PARIS 7 LOGIQUE

CNRS

N° 90

Séminaire de Structures Algébriques Ordonnées

2013 -- 2015

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

Mars 2015

Equipe de Logique Mathématique

Prépublications

Institut de Mathématiques de Jussieu - Paris Rive Gauche
Université Denis Diderot - Paris 7
Bâtiment Sophie Germain, 5 rue Thomas Mann - 75205 Paris Cedex 13
Tel. : (33 1) 57 27 91 71 - Fax : (33 1) 57 27 91 78

UNIVERSITES PARIS VI et VI
Projets Logique Mathématique et Théorie des Nombres
Institut de Mathématiques de Jussieu – Paris Rive Gauche (UMR 7586, CNRS)

SEMINAIRE DE STRUCTURES ALGEBRIQUES ORDONNEES

Responsables: F. Delon, M. Dickmann, D. Gondard

2013-2015

Liste des exposés

08/10/13 **Esther ELBAZ** (Université Paris 7-Paris Diderot)
Autour des anneaux de Grothendieck.

26/11/13 **Bruno POIZAT** (Université Lyon I)
Supergenerix.

07/10/14 **Laura PHILLIPS** (Univ. of Manchester, Grande-Bretagne)
Some structures interpretable in the ring of continuous semi-algebraic functions on the line.

10/02/15 **Francisco MIRAGLIA** (Universidade de São Paulo, Brésil)
Constructions on real semigroups.

17/02/15 et 03/03/15 **Max DICKMANN** (Equipe de Logique, IMJ-PRG, Paris 7)
Eventails dans la théorie des semigroupes réels.

10/03/15 **Gérard LELOUP** (Université du Mans)
Groupes cycliquement ordonnés pseudo-c-archimédiens et pseudo-cycliques.

23/06/15 **Anand PILLAY** (Notre Dame University, Indiana, USA)
Minimal flows, definably amenable groups, and o-minimality.

30/06/15 **Pawel GŁADKI** (Université de Silésie, Katowice, Pologne)
Witt equivalence of function fields over global and local fields.

UNIVERSITES PARIS VI et VI

Projets Logique Mathématique et Théorie des Nombres
Institut de Mathématiques de Jussieu – Paris Rive Gauche (UMR 7586, CNRS)

SEMINAIRE DE STRUCTURES ALGEBRIQUES ORDONNEES

Responsables: F. Delon, M. Dickmann, D. Gondard

2013-2015

Liste des contributions

Les volumes des contributions au Séminaire de Structures Algébriques Ordonnées rendent compte des activités principales du séminaire de l'année indiquée sur chaque volume. Les contributions sont présentées par les auteurs, et publiées avec l'agrément des éditeurs, sans qu'il soit mis en place une procédure de comité de lecture.

Ce séminaire est publié dans la série de prépublications de l'Equipe de Logique Mathématique, Institut de Mathématiques de Jussieu–Paris Rive Gauche (CNRS -- Universités Paris 6 et 7). Il s'agit donc d'une édition informelle, et les auteurs ont toute liberté de soumettre leurs articles à la revue de leur choix.

Cette publication a pour but de diffuser rapidement des résultats ou leur synthèse, et ainsi de faciliter la communication entre chercheurs.

The proceedings of the Séminaire de Structures Algébriques Ordonnées constitute a written report of the main activities of the seminar during the year of publication. Papers are presented by each author, and published with the agreement of the editors, but are not refereed.

This seminar is published in the preprint series of the Equipe de Logique Mathématique, Institut de Mathématiques de Jussieu–Paris Rive Gauche (CNRS -- Universités Paris 6 et 7). It has the character of an informal publication aimed at speeding up the circulation of information and, hence, facilitating communication among researchers in the field. The authors are free to submit to any journal the papers preprinted in these proceedings.

Autour des anneaux de Grothendieck

Esther Elbaz

February 2016

Nous allons présenter la notion d'anneaux de Grothendieck introduite en théorie des modèles par Jan Krajicek et Thomas Scanlon dans [1]. Ces anneaux de Grothendieck reflètent certaines propriétés combinatoires de la structure à laquelle ils sont rattachés. Après avoir donné les définitions élémentaires, nous donnerons deux exemples de telles propriétés combinatoires : l'onto-PHP ou principe des tiroirs surjectf, qui est équivalent à ce que l'anneau de Grothendieck ne soit pas trivial ; et le principe de comptage modulaire qui permet de s'assurer que cet anneau de Grothendieck admet $\mathbb{F}_p$ comme quotient. Nous donnerons plusieurs exemples d'anneaux de Grothendieck connus. Puis nous terminerons en démontrant que pour tout p, il existe une structure M dont l'anneau de Grothendieck est de caractéristique p.

Dans tout l'exposé "définissable" signifiera "définissable avec paramètres".

1 Anneaux de Grothendieck et onto-PHP

Soit M une structure. Son anneau de Grothendieck est construit à partir de ses sous-ensembles définissables en identifiant ceux qui sont en bijection définissable. Cet anneau dépend donc du langage utilisé. Ce qui suit détaille la construction de cet anneau.

1.0.1 Le premier quotient

Soit M une structure et soit $Def(M)$ l'ensemble des sous-ensembles définissables de M^n pour n variant dans $\mathbb{N}$.

Soit $\sim$ la relation d'équivalence définie sur $Def(M)$ par :

$A \sim B$ si et seulement si A est en bijection définissable avec B.

On note $\tilde{Def}(M)$ l'ensemble $Def(M)$ quotienté par $\sim$.

Si $A \in \tilde{Def}(M)$, on note $[A]$ la classe d'équivalence de A.

1.0.2 Les lois du futur anneau

On peut alors munir $\tilde{Def}(M)$ des opérations $+$ et $\times$ suivantes.

La loi $+$ correspond à l'union disjointe. Elle est définit par :

$[A] + [B] = [A' \cup B']$ où $[A] = [A'], [B] = [B']$ et $A' \cap B' = \emptyset$.

L'élément neutre de $+$ correspond à la classe d'équivalence de l'ensemble vide.

La loi $\times$ correspond au produit cartésien. Elle est définit par : $[A] \times [B] = [A \times B]$. L'élément neutre de $\times$ correspond à la classe d'équivalence d'un singleton.

1.0.3 On quotiente une deuxième fois

$(\tilde{Def}(M), +, \times)$ n'est pas un anneau. En effet, la loi $+$ n'est pas inversible. Elle n'est même pas simplifiable. En effet, $[A] + [B] = [A] + [C]$, n'implique pas $[A] = [C]$.

Par exemple, soit $\mathbb{N}$ l'ensemble des entiers naturels, considéré comme une structure naturelle du langage $\{+, =\}$.

On peut trouver une bijection définissable entre $\mathbb{N} \cup \{(0,0)\}$ et $\mathbb{N}$ (par exemple la fonction f telle que $f((0,0)) = 0$ et $f(n) = n + 1$ pour tout $n \in \mathbb{N}$.)

Ainsi $[\mathbb{N}] + [\{(0,0)\}] = [\mathbb{N}]$. Mais il n'y a évidemment pas de bijection entre $\{(0,0)\}$ et le vide et $[\{(0,0)\}]$ n'est donc pas égal à 0.

Afin d'obtenir un monoïde simplifiable, on quotiente $(\tilde{Def}(M), +)$ par la relation d'équivalence $\simeq$ définie par $a \simeq b$ si et seulement si il existe $c \in \tilde{Def}(M)$ tel que $a + c = b + c$.

Comme, tout monoïde simplifiable, $(\tilde{Def}(M), +)$ quotienté par $\simeq$, se plonge dans un groupe unique à isomorphisme près et minimal pour la relation d'inclusion. $(\tilde{Def}(M), +, \times)$ quotienté par $\simeq$, se plonge donc dans un anneau unique à isomorphisme près.

C'est cet anneau qu'on appelle anneau de Grothendieck de M. Il est noté $K_0(M)$.

1.1 Le principe des tiroirs surjectif

Reprenons l'exemple de $\mathbb{N}$ considéré comme une structure du langage $\{+, =\}$. Nous avons vu que $[\mathbb{N}] + [\{(0,0)\}] = [\mathbb{N}]$ donc, dans $K_0(M)$, $[\{(0,0)\}] = 0$. Autrement dit $1 = 0$ (puisque la classe d'équivalence d'un singleton correspond à l'élément neutre de la multiplication). Et $K_0(M)$ est trivial.

Ceci est un exemple particulier du lemme plus général :

Lemme 1.1. *Soit M une structure. Il y a équivalence entre :*
- *Il existe A un ensemble définissable de $\bigcup_{n \in \mathbb{N}} M^n$ en bijection définissable avec lui même privé d'un point.*
- *L'anneau de Grothendieck de M est trivial.*

Démonstration. L'implication directe se démontre exactement comme nous l'avons fait dans le cas de $\mathbb{N}$: puisque A est en bijection définissable avec $A - \{a\}$, $[A - \{a\}] = [A]$, $[\{a\}] = 0$ c'est-à-dire $1 = 0$. $K_0(M)$ est donc trivial.

