;

(b) $(\mathbb{Z}_p, \theta) \in \mathcal{C}_p''$ for every continuous homomorphism $\theta: \mathbb{Z}_p \to 1 + p\mathbb{Z}_p$;

(c) $(G_L(p), \chi_{L,p}) \in \mathcal{C}_p''$ for every finite extension L of $\mathbb{Q}_p$ containing the roots of unity of order p;

(d) When $p = 2$, $(\mathbb{Z}/2\mathbb{Z}, -1) \in \mathcal{C}_2''$;

(e) If $(G_1,\theta_1),\ldots,(G_n,\theta_n)\in\mathcal{C}_p''$ then $(G_1 *_p \cdots *_p G_n, \theta_1 *_p \cdots *_p \theta_n)\in\mathcal{C}_p''$, where $\theta_1 *_p \cdots *_p \theta_n: G_1 *_p \cdots *_p G_n \to 1+p\mathbb{Z}_p$ is the continuous homomorphism induced by $\theta_1,\ldots,\theta_n$ by the universal property of the free product;

(f) If $(\bar{G},\bar{\theta})\in\mathcal{C}_p''$ and $m\in\mathbb{N}$ then $(\mathbb{Z}_p^m \rtimes \bar{G},\theta)\in\mathcal{C}_p''$, where $\bar{G}$ acts on $\mathbb{Z}_p^m$ according to $\tau^\sigma = \tau^{\bar{\theta}(\sigma)}$ for $\sigma\in\bar{G}$ and $\tau\in\mathbb{Z}_p^m$, and where $\theta:\mathbb{Z}_p^m\rtimes\bar{G}\to 1+p\mathbb{Z}_p$ is the composition of the projection $\mathbb{Z}_p^m\rtimes\bar{G}\to\bar{G}$ with $\bar{\theta}$.

Without proof we mention the following

PROPOSITION: *$\mathcal{C}_p''\subseteq\mathcal{C}_p'$. Assuming the above-mentioned conjectures, $\mathcal{C}_p'=\mathcal{C}_p''$.*

5. Witt rings of elementary type. These conjectures originate in the attempts to axiomatize the theory of quadratic forms, by means of the purely combinatorial notion of *abstract Witt rings* [M]. Marshall asked in [M] whether every finitely generated abstract Witt ring can be constructed from certain "building blocks" (the Witt rings of real closed fields, dyadic fields, and fields K with $G_K(2)\cong\mathbb{Z}_2$) by means of two operations (called direct product and extension). This statement became known as the *"elementary type conjecture"* and was proved in numerous cases; e.g., Carson and Marshall [CM] verified it with the aid of a computer for abstract Witt rings with at most 32 square classes. The connection with Galois theory has been fully revealed by Jacob and Ware ([JWr1], [JWr2]): they showed that if $\mathcal{C}_p'=\mathcal{C}_p''$ then the elementary type conjecture holds. Furthermore, their results show that the converse is also true, provided that whenever L is a finite extension of $\mathbb{Q}_p$ and $W(K)\cong W(L)$ then $(G_K(2),\chi_{K,2})\cong(G_L(2),\chi_{L,2})$ in the natural sense.

The elementary type conjecture has far-reaching consequences in the theory of quadratic forms. For instance it implies the following long-standing conjectures:

(1) Define the *level* of a field K of characteristic $\neq 2$ as the minimal number of squares in K whose sum is -1 (∞ if K is formally real). By classical results of Pfister [S, Ch. II, Th. 10.8 and Ch. IV, Th. 4.3], the possible values of this invariant are 2^n, $n\in\mathbb{N}$, and ∞. The *"level conjecture"* asserts however that if $(K^\times:(K^\times)^2)<\infty$ then the level of K is either 1, 2, 4 or ∞. By induction on the complexity of the construction one can show that this holds whenever $(G_K(2),\chi_{K,2})\in\mathcal{C}_2''$. Therefore the level conjecture would follow from the equality $\mathcal{C}_2'=\mathcal{C}_2''$.

(2) Given a field K of characteristic $\neq 2$, let $u(K)=\sup\dim\varphi$, where φ ranges over all anisotropic quadratic forms over K. An old conjecture of Kaplansky stated that if $u(K)$ is finite then it is a power of 2. Merkurjev ([Me]; [L2]) constructed counterexamples of fields with any given even u-invariant. Yet, Kaplansky's conjecture holds whenever $(G_K(2),\chi_{K,2})\in\mathcal{C}_2''$. Therefore, the equality

$C_2' = C_2''$ will imply that Kaplansky's conjecture is true whenever $(K^\times : (K^\times)^2) < \infty$.

(3) Let K be again a field of characteristic $\neq 2$, let $I(K)$ be the fundamental ideal of the Witt ring of K, and for each $l \geq 0$ let $H^l(K) = H^l(G_K(2), \mathbb{Z}/2\mathbb{Z})$ be the Galois cohomology group. For any $a \in K^\times$ let (a) be the element of $H^1(K)$ corresponding to $a(K^\times)^2$ via the Kummer isomorphism $K^\times/(K^\times)^2 \cong H^1(K)$. A conjecture of Milnor states that there is an isomorphism $I(K)^l/I(K)^{l+1} \cong H^l(K)$ mapping any Pfister form $\langle 1, -a_1\rangle \otimes \cdots \otimes \langle 1, -a_n\rangle$, $a_1, \ldots, a_n \in K^\times$, into $(a_1) \cup \cdots \cup (a_n)$. This is known to hold for $l \leq 3$ ([Mel], [MeS], [R]). One can show that this conjecture is true when $(G_K(2), \chi_{K,2}) \in C_2''$. So again it would follow from $C_2' = C_2''$ that it holds when $(K^\times : (K^\times)^2) < \infty$. See [AEJ1], [AEJ2] for more details and references.

6. A decomposition theorem. A partial result towards a possible proof of the elementary type conjecture is given in [E3] (where proofs of the announcements in this section can be found)

THEOREM: *Suppose that $K = \hat{K}_1 \cap \cdots \cap \hat{K}_n$ where $\hat{K}_1, \ldots, \hat{K}_n$ satisfy (I) or (II) of §4 and suppose that n is the minimal positive integer such that K has this form. Then $G_K(p) = G_{\hat{K}_1}(p) *_p \cdots *_p G_{\hat{K}_n}(p)$.*

In particular, this proves the first conjecture of §4 when K is an intersection of an arbitrary collection of fields of the form (I) or (II).

For algebraic extensions of $\mathbb{Q}$ a similar decomposition theorem was proved by Eršov [Er] and Neukirch [N]. Jacob [J], leaning on previous results of Marshall, proved the theorem (with $p = 2$) for fields K with $(K^\times : (K^\times)^2) < \infty$ which are *real-pythagorean* (i.e., K is an intersection of a non-empty collection of its euclidean closures). See also [Mi] and [E2] for somewhat more precise results in the real-pythagorean case. Jacob and Wadsworth [JW, Th. 4.3] treated the case where K is an intersection of two fields of type (I) with residue characteristic $\neq p$ which are immediate over K and which induce distinct topologies; but although the result is correct, there is a gap in the proof. We refer to [H] for another result in this direction.

The decomposition in the theorem above is close to being the finest: with possible exceptions when the residue characteristic in case (I) is p, or when $p = 2$ and $G_{\hat{K}_i}(2) \cong (\mathbb{Z}/2\mathbb{Z}) *_2 (\mathbb{Z}/2\mathbb{Z})$, the groups $G_{\hat{K}_i}(p)$ cannot be decomposed any further as free pro-p products. Furthermore, for K as in the theorem (and with similar exceptions) and for any free pro-p product decomposition $G_K(p) = \Gamma_1 *_p \cdots *_p \Gamma_n$, each Γ_i is generated by groups of the form $G_{\hat{K}}(p)$, with $\hat{K}$ as in (I) or (II).

Using this theorem and [E1, Cor. 4.4] we get:

COROLLARY: *Let $p = 2$ and let $K, \hat{K}_1, \ldots, \hat{K}_n$ be as in the theorem. Then a quadratic form over K which is isotropic in each $\hat{K}_i$ is also isotropic in K.*

This is a partial generalization of a local-global principle for (weak) isotropy of quadratic forms due (independently) to Bröcker and Prestel [L1, §18]; in one of its equivalent forms, this principle says that a quadratic form over a real-pythagorean field K is isotropic if and only if it is isotropic in all subextensions of $K(2)/K$ of types (I) and (II).

References

[AEJ1] J.K. Arason, R. Elman and B. Jacob, *The graded Witt ring and Galois cohomology I*, Canad. Math. Soc. Conf. Proc. **4** (1984), 17–50.

[AEJ2] J.K. Arason, R. Elman and B. Jacob, *Graded Witt rings of elementary type*, Math. Ann. **272** (1985), 267–280.

[B] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. reine angew. Math. **268–269** (1974), 41–52.

[CM] A.B. Carson and M. Marshall, *Decomposition of Witt rings*, Canad. J. Math. **34** (1982), 1276–1302.

[E1] I. Efrat, *Local-global principles for Witt rings*, J. Pure Appl. Algebra **90** (1993), 153–166.

[E2] I. Efrat, *Free product decompositions of Galois groups over pythagorean fields*, Comm. Algebra **21** (1993), 4495–4511.

[E3] I. Efrat, *Free pro-p product decompositions of Galois groups* (to appear).

[EH] I. Efrat and D. Haran, *On Galois groups over pythagorean and semi-real closed fields*, Isr. J. Math. **85** (1994), 57–78.

[Er] Yu. L. Eršov, *Semilocal fields*, Dokl. Akad. Nauk. SSSR **215**(2) (1974), 41–44 (Russian); Sov. Math. Dok. **15** (1974), 424–428 (English translation).

[H] B. Heinemann, *On finite intersections of "Henselian valued" fields*, manusc. math. **52** (1985), 37–61.

[J] B. Jacob, *On the structure of pythagorean fields*, J. Algebra **68** (1981), 247–267.

[JW] B. Jacob and A. Wadsworth, *A new construction of noncrossed product algebras*, Trans. Amer. Math. Soc. **293** (1986), 693–721.

[JWr1] B. Jacob and R. Ware, *A recursive description of the maximal pro-2 Galois group via Witt rings*, Math. Z. **200** (1989), 379–396.

[JWr2] B. Jacob and R. Ware, *Realizing dyadic factors of elementary type Witt rings and pro-2 Galois groups*, Math. Z. **208** (1991), 193–208.

[L1] T.Y. Lam, *Orderings, valuations and quadratic forms*, Conf. Board of the mathematical sciences **52**, AMS 1983.

[L2] T.Y. Lam, *Fields of u-invariant 6 after A. Merkurjev*, Israel Math. Conf. Proc. **1** (1989), 12–30.

[M] M. Marshall, *Abstract Witt Rings*, Queen's Pap. Pure Appl. Math. **57** (1980).

[Me1] A. Merkurjev, *On the norm residue symbol of degree* 2, Dokl. Akad. Nauk SSSR **261** (1981), 542-547 (Russian); Sov. Math. Dok. **24** (1981), 546–551 (English translation).

[Me2] A.S. Merkurjev, *Simple algebras and quadratic forms*, Izv. Akad. Nauk SSSR **55** (1991), 218–224 (Russian); Math. USSR Izv. **38** (1992), 215–221 (English translation).

[MeS] A.S. Merkuriev and A.A. Suslin, *The norm reisdue homomorphism of degree* 3, Izv. Akad. Nauk SSSR, Ser. Mat. **54** (1990), 339–356 (Russian); Math. USSR Izv. **36** (1991), 349–368 (English translation).

[Mi] J. Mináč, *Galois groups of some 2-extensions of ordered fields*, C.R. Math. Rep. Acad. Sci. Canada **8** (1986), 103–108.

[N] J. Neukirch, *Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen*, J. reine angew. Math. **259** (1973), 1–47.

[R] M. Rost, *Hilbert's theorem 90 for K_3^M for degree-two extensions*, preprint, Regensburg, 1986.

[S] W. Scharlau, *Quadratic and Hermitian Forms*, Springer, Berlin 1985.

[Se] J.-P. Serre, *Cohomologie Galoisienne*, Lect. Notes Math. **5**, Springer 1965.

Definable Valuations

Jochen Koenigsmann

Abstract

We prove that any non-trivially henselian valued field which is neither separably closed nor real closed admits a first-order definable valuation inducing the henselian topology. A general account of definability of valuations from multiplicative or additive subgroups of fields is developed.