La réciproque se démontre tout aussi facilement. Si $K_0(M)$ est trivial, alors $1=0$. Ce qui signifie en remontant à $Def(M)$ qu'il existe A un ensemble définissable tel que $[A] + 1 = [A]$. Autrement dit en prenant a un élément de $\bigcup_n M^n$ n'appartenant pas à A, $A \cup \{a\}$ est en bijection avec A, c'est-à-dire lui-même privé d'un point. □

La propriété de ne pas admettre d'ensembles définissables en bijection définissable avec eux-même privés d'un point, est appelé principe des tiroirs surjectif, ou en anglais onto-pigeonhole principle, abrégé onto-PHP.

C'est une propriété du premier ordre.

Ainsi ce principe, qui correspond à une propriété combinatoire des structures, détermine si l'anneau de Grothendieck de ces structures est ou non trivial.

2 Exemples d'anneaux de Grothendieck connus

2.1 Les structures finies

Soit M une structure finie. Il est évident que $K_0(M)$ est isomorphe à $\mathbb{Z}$, puisque deux ensembles définissables sont en bijection définissable si, et seulement si, ils ont le même cardinal.

2.2 Certains corps valués dans le langage des anneaux

Des résultats sont aussi connus pour certains corps valués dans le langage $L_{anneaux}$. Ainsi, il a été montré par Lou van den Dries dans [4] que l'anneau de Grothendieck de $\mathbb{Q}_p$ comme $L_{anneaux}$-structure est trivial. On rappelle que la valuation de $\mathbb{Q}_p$ est définissable dans $L_{anneaux}$.

Dans [5], Raf Cluckers a montré la trivialité de l'anneau de Grothendieck de certaines séries de Laurent dans le langage $L_{anneaux}$:

Théorème 2.1. *Soit L un des corps suivant :*

- *$L = \mathbb{F}_q$ le corps de caractéristique p à q éléments*
- *$L = \mathbb{Q}_p$*
- *L est une extension finie de $\mathbb{Q}_p$.*

Soit K un corps de séries de Laurent itérées sur L, c'est-à-dire qu'il existe $n \in \mathbb{N}^*$ tel que $K = L((t_1))\dots((t_{n-1}))((t_n))$. Le corps valué K peut être considéré comme une $L_{anneaux}$-structure. (On rappelle que la valuation de K peut être définie dans $L_{anneaux}$.) Dans ce langage, il existe une bijection définissable entre K et K^*. L'anneau de Grothendieck de K dans le langage $L_{anneaux}$ est donc trivial.

2.3 D'autres corps valués

La non-satisfaction du onto-PHP est souvent utilisée pour démontrer que l'anneau de Grothendieck d'une structure est trivial. C'est en particulier grâce à lui que Deirdre Haskell et Raf Cluckers ont montré ([7]) la trivialité des anneaux de Grothendieck des corps $\mathbb{Z}$-valués qui vérifient la condition détaillée ci-dessous.

Un corps $\mathbb{Z}$-valué est un corps K muni d'une valuation $v : K^* \to \mathbb{Z}$. On définit l'anneau de valuation $R := \{x \in K | v(x) \geq 0\}$. Celui-ci admet un unique idéal maximal m l'ensemble $\{x \in K | v(x) > 0\}$.

K admet une **composante angulaire** si on peut définir un homomorphisme ac de K^* dans $(R/m)^*$ tel que $ac(x)$ correspond à la classe de x modulo m si $v(x) = 0$.

Soit L une extension du langage des anneaux dans lequel l'ensemble $\{x \in K | ac(x) = 1\}$ est définissable.

Enfin, on suppose que le corps est hensélien c'est-à-dire qu'il vérifie le lemme de Hensel. Alors, il est possible, grâce notamment à l'utilisation du lemme de Hensel, d'exhiber une bijection L-définissable entre K^2 et K^2 privé d'un point. L'anneau de Grothendieck de K dans ce langage L est donc trivial.

De façon plus générale, soit K est un corps valué dont le groupe de valeurs a un unique plus petit élément strictement positif. Soit ac une composante angulaire et $A := \{x \in K | ac(x) = 1\}$.

Soit $L = (L_{anneaux}, R)$ le langage des anneaux enrichi d'un symbole de relation unaire qui correspond à l'anneau de valuation. Soit L' une extension du langage L dans lequel A est définissable. Alors, considéré comme une L'-structure, K a un anneau de Grothendieck trivial ([5]).

2.4 Les corps algébriquement clos

Avant d'être étudiés par les théoriciens des modèles, les anneaux de Grothendieck avaient été introduits en géométrique algébrique. Leur définition dans ce cadre correspondait bien sûr à celle généralisée plus tard en théorie des modèles à toutes les structures : le groupe de Grothendieck d'un corps K est le quotient du groupe abélien libre constitué des classes d'isomorphisme des variétés sur K par les relations de la forme $[X] = [Y] + [X \setminus Y]$ pour toutes X, Y variétés sur K. On le munit d'une structure d'anneau en définissant une loi $\times$ définie par

$[X] \times [Y] = [(X \times Y)_{red}]$,

Ils apparaissent notamment en intégration motivique qui a été élaborée par Kontsevich pour montrer que deux variétés de Calabi-Yau birationnellement équivalentes ont les mêmes nombres de Hodge. La théorie a par la suite été considérablement développée par Denef et Loeser ([6]).

Bien sûr les corps algébriquement clos n'ont pas tous le même anneau de Grothendieck. Celui de $\mathbb{C}$ par exemple est très complexe. On sait notamment qu'il admet $\mathbb{Z}[u, v]$ comme quotient.

Il est toutefois facile, grâce à l'onto-PHP, de montrer que tous les corps algébriquement clos admettent un anneau de Grothendieck non trivial. En effet, dans le cas des corps algébriquement clos, le onto-PHP est une conséquence facile du théorème de Ax injectif. Celui-ci affirme que toute application polynômiale injective d'une variété algébrique dans elle-même, est aussi surjective et donc bijective.

Ce théorème d'Ax, ainsi que l'élimination des quantificateurs dans les corps algébriquement clos, permet de démontrer très facilement que l'onto-PHP est satisfait, et donc que l'anneau de Grothendieck d'un corps algébriquement clos est non trivial.

2.5 Corps réel clos

Soit $\mathbb{R}$ le corps réel clos considéré comme $L_{anneaux}$-structure. $K_0(\mathbb{R}) = \mathbb{Z}$.

Avant d'expliquer comment cela se démontre, nous allons faire quelques rappels sur les caractéristiques d'Euler.

On dit qu'une application de $Def(M)$ dans un anneau U unitaire commutatif est une caractéristique d'Euler faible si elle est de la forme $\chi' \circ [\cdot]$ où χ' est un $L(0,1,+,\times)$-homomorphisme de $\tilde{Def}(M)$ dans U et $[\cdot]$ est la projection canonique de $Def(M)$ dans $\tilde{Def}(M)$. L'existence d'une caractéristique d'Euler non triviale implique donc que $0 \neq 1$ et donc que $K_0(M)$ n'est pas trivial.

Revenons à $\mathbb{R}$ considéré comme $L_{anneaux}$-structure. Il est bien connu que $\mathbb{R}$ possède une caractéristique d'Euler faible qui n'est autre que sa caractéristique d'Euler géométrique.

La caractéristique d'Euler géométrique des ensembles définissables de $\mathbb{R}$ est définie à l'aide de leurs décompositions cellulaires. On rappelle qu'on peut définir des ensembles définissables d'une forme particulièrement simples, les cellules, qui permettent de recomposer tous les ensembles définissables : tout ensemble définissable admet une partition finie en cellules.

À chaque cellule est associée une dimension et étant donnée une partition d'un ensemble définissable A, on peut lui associer l'entier suivant :

$$\sum_{i \in \mathbb{N}} k_i (-1)^i$$

où k_i est le nombre de cellules de dimension i dans la partition. On peut montrer que ce nombre ne dépend pas de la partition choisie et est donc une caractéristique de A. Ce nombre est la caractéristique d'Euler géométrique de A.

L'anneau de Grothendieck de $\mathbb{R}$ est donc non trivial et admet $\mathbb{Z}$ comme quotient. Montrons qu'il est isomorphe à $\mathbb{Z}$. Soit χ la caractéristique d'Euler géométrique de $\mathbb{R}$. On sait ([2]) que si A, B sont deux ensembles définissables de même dimension et de même caractéristique d'Euler géométrique, alors il existe une bijection définissable entre eux. Cela suffit pour conclure : en effet supposons que A et B sont deux ensembles définissables de même caractéristique d'Euler géométrique mais qu'ils n'ont pas la même dimension. Alors n'importe quel ensemble C disjoint de A et de B et dont la dimension est supérieure à $\dim(A)$ et $\dim(B)$, permet d'obtenir deux ensembles définissables $A \cup C$ et $B \cup C$ de même caractéristique d'Euler géométrique et de même dimension. Autrement dit si A et B sont deux ensembles définissables de même caractéristique d'Euler géométrique, alors il existe C un ensemble définissable disjoint de $A \cup B$, tel que $A \cup C$ et $B \cup C$ sont en bijection définissable donc tel que $[A]+[C] = [B]+[C]$. Ainsi, deux ensembles définissables de même caractéristique d'Euler géométrique ont la même image dans $K_0(\mathbb{R})$ et χ n'est autre que la projection canonique de $Def(M)$ dans $K_0(M)$: $K_0(M) = \mathbb{Z}$.

2.6 Modules

Amit Kuber dans sa thèse ([9]) a démontré que les anneaux de Grothendieck des modules M dont la théorie T vérifie $T = T^{\aleph_0}$ sont des quotients du monoïde $\mathbb{Z}[X]$, où X est le monoïde multiplicatif des classes d'isomorphismes d'ensembles définissables fondamentaux (dans le sens qu'ils permettent par combinaison booléenne de reconstituer tout ensemble définissable)- les sous-groupes pp-définissables. Il a pour cela introduit des concepts de natures géométrique et topologique pour mieux comprendre la structure des ensembles définissables.

L'onto-PHP lui a permis d'établir que les anneaux de Grothendieck de ces modules sont non triviaux. Puis grâce à une caractéristique d'Euler qu'il définit, il parvient à les calculer plus explicitement.

3 Le principe du comptage modulaire

Nous allons donner un autre exemple de propriété combinatoire qui lorsqu'elle est satisfaite par une structure M, se reflète dans l'anneau de Grothendieck de cette structure.

Soit A un ensemble. On dit que A admet une m-partition s'il existe une partition de A en blocs définissables de cardinal m.

Définition 3.1. Le principe du comptage modulaire pour $m \geq 2$ affirme qu'il n'existe pas d'ensemble A et de sous-ensemble $B \subsetneq A$ de cardinal compris entre 1 et m tel que A et $A \setminus B$ admettent chacun une m-partition.

On dit qu'une structure M satisfait le principe du comptage modulaire si le principe est valable lorsque la partition considérée est définissable.

Tout comme l'onto-PHP, le principe du comptage modulaire est une propriété du premier ordre.

Il a été montré ([3], Thm.7.3].) que le principe de comptage modulaire permet de s'assurer que l'anneau de Grothendieck d'une structure admet comme quotient un corps fini particulier.

Théorème 3.2. *Soient p un nombre premier et M une structure. Supposons que M satisfait le principe du comptage modulaire pour p. Alors $K_0(M)$ admet $\mathbb{F}_p$ comme quotient.*

Théorème 3.3. *La réciproque n'est pas tout à fait vraie. Toutefois : si un ordre linéaire est définissable sur M et si $K_0(M)$ admet $\mathbb{F}_p$ comme quotient, alors M satisfait le principe du comptage modulaire pour p.*

4 Exemple de structures dont l'anneau de Grothendieck est de caractéristique p

Un anneau de Grothendieck d'une structure M est de caractéristique p si et seulement si il existe $A \subseteq M^n$ un ensemble définissable en bijection définissable avec lui-même privé de p points et que M satisfait l'onto-PHP.

Nous allons montrer que pour chaque entier p il existe une structure M telle que $K_0(M)$ est isomorphe à $\mathbb{F}_p$.

Les exemples que nous construirons seront des structures de Zariski.

Définition 4.1. Une géométrie de Zariski est la donnée d'un ensemble infini D tel que chacune des puissances D^n avec $n \geq 1$ est munie d'une topologie noethérienne vérifiant les conditions suivantes :

(Z0) [Cohérence et Séparation]

i) Si $f : D^n \to D^m$ est définie par $f(x) = (f_1(x), \ldots, f_n(x))$ où chacun des $f_i : D^n \to D$ est soit constant soit une projection coordonnée, alors f est continue.

ii) Chaque diagonale $\Delta^n_{i,j} = \{x \in D^n : x_i = x_j\}$ est fermée.

(Z1) [Élimination faible des quantificateurs]
Si $C \subseteq D^n$ est fermé et irréductible et si $\pi : D^n \to D^m$ est une projection, il existe un fermé $F \subsetneq \overline{\pi(C)}$ tel que $\pi(C) \supseteq \overline{\pi(C)} \setminus F$.

(Z2) [Uni-dimensionalité uniforme]

i) D est irréductible.

ii) Soit $C \subsetneq D^n \times D$ un fermé irréductible. Pour $\overline{a} \in D^n$, soit $C(\overline{a}) = \{x \in D : (\overline{a}, x) \in C\}$. Il existe alors un entier N tel que pour tout $\overline{a} \in D^n$, soit $|C(\overline{a})| \leq N$ soit $C(\overline{a}) = D$. En particulier, tout fermé propre de D est fini.

(Z3) [Théorème de la dimension]
Soit $C \subseteq D^n$ un fermé irréductible. Soit W une composante irréductible non-vide de $C \cap \Delta^n_{i,j}$. Alors $\dim(C) \leq \dim(W) + 1$.

Définition 4.2. Un ensemble est dit **constructible** s'il est combinaison booléenne de fermés.

Définition 4.3. Une structure est une structure de Zariski si l'ensemble de ses ensembles définissables correspond à l'ensemble des constructibles d'une géométrie de Zariski. Si de plus la projection de tout fermé est un fermé, alors on dit que M est une structure de Zariski projective.

Pour définir notre structure de Zariski, prenons $\mathbb{N}$ comme ensemble de base. Définissons la famille de topologies suivantes sur les puissances cartésiennes de $\mathbb{N}$.

Sur $\mathbb{N}$, les fermés sont les ensembles finis et $\mathbb{N}$.
Sur $\mathbb{N}^2$, une base de fermés est donnée par :
- les produits de fermés de $\mathbb{N}$
- la diagonale
- pour tout entier j multiple de p
- les ensembles $H_j = \{(n, n+j) | n \in \mathbb{N}\} \cup \{(0,0), (0,1), \ldots, (0, j-1)\}$ et leurs symétriques.

Pour $n \geq 3$, une base de fermés de $\mathbb{N}^n$ est donnée par les produits de fermés de $\mathbb{N}$, de diagonales et, pour tout $k \in \mathbb{N}$ multiple de p, tout $i, j \in [|1, n|]$,
d'ensembles $H_{k,i,j} = \{(x_1, \ldots, x_n) \in \mathbb{N}^n | (x_i = x_j + k) \vee (x_j = 0 \wedge x_i \in \{1, \ldots, k-1\})\}$.

Il est clair que chacune de ces topologies est noethérienne.
On peut montrer que cette famille de topologies définit une structure de Zariski projective.

- $\mathbb{N}$ est bien irréductible.
- Les diagonales sont fermées par définitions. De plus, si f est une fonction de $\mathbb{N}^n$ dans $\mathbb{N}^m$, définie par $f(x) = (f_1(x), \ldots, f_n(x))$ où chaque $f_j : \mathbb{N}^n \to \mathbb{N}$ est soit constante soit une projection sur une des coordonnées, il est clair que f est continue.
- La projection d'un fermé est un fermé
- On vérifie sans peine que si F est un fermé irréductible de $\mathbb{N}^{n+1}$, alors il existe un entier A tel que pour tout $a \in \mathbb{N}^n$, $\{x|(a,x) \in F\}$ est soit égal à $\mathbb{N}$ soit de cardinal inférieur à A.
- Il est également aisé de vérifier que si F est un fermé de $\mathbb{N}^n$ et F' une composante irréductible non vide de $F \cap \Delta_{i,j}$ où $\Delta_{i,j}$ est l'ensemble défini par $\{x_i = x_j\}$, alors $\dim(F) \leq \dim(F') + 1$. En effet, si F est un fermé irréductible, alors il est clair que sa dimension est égale au nombre de ses variables libres c'est-à-dire le cardinal maximal de l'ensemble I tel que $\forall\ i, j \in I$, aucune relation entre x_i et x_j n'est impliquée par la définition de F. Il est évident qu'intersecter F avec une diagonale diminue au plus de 1 le cardinal de I.

Il est évident que si l'anneau de Grothendieck de cette structure est non trivial, alors il est de caractéristique p.
En effet, $H_p - \{(0,0), \ldots, (0, p-1)\}$ est le graphe d'une bijection entre $\mathbb{N}$ et $\mathbb{N} - \{0, \ldots, p-1\}$.

Pour montrer que son anneau de Grothendieck est non trivial, il suffit de vérifier que le onto-PHP est satisfait.
Soit f une injection de $\mathbb{N}$ dans $\mathbb{N}^*$.
Soit $G \in \mathbb{N}^2$ le graphe de f ; G est un ensemble définissable de $\mathbb{N}^2$ et s'écrit donc comme combinaison booléenne d'ensembles H_j.
On remarque que deux ensembles H_i, H_j distincts sont d'intersection finie.
G est donc de la forme $H_j - F \cup F'$ où F, F' sont des ensembles finis.
Ainsi, il existe C un ensemble cofini de $\mathbb{N}$ sur lequel f est de la forme $n \mapsto n + j$ où $|j| > p - 1$ ou $j = 0$.
Soit $E = \{a_1, \ldots, a_n\}$ le complémentaire de C et E' le complémentaire de $f(C)$ dans $\mathbb{N}^*$.
Si $|j| > p - 1$ et $j > 0$, alors $E' = \{1, \ldots, j - 1, a_1 + j, \ldots, a_n + j\}$ est de cardinal strictement supérieur à celui de E et f ne peut établir de bijection entre E et E' ; f ne peut donc pas être une bijection entre $\mathbb{N}$ et $\mathbb{N}^*$.
Si $j = 0$, alors f est l'identité sur C, et donc $C \subsetneq \mathbb{N}^*$ et $E = E'$: l'image de f est donc forcément $\mathbb{N}$ ce qui contredit l'hypothèse de départ. Si $|j| > p - 1$ et $j < 0$, alors $E \supset \{1, \ldots, -j\}$, disons $E = \{1, \ldots, -j, a_1, \ldots, a_n\}$ où $a_1, \ldots, a_n$ sont des entiers strictement supérieurs à $-j$.
$E' = \{, a_1 + j, \ldots, a_n + j\}$ est de cardinal strictement inférieur à celui de E et f ne peut établir de bijection entre E et E', f ne peut donc pas être une bijection entre $\mathbb{N}$ et $\mathbb{N}^*$.