Introduction

The properties of henselian valued fields are, as we know from the work of Ax-Kochen and Ershov, to a great extent determined by the data going along with a henselian valuation, notably its residue field and its value group. In this paper, we investigate some kind of a converse of this insight, namely, that for a field which admits a henselian valuation, we can describe a canonical valuation on that field in purely field theoretic terms, even in a first-order manner: we define that valuation in a similar fashion as, say, the ordering of a real closed field is defined in terms of the quadratic elements of the field, or, indeed, the p-adic valuation on the field $\mathbf{Q}_p$ of p-adic numbers is defined, e.g. by describing the valuation ring, the ring $\mathbf{Z}_p$ of p-adic integers, by $\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid \exists y : y^2 - y = px^2\}$. It is in this sense that the field 'determines' the valuation.

Unfortunately, there are two factors which complicate matters with henselian valued fields. One is that we can only expect the envisaged result, that a henselian valued field carries a field theoretically first-order definable (non-trivial) valuation, if the field in question is neither separably closed nor real closed. For any non-trivial definable valuation on a separably closed field is definable with finitely many parameters from that field and, therefore, induces a non-trivial valuation on a finitely generated subfield containing those

parameters; but there are no finitely generated henselian fields, so the valuation on the small field extends in different, though conjugate ways to its separable closure, and thus to the separably closed field we started off with — hence the valuation could not have been definable after all. And for a real closed field, any non-trivial definable valuation ring would have to be definable without quantifiers, i.e. a finite union of intervals and points, which we know to be impossible on the real numbers, and hence, on any real closed field.

The other complication arises from the fact that there are fields which are not separably or real closed and which do not admit any non-trivial henselian valuation, but which are elementarily equivalent to some field *with* a non-trivial henselian valuation (such fields have been constructed by A.Engler, cf. the example in [PZ], p. 338). In particular, the canonical henselian valuation ring attached to each henselian valued field (cf.[EE]) will, in general, not be definable.

Yet in the light of these obstructions we shall prove the best possible result, the formulation of which already reflects the topological character of its proof. One has to recall that on a field which is not separably closed, any two non-trivial henselian valuations are dependent ([EE]), i.e. have a non-trivial common coarsening, or equivalently, induce the same topology, which we may therefore call **the henselian topology**.

Main Theorem *Any field with non-trivial henselian valuation which is not separably closed or real closed, admits a definable valuation inducing the henselian topology.*

For henselian valued fields with real closed residue field (so-called almost real closed fields) such definable valuations have already been found in special cases in [J1] and [J2], and systematically in [DF] (cf. also [BBG]). Other instances arose in the context of half-ordered fields (cf. [K1]).

We shall prove the main theorem, or, rather, a more general result about fields with a non-trivial 't-henselian' valuation (cf. section 4), by finding to any such field a finite valued field extension where for some prime p a p-henselian valuation inducing the (t-)henselian topology can be defined essentially in terms of the multiplicative group of p-th powers of that field, or, if the characteristic is p, the additive analogue to this group (section 3).

This leads naturally to the task of defining valuations from a given (mul-

tiplicative or additive) subgroup of a field (section 2), a problem that has been dealt with in many special situations and has to our knowledge so far received its most extensive treatment in [AEJ] (though only for the multiplicative case). The crucial notion here has always been that of 'compatibility' between a valuation and a subgroup of a field. It turned out in the course of our investigations that this notion needs to be both generalized and refined (section 1) in order to gain the survey necessary for the definability results of section 2. With this at hand we can then not only provide precise criteria for the (first-order) definability of valuations in terms of a given subgroup (thm.2.5), but actually give explicit first-order formulas wherever they exist, and second-order formulas in all other cases (thm.2.11).

Readers only interested in the proof of the main theorem may omit the discussion of general definability of valuations from subgroups by consulting, instead, the direct argument in [K2] for the definability of p-henselian valuations, and then proceed to section 4 of the present paper.

Notation: For a valued field (F, v), we denote by $\mathcal{O}_v, \mathcal{M}_v, F_v$ and Γ_v the corresponding valuation ring, maximal ideal, residue field and value group, the latter being written additively. (For background in valuation theory cf.e.g. [E] or [R].)

1 Compatibility between Valuations and Submonoids of Fields

In this section we consider a field F together with an additive resp. multiplicative submonoid T, that is, $T \subseteq F$ resp. $T \subseteq F^\times$ is additively resp. multiplicatively closed and contains 0 resp. 1. We want to study the collection of all valuations of F that are in some sense compatible with T. This will enable us to find a distinguished valuation ring $\mathcal{O}_T$ of F canonically associated with T. In order to obtain the full picture, we have to introduce three notions of compatibility:

Definition 1.1 *Let v be a valuation of F, T an additive resp. multiplicative submonoid of F.*

1. *v is* **compatible** *with T iff $\mathcal{M}_v \subseteq T$ resp. $1 + \mathcal{M}_v \subseteq T$.*

2. v *is* **weakly compatible** *with* T *iff* $\mathcal{A} \subseteq T$ *resp.* $1 + \mathcal{A} \subseteq T$ *for some* $\mathcal{O}_v$*-ideal* $\mathcal{A}$ *with* $\sqrt{\mathcal{A}} = \mathcal{M}_v$.

3. v *is* **coarsely compatible** *with* T *iff* v *is weakly compatible with* T *and there is no proper coarsening* w *of* v *such that* $\mathcal{O}_w^\times \subseteq T$.

The first notion of compatibility is — at least when T is a multiplicative subgroup of F — widely used, and stands in no need of justification (cf. e.g. [AEJ]). The notion of *weak* compatibility is required to cover situations where a valuation *is* related to T without being (fully) compatible, e.g. when T is itself a non-maximal valuation ideal, or when $(F, T) = (\mathbf{Q}_p, (\mathbf{Q}_p^\times)^p)$, where, for the p-adic valuation v on $\mathbf{Q}_p$, on the one hand $1 + \mathcal{M}_v \not\subseteq T$, on the other hand $1 + \mathcal{M}_v^3 \subseteq T$. The additional condition for *coarse* compatibility becomes only relevant in case $\mathcal{O}_v^\times \subseteq T$ (when T is additive, this is equivalent to $\mathcal{O}_v \subseteq T$). In this case any refinement of v has this property, and there is no way to distinguish between those refinements in terms of T. On the other side, each valuation v with $\mathcal{O}_v^\times \subseteq T$ allows a maximal coarsening with the same property, which will then be coarsely compatible; so the notion of coarse compatibility is only designed to ignore unnecessarily fine valuations. The same is true for the radical condition '$\sqrt{\mathcal{A}} = \mathcal{M}_v$' in the definition of weak compatibility: without the condition, any refinement would be weakly compatible without being further distinguishable in terms of T; yet, again, the condition can easily be brought about by passing to a suitable coarsening: if $\mathcal{A} \subseteq T$ resp. $1 + \mathcal{A} \subseteq T$ for some $\mathcal{O}_v$-ideal $\mathcal{A}$, localizing modulo the maximal prime ideal of $\mathcal{O}_v$ containing $\mathcal{A}$ leads to a valuation w where the radical condition is fulfilled for some $\mathcal{O}_w$-ideal contained in $\mathcal{A}$, e.g. for $\mathcal{O}_w\mathcal{A}^2$.

With the distinction between full and weak compatibility being justified, one finds, nevertheless, important situations where the two notions coincide:

Lemma 1.2 *Let* v *be a valuation on* F. *If either* T *is multiplicative such that for some* $n \in \mathbf{N}$: $(F^\times)^n \subseteq T$ *and* $(n,\ char\ F_v) = 1$, *or* T *is additive, char* $F = p$ *and* $\{x^p - x \mid x \in F\} \subseteq T$, *then* v *is (fully) compatible with* T *iff* v *is weakly compatible with* T.

Proof: Suppose T satisfies the assumption, and is weakly, but not fully compatible with v. Let $\mathcal{A}$ be the $\mathcal{O}_v$-ideal which is maximal with the property $\mathcal{A} \subseteq T$ resp. $1 + \mathcal{A} \subseteq T$. Then $\mathcal{A} \neq \mathcal{M}_v$, and, by the radical condition for

weak compatibility, we can find an $\mathcal{O}_v$-ideal $\mathcal{B}$ with $\mathcal{B}^2 \subseteq \mathcal{A} \subset_{\neq} \mathcal{B}$ (choose $a \in \mathcal{M}_v \setminus \mathcal{A}$, so $a^k \notin \mathcal{A}$, $a^{k+1} \in \mathcal{A}$ for some $k \in \mathbb{N}$, and let $\mathcal{B} := a^k \mathcal{O}_v$). Then, if T is additive, for all $b \in \mathcal{B}$: $\pm b^p \in T$ and $(-b)^p + b \in T$, so $b \in T$, and if T is multiplicative,

$$(1 + (\frac{b}{n}))^n = \overbrace{1+b}^{\in \mathcal{O}_v^\times} + \overbrace{\binom{n}{2}(\frac{b}{n})^2 + \ldots}^{\in \mathcal{B}^2 \subseteq \mathcal{A}, \text{ since } n \in \mathcal{O}_v^\times} \in [(1+b)(1+\mathcal{A})] \cap T,$$

so $1 + b \in T$, because $(1+\mathcal{A})^{-1} = (1+\mathcal{A}) \subseteq T$. But then $\mathcal{B} \subseteq T$ resp. $1 + \mathcal{B} \subseteq T$, contradicting the maximality of $\mathcal{A}$. □

Having introduced the correct notions of compatibility, the main result of this section is based on the following simple

Observation 1.3 *Let v_1, v_2 be two non-comparable valuations (i.e. $\mathcal{O}_{v_1} \not\subseteq \mathcal{O}_{v_2}$ and $\mathcal{O}_{v_2} \not\subseteq \mathcal{O}_{v_1}$), and let w denote the finest common coarsening of v_1 and v_2. Then, for any $\mathcal{O}_{v_1}$-ideal $\mathcal{A}_1$ with $\mathcal{M}_w \subset_{\neq} \mathcal{A}_1$ and any $\mathcal{O}_{v_2}$-ideal $\mathcal{A}_2$ with $\mathcal{M}_w \subset_{\neq} \mathcal{A}_2$, one has*

$$\mathcal{O}_w = \mathcal{A}_1 + \mathcal{A}_2 \text{ and } \mathcal{O}_w^\times = (1+\mathcal{A}_1)(1+\mathcal{A}_2).$$

Proof: The two valuations $\overline{v_1}, \overline{v_2}$ induced by v_1, v_2 on the residue field F_w of w are independent. So for each $x \in \mathcal{O}_w$ one finds, by the approximation theorem, that $(\overline{x} - \overline{\mathcal{A}_1}) \cap \overline{\mathcal{A}_2} \neq \emptyset$, so $\overline{x} \in \overline{\mathcal{A}_1} \cap \overline{\mathcal{A}_2}$ and, hence, as $\mathcal{M}_w \subseteq \mathcal{A}_1 \cap \mathcal{A}_2$, also $x \in \mathcal{A}_1 + \mathcal{A}_2$.

Similarly, one finds for $x \in \mathcal{O}_w^\times$ that $(\overline{x} + \overline{x}\overline{\mathcal{A}_1}) \cap (1 + \overline{\mathcal{A}_2}) \neq \emptyset$, so

$$\overline{x} \in (1+\overline{\mathcal{A}_1})^{-1}(1+\overline{\mathcal{A}_2}) = (1+\overline{\mathcal{A}_1})(1+\overline{\mathcal{A}_2}),$$

and hence

$$x \in (1+\mathcal{A}_1)(1+\mathcal{A}_2) + \mathcal{M}_w \subseteq (1+\mathcal{A}_1)(1+\mathcal{A}_2)(1+\mathcal{M}_w) \subseteq (1+\mathcal{A}_1)(1+\mathcal{A}_2),$$

using that $1 + \mathcal{A}_i \leq \mathcal{O}_{v_i}^\times \leq \mathcal{O}_w^\times$. □

Proposition 1.4 *For an additive resp. multiplicative submonoid T of a field F, any two coarsely compatible valuations are comparable, and there is a unique finest coarsely compatible valuation ring $\mathcal{O}_T$ of F. Moreover, $\mathcal{O}_T$ is non-trivial, whenever T is non-trivial (i.e. $T \neq F$ resp. $F^\times$) and admits some non-trivial weakly compatible valuation.*

Proof: Our observation tells us that for any two weakly compatible valuations v_1, v_2 which are not comparable, the finest common coarsening w satisfies $\mathcal{O}_w^\times \subseteq \mathcal{O}_w \subseteq \mathcal{A}_1 + \mathcal{A}_2 \subseteq T$ resp. $\mathcal{O}_w^\times \subseteq (1+\mathcal{A}_1)(1+\mathcal{A}_2) \subseteq T$, where $\mathcal{A}_i$ is an $\mathcal{O}_{v_i}$- ideal with $\mathcal{A}_i \subseteq T$ resp. $1+\mathcal{A}_i \subseteq T$ and $\sqrt{\mathcal{A}_i} = \mathcal{M}_{v_i}$ $(i=1,2)$: note that the radical condition makes sure that $\mathcal{M}_w \subset_{\neq} \mathcal{A}_i$. So v_1 and v_2 are both not coarsely compatible and $\mathcal{O}_{v_i}^\times \subseteq \mathcal{O}_w^\times \subseteq T$. In particular, it follows by contraposition, that any two coarsely compatible valuations are comparable.

Therefore, the ring

$$\mathcal{O}_T := \bigcap_{v \text{ coarsely compatible with } T} \mathcal{O}_v$$

is a valuation ring.

If T admits some valuation v with $\mathcal{O}_v^\times \subseteq T$, then $\mathcal{O}_T$ is the unique coarsely compatible valuation ring with that property: on the one hand, the valuation ring

$$\mathcal{O} := \bigcup_{\mathcal{O}_v \subseteq \mathcal{O}_w \,\&\, \mathcal{O}_w^\times \subseteq T} \mathcal{O}_w$$

is a coarsely compatible valuation ring with $\mathcal{O}^\times \subseteq T$: on the other hand, no proper subring of $\mathcal{O}$ is coarsely compatible, so $\mathcal{O} = \mathcal{O}_T$, and the coarsely compatible valuation rings are just the subrings of F containing $\mathcal{O}_T$. They are all fully compatible, as for $\mathcal{O}_T \subseteq \mathcal{O}_w$: $\mathcal{M}_w \subseteq \mathcal{M}_T \subseteq \mathcal{O}_T$ resp. $1+\mathcal{M}_w \subseteq 1+\mathcal{M}_T \subseteq \mathcal{O}_T^\times \subseteq T$: in that case all weakly compatible valuations are fully compatible.

If, however, T admits a weakly compatible valuation ring, which is not fully compatible, then $\mathcal{O}_T$ is the unique such valuation ring (any smaller ring would violate the radical condition), and all weakly compatible valuations are coarsely compatible.

If, finally, all weakly compatible valutions are fully compatible and no valuation has all its units contained in T, then $\mathcal{O}_T$ is the smallest compatible valuation ring:

$$\mathcal{M}_T = \bigcup_{v \text{ coars comp w. } T} \mathcal{M}_v,$$

so $\mathcal{M}_T \subseteq T$ resp. $1+\mathcal{M}_T \subseteq T$.

The 'moreover' follows readily in each of these cases. □

We are now in a position to survey all possibilities for weakly compatible valuations with the classification given in the proof. We rephrase this classification, also for further reference, in the following

Corollary 1.5 *For any additive or multiplicative submonoid T of a field F one of the three following cases holds:*

- **group case**: *there is a valuation v with $\mathcal{O}_v^\times \subseteq T$.*
  In this case, $\mathcal{O}_T$ is the only coarsely compatible valuation ring with this property; the valuations with this property are exactly the refinements of $\mathcal{O}_T$; all weakly compatible valuations are fully compatible; the submonoid induced on the residue field of $\mathcal{O}_T$ is trivial; if T is multiplicative, it is determined by its values: $T = v^{-1}(v(T))$.

- **weak case**: *there is a weakly, but not fully compatible valuation.*
  In this case, $\mathcal{O}_T$ is the only valuation ring with this property; the weakly compatible valuations are the coarsenings of $\mathcal{O}_T$; there is no valuation v with $\mathcal{O}_v^\times \subseteq T$.

- **residue case**: *all weakly compatible valuations are fully compatible and there is no valuation v with $\mathcal{O}_v^\times \subseteq T$.*
  In this case, $\mathcal{O}_T$ is the finest compatible valuation ring and the submonoid induced on the residue field is non-trivial.

Corollary 1.6 *$\mathcal{O}_T$ is fixed under T-automorphisms, that is, under automorphisms of the field F mapping T to T.*

Proof: Pick $\sigma \in Aut(F)$ with $\sigma(T) = T$. Then $\sigma(\mathcal{O}_T)$ is coarsely compatible with $\sigma(T) = T$. So, by the theorem, $\mathcal{O}_T \subseteq \sigma(\mathcal{O}_T)$. But, similarly, $\mathcal{O}_T \subseteq \sigma^{-1}(\mathcal{O}_T)$, i.e. $\sigma(\mathcal{O}_T) \subseteq \mathcal{O}_T$. □

Remark 1.7 *Extending earlier work of B.Jacob ([J1]) and R.Ware ([W]), in [AEJ], the question of compatibility of a valuation with a multiplicative subgroup T of a field F has already been explored in great detail. In order to find some canonical valuation associated to T, the authors introduce for a T-compatible valuation v of F the property of being T-**coarse** which is that $v(T)$ $(= v(T \cdot \mathcal{O}_v^\times))$ contains no non-trivial convex subgroup. They prove that any two T-compatible, T-coarse valuations are comparable (Cor.3.7), and that there is a unique smallest T-compatible, T-coarse valuation ring*

$\mathcal{O}_F(T)$ of F (Thm.3.8). We shall call $\mathcal{O}_F(T)$ the **Jacob-ring** *associated to the multiplicative group T. Since any T-compatible, T-coarse valuation is coarsely compatible in our sense, these results are immediate from our prop.1.4. One always has $\mathcal{O}_T \subseteq \mathcal{O}_F(T)$, with equality in the group case, strict inclusion in the weak case and both possibilities in the residue case. $\mathcal{O}_F(T)$ is also canonical in the sense of being fixed under T-automorphisms. Yet $\mathcal{O}_F(T)$ may become trivial even though there do exist non-trivial 'T-relevant' valuations. This can happen for two reasons: one is that T admits weakly compatible valuations, but no non-trivial fully compatible ones (cf. the remarks following the definition1.1). The other is that elements of T may attain any value under a compatible valuation. For example, if T is an ordering, $\mathcal{O}_F(T) = F$, whereas $\mathcal{O}_T$ is the canonical valuation ring attached to each ordering, i.e. the convex hull of $\mathbb{Q}$ in F w.r.t. T, so $\mathcal{O}_T$ is non-trivial iff T is non-archimedean.*

2 Valuations Definable from Subgroups

From now on, T will be an additive or multiplicative sub*group* of the field F. In the preceding section, we gave an *external* definition for the valuation ring $\mathcal{O}_T$ canonically associated to T: $\mathcal{O}_T$ was the finest valuation ring coarsely compatible with T. We shall now try to give an *internal* characterisation of $\mathcal{O}_T$, that is, a characterisation which does not require that we know about all (or any) other coarsely compatible valuations, a characterisation only in terms of T. Stronger even, and more precisely, we are looking for a first-order formula in the language $\mathcal{L} := (+, -, \cdot, 0, 1, \underline{T})$, the language of fields augmented by a single (one-place) predicate for the subgroup T.

If we can find such a formula for $\mathcal{O}_T$ in terms of T, i.e. if $\mathcal{O}_T$ is (first-order) definable in $\mathcal{L}$, then, in particular, the property, that (F, T) admits some non-trivial weakly compatible valuation, becomes a first-order property, since this is, by proposition1.4, equivalent to $\mathcal{O}_T$ being non-trivial. In fact, we shall see that, whenever T is a proper subgroup of F resp. $F^\times$ which is not (the strictly positive cone of) an ordering, weak compatibility with some non-trivial valuation *is* a first-order property (in case T is an ordering, this can, in general, not be expected because archimedeanity or non-archimedeanity is not a first-order property). *Full* compatibility with some non-trivial valuation, in contrast, cannot be described by a first-order

formula:

Example 2.1 *Let $F := \mathbf{Q}_p$, $T := (\mathbf{Q}_p^\times)^p$ and let v denote the p-adic valuation on $\mathbf{Q}_p$. Then v is weakly, but not fully compatible with T, and there is no non-trivial fully compatible valuation on $\mathbf{Q}_p$ (as we are in the 'weak case', it would have to be a coarsening of $\mathcal{O}_T = \mathcal{O}_v$). Passing to an ω-saturated elementary extension $(F', v') \succeq (F, v)$, with $T' := (F'^\times)^p$ extending T, one does, however, find non-trivial valuations fully compatible with T'; take, for example, the coarsening w of v' with maximal ideal $\mathcal{M}_w := \bigcap_{n=1}^\infty p^n \mathcal{M}_{v'}$: it is fully compatible, since $1 + \mathcal{M}_w \subseteq 1 + p^2 \mathcal{M}_{v'} \subseteq T'$, and it is non-trivial, since, by saturation, $\bigcap_{n=1}^\infty \mathcal{M}_{v'} \neq \{0\}$.*

The reason why the existence of a non-trivial weakly compatible valuation can be expressed in a first-order formula (unless T is trivial or an ordering) is of a topological nature. We shall associate to each subgroup T of F a topology induced by T on F. It will then turn out that T is weakly compatible with some non-trivial valuation iff T induces a T_1-topology on F, and that this can be said in first-order terms. Using this fact, we shall see that $\mathcal{O}_T$ is in most cases first-order definable (a precise criterion will be given). Finally, we shall present an explicit formula for $\mathcal{O}_T$ which works for all definable cases simultaneously. For the non-definable cases, an intrinsic, though not first-order, construction will be given.

Definition 2.2 *Let T be an additive resp. multiplicative subgroup of a field F. We shall denote the coarsest topology on F for which T is open and for which Möbius transformations resp. linear transformations are continuous, by τ_T; we call τ_T* **the topology induced by T on F.**

So if T is additive, the sets $\{\frac{ax+b}{cx+d} \mid x \in T, x \neq -\frac{c}{d}\}$ for $a, b, c, d \in F$ with $ad - bc \neq 0$ form a subbase of τ_T; if T is multiplicative, a subbase is given by sets of the form $aT + b$ with $a \in F^\times, b \in F$.

We shall not investigate this topology any further here (in general, τ_T will not make F a topological ring, not even a topological group), but only prove the following fact, which is well known for the special case that T is an ordering (then τ_T is the order-topology of T):

Proposition 2.3 *Let T be a* proper *additive resp. multiplicative subgroup of F, and let v be a non-trivial valuation of F, inducing on F the topology*

τ_v. *Then* $\tau_T = \tau_v$ *iff* T *is weakly compatible with some non-trivial coarsening* w *of* v.

In this case, sets of the form $\{\frac{ax+b}{cx+d} \mid x \in T, x \neq -\frac{d}{c}\}$ *with* $ad - bc \neq 0$ *resp. of the form* $(aT+b) \cap (cT+d)$ *with* $a, c \neq 0$ *form a* base *of the topology* τ_T.

Proof: If $\tau_T = \tau_v$, T must be open w.r.t. τ_v, so for some non-zero $\mathcal{O}_v$-ideal $\mathcal{A}$ one has $\mathcal{A} \subseteq T$ resp. $1 + \mathcal{A} \subseteq T$. Therefore, the coarsening w of v with $\mathcal{M}_w = \sqrt{\mathcal{A}}$ $(\neq \{0\})$ is non-trivial and weakly compatible with T.

For the converse, we may assume that $w = v$ is weakly compatible with T, as comparable non-trivial valuations induce the same topology. We fix some non-zero $\mathcal{O}_v$-ideal $\mathcal{A}$ with $\mathcal{A} \subseteq T$ resp. $1 + \mathcal{A} \subseteq T$. Since $T = \bigcup_{x \in T}(x + \mathcal{A})$ resp. $T = \bigcup_{x \in T} x(1 + \mathcal{A})$ $T \in \tau_v$, and so $\tau_T \subseteq \tau_v$, as τ_v is a field topology, and hence Möbius or linear transformations *are* continuous.

In order to see that also $\tau_v \subseteq \tau_T$, it suffices to check that $\mathcal{M}_v \in \tau_T$, because the sets $a\mathcal{M}_v + b$ with $a \in F^\times, b \in F$ form a base for τ_v. And, again, to check this, it suffices to find an open τ_T-neighbourhood U of 0 with $U \subseteq \mathcal{M}_v$, as then $\mathcal{M}_v = \bigcup_{x \in \mathcal{M}_v} x + U$. We shall treat the additive and the multiplicative case separately.