On montre de façon similaire qu'il n'existe pas de bijection entre $\mathbb{N}^n$ et $\mathbb{N}^n$ privé d'un point : le onto-PHP est satisfait et l'anneau de Grothendieck est non trivial.

5 Bibiographie

1. J. Krajicek and T. Scanlon, Combinatorics with definable sets : Euler characteristics and Grothendieck rings, this Bulletin, vol. 6 (2000), pp. 311-330.
2. L. van den Dries, Tame topology and o-minimal structures, London Math. Soc. Lecture Note Series, Vol. 248, (1998), Cambridge University Press.
3. J. Krajicek, Uniform families of polynomial equations over a finite field and structures admitting an Euler characteristic of definable sets, Proc. London Mathematical Society.
4. Lou van den Dries, Tame topology and o-minimal structures, Lecture note series, vol. 248, Cambridge University Press, 1998.
5. R. Cluckers. Grothendieck rings of Laurent series fields. Journal of Algebra, to appear. available at arXiv :math.LO/0210350.
6. J. Denef and F. Loeser, Definable sets, motives and p-adic integrals, Journal of the American Mathematical Society.
7. Raf Cluckers and Deirdre Haskell, Grothendieck Rings of $\mathbb{Z}$-Valued Fields, The Bulletin of Symbolic Logic, Vol. 7, No. 2 (2001), pp. 262-269.
8. A. Kuber, Grothendieck rings of theories of modules, Preprint, arXiv :1302.4229, 2013.

Groupes cycliquement ordonnés pseudo-c-archimédiens et pseudo-cycliques.

Gérard Leloup

10 mars 2015

L'exposé qui suit est tiré d'un article rédigé avec François Lucas ([LL 14]).

1 Groupes cycliquement ordonnés.

1.1 Définition. Soit G un groupe muni d'une relation ternaire R. On dit que (G, R) est un *groupe cycliquement ordonné* s'il vérifie les propriétés suivantes.
(1) $\forall(x,y,z) \in G^3$, $R(x,y,z) \Rightarrow x \neq y \neq z \neq x$ (R est stricte),
(2) $\forall(x,y,z) \in G^3$, $R(x,y,z) \Rightarrow R(y,z,x)$ (R est cyclique),
(3) Pour tout $x \in G$, $R(x,\cdot,\cdot)$ définit une relation d'ordre linéaire sur $G\backslash\{x\}$,
(4) $R(\cdot,\cdot,\cdot)$ est compatible, i.e.

$$\forall(x,y,z,u,v) \in G^5,\ R(x,y,z) \Rightarrow R(uxv, uyv, uzv).$$

Le langage des groupes cycliquement ordonnés est celui des groupes, auquel on ajoute un prédicat ternaire R. Un morphisme de groupes cycliquement ordonnés est un morphisme de groupes qui respecte l'ordre cylclique.

Un exemple simple de groupe cycliquement ordonné est obtenu par le cercle trigonométrique identifié au groupe $\mathbb{K}$ des complexes de module 1, parcouru dans le sens inverse des aiguilles d'une montre. Supposons que l'on parte d'un point de $\mathbb{K}$ et l'on rencontre les points x, y, z dans cet ordre, alors on pose $R(x,y,z)$. En partant d'un autre point, on peut les rencontrer dans l'ordre y, z, x ou z, x, y, on a donc également $R(y,z,x)$ et $R(z,x,y)$.

Sur tout groupe linéairement ordonné il existe une structure de groupe cycliquement ordonné. On pose: $R(x, y, z)$ si, et seulement si, $x < y < z$ ou $y < z < x$ ou $z < x < y$. Dans ce cas, on dit que G est un groupe *linéairement cycliquement ordonné.*

On adoptera la notation $R(x_1, \ldots, x_n)$, où $x_1, \ldots,\ x_n$ sont dans G, pour:

$$\bigcup_{1 \leq i < j < k \leq n} R(x_i, x_j, x_k), \text{ ce qui revient à: } \bigcup_{1 \leq i \leq n-2} R(x_i, x_{i+1}, x_n)$$

Si G est un groupe linéairement ordonné et $z \in G$, $z > e$, est un élément central et cofinal de G, alors le groupe quotient $G/\langle z \rangle$ peut être cycliquement ordonné par:
$R(\overline{g_1}, \overline{g_2}, \overline{g_3})$ si et seulement s'il existe g'_1, g'_2, g'_3 tels que $\overline{g_1} = \overline{g'_1}$, $\overline{g_2} = \overline{g'_2}$, $\overline{g_3} = \overline{g'_3}$ et $e \leq g'_{\sigma(1)} < g'_{\sigma(2)} < g'_{\sigma(3)} < z$ pour un σ dans le groupe alterné A_3 de degré 3 (ou encore, $e \leq g'_1 < g'_2 < g'_3 < z$ ou $e \leq g'_2 < g'_3 < g'_1 < z$ ou $e \leq g'_3 < g'_1 < g'_2 < z$).

$G/\langle z \rangle$ est *l'enroulé* (*wound-round*) associé à G et z.

Par exemple, si G est égal au groupe additif $\mathbb{R}$ des réels et $z = 2\pi$, on a concrètement une application $x \mapsto \exp(ix)$ dont le noyau est $\langle 2\pi \rangle$, $\mathbb{R}/2\pi\mathbb{Z}$ est isomorphe au groupe multiplicatif $\mathbb{K}$ des complexes de module 1.

Tout groupe cycliquement ordonné est l'enroulé d'un groupe linéairement ordonné, comme le montre le théorème suivant.

1.2 Théorème. *(Rieger). Si G est un groupe cycliquement ordonné, alors il existe sur $\Gamma = \mathbb{Z} \times G$ une structure de groupe linéairement ordonné, où $z_G = (1, e)$ est positif, central, cofinal, et tel que $G \simeq \Gamma/\langle z_G \rangle$.*

Le groupe Γ ainsi obtenu est appelé le *déroulé* de G, et on le notera $\text{uw}(G)$, (car déroulé se dit *unwound* en anglais). On notera également e son élément neutre dans le cas où cela n'apporte pas de confusion.

Dans le cas où G est le groupe $\mathbb{K}$ des complexes de module 1, le déroulé est le corps $\mathbb{R}$ des réels, la bijection entre $\mathbb{R}$ et $\mathbb{Z} \times \mathbb{K}$ est obtenu de la manière suivante. Soit $x \in \mathbb{R}$, n la partie entière de $x/(2\pi)$ et $\theta = x - 2n\pi$, alors l'image de x est $(n, \exp(i\theta))$. L'ordre et la multiplication sur $\mathbb{Z} \times \mathbb{K}$ sont construits de manière à ce que cette bijection soit un isomorphisme de groupes ordonnés.

Le plus grand sous-groupe convexe de $\text{uw}(G)$ contenu dans $]z_G^{-1}, z_G[$ s'injecte dans G, son image $l(G)$ est appelée la *partie linéaire* de G. G est linéairement cycliquement ordonné si, et seulement si, $l(G) = G$.

On notera $K(G)$ le groupe quotient $G/l(G)$. La classe modulo $l(G)$ d'un élément a de G sera notée $\bar{a}$. $K(G)$ est muni d'une structure de groupe cycliquement ordonné, qui se déduit de celle de G. On sait que $K(G)$ s'injecte dans $\mathbb{K}$.

Pour obtenir une description des groupes cycliquement ordonnés on définit les produits lexicographiques.

1.3 Définition. Soit (G, R) un groupe cycliquement ordonné et $(L, \leq)$ un groupe linéairement ordonné. Le *produit lexicographique* de (G, R) et $(L, \leq)$, noté $G \overrightarrow{\times} L$, est le groupe produit $G \times L$ muni de la relation R' définie comme suit. Pour tous x, y, z dans G et l, m, n dans L, on pose $R'((x, l), (y, m), (z, n))$ si, et seulement si, l'une des conditions suivantes est vérifiée:
$R(x, y, z)$
$x = y \neq z$ et $l < m$
$x \neq y = z$ et $m < n$
$x = z \neq z$ et $n < l$
$x = y = z$ et $l < m < n$
$x = y = z$ et $m < n < l$
$x = y = z$ et $n < l < m$.
C'est-à-dire que l'on regarde d'abord l'ordre cyclique sur G, et en cas d'égalité sur la première composante on tient compte de l'ordre sur L.

On remarque que le sous-groupe $\{e\} \overrightarrow{\times} L$ muni de la restriction de R est linéairement cycliquement ordonné.