If T is additive, we can pick some $d \in F \setminus T$ with $d^{-1} \in \mathcal{A}$. This is possible, because T is a *proper* subgroup of F, while $\frac{1}{\mathcal{A} \setminus \{0\}}$ additively generates the whole group F. Now choose $a \in d^{-1} \cdot \mathcal{A}, b \in a \cdot \mathcal{A}$. Then $0 \in U := \{\frac{ax+b}{x+d} \mid x \in T\} \subseteq \mathcal{M}_v$: $b \in a \cdot \mathcal{A} \subseteq a \cdot T$ implies $0 \in U$; and for $x \in T$,

$$v(\frac{ax+b}{x+d}) \begin{cases} = v(a) > 0, \text{ if } v(x) < v(d), \text{ as } v(b) > v(a) > v(ad) > v(ax) \\ > 0, \text{ if } v(x) = v(d), \text{ as } x + d \in F \setminus T \subseteq F \setminus \mathcal{A}, \text{ but } ax + b \in \mathcal{A} \\ > v(a) > 0, \text{ if } v(x) > v(d), \text{ as } v(bd^{-1}) > v(b) > v(a) \end{cases}$$

If T is multiplicative, we can pick $c, d \in F^\times$ with $cT \neq dT$ and $\mathcal{A} \cap cT \neq \emptyset \neq \mathcal{A} \cap dT$; for otherwise $\mathcal{A} \subseteq cT \cup \{0\}$ for some $c \in F^\times$, say $0 \neq a = c \cdot x \in \mathcal{A}$ for some $x \in T$, so $a^2 = c^2x^2 \in cT$, i.e. $c \in T$, and, thus, $\mathcal{A} \setminus \{0\} \subseteq T$; but then $F^\times = \langle \mathcal{A} \setminus \{0\} \rangle \subseteq T$, contradicting the assumption that T is a *proper* subgroup of $F^\times$. Now choose $a \in \mathcal{A} \cap cT, b \in \mathcal{A} \cap dT$. Then $0 \in U := (a - cT) \cap (b - dT) \subseteq \mathcal{M}_v$: if not, we could find some $x = a - cx_1 = b - dx_2 \notin \mathcal{M}_v$ with $x_i \in T$, so $-cx_1 = x - a = x(1 - ax^{-1}) \in x(1 + \mathcal{A}) \subseteq xT$, and, similarly, $-dx_2 \in xT$; but then $-x \in cT \cap dT$, which is impossible, because distinct cosets of T are disjoint.

The statement about the base of τ_T follows immediately from the definition of U and the observation that, because the sets $x.\mathcal{M}_v$ for $x \in F^\times$ form a base of neighbourhoods of 0, the same holds for the sets xU. □

Corollary 2.4 *Let F be a field with a proper additive resp. multiplicative subgroup T which is not an ordering. Then weak compatibility of T with some non-trivial valuation is an elementary property (in the language of fields with an extra predicate for T).*

Proof: The first-order sentence expressing this property is that τ_T is a V-topology. For V-topologies arise either from valuations or from archimedean absolute values. In the first case, T is weakly compatible with some non-trivial valuation, by the proposition. The second case, however, cannot occur, because otherwise T would contain some neighbourhood U of 0 resp. 1 which is open w.r.t. an archimedean absolute value. Yet, by archimedeanity, U additively generates F, so $F \subseteq T$ in the additive case, and U multiplicatively generates the positive cone P of an ordering for a real archimedean absolute value, or all of $F^\times$ for a complex archimedean absolute value, so $P \subseteq T$ or $F^\times \subseteq T$ in the multiplicative case, contrary to the assumptions of the corollary.

That the property that τ_T is a V-topology, is, indeed, first-order expressible, follows, again, from the proposition which provides a uniformly parametrized base of the topology τ_T, whenever T *is* weakly compatible with some non-trivial valuation; and, clearly, 'to be a ring topology of type V' can be expressed in terms of a base of the topology (cf. e.g. [PZ]). □

The next theorem provides exact criteria for the definability of the valuation ring $\mathcal{O}_T$ canonically associated to a subgroup T in each of the three cases described in corollary1.5.

Theorem 2.5 *Let F be a field with an additive resp. multiplicative subgroup T. Then $\mathcal{O}_T$ is first-order definable in the language $\mathcal{L} := \{+, -, \cdot, 0, 1; \underline{T}\}$ in the following cases:*

	$T \leq (F,+)$		$T \leq F^\times$
group case	*iff*	*either $\mathcal{O}_T$ is discrete or $\forall x \in \mathcal{M}_T : x^{-1}\mathcal{O}_T \not\subseteq T$*	*yes*
weak case	*iff $\mathcal{O}_T$ is discrete*		
residue case	*yes*		*iff T is no ordering*

Here, $\mathcal{M}_T$ denotes the maximal ideal of $\mathcal{O}_T$, and $\overline{T}$ denotes the subgroup induced by T on the residue field of $\mathcal{O}_T$.

Proof: By corollary1.6, $\mathcal{O}_T$ is fixed under T-automorphisms of F. It thus follows from Beth's definability theorem, that $\mathcal{O}_T$ is definable, whenever we can elementarily express its defining property, namely that $\mathcal{O}_T$ is the finest valuation ring coarsely compatible with T.

In the **group case** this is equivalent to saying that $\mathcal{O}_T$ is a valuation ring with $\mathcal{O}_T^\times \subseteq T$ (this can, obviously, be expressed in first-order terms) and with the property that no proper coarsening $\mathcal{O}_w$ of $\mathcal{O}_T$ satisfies $\mathcal{O}_w^\times \subseteq T$.

If T is *multiplicative*, this property is expressed by the formula

$$\forall x \in \mathcal{M}_T : \mathcal{M}_T \setminus x\mathcal{M}_T \not\subseteq T.$$

For, given $x \in \mathcal{M}_T$, we have:

$$\begin{aligned} \mathcal{M}_T \setminus x\mathcal{M}_T &\iff \langle \mathcal{M}_T \setminus x\mathcal{M}_T \rangle \subseteq T \\ &\iff \mathcal{O}_w^\times = \langle \mathcal{M}_T \setminus x\mathcal{M}_T \rangle \subseteq T \end{aligned}$$

where $\mathcal{O}_w = S^{-1}\mathcal{O}_T$ for the multiplicative closure $S \subseteq \mathcal{O}_T$ of $\mathcal{M}_T \setminus x\mathcal{M}_T$: $\mathcal{O}_w$ *is* a proper coarsening of $\mathcal{O}_T$. Conversely, for a proper coarsening $\mathcal{O}_w$ of $\mathcal{O}_T$ with $\mathcal{O}_w^\times \subseteq T$, one could find some $x \in \mathcal{M}_T$ violating the formula: $x \in \mathcal{M}_T \setminus \mathcal{M}_w$ would satisfy $\mathcal{M}_T \setminus x\mathcal{M}_T \subseteq \mathcal{M}_T \setminus \mathcal{M}_w \subseteq \mathcal{O}_w^\times \subseteq T$.

If T is *additive*, and $\forall x \in \mathcal{M}_T : x^{-1}\mathcal{O}_T \not\subseteq T$, then this formula already guarantees that $\mathcal{O}_T$ does not admit a coarsening $\mathcal{O}_w$ with $\mathcal{O}_w^\times \subseteq T$ (or, equivalently, $\mathcal{O}_w \subseteq T$), for if there were such a coarsening $\mathcal{O}_w$, the formula would not hold for $x \in \mathcal{M}_T \setminus \mathcal{M}_w$: $x^{-1}\mathcal{O}_T \subseteq \mathcal{O}_w \subseteq T$.

If $\mathcal{O}_T$ is discrete, say $\mathcal{M}_T = x\mathcal{O}_T$, then, for some $n \in \mathbf{N}$, $x^{-n}\mathcal{O}_T \subseteq T$, but $x^{-(n+1)}\mathcal{O}_T \not\subseteq T$. Together with '$\mathcal{O}_T \subseteq T$', the existence of such an x, again, elementarily distinguishes $\mathcal{O}_T$ from any other valuation ring.

On the other hand, if T is additive, $\mathcal{O}_T \subseteq T$, but $\mathcal{O}_T$ is not discrete, and for some $x \in \mathcal{M}_T$: $x^{-1}\mathcal{O}_T \subseteq T$, then

$$\Phi(y) := \{0 \neq y \in \mathcal{M}_T \wedge y^{-n}\mathcal{O}_T \subseteq T \mid n \in \mathbf{N}\}$$

is a type (by non-discreteness, there always exists some $y \in \mathcal{M}_T \setminus \{0\}$ with $x\mathcal{O}_T \subseteq y^n\mathcal{O}_T$), so realizing $\Phi(y)$ in some ω-saturated elementary extension $(F', T', \mathcal{O}') \succeq (F, T, \mathcal{O}_T)$, say by $y' \in \mathcal{M}'$, we see that $\mathcal{O}'$ admits a proper

coarsening $\mathcal{O}'' := \bigcup_{n=1}^{\infty} y'^{-n}\mathcal{O}'$ with $\mathcal{O}''^{\times} \subseteq T'$, so $\mathcal{O}' \neq \mathcal{O}_{T'}$, and, therefore, $\mathcal{O}_T$ cannot be first-order definable in terms of T.

For the **weak case**, one essentially repeats the argument for the additive group case. $\mathcal{O}_T$ is the unique valuation ring which is weakly, but not fully compatible with T. If $\mathcal{O}_T$ is discrete, this, for some $n \in \mathbf{N}$, is equivalent to

$$\exists x : \mathcal{M}_T = x\mathcal{O}_T \quad \wedge \quad x^n\mathcal{O}_T \not\subseteq T \quad \wedge \quad x^{n+1} \subseteq T$$

resp.

$$\exists x : \mathcal{M}_T = x\mathcal{O}_T \quad \wedge \quad 1 + x^n\mathcal{O}_T \not\subseteq T \quad \wedge \quad 1 + x^{n+1} \subseteq T$$

(note that, like in the additive group case with $\mathcal{O}_T$ discrete, we don't have a uniform formula, but, rather, a countable case distinction with a formula for each case).

For $\mathcal{O}_T$ non-discrete, no first-order formula can express the radical condition required for weak compatibility. Indeed, if $(F', T', \mathcal{O}') \succeq (F, T, \mathcal{O}_T)$ is, again, an ω-saturated elementary extension, then $\mathcal{O}'$ is *not* weakly compatible with T': the type

$$\Phi(y) := \{y \in \mathcal{O} \setminus \mathcal{O}^{\times} \wedge y^n\mathcal{O} \not\subseteq T \text{ resp. } 1 + y^n\mathcal{O} \not\subseteq T \mid n \in \mathbf{N}\}$$

yields an element $y' \in \mathcal{M}'$ such that for the non-maximal $\mathcal{O}'$-prime ideal $\mathcal{P} := \bigcap_{n=1}^{\infty} y'^n\mathcal{O}'$, one has $\mathcal{P} \not\subseteq T$ resp. $1 + \mathcal{P} \not\subseteq T$; therefore, any $\mathcal{O}'$-ideal $\mathcal{A}$ with $\mathcal{A} \subseteq T$ resp. $1 + \mathcal{A} \subseteq T$ is contained in $\mathcal{P}$, so one never has $\sqrt{\mathcal{A}} = \mathcal{M}'$.

In the **residue case**, we have to express that $\mathcal{O}_T$ is the finest valuation ring compatible with T. Because T induces a proper subgroup $\overline{T}$ on the residue field, this is equivalent to saying that $\mathcal{O}_T$ is (fully) compatible with T and that $\overline{T}$ is not weakly compatible with any non-trivial valuation (any such valuation gave rise to a refinement of $\mathcal{O}_T$ weakly compatible with T). By corollary2.4, this is elementarily expressible, unless $\overline{T}$ is an ordering. If, however, $\overline{T}$ *is* an ordering, then $\overline{T}$ must be archimedean. Yet, once more, we can find some elementary extension $(F', T', \mathcal{O}') \succeq (F, T, \mathcal{O}_T)$ with $\overline{T}'$ non-archimedean, so, again, $\mathcal{O}' \neq \mathcal{O}_{T'}$. □

Corollary 2.6 *The distinction between the three cases described in corollary 1.5, i.e. the group case, the weak case and the residue case, is an* elementary *classification of the class of fields with an additive resp. multiplicative subgroup.*

Proof: Let us begin with the class of fields with **multiplicative** subgroups.

The group case is elementarily described by expressing that the defining formula for $\mathcal{O}_T$ (which exists by the theorem) defines a valuation ring $\mathcal{O}$ with $\mathcal{O}^\times \subseteq T$.