1.4 Théorème. *(Świerczkowski [Sw 59]). Soit G un groupe cycliquement ordonné. Il existe un groupe linéairement ordonné L tel que G s'injecte, comme groupe cycliquement ordonné, dans $\mathbb{K} \overrightarrow{\times} L$.*

Cette injection n'est pas canonique, seule la première projection l'est, à tout élément elle associe sa classe modulo $l(G)$.

On déduit de ce théorème que le groupe de torsion de G s'injecte dans le sous-groupe $\mathbb{U}$ des éléments de torsion de $\mathbb{K}$, c'est-à-dire les racines de 1 dans le corps $\mathbb{C}$ des complexes.

Le *cône positif* de G est constitué de e et des $x \in G$ qui vérifient $R(e, x, x^{-1})$. Si l'on note $(e^{i\theta}, l)$ l'image de x par l'injection de Świerczkowski, alors la propriété $R(e, x, x^{-1})$ revient à dire que ou bien $0 < \theta < \pi$, ou bien $\theta = 0$ et

$l \geq 0$, ou bien $\theta = \pi$ et $l < 0$.

Dans ce qui suit, (G, R) est un groupe cycliquement ordonné abélien. Comme G est commutatif, on adoptera la notation additive, sauf dans le cas des sous-groupes de $\mathbb{K}$, car la notation multiplicative y est plus habituelle.

G est dit *c-archimédien* si $l(G) = \{0\}$. Świerczkowski a prouvé que G est c-archimédien si, et seulement si, pour tous x et y dans G il existe un entier $n > 0$ tel que $R(0, nx, y)$ n'est pas vérifié. Noter que ce n'est pas une propriété du premier ordre. Si G est c-archimédien, alors il s'injecte dans $\mathbb{K}$, donc G est abélien.

Un *sous-groupe c-convexe* de G est un sous-groupe H qui ne contient pas d'élément d'ordre 2 et qui vérifie pour tous x et y dans G:

$$(y \in H \,\&\, R(0, y, -y) \,\&\, R(0, x, y)) \Rightarrow x \in H.$$

L'ensemble des sous-groupes c-convexes propres de G est canoniquement en bijection avec l'ensemble des sous-groupes convexes de $l(G)$ non réduits à $\{0\}$. On voit que G est c-archimédien si et seulement s'il ne contient pas de sous-groupe c-convexe propre.

On dira que G est *c-n-divisible* s'il est n-divisible et contient un sous-groupe isomorphe au sous-groupe de $(\mathbb{U}, \cdot)$ engendré par une racine primitive n-ième de l'unité. On voit que cette propriété s'exprime par des formules du premier ordre. G est c-n-divisible si, et seulement si, $\mathrm{uw}(G)$ est n-divisible. On dira que G est *c-divisible* s'il est divisible et contient un sous-groupe isomorphe à $(\mathbb{U}, \cdot)$.

2 Groupes c-réguliers.

2.1 Définitions. Soit n un entier au moins égal à 2. On note (re-n) la propriété: pour tous $x_1, \dots, x_n$ dans G tels que $R(0, x_1, \dots, x_n, -x_n)$, il existe $x \in G$ tel que $(R(x_1, nx, x_n)$ ou $nx = x_1$, ou $nx = x_n)$ et $R(0, x, \dots, (n-1)x, x_n)$.
On dira que (G, R) est *c-n-régulier* si pour tous $x_1, \dots, x_n$ dans G tels que $R(0, x_1, \dots, x_n)$, il existe $x \in G$ tel que $(nx = x_1$, ou $nx = x_n$, ou $R(x_1, nx, x_n))$ et $R(0, x, \dots, (n-1)x, x_n)$.
On dira que (G, R) vérifie (re) s'il vérifie (re-n) pour tout $n \geq 2$, et on dira que (G, R) est *c-régulier* s'il est c-n-régulier pour tout $n \geq 2$.

On remarque que ces propriétés sont du premier ordre et, clairement, si (G, R) est c-n-régulier, alors il vérifie (re-n). Un groupe linéairement cycliquement ordonné non trivial n'est pas c-n-régulier. Le fait suivant montre en quoi la propriété (re-n) généralise la définition de n-régulier connue sur les groupes totalement ordonnés.

2.2 Fait. *Si (G, R) est linéairement cycliquement ordonné, alors il vérifie (re-n) si et seulement s'il est n-régulier au sens usuel.*

2.3 Lemme. *Tout sous-groupe de $\mathbb{K}$ est c-régulier.*

2.4 Théorème. *Soit $n \geq 2$. G vérifie (re-n) si, et seulement si, l'une des deux conditions suivantes est vérifiée.*
1) G est linéairement cycliquement ordonné, et n-régulier comme groupe linéairement ordonné.
2) G n'est pas linéairement cycliquement ordonné, et est c-n-régulier.
En d'autres termes, la classe des groupes cycliquement ordonnés qui vérifient (re-n) est l'union de la classe des groupes linéairement cycliquement ordonnés n-réguliers et de la classe des groupes cycliquement ordonnés c-n-réguliers.

2.5 Théorème. *Soit $n \geq 2$. Les conditions suivantes sont équivalentes.*
(1) $uw(G)$ est n-régulier
(2) G est c-n-régulier
(3) ou bien G est c-archimédien,
ou bien $l(G)$ est n-régulier, $K(G)$ est n-divisible et contient une racine primitive n-ième de l'unité
(4) le quotient de G par tout sous-groupe c-convexe propre est c-n-divisible.

3 Équivalences élémentaires de groupes abéliens cycliquement ordonnés c-réguliers.

Si A est un groupe abélien et $n \in \mathbb{N}^*$, on définit ce que nous appellerons ici le n-ième *invariant de Zakon* de A par: $[n]A$ est le nombre maximum d'éléments de A non congrus deux à deux modulo n dans A. C'est un élément de $\mathbb{N}^* \cup \{\infty\}$, c'est-à-dire qu'on ne distingue pas les différents infinis. Cette définition permet de voir que si $B \equiv A$, alors pour tout n on a: $[n]A = [n]B$. En fait, si $[n]A$ est fini, alors il est égal au cardinal de A/nA. Si n est premier, alors $[n]A$ sera appelé un *invariant premier de Zakon.*

3.1 Groupes abéliens cycliquement ordonnés c-réguliers denses.

3.1 Proposition. *Soit G_1 et G_2 deux groupes cyliquement ordonnés c-réguliers denses tels que G_1 est un sous-groupe de G_2. Alors G_1 est une sous-structure élémentaire de G_2 si, et seulement si, G_1 est pur dans G_2, et pour tout p premier $[p]G_1 = [p]G_2$.*

3.2 Proposition. *Pour toute famille d'invariants premiers de Zakon $\mathcal{Z}$ et tout sous-groupe T de $\mathbf{U}$, il existe un groupe cycliquement ordonné c-archimédien dénombrable dense G de groupe de torsion T de famille d'invariants premiers de Zakon $\mathcal{Z}$.*

3.3 Théorème. *Il existe un groupe cycliquement ordonné c-archimédien infini élémentairement équivalent à G si, et seulement si, G est c-régulier et dense.*
Deux groupes cycliquement ordonnés c-réguliers denses sont élémentairement équivalents si et seulement s'ils ont des groupes de torsion isomorphes et la même famille d'invariants premiers de Zakon.

On déduit, par exemple du théorème 2.5, que tout groupe abélien cycliquement ordonné c-divisible est c-régulier, donc par le théorème 3.3 un groupe abélien cycliquement ordonné est c-divisible si et seulement s'il est élémentairement équivalent à $\mathbf{U}$.

3.4 Proposition. *On suppose que G est c-régulier, dense et ω_1-saturé. Alors G contient une sous-structure élémentaire dénombrable qui est un groupe c-archimédien.*

3.2 Groupes abéliens cycliquement ordonnés c-réguliers discrets.

3.5 Proposition. *Soit G_1 et G_2 deux groupes cyliquement ordonnés c-réguliers discrets tels que G_1 est un sous-groupe de G_2. Alors G_1 est une sous-structure élémentaire de G_2 si, et seulement si, G_1 est pur dans G_2 et les cônes positifs de G_1 et G_2 ont le même premier élément.*

3.6 Proposition. *On suppose que G est c-régulier discret et non c-archimédien. Alors G contient un sous-groupe pur H c-régulier discret tel que $K(H) = \mathbb{U}$ et $l(H) \simeq \mathbb{Z}$ et qui de plus est une sous-structure élémentaire de G.*

3.7 Définition. Soit T un groupe abélien linéairement ordonné discret, de premier élément strictement positif 1_T, et contenant un élément fixé z_T que l'on met dans le langage. Comme 1_T est définissable, on peut également considérer qu'il est dans le langage. Pour p premier, $n \in \mathbb{N}^*$ et $k \in \{0, \ldots, p^n - 1\}$, on définit la formule $DD_{p^n,k}$: $\exists x,\ p^n x = z_T + k1_T$.

3.8 Lemme. *Soit T un groupe abélien linéairement ordonné discret, de premier élément strictement positif 1_T, et contenant un élément positif cofinal fixé z_T, que l'on met dans le langage. On suppose que $T/\langle 1_T \rangle$ est divisible.*
1) Pour tous p premier et $n \in \mathbb{N}^*$, il existe exactement un entier $k \in \{0, \ldots, p^n - 1\}$ tel que $DD_{p^n,k}$ est vérifié dans T.
2) Soit p premier, $n \in \mathbb{N}^*$, et $k \in \{0, \ldots, p^n - 1\}$ tels que $DD_{p^n,k}$ est vérifié dans T. On décompose k sous la forme $k = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}$, où, pour $1 \leq j \leq n$, $a_j \in \{0, \ldots, p-1\}$, alors pour tout $j \leq n$, et $k_j = a_0 + \cdots + a_{j-1}p^{j-1}$, DD_{p^j,k_j} est vérifiée dans T.

3.9 Définition. Si G est discret et non c-archimédien, alors le plus petit élément non nul 1_G du cône positif de G est définissable, on peut considérer qu'il est dans le langage. Pour p premier, $n \in \mathbb{N}^*$ et $k \in \{0, \ldots, p^n - 1\}$, $D_{p^n,k}$ sera la formule:
$\exists x,\ R(0, x, 2x, \ldots, (p^n - 1)x) \wedge p^n x = k1_G$.

La formule $R(0, x, 2x, \ldots, (p^n - 1)x) \wedge p^n x = k1_G$ dit que les jx où $1 \leq j \leq p^n - 1$ "ne font pas le tour complet du cercle", mais que $p^n x$ "fait le tour", et vaut $k1_G$. Ceci revient à dire que l'image de x dans uw(G) vérifie $p^n x = z_G + k1_G$.

On remarque que G contient un élément de torsion p^k relevant une racine p^k-ième de l'unité dans $G/\langle 1_G \rangle$ si et seulement s'il vérifie la formule $D_{p^k,0}$. En particulier, G contient un sous-groupe isomorphe à $\mathbb{U}$ si et seulement s'il vérifie les formules $D_{p^k,0}$ pour tout p premier et $k \in \mathbb{N}^*$.

3.10 Lemme. *On suppose que G est c-régulier discret infini. Pour tous p premier, $n \in \mathbb{N}^*$ et $k \in \{0, \ldots, p^n - 1\}$, G vérifie la formule $D_{p^n,k}$ si,* *et seulement si, $uw(G)$ vérifie la formule $DD_{p^n,k}$, où l'élément mis dans le langage est z_G.*

3.11 Lemme. *On suppose que G est discret, non c-archimédien, et que $G/\langle 1_G\rangle$ est c-divisible.*
1) Pour tous p premier et $n \in \mathbb{N}^*$, il existe exactement un entier $k \in \{0, \dots, p^n - 1\}$ tel que $D_{p^n,k}$ est vérifié dans G.
2) Soit p premier, $n \in \mathbb{N}^*$, et $k \in \{0, \dots, p^n - 1\}$ tels que $D_{p^n,k}$ est vérifié dans G. On décompose k sous la forme $k = a_0 + a_1p + \cdots + a_{n-1}p^{n-1}$, où, pour $1 \leq j \leq n$, $a_j \in \{0, \dots, p-1\}$. Alors pour tout $j \leq n$, et $k_j = a_0 + \cdots + a_{j-1}p^{j-1}$, D_{p^j,k_j} est vérifiée dans G.
3) Il existe une unique suite (φ_p), où p parcourt la suite croissante des nombres premiers et φ_p est une application de $\mathbb{N}^*$ dans $\{0, \dots, p-1\}$ telle que pour tous p premier, $n \in \mathbb{N}^*$ et $k \in \{0, \dots, p^n - 1\}$, G satisfait $D_{p^n,k}$ si, et seulement si, $k = \varphi_p(1) + \varphi_p(2)p + \cdots + \varphi_p(n)p^{n-1}$.

3.12 Définition. On suppose que G est discret, non c-archimédien, et que $G/\langle 1_G\rangle$ est divisible. La suite (φ_p), où p parcourt la suite croissante des nombres premiers et φ_p est une application de $\mathbb{N}^*$ dans $\{0, \dots, p-1\}$, définie dans le 3) du lemme 3.11 sera appelée la *suite caractéristique* de G.

On remarque que G contient un sous-groupe isomorphe à $\mathbb{U}$ si, et seulement si, pour tout p premier l'application φ_p est l'application nulle.

3.13 Proposition. *Soit C_1 et C_2 deux groupes cycliquement ordonnés discrets non c-archimédiens tels que $C_1/\langle 1_{C_1}\rangle \simeq \mathbb{U} \simeq C_2/\langle 1_{C_2}\rangle$. Les conditions suivantes sont équivalentes.*
C_1 et C_2 sont isomorphes
C_1 et C_2 vérifient les mêmes formules $D_{p^n,k}$
$C_1 \equiv C_2$.
La suite caractéristique de C_1 est égale à la suite caractéristique de C_2.

3.14 Théorème. *Deux groupes cycliquement ordonnés c-réguliers discrets non c-archimédiens sont élémentairement équivalents si et seulement s'ils vérifient les mêmes formules $D_{p^n,k}$.*

3.15 Corollaire. *Deux groupes cycliquement ordonnés c-réguliers discrets non c-archimédiens sont élémentairement équivalents si, et seulement si, leurs suites caractéristiques sont égales.*

3.16 Proposition. *Pour toute suite (φ_p) de fonctions de $\mathbb{N}^*$ dans $\{0,\ldots,p-1\}$, où p parcourt la suite croissante des nombres premiers, il existe un groupe cycliquement ordonné c-régulier discret H non c-archimédien ayant la suite (φ_p) comme suite caractéristique.*

3.17 Définitions. Pour chaque p premier, soit φ_p une application de $\mathbb{N}^*$ dans $\{0,\ldots,p-1\}$. Pour tous p premier et $n \in \mathbb{N}^*$, on note N_{p^n,φ_p} l'ensemble $p^n\mathbb{N}^* - (\sum_{k=1}^{n} p^{k-1}\varphi_p(k))$. L'ensemble des N_{p^n,φ_p} sera appelé la *famille des sous-ensembles de $\mathbb{N}^*$ caractéristique de (φ_p)*. La famille des sous-ensembles de $\mathbb{N}^*$ caractéristique de la suite caractéristique de G sera appelée la *famille des sous-ensembles de $\mathbb{N}^*$ caractéristique de G.*

3.18 Proposition.
1) Pour tout ultrafiltre U sur $\mathbb{N}^*$, il existe exactement une suite (φ_p), où p parcourt la suite croissante des nombres premiers et φ_p est une application de $\mathbb{N}^*$ dans $\{0,\ldots,p-1\}$, telle que U contient la famille des sous-ensembles de $\mathbb{N}^*$ caractéristique de (φ_p).
2) Pour toute suite (φ_p), où p parcourt la suite croissante des nombres premiers et φ_p est une application de $\mathbb{N}^*$ dans $\{0,\ldots,p-1\}$, il existe un ultrafiltre non principal U sur $\mathbb{N}^*$ contenant la famille de sous-ensembles de $\mathbb{N}^*$ caractéristique de (φ_p).

3.19 Définition. Soit U un ultrafiltre sur $\mathbb{N}^*$, la famille de sous ensembles définie dans le 1) de la proposition 3.18 sera appelée *la famille des sous-ensembles de $\mathbb{N}^*$ définie par U.*

3.20 Théorème.
1) Soit U un ultrafiltre non principal sur $\mathbb{N}^*$, C l'ultraproduit des groupes cycliquement ordonnés $\mathbb{Z}/n\mathbb{Z}$ modulo U, p un nombre premier, $n \in \mathbb{N}^*$ et $k \in \{0,\ldots,p^n-1\}$. Alors C vérifie la formule $D_{p^n,k}$ si, et seulement si, $p^n\mathbb{N}^* - k \in U$.
2) Soit U un ultrafiltre non principal sur $\mathbb{N}^*$, C l'ultraproduit des groupes cycliquement ordonnés $\mathbb{Z}/n\mathbb{Z}$ modulo U. La famille des sous-ensembles de $\mathbb{N}^*$ définie par U est égale à la famille de sous-ensembles de $\mathbb{N}^*$ caractéristique de C.
3) Soit U_1 et U_2 deux ultrafiltres non principaux sur $\mathbb{N}^*$, C_1 (resp. C_2) l'ultraproduit des groupes cycliquement ordonnés $\mathbb{Z}/n\mathbb{Z}$ modulo U_1 (resp. U_2). Alors $C_1 \equiv C_2$ si, et seulement si, la famille de sous-ensembles de $\mathbb{N}^*$ définie par U_1 est égale à la famille de sous-ensembles de $\mathbb{N}^*$ définie par U_2.

3.21 Corollaire. *1) Si G est infini, c-régulier et discret, et U est un ultrafiltre non principal sur $\mathbb{N}^*$, alors G est élémentairement équivalent à l'ultraproduit des groupes cycliquement ordonnés $\mathbb{Z}/n\mathbb{Z}$ modulo U si, et seulement si, la famille de sous-ensembles de $\mathbb{N}^*$ caractéristique de G est égale à la famille de sous-ensembles de $\mathbb{N}^*$ définie par U.*
2) G est c-régulier et discret si seulement s'il existe un ultrafiltre sur $\mathbb{N}^*$ tel que G est élémentairement équivalent à l'ultraproduit des groupes cycliquement ordonnés $\mathbb{Z}/n\mathbb{Z}$ modulo U.