Similarly, in the residue case, if $\overline{T}$ is not an ordering, we express that the defining formula for $\mathcal{O}_T$ defines a fully compatible valuation ring $\mathcal{O}$ with $\mathcal{O}^\times \not\subseteq T$ and with $\overline{T}$ not inducing a V-topology on the residue field of $\mathcal{O}$.

If, in the residue case, $\overline{T}$ *is* an ordering, then $\mathcal{O}_T^\times \subseteq T \cup -T \leq F^\times$, and T induces an ordering on the residue field of $\mathcal{O}_{T\cup -T}$: note that $\mathcal{O}_{T\cup -T}^\times \subseteq T\cup -T$, but $\not\subseteq T$, since $\mathcal{O}_{T\cup -T}^\times \supseteq \mathcal{O}_T^\times \not\subseteq T$, so T induces a multiplicative subgroup of index 2 on the residue field of $\mathcal{O}_{T\cup -T}$; this must, however, be additively closed, as otherwise $\mathcal{O}_T^\times \subseteq \mathcal{O}_{T\cup -T}^\times \subseteq T+T$, contrary to the assumption that T induces an ordering on the residue field of $\mathcal{O}_T$. So the residue case with T inducing an ordering on the residue field of $\mathcal{O}_T$ is expressed by saying that the defining formula for $\mathcal{O}_{T\cup -T}$ defines a valuation ring $\mathcal{O}$ with $\mathcal{O}^\times \subseteq T\cup -T$ such that T induces an ordering on the residue field of $\mathcal{O}$.

(One should point out, that the residue case with $\overline{T}$ an ordering is well known to be elementary by the works of B.Jacob [J1] and [J2]: this is exactly the case where T is a **valuation fan** which has the much simpler elementary characterisation:

$$-1 \notin T \ \wedge\ T+T \subseteq T \ \wedge$$
$$\forall x \in F \setminus \pm T:\ 1+x \in T \cup xT \ \wedge\ (1+x \in T \rightarrow 1-x \in T).$$

The ring $\mathcal{O}_{T\cup -T}$ is exactly $\mathcal{O}_F(T)$, the ring introduced in remark 1.7, for which Jacob gives an explicit elementary description.)

With the group case and the residue case being thus finitely axiomatized in elementary terms, the weak case can be elementarily characterized as complementary to those two cases.

In the class of fields with **additive** subgroups, it is — by the same token as, e.g., the multiplicative group case — clear, that the residue case is elementary.

(F,T) belongs to the group case iff it does not belong to the residue case, but the formula

$$o:\ \forall x \in F:\ x \in T \vee x^{-1} \in T$$

holds; for this, we only have to prove that o does not hold in the weak case (o obviously holds in the group case: $\mathcal{O}_T \subseteq T$). In the weak case, however,

we have some $\mathcal{O}_T$-ideal $\mathcal{A}$ with $\mathcal{A} \subsetneq T$ and some $x \in \mathcal{M}_T$ s.t. $x \notin T$ and $x^2 \in \mathcal{A}$; assuming that o holds, we get:

$$\begin{array}{ll} & 1 \in T, x \notin T \\ \Rightarrow & 1+x \notin T, 1-x \notin T \\ \Rightarrow & \frac{1}{x} \in T, \frac{1}{1+x} \in T, \frac{1}{1-x} \in T \\ & \\ & \frac{x}{1 \pm x} = x \mp \frac{x^2}{1 \pm x} \in x + \mathcal{A} \subseteq x + T \\ \Rightarrow & \frac{x}{1+x} \notin T \\ \Rightarrow & \begin{cases} \frac{1-x}{1+x} = \frac{1}{1+x} - \frac{x}{1+x} \notin T \\ \frac{1+x}{1-x} = \frac{1}{1-x} + \frac{x}{1-x} \notin T \end{cases} \quad \text{contradicting } o \end{array}$$

Having finitely axiomatized the group and the residue case, the weak case, again, must also be elementary. □

Corollary 2.7 *If $\mathcal{O}_T$ is definable, all convex subgroups of the value group Γ_T of $\mathcal{O}_T$ definable in terms of $v(T)$ (where v denotes the valuation corresponding to $\mathcal{O}_T$) give rise to a definable coarsening of $\mathcal{O}_T$.*

In particular, if T is multiplicative, the Jacob-ring $\mathcal{O}_F(T)$ (cf. remark 1.7) is definable both in the group case and in the residue case.

Proof: If a convex subgroup Δ of Γ_T is definable in terms of $v(T)$, and if $\mathcal{O}_T$ is definable, then the coarsening of $\mathcal{O}_T$ with value group Γ_T/Δ is again definable: it is the localization $S^{-1}\mathcal{O}_T$ with $S = v^{-1}(\Delta)$.

If T is multiplicative, then $\mathcal{O}_F(T) = \mathcal{O}_T$, so $\mathcal{O}_F(T)$ is definable by the theorem. In the residue case, either T does not induce an ordering on the residue field of $\mathcal{O}_T$: then, again by the theorem, $\mathcal{O}_T$ is definable and the coarsening $\mathcal{O}_F(T)$ is obtained by passing to the factor group Γ_T/Δ_T, where Δ_T is the maximal convex subgroup of Γ_T contained in $v(T)$; for Δ_T is definable in terms of $v(T)$:

$$\Delta_T = \{\gamma \in \Gamma_T \mid \forall \delta \in \Gamma_T : (|\delta| \leq |\gamma| \rightarrow \delta \in v(T)\}.$$

If T induces an ordering on the residue field of $\mathcal{O}_T$, then, as described in the proof of the previous corollary, $\mathcal{O}_F(T) = \mathcal{O}_{T \cup -T}$ which is definable in terms of $T \cup -T$, and so also in terms of T. □

Remark 2.8 *In [J1], for a valuation fan T, $\mathcal{O}_F(T)$ was explicitly defined in first-order terms, and, in [AEJ], generalizing to the situation, where T is any*

multiplicative subgroup of $F^\times$, $\mathcal{O}_F(T)$ was described constructively in terms of T: With the notation

$$B_F(T) := \{a \in F \mid T + aT \not\subseteq T \cup aT \text{ or } T - aT \not\subseteq T \cup -aT\},$$

*the set of T-***basic** *elements of F, which generate the multiplicative subgroup $\langle B_F(T)\rangle$ of $F^\times$, the construction is as follows:*

$$\begin{aligned}&\mathcal{O}_F(T) = \mathcal{O}_F^-(T) \cup \mathcal{O}_F^+(T), \text{ where}\\ &\mathcal{O}_F^-(T) := \{x \in F \mid x \notin \langle B_F(T)\rangle \text{ and } 1 + x \in T\}\\ &\mathcal{O}_F^+(T) := \{x \in F^\times \mid x \in \langle B_F(T)\rangle \text{ and } x \cdot \mathcal{O}_F^-(T) \subseteq \mathcal{O}_F^-(T)\},\end{aligned}$$

provided T is not exceptional: T is called **exceptional**, *if $B_F(T) = \pm T$ and either $-1 \in T$ or T is additively closed. In this case, in the construction of $\mathcal{O}_F(T)$, the group $\langle B_F(T)\rangle$ may have to be replaced by a subgroup $H \leq F^\times$ with $B_F(T) \subseteq H$ and $[H : \langle B_F(T)\rangle] \leq 2$. (Cf. [AEJ], Def.2.2., Obs.2.3.(3) and Thm.3.9.)*

Having this nice construction of $\mathcal{O}_F(T)$ for arbitrary multiplicative subgroups T, it is, however, not clear that this construction leads to an *elementary* definition of $\mathcal{O}_F(T)$ in terms of T, as the construction, as given, involves quantification over $\mathbb{N}$ by talking about 'the group generated by' $B_F(T)$. So our corollary about the *definability* of $\mathcal{O}_F(T)$ in the group and the residue case is not quite redundant. In fact, in the weak case, $\mathcal{O}_F(T)$ will, in general, *not* be first-order definable, even if $\mathcal{O}_T$ is definable:

Example 2.9 *Let (F, v) be a valued field with $\Gamma_v = \mathbb{Z}$, and let $T := 1 + \mathcal{M}_v^2$. Then, being in the weak discrete case, $\mathcal{O}_T = \mathcal{O}_v$ is definable in terms of T, and $\mathcal{O}_F(T) = F$ is trivial.*

Passing to an ω-saturated elementary extension $(F', T') \succeq (F, T)$, we see, as in example 2.1, that the valuation v' corresponding to $\mathcal{O}_{T'}$ admits a fully compatible non-trivial coarsening, the finest such being the valuation w with $\mathcal{M}_w = \bigcap_{n=1}^\infty \mathcal{M}_{v'}^n$. But $T' = 1 + \mathcal{M}_{v'}^2 \subseteq \mathcal{O}_{v'}^\times \subseteq \mathcal{O}_w^\times$, so $w(T') = \{0\}$ does not contain any non-trivial convex subgroup, and, thus, $\mathcal{O}_{F'}(T') = \mathcal{O}_w \neq F'$. As $\mathcal{O}_F(T)$ is trivial and $\mathcal{O}_{F'}(T')$ is non-trivial, but $(F, T) \equiv (F', T')$, we cannot have definability here.

Explicit Formulas

The explicit fomulas we have found for valuations definable from subgroups

will not come as a surprise because they essentially describe the topological properties of such subgroups. So even when, perhaps, they lack elegance or brevity, these formulas are well motivated, natural in a sense. The idea is to define, in terms of a subgroup T a zero-neighbourhood U which is approximately as large as $\mathcal{O}_T$, so that the elements $x \in F$ for which $x \cdot U \subset_{\neq} U$ are the elements of $\mathcal{M}_T$. Such neighbourhoods will be of the form

$$U_{a,b} := \begin{cases} \{\frac{ax}{x-b} \mid x \in T \setminus \{b\}\} & \text{if } T \text{ is additive} \\ a(1-T) \cap b(1-T) & \text{if } T \text{ is multiplicative} \end{cases}$$

for some $a, b \in F^\times$. To find a good choice for the elements a, b, we have to see how these neighbourhoods $U_{a,b}$ are bounded above and below by some basic $\mathcal{O}_T$-open sets, namely fractional $\mathcal{O}_T$-ideals, or, if one prefers, preimages of upper segments of $\Gamma_T \cup \{\infty\}$ w.r.t. v_T. (Those fractional valuation ideals are, of course, linearly ordered by inclusion.) As usual, we denote for some fractional $\mathcal{O}_T$-ideal $\mathcal{A}$ the inverse fractional ideal by $\mathcal{A}^{-1} := \{x \in F \mid x \cdot \mathcal{A} \subseteq \mathcal{O}_T\}$ (note though, that this operation is not injective, unless $\mathcal{O}_T$ corresponds to a discrete valuation).

Lemma 2.10 *Let (F, T) be a field with additive resp. multiplicative subgroup, let $\mathcal{A}_T$ be the largest (in the additive group case eventually) fractional $\mathcal{O}_T$-ideal contained in T resp. $-1+T$, and pick $a, b \in F^\times$.*
(a) If T is additive and $b \notin T$, then

$$\frac{a}{b}\mathcal{A}_T \subseteq U_{a,b} \subseteq ab\mathcal{A}_T^{-1}\mathcal{M}_T$$

and $\frac{a}{b}\mathcal{A}_T$ is the largest fractional $\mathcal{O}_T$-ideal contained in $U_{a,b}$.
(b) If T is multiplicative, $aT \neq bT$, and, say, $v_T(a) \leq v_T(b)$, then

$$b\mathcal{A}_T \subseteq U_{a,b} \subseteq a\mathcal{A}_T^{-1}\mathcal{M}_T$$

and $b\mathcal{A}_T$ is the largest fractional $\mathcal{O}_T$-ideal contained in $U_{a,b}$.

Proof: (a) If $y \in \mathcal{A}_T$ and $b \notin \mathcal{A}_T$, $v_T(y) > v_T(b)$. So $v_T(\frac{by}{y-b}) = v_T(y)$, i.e. $x := \frac{by}{y-b} \in \mathcal{A}_T \subseteq T$. Hence $\frac{a}{b}y = \frac{ax}{x-b} \in U_{a,b}$.

On the other hand, $U_{a,b}$ does not contain any fractional $\mathcal{O}_T$-ideal $\mathcal{I}$ with $\frac{a}{b}\mathcal{A}_T \subset_{\neq} \mathcal{I}$: for either $b\mathcal{M}_T = \mathcal{A}_T$, but then $\frac{a}{b}b\mathcal{O}_T \subseteq \mathcal{I} \subseteq U_{a,b}$, so $a \in U_{a,b}$ which is impossible; or $\mathcal{A}_T \subset_{\neq} b\mathcal{M}_T$, so one finds $x \in b\mathcal{M}_T \setminus T$ such that $\frac{a}{b}x \in \mathcal{I}$, and thus $\frac{ax}{b-x} \in \mathcal{I} \setminus U_{a,b}$.

To see that $U_{a,b} \subseteq ab\mathcal{A}_T^{-1}\mathcal{M}_T$, first observe that $\mathcal{O}_T \subseteq b\mathcal{A}_T^{-1}\mathcal{M}_T$, as $v_T(b) < v_T(y)$ for all $y \in \mathcal{A}_T$. So for $x \in T$ with $v_T(x) > v_T(b)$ resp. $v_T(x) < v_T(b)$ we have $v_T(\frac{ax}{x-b}) = v_T(\frac{ax}{b}) > v_T(a)$ resp. $v_T(\frac{ax}{x-b}) = v_T(\frac{ax}{x}) = v_T(a)$, i.e. $\frac{ax}{x-b} \in y\mathcal{O}_T \subseteq ab\mathcal{A}_T^{-1}\mathcal{M}_T$. If $x \in T$ with $v_T(x) = v_T(b)$, we still have that $v_T(x-b) < v_T(y)$ for all $y \in \mathcal{A}_T$, as $x - b \notin T$, so $v_T(\frac{ax}{x-b}) > v_T(\frac{ab}{y})$ for all $y \in \mathcal{A}_T$, i.e. $\frac{ax}{x-b} \in ab\mathcal{A}_T^{-1}\mathcal{M}_T$.

(b) If $y \in \mathcal{A}_T$, then $b - by \in b(1 + \mathcal{A}_T) \subseteq bT$ and $a - by = a(1 - ba^{-1}y) \in a(1 + \mathcal{A}_T) \subseteq aT$, as $v_T(a) \leq v_T(b)$, so $by \in U_{a,b}$. On the other hand, any fractional $\mathcal{O}_T$-ideal $\mathcal{I}$ with $b\mathcal{A}_T \subsetneq \mathcal{I}$ contains some z with $b - z \notin bT$, so $z \notin U_{a,b}$. If, finally, $z \notin a\mathcal{A}_T^{-1}\mathcal{M}_T$, i.e. $az^{-1} \in \mathcal{A}_T$, then $a - z = -z(1 - az^{-1}) \in -zT$ and $b - z = -z(1 - bz^{-1}) \in -zT$, so either $-zT \neq aT$ or $-zT \neq bT$, as $aT \neq bT$, and hence $z \notin U_{a,b}$. □

If it happens that T is itself a valuation ring or some (fractional) valuation ideal in the additive case, or the group of units or of 1-units of some valuation in the multiplicative case, it is not difficult to find a formula for $\mathcal{O}_T$. In these cases (and in a few other exceptional cases) one also finds $a, b \in F$ with $U_{a,b} = \mathcal{M}_T$ or, in the additive group case also $U_{a,b} = \mathcal{O}_T$. Whenever this is possible, and, moreover, T is fully compatible with v_T, we call T **valuational**.

Theorem 2.11 *Let (F, T) be a field with additive resp. multiplicative subgroup, and let $\mathcal{P}_T \subseteq F$ be defined as follows:*

$$x \in \mathcal{P}_T \Leftrightarrow \exists a, b \in F^\times : (b \notin T \text{ resp. } aT \neq bT) \wedge o_{a,b}(x) \wedge v_{a,b}(x) \wedge \chi_{a,b}(x),$$

where $o_{a,b}(x)$, $v_{a,b}(x)$ and $\chi_{a,b}(x)$ abbreviate the formulas:

$$\begin{aligned} o_{a,b}(x): &\quad xU_{a,b} \subseteq T \text{ resp. } 1 + xU_{a,b} \subseteq T \\ v_{a,b}(x): &\quad x^2(U_{a,b} \dot{-} U_{a,b}) \subseteq U_{a,b} \\ \chi_{a,b}(x): &\quad \forall y, z : [y \cdot z \in x^4 U_{a,b} \rightarrow (y \in U_{a,b} \vee z \in U_{a,b})] \end{aligned}$$

If T is valuational, $\mathcal{O}_T = \mathcal{P}_T$.
If T is not valuational, but strongly compatible with $\mathcal{O}_T$ and for the additive group case $\mathcal{A}_T = \mathcal{O}_T$, then $\mathcal{M}_T = \mathcal{P}_T$.
In all other cases $\mathcal{M}_T = \{x \in F \mid \exists n \in \mathbb{N} : x^n \in \mathcal{P}_T\}$, where for discrete v_T a fixed exponent n works uniformly.

Proof: As above, we denote by $\mathcal{A}_T$ the largest fractional $\mathcal{O}_T$-ideal contained in T resp. $T - 1$. Then the theorem follows from the two following claims:

Claim 1: $\mathcal{M}_T \cap \mathcal{A}_T \subseteq \mathcal{P}_T$, and, if T is valuational, $\mathcal{O}_T \subseteq \mathcal{P}_T$.
Claim 2: $\mathcal{P}_T \subseteq \mathcal{O}_T$ and, if T is *not* valuational, $\mathcal{P}_T \subseteq \mathcal{M}_T$.

Proof of claim 1: Pick $x \in \mathcal{M}_T \cap \mathcal{A}_T$. We have to find $a, b \in F^\times$ with $b \notin T$ resp. $aT \neq bT$ such that

$$\begin{array}{lll} o': & xab\mathcal{A}_T^{-1}.\mathcal{M}_T \subseteq \mathcal{A}_T & \text{resp. } xa\mathcal{A}_T^{-1}.\mathcal{M}_T \subseteq \mathcal{A}_T \\ v': & x^2ab\mathcal{A}_T^{-1}.\mathcal{M}_T \subseteq \frac{a}{b}\mathcal{A}_T \subseteq \mathcal{O}_T & \text{resp. } x^2a\mathcal{A}_T^{-1}.\mathcal{M}_T \subseteq b\mathcal{A}_T \subseteq \mathcal{O}_T \\ \lambda': & x^4ab\mathcal{A}_T^{-3}.\mathcal{M}_T \subseteq \frac{a^2}{b^2}\mathcal{A}_T^2 & \text{resp. } x^4a\mathcal{A}_T^{-1}.\mathcal{M}_T \subseteq b^2\mathcal{A}_T^2 \end{array}.$$

By the previous lemma, such a, b then guarantee the conditions $o_{a,b}(x)$, $v_{a,b}(x)$ and $\lambda_{a,b}(x)$, so then $x \in \mathcal{P}_T$.

We first rewrite those conditions:

$$\begin{array}{lll} o' & \Leftrightarrow & ab \in x^{-1}\mathcal{A}_T^2.\mathcal{M}_T^{-1} \quad \text{resp. } a \in x^{-1}\mathcal{A}_T^2.\mathcal{M}_T^{-1} \\ v' & \Leftrightarrow & b \in x^{-1}\mathcal{A}_T \wedge a \in b\mathcal{A}_T^{-1} \quad \text{resp. } a \in x^{-2}b\mathcal{A}_T^2.\mathcal{M}_T^{-1} \\ \lambda' & \Leftrightarrow & \frac{b^3}{a} \in x^{-4}\mathcal{A}_T^3.\mathcal{M}_T^{-1} \quad \text{resp. } \frac{a}{b^2} \in x^{-4}\mathcal{A}_T^3.\mathcal{M}_T^{-1} \end{array}$$

One now easily verifies that choosing $b \in x^{-1}\mathcal{A}_T \setminus T$ and $a \in x\mathcal{O}_T^\times$ resp. $a \in \mathcal{A}_T^3 \setminus bT$ does the job (note that the choice for a in the multiplicative case is possible since $\mathcal{A}_T^3 \setminus \{0\}$ multiplicatively generates all of $F^\times$).

If T is valuational, we find a, b such that $U_{a,b} = \mathcal{M}_T$ or in the additive group case $U_{a,b} = \mathcal{O}_T$ and we can even find such a, b with $b \notin T$ resp. $aT \neq bT$. But then any such $U_{a,b}$ is good for any $x \in \mathcal{O}_T^\times$, so in this case $\mathcal{O}_T \subseteq \mathcal{P}_T$.

Proof of claim 2: Pick $x \in \mathcal{P}_T \setminus \{0\}$ and let $a, b \in F^\times$ witness the corresponding formulas. We may assume that $U_{a,b} \neq \{0\}$, as otherwise $\mathcal{O}_T = \mathcal{P}_T = F$, and we are done. We consider the set

$$\mathcal{M} := \bigcap_{n=1}^{\infty} x^n U_{a,b}.$$

Our formulas are so designed that $\mathcal{M}$ obviously defines the maximal ideal, or, if T is additive, possibly the valuation ring, of some valuation compatible with T. Passing to a saturated elementary extension $(F', T') \succ (F, T)$, we see that for the corresponding set one has $\mathcal{M}' \neq \{0\}$, so T' is weakly compatible with some non-trivial valuation, which — being an elementary property by corollary 2.4 — must also be true of T. Hence $\mathcal{A}_T \neq \{0\}$.

We now assume that $x \notin \mathcal{M}_T$. Then

$$\frac{a}{b}\mathcal{A}_T \subseteq x^2\frac{a}{b}\mathcal{A}_T \subseteq x^2 U_{a,b} \subseteq U_{a,b}$$

resp. with, say, $v_T(a) \leq v_T(b)$

$$b\mathcal{A}_T \subseteq x^2 b\mathcal{A}_T \subseteq x^2 U_{a,b} \subseteq U_{a,b}.$$

But $\frac{a}{b}\mathcal{A}_T$ resp. $b\mathcal{A}_T$ is according to lemma 2.10 the *largest* $\mathcal{O}_T$-ideal contained in $U_{a,b}$, so x must be a unit: $x \in \mathcal{O}_T^\times$.

We deduce that $\frac{a}{b}\mathcal{A}_T \subseteq \mathcal{M} \subseteq U_{a,b}$ resp. $b\mathcal{A}_T \subseteq \mathcal{M} \subseteq U_{a,b}$, and, therefore, we cannot be in the weak case: $\mathcal{M}$ would then be an $\mathcal{O}_T$-ideal, hence (again by 2.10) of the form $\mathcal{M} = \frac{a}{b}\mathcal{A}_T$ resp. $\mathcal{M} = b\mathcal{A}_T$, but being non-maximal (weak case!) and prime this is impossible. In fact, the same argument shows that if $\mathcal{M}$ is a fractional $\mathcal{O}_T$-ideal it must equal $\mathcal{M}_T$ or, in the additive group case, possibly $\mathcal{O}_T$. But then we are only in cases where we know $\mathcal{O}_T$ to be definable (in the additive group case $\mathcal{M} = \frac{a}{b}\mathcal{A}_T$ implies $\mathcal{A}_T = \mathcal{O}_T$ or $\mathcal{O}_T$ corresponds to a discrete valuation), so we may assume to be in a saturated model, where, however, as T is not valuational, we find in each $x^n U_{a,b}$ (and hence, by saturation, in $\mathcal{M}$) elements outside $\mathcal{M}_T$ or $\mathcal{O}_T$.