3.22 Proposition. *Pour tout sous-groupe S de $\mathbb{U}$, il existe un ultraproduit de groupes cycliques finis dont le groupe de torsion est S.*

3.23 Théorème. *1) La classe des groupes abéliens cycliquement ordonnés c-réguliers discrets est la plus petite classe élémentaire contenant tous les groupes cycliques finis.*
2) La classe des groupes abéliens cycliquement ordonnés discrets vérifiant (re) est la plus petite classe élémentaire contenant tous les groupes monogènes. Si G est dans cette classe, alors ou bien G est linéairement cycliquement ordonné élémentairement équivalent à $\mathbb{Z}$, ou bien G est c-régulier et élémentairement équivalent à un ultraproduit de groupes cycliques finis.

4 Avec ou sans l'ordre cyclique.

Bien que naturelle, la relation d'ordre cyclique sur $\mathbb{K}$ apparaît beaucoup moins que la relation d'ordre sur $\mathbb{R}$. Pour mieux cerner ce qu'elle apporte ici, nous allons faire le lien avec l'étude de ces mêmes groupes en se restreignant au langage des groupes. Dans ce langage, on sait que deux groupes abéliens sont élémentairement équivalents si et seulement s'ils ont les mêmes invariants de Szmielew (cf. [Sz 55]). On peut montrer que si le groupe de torsion d'un groupe abélien s'injecte dans $\mathbb{U}$, alors les invariants de Szmielew sont entièrement déterminés par le groupe de torsion et les invariants de Zakon.

On peut reformuler l'un des résultats.

4.1 Proposition. *Deux groupes cycliquement ordonnés c-réguliers denses sont élémentairement équivalents comme groupes cycliquement ordonnés si et seulement s'ils sont élémentairement équivalents comme groupes. La même chose est vraie pour deux groupes linéairement ordonnés réguliers denses.*

En ce qui concerne les groupes cycliquement ordonnés c-réguliers discrets, pour un groupe de torsion fixé ils ont tous les mêmes invariants de Szmielew (ou invariants de Zakon, cela revient au même), donc ils sont élémentairement équivalents dans le langage des groupes, mais ils ne sont pas nécessairement élémentairement équivalents dans le langage des groupes cycliquement ordonnés, à cause des prédicats $D_{p^n,k}$.

On sait qu'un groupe abélien est ordonnable si et seulement s'il est sans torsion, cela dépend donc de sa théorie du premier ordre. De même, le fait d'être cycliquement ordonnable dépend de la théorie du premier ordre d'un groupe. On va voir que le fait de pouvoir être muni d'une structure de groupe cycliquement ordonné c-régulier discret, ou d'une structure de groupe linéairement ordonné régulier discret ne dépend pas de la théorie du premier ordre d'un groupe. Il existe des groupes ordonnables qui ne peuvent pas être munis d'une structure de groupe linéairement ordonné régulier dense, ni de groupe cycliquement ordonné c-régulier dense.

4.2 Proposition. *Soit G un groupe abélien sans torsion.*
Il existe sur G une structure de groupe linéairement ordonné régulier avec un plus petit sous-groupe convexe propre si, et seulement si, pour tout p premier il existe une famille maximale I_p d'éléments deux à deux non congrus modulo p de cardinal au plus égal au cardinal de $\mathbb{R}$.
Il existe sur G une structure de groupe linéairement ordonné régulier discret si, et seulement si, pour tout p premier $[p]G = p$ et il existe un élément qui n'est divisible par aucun p premier.

Supposons maintenant que G soit un groupe abélien sans torsion tel qu'il existe un nombre premier p et une famille maximale I_p d'éléments deux à deux non congrus modulo p et de cardinal strictement plus grand que celui de $\mathbb{R}$ et, pour tout q premier distinct de p, G est q-divisible. On considère la clôture divisible H du sous-groupe engendré par la famille I_p. Considérons un sous-groupe pur C de H distinct de H. Donc l'un des éléments de la famille I_p n'est pas dans C, donc H/C n'est pas divisible. Comme le cardinal de H est strictement plus grand que celui de $\mathbb{R}$, il ne peut pas y avoir de structure de groupe linéairement ordonné archimédien. Ainsi, il n'existe pas de structure de groupe ordonné régulier sur H. Pour la même raison, il n'existe pas de structure de groupe cycliquement ordonné c-régulier.

Si G est un groupe abélien infini sur lequel il existe une structure de groupe cycliquement ordonné c-régulier discret, alors son groupe de torsion s'injecte dans $\mathbb{U}$, et G contient un élément e qui n'est divisible par aucun p premier et tel que le groupe quotient $G/\mathbb{Z}e$ est divisible. Le fait que e ne soit divisible par aucun p premier ne peut pas s'exprimer par une formule du premier ordre du langage des groupes (l'exemple qui suit va le prouver), alors que c'est une conséquence d'une formule du langage des groupes cyliquement ordonnés (e est le plus petit élément du cône positif).

4.3 Exemples de groupes qui sont élémentairement équivalents à des groupes cycliquement ordonnés c-réguliers discrets dans le langage des groupes, mais qui ne peuvent pas être munis d'une structure de groupe cycliquement ordonné c-régulier discret. Considérons une famille a_n, $n \in \mathbb{N}^*$, d'éléments de $\mathbb{K}\backslash\mathbb{U}$ rationnellement indépendants, et G la somme directe des $\mathbb{Z}_{(p_n)}a_n$ (où $(p_n)_{n\in\mathbb{N}^*}$ est la suite croissante des nombres premiers, et $\mathbb{Z}_{(p_n)}$ le localisé de $\mathbb{Z}$ en p_n). Tout élément de G est contenu dans une somme finie $\mathbb{Z}_{(p_{n_1})}a_{n_1} + \cdots + \mathbb{Z}_{(p_{n_k})}a_{n_k}$, donc divisible par tout p premier distinct de $p_{n_1}, \ldots, p_{n_k}$. Ainsi, G ne contient pas d'élément qui ne soit divisible par aucun nombre premier, donc ne peut pas être muni d'une structure de groupe cycliquement ordonné c-régulier discret. Cependant, comme on l'a déjà remarqué, pour tout p premier on a $[p]G = p$, donc G est élémentairement équivalent dans le langage des groupes à tout groupe cycliquement ordonné c-régulier discret sans torsion. On remarque que G est aussi élémentairement équivalent à $\mathbb{Z}$, mais ne peut pas être muni d'une structure de groupe linéairement ordonné régulier discret.

Bibliographie

[GLL 13] M. Giraudet, G. Leloup & F. Lucas, *First order theory of cyclically ordered groups* (soumis), hall-00879429, version 1 ou arXiv:1311.0499v1[mathLO].

[LL 14] G. Leloup & F. Lucas, *c-regular cyclically ordered groups* (preprint), hal-00919983, version 1 ou arXiv:1312.5269v1[mathLO]

[RZ 60] A. Robinson & E. Zakon, *Properties of ordered abelian groups*, Transactions of the American Mathematical Society **96** n°2 (1960), pp. 222-236.

[Sw 59] S. Świerczkowski, *On cyclically ordered groups*, Fund. Math. **47** (1959), pp. 161-166.

[Sz 55] W. Szmielew, *Elementary properties of Abelian groups*, Fund. Math. **41** (1955), pp. 203-271.

[Za 61] E. Zakon, *Archimedean groups*, Transactions of the American Mathematical Society **99** n°1 (1961), pp. 21-40.

Fans in the Theories of Real Semigroups and of Abstract Real Spectra. A Summary of Results.

M. Dickmann A. Petrovich

February 2016

Introduction

We present here a summary, omitting proofs, of the main results of the paper [DP5], submitted.

In [DP1] we introduced the notion of a *real semigroup* (henceforth abbreviated RS), an axiomatic framework aimed at studying diagonal quadratic forms with arbitrary entries over commutative, unitary rings [1] admitting a minimum of orderability. [2] The axioms defining RSs and their underlying structures, the *ternary semigroups* (abbreviated TS), appear in 1.1 and 1.2 of the paper [DMP] in this volume. For more details the reader is referred to [DP1], §§ 1,2, pp. 100-112, or to [DP2], § 2, pp. 57-59. We proved ([DP1], Thm. 4.1, p. 115) that the RSs are categorically dual to the *abstract real spectra* (ARS), previously introduced in [Br] and [M], Chs. 6 – 9, with a similar goal.

In [DP2], [DP3] we introduced and studied two outstanding classes of RSs, the Post algebras and the spectral real semigroups, and their dual ARSs. The aim of this paper is to present a third natural class of RSs (and their dual ARSs), namely *fans*, and develop their theory.

Initially, fans were discovered by Becker and Köpping [BK] [3] as a distinguished class of preorders in fields, and further investigated by several authors. Chapter 5 of the monograph [La] gives a quite complete picture of the role of fans in the context of fields, and contains many bibliographical references.