So $\mathcal{M}$ is not any fractional $\mathcal{O}_T$-ideal, so it must belong to a fully compatible valuation strictly finer than v_T. In particular, this brings us into the group case. Yet $U_{a,b} \subseteq \mathcal{O}_T$, as otherwise for some $y \in U_{a,b} \setminus \mathcal{O}_T$ one would have

$$x^2 \cdot y \cdot \frac{a}{b}\mathcal{A}_T = y\frac{a}{b}\mathcal{A}_T \subseteq U_{a,b} \text{ resp. } yb\mathcal{A}_T \subseteq U_{a,b}.$$

So $\frac{a}{b}\mathcal{A}_T = \mathcal{M}_T$ resp. $b\mathcal{A}_T = b\mathcal{M}_T = \mathcal{M}_T$, i.e. in the additive case v_T must be discrete with $v_T(a) = v_T(b) - \min v_T(\mathcal{A}_T) + 1$, and in the multiplicative case $b \in \mathcal{O}_T^\times$ and so $a \notin \mathcal{O}_T$. But then it is not difficult to find elements in $U_{a,b}$ which do not belong to $\mathcal{O}_T$. □

3 p-Henselian Valuations

A valued field (F, v) is called **p-henselian** if v extends uniquely to the maximal Galois-p-extension $F(p)$ of F. Equivalently, Hensel's Lemma or Newton's Lemma holds for polynomials splitting over $F(p)$ (cf. [Wd] or [K2]). In particular, if F contains a primitive p-th root ζ_p of unity, this implies

that $1 + \mathcal{M}_v \subseteq (F^\times)^p$, provided $char\, F_v \neq p$, or $1 + p^2\mathcal{M}_v \subseteq (F^\times)^p$, if $char\, F_v = p \neq char\, F$. If $char\, F = p$, it implies that $\mathcal{M}_v$ be contained in the (additive) Artin-Schreier-group $F^{(p)} := \{x^p - x \mid x \in F\}$. Applying the results of the previous section to the group $T = (F^\times)^p$ resp. $T = F^{(p)}$, we can therefore prove the following

Theorem 3.1 *Let F be a field which is not p-closed (i.e. $F \neq F(p)$) with $char\, F = p$ or $\zeta_p \in F$. If F admits a non-trivial p-henselian valuation v, then it admits a definable valuation inducing the same topology as v, unless $p = 2$ and F is euclidean.*

Proof: Let us begin with the case $char\, F = p$. Then Lemma 1.2 tells us that for $T = F^{(p)}$, $\mathcal{O}_T$ is fully compatible with T. So we are either in the group case or in the residue case. Following theorem 2.5, we know that in the latter case, $\mathcal{O}_T$ *is* definable, whereas in the first case this is so, if $\forall x \in \mathcal{M}_T : x^{-1}\mathcal{O}_T \not\subseteq T$.

But luckily this is the case: For otherwise the largest fractional $\mathcal{O}_T$-ideal $\mathcal{A}_T$ contained in T properly contains $\mathcal{O}_T$ (but no larger valuation ring). In particular, the (non-trivial, archimedean) convex subgroup of Γ_T generated by $v_T(\mathcal{A}_T \setminus \mathcal{O}_T)$ is p-divisible, so for any $\alpha \in \mathbf{R}$ with $\alpha > 1$ the fractional $\mathcal{O}_T$-ideal

$$\mathcal{A}_T^\alpha := \{x \in F \mid v_T(x) \geq \alpha \cdot v_T(y) \text{ for some } y \in \mathcal{A}_T\}$$

strictly contains $\mathcal{A}_T$. To get a contradiction, we now choose $\alpha \in]1, 2 - \frac{1}{p}]$ and show that $\mathcal{A}_T^\alpha \subseteq T$. Pick $x \in \mathcal{A}_T^\alpha \setminus \mathcal{A}_T$, say $v_T(x) \geq \alpha v_T(y)$ for some $y \in \mathcal{A}_T$. Then, as $1 < \alpha < 2$, $0 > v_T(xy^{-1}) > v_T(y)$, so $xy^{-1} \in \mathcal{A}_T \setminus \mathcal{O}_T$, hence $xy^{-1} \in a^p\mathcal{O}_T^\times$ and $xa^{-p} = b^p - b$ for some $a, b \in F \setminus \mathcal{O}_T$. Now $x = a^pb^p - a^pb$, but

$$\begin{aligned} v_T(a^pb) &= v_T(xy^{-1}) + v_T(b) \\ &= v_T(x) - v_T(y) + \tfrac{1}{p}v_T(y) \\ &\geq (\alpha - 1 + \tfrac{1}{p})v_T(y) \\ &\geq v_T(y), \end{aligned}$$

so $v_T(ab) > v_T(a^pb) \geq v_T(y)$, i.e. $ab, a^pb \in T$. Thus $x = (ab)^p - (ab) + ab - a^pb \in T$, which finishes the case $char\, F = p$.

If $char\, F \neq p$ and $T := (F^\times)^p$ is fully compatible with v_T, then, again by theorem 2.5, $\mathcal{O}_T$ is definable, unless we are in the residue case and $\bar{T}$ is an ordering; but this can only happen when $p = 2$, and in this case we

have assumed F to be non-euclidean, so $T \cup -T$ is still a proper subgroup of $F^\times$ for which then $\mathcal{O}_{T\cup -T}$ becomes definable, being in the group case again. So what remains is the weak case in which we better not try and define $\mathcal{O}_T$, as this is, once more by theorem 2.5, impossible, if $\mathcal{O}_T$ doesn't happen to be discrete. Rather, we have to observe that in this case, by lemma 1.2, the residue characteristic of $\mathcal{O}_T$ must be p. So we may pass to the coarsest coarsening w of v_T which still has residual characteristic p. For this coarsening, $1 + p^2.\mathcal{M}_w \subseteq (F^\times)^p$, and thus, arguing as in 1.4(c) and 1.5 of [K2], w is p-henselian. We now consider the Artin-Schreier group $F_w^{(p)}$ on the residue field of w and claim, that the refinement w' of w by the valuation corresponding to $\mathcal{O}_{F_w^{(p)}}$ on F_w is definable, even if w is not. For w' is elementarily determined by the following properties:

- $char\ F_{w'} = p$ and $1 + p^2.\mathcal{M}_{w'} \subseteq (F^\times)^p$:
  this makes sure, w' is a refinement of w
- $.\mathcal{M}_{w'} \subseteq \{x^p - x \mid x \in F\}$:
  this guarantees that w' is p-henselian (cf. 1.5 of [K2])
- if $F_{w'}^{(p)} \neq F_{w'}$, then $F_{w'}^{(p)}$ induces no V-topology on $F_{w'}$:
  then w' has no p-henselian refinement
- if $F_{w'}^{(p)} = F_{w'}$, then $\forall x \in .\mathcal{M}_{w'} : x^{-1}\mathcal{O}_{w'} \not\subseteq \{x^p - x \mid x \in F\}$:
  then w' is the coarsest valuation with p-closed residue field; the condition *does* hold according to the $char\ F = P$-case above. □

4 t-Henselian Fields

The adequate notion to state and prove our main theorem for is the generalisation of henselian valued fields introduced by Prestel and Ziegler in [PZ] under the name of 't-henselianity': they call a V-topological field (F, τ) (where τ denotes the filter of neighbrouhoods of 0) **t-henselian** if it is locally equivalent to some henselian valued field, or, equivalently, if for each $n \in \mathbf{N}$ one finds some $U_n \in \tau$ such that

$$\forall u_0, \ldots, u_{n-2} \in U_n \exists x \in F : x^n + x^{n-1} + u_{n-2}x^{n-2} + \ldots + u_0 = 0.$$

This obviously generalises henselianity, because for a henselian valuation v this condition is just one of the versions of Hensel's lemma if one takes

$U_n = \mathcal{M}_v$ for all n. In this context the well-known theorem of F.K.Schmidt on the dependence of henselian valuations has its natural setting: Any field F which is not separably closed admits at most one t-henselian topology. Indeed, this topology then proves to be definable; for some non-linear, irreducible, separable $f \in F[X]$ the sets $x \cdot f(F)^{-1} \cup \{0\}$ $(x \in F^\times)$ form a base of neighbourhoods of 0 ([PZ], p.337). We shall go beyond this result in proving the existence of some rather well shaped definable neighbourhood of 0, namely some definable valuation ring.

Due to the uniqueness of t-henselian topologies for non-separably-closed fields it makes sense to speak of t-henselian fields without mentioning th topology. It then follows from the definability of the topology that a field F which is not separably closed is t-henselian iff F is (as a field) elementarily equivalent to some henselian valued field. So, for example, any real closed field is t-henselian, but as was already indicated in the introduction, there are t-henselian fields which are neither real closed nor separably closed and which do not admit any henselian valuation.

Our main theorem now clearly follows from the following

Theorem 4.1 *Any t-henselian field which is neither real closed nor separably closed admits a definable valuation inducing the t-henselian topology.*

Proof: If F satisfies the hypothesis of the theorem then for some prime p dividing $\sharp G_F$, where G_F denotes the absolute Galois group of F, there is a finite separable extension L/F with $L \neq L(p)$, $\zeta_p \in L$ or $char\, L = p$, and, if $p = 2$, L is not euclidean.

Then, because of the elementary equivalence of t-henselian fields with henselian fields, L is also t-henselian, as, of course, henselianity extends to algebraic extensions, and the t-henselian topology on L induces the t-henselian topology on F by virtue of the definability of the topology and the corresponding fact for algebraic extensions of valued fields.

Now by the very choice of L and theorem 3.1, an elementarily equivalent henselian (and hence p-henselian) field L' admits a definable valuation inducing the (t-)henselian topology on L'. Thus the same is true for L. But definable in L means definable over F since we may consider the elements of L as n-tuples over F for $n = [L : F]$ (and, clearly, the operations on L are also F-definable). The restriction of the non-trivial p-henselian F-definable valuation on L to F now gives us what we want. □

One should point out that for the definition of the valuation described in the proof one may need parameters, namely the coefficients of the irreducible polynomial of some primitive element for the extension L/F. If, however, $F \neq F^p$ form some prime $p \neq char\, F$, one may choose $L = F(\zeta_p)$, and then the valuation can be defined without parameters, because we needed no parameters for our definable p-henselian valuation of theorem 3.1.

References

[AEJ] J.Arason, R.Elman, B.Jacob: *Rigid elements, valuations, and realization of Witt rings*, J.Algebra **110**, 449-467, 1987.

[BBG] E.Becker, R.Berr, D.Gondard-Cozette: *Henselian fields with real-closed residue field*, in: Prèpublications de l'Equipe de Logique No. 49, Paris, 1994.

[DF] F.Delon, R.Farrè: *Some model theory for almost real closed fields*, in: Prèpublications de l'Equipe de Logique No. 49, Paris, 1994.

[E] O.Endler: *Valuation Theory*, Springer, 1972.

[EE] O.Endler and J.Engler: *Fields with Henselian Valuation Rings*, Math.Z. **152**, 149-163, 1976.

[J1] B.Jacob: *The model theory of pythagorean fields*, Ph.D.Thesis, Princeton, 1979.

[J2] B.Jacob: *The model theory of generalized real-closed fields*, J.reine u. angew.Math. **323**, 213-220, 1981.

[K1] J.Koenigsmann: *Half-ordered fields*, Ph.D.Thesis, Konstanz, 1993.

[K2] J.Koenigsmann: *p-henselian fields*, to appear in Proc. Escola d'Algebra Campinas, 1995.

[PZ] A.Prestel and M.Ziegler: *Model theoretic methods in the theory of topological fields*, J.reine u. angew.Math. **299/300**, 318-341, 1978.

[R] P.Ribenboim: *Thèorie des Valuations*, Montreal, 1968.

[Wd] A.Wadsworth: *p-henselian fields: K-thoery, Galois cohomology, and graded Witt rings*, Pac.J.Math., vol.105, no.2, 473-496, 1983.

[W] R.Ware: *Valuation Rings and Rigid Elements in Fields*, Can.J.Math., vol.33, no.6, 1338-1355, 1981.

Fakultät für Mathematik
Universität Konstanz
Postfach 5560
D-78464 Konstanz
GERMANY

Separably Closed Fields with Higher Derivations I

Margit Messmer and Carol Wood

Abstract

We define a complete theory SHF_e of separably closed fields of finite invariant e (=degree of imperfection) which carry an infinite stack of Hasse-derivations. This work will appear in the Journal of Symbolic Logic. Below we indicate the main definitions and results without proof.

This paper is motivated by the following two problems:
(1) Find a theory of differential fields of characteristic $p \neq 0$ which eliminates imaginaries.
(2) Find a 'natural' language for the theory of separably closed fields of characteristic $p \neq 0$ which eliminates imaginaries without naming a p-basis.

We work in the first-order language $\mathcal{L} = \{+, -, \cdot, ^{-1}, 0, 1\} \cup \{D_{p^i} : i \in \omega\}$, where the D_{p^i} are unary function symbols. $\overbrace{D_{p^i}(D_{p^i}(\cdots(D_{p^i}}^{c \text{ times}}(x))))$ will be abbreviated by $D_{p^i}^{(c)}(x)$. Furthermore, for any $\nu \in \omega$, D_ν stands for

$$\frac{(p!)^{c_1}(p^2!)^{c_2}\cdots(p^n!)^{c_n}}{\nu!} D_1^{(c_0)}(D_p^{(c_1)}(D_{p^2}^{(c_2)}(\cdots(D_{p^n}^{(c_n)})\cdots))),$$

where $\nu = c_0 + c_1 p + \cdots c_n p^n$ $(0 \leq c_j \leq p-1)$, the p-adic expansion of ν. Note that the coefficient $\frac{(p!)^{c_1}(p^2!)^{c_2}\cdots(p^n!)^{c_n}}{\nu!}$ is not divisible by p. D_0 stands for the identity function.

For $e \geq 1$, let $\omega^{<\omega *}$ denote the set of finite tuples $\langle c_0, \ldots, c_n \rangle$ with $c_i \in \omega$ and $c_n \neq 0$. For $\bar{c} \in \omega^{<\omega *}$ we will write $D^{(\bar{c})} = D^{(\langle c_0, c_1, \ldots c_n \rangle)}$ for $D_1^{(c_0)}(D_p^{(c_1)}(D_{p^2}^{(c_2)}(\cdots(D_{p^n}^{(c_n)})\cdots)))$, where $D^{(\emptyset)} = D_0 = Id$.

Definition 1 *The field $(F, D_{p^i}; i \in \omega)$ is called a* ***Hasse field*** *if it satisfies the following axioms:*

(H1) For all $i \in \omega$: $\forall x \forall y D_{p^i}(x + y) = D_{p^i}(x) + D_{p^i}(y)$.

(H2) For all $i \in \omega$: $\forall x \forall y D_{p^i}(x \cdot y) = \sum_{\substack{\nu+\mu=p^i \\ \nu,\mu \geq 0}} D_\nu(x) \cdot D_\mu(y)$.

(H3) For all $i, j \in \omega$: $\forall x D_{p^i}(D_{p^j}(x)) = D_{p^j}(D_{p^i}(x))$.

Note: Let $(F, D_{p^i}; i \in \omega)$ be a Hasse field. Then:

(A) D_1 is an (ordinary) derivation on F; so in particular F is a differential field.

(B) $D_{p^i}(x^{p^{i+1}}) = 0$ for all $x \in F$.

(C) For $i, j \geq 1$, $D_{p^i}(x^{p^j}) = (D_{p^{i-1}}(x^{p^{j-1}}))^p$ for all $x \in F$. This shows that D_{p^i} is an (ordinary) derivation on the subfield F^{p^i} of p^ith powers.

(D) For all $\nu \geq 1$, D_ν defined as above, satisfies a product rule as in (H2).

Definition 2 *Let $e \geq 1$.*

(a) HF_e is the theory of Hasse fields of invariant $\leq e$ satisfying the following axioms in the language $\mathcal{L}$:

(F_p) *Axioms for fields of characteristic p.*

(HF) *Axioms (H1)–(H3) for Hasse fields.*

(H4) *For all $i \in \omega$: $\forall x D_{p^i}^{(p^e)}(x) = 0$.*

(b) SHF_e denotes the ***theory of separably closed, strict Hasse fields*** *F of invariant e which in addition to the axioms in (a) satisfy the following axioms:*

(H5) $\exists x D_1^{(p^e-1)}(x) \neq 0$.

(H6) *Strictness:* $\forall x(D_1(x) = 0 \rightarrow \exists y\ x = y^p)$.

(H7) *F is separably closed.*

Main Theorem 3 *The theory SHF_e is complete and has quantifier elimination.*

Proposition 4 *Let F be a separably closed field of finite invariant e. Then F can be expanded to a model of SHF_e.*

Proposition 5 *Let T be the theory of a stable field. Suppose that for every $n \geq 1$ there is a (possibly infinite) set of indeterminates X_i, $i \in J$, such that for each model F of T there is a one-to-one correspondence between complete n-types over F and certain ideals in the polynomial ring $F[X_i : i \in J]$, such that for every automorphism σ of F (as a T-structure), σ fixes the type (setwise) iff σ fixes the corresponding ideal (setwise). Then T eliminates imaginaries.*

Corollary 6 *The theory SHF_e of separably closed strict Hasse fields of invariant $e < \omega$ eliminates imaginaries.*

References

[1] Chang C., Keisler H. *Model Theory.* North-Holland, 1973.

[2] Delon F. *Ideaux et types sur les corps séparablement clos.* Supplément au Bulletin de la société Mathématique de France. Mémoire No.33. Tome 116 (1988).

[3] Eršov J. *Fields with a solvable theory.* Doklady Akadéemii Nauk SSSR, vol.174 (1967), pp.19–20. English translation, Soviet Mathematics, vol.8 (19670, pp.575–576.

[4] Evans E., Pillay A., Poizat B. *A group in a group* Algebra i Logika, No.3 (1990), pp.368–378.

[5] Hasse H. *Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik.* Journ. f. Math., vol.175 (1936), pp.50–54.

[6] Hrushovski E. *The Mordell-Lang conjecture for function fields.* Preprint.

[7] Jacobson N. *Lectures in Abstract Algebra III.* D.Van Nostrand Company, New York, 1964.

[8] Kolchin E. *Differential Algebra and Algebraic Groups.* Academic Press, 1973.

[9] Messmer M. *Groups and fields interpretable in separably closed fields.* Transactions of the AMS, to appear.

[10] Okugawa K. *Basic properties of differential fields of arbitrary characteristic and the Picard-Vessiot theory.* Journal of Mathematics of Kyoto University, vol.2, No.3 (1963), pp.294–322.

[11] Poizat B. *Cours de Théories des Modèles.* Nur alMantiq walMa'arifah, Villeurbanne, France, 1987.

[12] Poizat B. *Une théorie de Galois imaginaire.* The Journal of Symbolic Logic, vol.48 (1983), pp.1151–1171.

[13] Wood C. *The model theory of differential fields of characteristic $p \neq 0$.* Proceedings of the AMS, Vol.40 (1973), pp.577–584.

[14] Wood C. *Prime model extensions for differential fields of characteristic $p \neq 0$.* The Journal of Symbolic Logic, vol.39 (1974), pp.469–477.

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

[16] Wood C. *Notes on the stability of separably closed fields.* The Journal of Symbolic Logic, vol.44 (1979), pp.412–416.

Wesleyan University
Department of Mathematics
Middletown, CT 06459
(E.U.)

Prépublications de l'Equipe de Logique.

N° 1 **D. Lascar.**
Les beaux automorphismes, janvier 1990.

N° 2 **F. Delon, M. A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1988-89), janvier 1990.

N° 3 **J.-L. Krivine.**
Opérateurs de mise en mémoire et traduction de Gödel, janvier 1990.

N° 4 **M. Giraudet.**
Groupes à moitié ordonnés. Première partie : Présentation axiomatique des groupes de permutations monotones de chaînes, février 1990.

N° 5 **M. Giraudet** et **F. Lucas.**
Groupes à moitié ordonnés. Deuxième partie : Sous-groupes de groupes à moitié réticulés, février 1990.

N° 6 **C. Michaux.**
Ordered rings over which output sets are recursively enumerable sets, février 1990.

N° 7 **V. Danos.**
Lambda-calculus and its dynamic algebra 1 : basic results, février 1990.

N° 8 **L. Régnier**
A propos de l'équivalence opérationnelle, avril 1990.

N° 9 **Ch. Berline.**
Rétractions et interprétation interne du polymorphisme : Le problème de la rétraction universelle, mai 1990.

N° 10 **D. Gondard-Cozette.**
Axiomatisations simples des théories des corps de Rolle, mai 1990.

N° 11 **A. Fleury** et **C. Rétoré.**
The MIX rule : a proofnet syntax for multiplicatives, their units and (A⊗B)-0(A&B), septembre 1990.

N° 12 **P. Malacaria** et **L. Régnier.**
Lambda-calculus and its dynamic algebra 3 : Weak Nilpotency, septembre 1990.

N° 13 **D. Lascar.**
Les automorphismes d'un ensemble fortement minimal, octobre 1990.

N° 14 **D. Gluschankof** et **M. Tilli.**
On some extension theorems in functional analysis and the theory of boolean algebras, novembre 1990.

N° 15 **U. Gropp.**
There is no sharp transitivity on q^6 when q is a type of Morley rank 2, décembre 1990.

N° 16 **M.A. Dickmann.**
A combinatorial geometric structure on the space of orders of a field, décembre 1990.

N° 17 **F. Delon, M. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées 1989-90, décembre 1990.

N° 18 **J.-Y. Girard.**
Logic and exceptions : A few remarks, décembre 1990.

N° 19 **J.-Y. Girard.**
Quantifiers in linear logic II, janvier 1991.

N° 20 **T. Jech.**
Singular cardinal problem : Shelah's theorem on $2^{\aleph\omega}$, janvier 1991.

N° 21 **G. Amiot.**
Sémantique des phases de la Logique Linéaire du second ordre, février 1991.

N° 22 **T. Ehrhard, P. Malacaria.**
Stone duality for stable functions, février 1991.

N° 23 **Z. Chatzidakis, L. van den Dries, A. Macintyre.**
Definable sets over finite fields, mars 1991.

N° 24 **J.-Y. Girard.**
A new constructive logic : classical logic, mai 1991.

N° 25 **P. Rozière.**
Règles admissibles en calcul propositionnel intuitionniste, mai 1991.

N° 26 **J.-Y. Girard.**
On the unity of logic, juin 1991.

N° 27 **S. Kuhlmann.**
Quelques propriétés des espaces vectoriels valués en théorie des modèles, juin 1991.

N° 28 **U. Gropp.**
Action d'un groupe ω-stable sur un ensemble de rang de Morley 2, juin 1991.

N° 29 **A.A. Voronkov.**
On completeness of program synthesis systems, juin 1991.

N°30 **D. Gondard-Cozette.**
Sur les ordres de niveau 2^n et sur une extension du 17ème problème de Hilbert, octobre 1991.

N°31 **P. Michel.**
Busy Beaver Competition and Collatz-like Problems, janvier 1992.

N° 32 **F. Delon, M. A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1990-91), janvier 1992.

N° 33 **M. A. Dickmann, K. Keimel** (eds).
Workshop « PROCOPE » - Paris, 8-10 novembre 1990, janvier 1992.

N° 34 Comptes-Rendus au Colloque Franco-Exsoviétique de Théorie des Modèles C.I.R.M., 27 janvier-1er février 1992, mai 1992.

N° 35 **J.-B. Joinet.**
Une preuve combinatoire de forte normalisation (du fragment multiplicatif et exponentiel) des réseaux de preuves pour la logique linéaire (PN1), mai 1992.

N° 36 **E. Bouscaren** et **E. Hrushovski.**
Interpreting groups in stable one-based theories, mai 1992.

N° 37 **F. Miraglia** et **U. Solitro.**
Sheaves over right side indempotent Quantales, juin 1992.

N° 38 **Ch. Berline.**
Λ-calcul, systèmes de typages et modélisations, octobre 1992.

N° 39 **F. Métayer.**
Homology of Proof-nets, octobre 1992.

N° 40 **J.-L. Krivine.**
Classical logic, storage operators and second order lambda-calculus, décembre 1992.

N° 41 **V. Danos, J.-B. Joinet** et **H. Schellinx.**
On the Linear Decoration of Intuitionistic Derivations, janvier 1993.

N° 42 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques ordonnées (1991-92), février 1993.

N° 43 **Z.I. Abud** et **F. Miraglia.**
The Measurability of Pettis integrable Functions and Applications, février 1993.

N° 44 **X. Gouy** et **Y. Jiang.**
Universal retractions on DI-domains, juin 1993.

N° 45 **C. Zylberajch.**
A model-theoretic method to prove ease in lambda-calculus (Types, Models, Ease), juin 1993.

N° 46 **S. Malecki.**
A survey about polymorphic type systems from the typability point of view, juin 1993.

N° 47 **C. Rétoré.**
Graph theory from linear logic : AGREGATES, octobre 1993.

N° 48 **M.R. Darnel, M. Giraudet, S.J. McCleary.**
Uniqueness of the group operation on the lattice of order-automorphisms of the real line, décembre 1993.

N° 49 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1992-93), février 1994.

N° 50 **Ch. Berline** et **K. Grue.**
A simple semantic consistency proof for Map Theory based on ξ-denotational semantics, septembre 1994.

N° 51 **V. Danos, J.-B. Joinet** et **H. Schellinx.**
LKQ and LKT : Sequent calculi for second order logic based upon dual linear decompositions of classical implication, octobre 1994.

N° 52 **V. Danos, J.-B. Joinet** et **H. Schellinx.**
A new deconstructive logic : linear logic, octobre 1994.

N° 53 **L. Tortora de Falco.**
Strong normalisation property for heterostytle Lk^{tq} and Free Deduction, décembre 1994.

N° 54 **F. Delon, M.A. Dickmann, D. Gondard.**
Séminaire de Structures Algébriques Ordonnées (1993-94), février 1995.