A further step was taken by Marshall, see [M], Ch. 3, who generalized the notion of a fan to the context of *abstract spaces of orderings* (AOS), an axiomatic framework extending the field case. In [Li] (see also [DM1], Ex. 1.7, pp. 8-9, and pp. 89-90) this notion was treated in the framework of *reduced special groups* (RSG), and its functorial duality with the corresponding notion of fan in the category of AOSs proved.

Fans surfaced again in [ABR], Chs. 3, 5, in the still more general context of *spaces of signs*, a framework equivalent to that of ARSs. However, the notion of a fan used in [ABR] (cf. Def. 3.12, p. 75) turns out to be essentially that of an AOS-fan suitably *embedded* in an ARS; see also [M], p. 162. Incidentally, the book [ABR] extensively witnesses the key role that fans play in real algebraic and real analytic geometry; see, e.g., [ABR], Thms. IV.7.3 and V.1.4 (the "generation formulae"), and [AR], pp. 1-7, where further references can be found.

However, *a sufficiently general and <u>intrinsic</u> notion of fan in the categories of ARSs and*

[1] In this paper referred to simply as *rings*.
[2] Namely, having a non-empty real spectrum or, equivalently, that -1 is not a sum of squares.
[3] See [ABR], p. 84, and [La], Notes on § 5, p. 48.

of RSs[4] *does not exist at present.* The aim of this paper is to fill this gap. The key leading to such a notion consists in bringing into play the (enriched) semigroup structures underlying the real semigroups, namely the *ternary semigroups* ([DMP], Def. 1.1, and [DP1], Def. 1.1, p. 100).

We start by briefly reviewing the definition of a fan in the (dual) categories **AOS** and **RSG** (for more details, see [M], Ch. 3; [Li], Ex. 1.1.6, pp. 30-31; [DM1], Ex. 1.7, pp. 8-9).

— A fan in the category **AOS** (henceforth called an **AOS-fan**) is an abstract space of orders (X, G) where "X is biggest possible"; there are two equivalent ways of making sense of this idea:

(1) X consists of all group homomorphisms $h : G \longrightarrow \{\pm 1\}$ such that $h(-1) = -1$.

(2) (X, G) is an AOS and X is closed under the product of any three of its members.

— A fan in the category **RSG** (henceforth an **RSG-fan**) is a reduced special group G whose binary representation relation is "smallest posible"; there is only one way of making sense of this:

[RSG-fan] $\qquad a \in D_G(b, c)$ iff either $b = -c$ or $(b \neq -c$ and $a \in \{b, c\})$.

Remarks 0.1 (a) While condition (1) above implies that (X, G) is an AOS, the last requirement in (2) alone is not sufficient to guarantee that (X, G) is an AOS; in addition, one must require that:

(i) X separates points in G, i.e., $\bigcap_{\sigma \in X} \ker(\sigma) = \{1\}$.

(ii) X verifies the following maximality condition (see [M], axiom [AX2] for AOSs, p. 22): for every group homomorphism $\sigma : G \longrightarrow \{\pm 1\}$, if $\sigma(-1) = -1$ and $a, b \in \ker(\sigma) \Rightarrow D_X(a, b) \subseteq \ker(\sigma)$, then $\sigma \in X$.

(b) The definition of binary representation given by condition [RSG-fan] above (together with $1 \neq -1$) implies that G is a RSG ([Li], Prop. 1.1.14, pp. 34-36). □

We define the notion of a fan in the category **ARS** of abstract real spectra by postulating the analogs of conditions (1) and (2) above, *upon replacing* the underlying notion of a group of exponent 2 with a distinguished element -1 *by that of a ternary semigroup* (abbreviated TS) and, of course, the target group $\{\pm 1\}$ by the ternary semigroup $\mathbf{3} = \{-1, 0, 1\}$:

Definition 0.2 Given a ternary semigroup G and a non-empty set $X \subseteq \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$[5],

(1) (X, G) is a **fan$_1$** iff X consists of <u>all</u> TS-homomorphisms from G to $\mathbf{3} = \{-1, 0, 1\}$, i.e., $X = \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$.

(2) (X, G) is a **fan$_2$** iff it is an ARS and X is closed under the product of <u>any three</u> of its members.

We shall frequently use in the sequel the following weaker notion to which we give a name:

(3) (X, G) is a **q-fan** (quasi-fan) iff X is closed under the product of any three of its members and X separates points in G, i.e., for every $a, b \in G$, $a \neq b$, there is $h \in X$ such that $h(a) \neq h(b)$. □

Remarks 0.3 (i) The set $\mathbf{3} = \{-1, 0, 1\}$ under obvious operations has a unique structure of TS. In fact, endowed with suitable ternary representation and transversal representation relations (cf. [DP1], Cor. 2.4, p. 109, or [DP2], Ex. 2.3 (3), p. 58) it has a *unique* structure of RS. It obviously is a fan$_1$.

[4] The categories of ARSs, RSs, AOSs, RSG's, under natural morphisms, will be denoted by boldfacing the corresponding acronyms.

[5] $\mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$ denotes the set of all TS-homomorphisms from the TS G into the TS $\mathbf{3}$.

(ii) In 0.2 (2) we allow products of type $h_1^2 h_2$; as opposed to the case of special groups, squaring a TS-homomorphism does not produce a map constantly equal to 1. Note also that $h^3 = h$, and that the product of any three TS-homomorphisms is again a TS-homomorphism.

(iii) An obvious example of q-fan over a TS, G, is $(\mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3}), G)$: $\mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$ is closed under product of any three members, and separates points in G by the separation theorem for TSs, [DP1], Thm. 1.9, pp. 103–104.

(iv) The notions fan_1 and fan_2 turn out to be equivalent (Corollary 2.4). □

As for the dual category **RS**, we shall prove that, under a suitable necessary condition, q-fans automatically produce real semigroups where both binary representation relations D^t and D are smallest possible (Theorem 2.1) .

1 Some basic definitions and preliminary remarks.

Reminder. The set $\mathrm{Hom}_{\mathrm{TS}}(T, \mathbf{3}) = X_T$ of all **TS-characters**, cf. footnote 5, is endowed with a natural spectral topology, introduced in [DMP], § 1.5 (b). [6]

We register the following simple facts, which play an essential role throughout this paper.

Lemma 1.1 (Characterization of the specialization partial order in X_T.)
Let T be a TS, and let $g, h \in X_T$. The following are equivalent:
(1) $g \rightsquigarrow h$ *(i.e., h is an specialization of g).*
(2) $h^{-1}[1] \subseteq g^{-1}[1]$ *(equivalently,* $h^{-1}[-1] \subseteq g^{-1}[-1]$*).*
(3) $g^{-1}[\{0,1\}] \subseteq h^{-1}[\{0,1\}]$.
(4) $Z(g) \subseteq Z(h)$ *and* $\forall\, a \in G\, (a \notin Z(h) \;\Rightarrow\; g(a) = h(a))$.
(5) $h = h^2 g$ *(equivalently,* $h^2 = hg$*).* □

Fact 1.2 *Let G be a ternary semigroup, let $X \subseteq \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$, and assume that (X, G) is a q-fan. A necessary condition for (X, G) to be an ARS is that for all $a, b \in G$, either $Z(a) \subseteq Z(b)$ or $Z(b) \subseteq Z(a)$. Here, $Z(a) = \{h \in X \mid h(a) = 0\}$.* □

The following result gives alternative characterizations of the necessary condition in 1.2.

Proposition 1.3 *Let T be a ternary semigroup. The following conditions are equivalent:*
(1) *The family $\{Z(a) \mid a \in T\}$ is totally ordered under inclusion.*
(2) *For all $a, b \in T$, either $a^2b^2 = a^2$ or $a^2b^2 = b^2$.*
(3) *Every proper ideal of T is prime (i.e., $ab \in I \Rightarrow a \in I$ or $b \in I$).*
(4) *The set of ideals of T is totally ordered under inclusion.* □

The representation partial order of a real semigroup.

In a reduced special group, G, the binary relation $a \leq b \Leftrightarrow a \in D_G(1, b)$ is a partial order for which the operation "multiplication by -1" is an involution. Further, this relation is induced from the partial order of the Boolean hull of G ([DM1], Cor. 4.4 (c), p. 62 and Cor. 4.12, p. 69).

In the context of RS's, none of the binary relations $a \in D(1, b)$ or $a \in D^t(1, b)$ defines a partial order for which the operation "$-$" (multiplication by -1) is an involution.

However, since every RS, G, is canonically embedded in a Post algebra (seen as a RS, its "Post hull" ([DP2], Prop. 4.1, p. 62), which is a distributive lattice, the latter induces a partial order on G given by:

[6] As a reference for spectral spaces we use [DST].

Definition 1.4 ([DP2], Rmk. 2.5, p. 59) Let G be a RS, and let $a, b \in G$. We set:

$$a \leq_G b \quad \text{iff} \quad a \in D_G(1, b) \text{ and } -b \in D_G(1, -a).$$

$\leq_G$ is called the **representation partial order** of G. [Unless necessary we omit the subscript in $\leq_G$.] □

When $G = \mathbf{3}$ this definition gives $1 <_{\mathbf{3}} 0 <_{\mathbf{3}} -1$, the opposite of the order of these elements as integers.

The following theorem summarizes the most important properties of the partial order $\leq_G$:

Theorem 1.5 ([DP4], Prop. I.6.4 et I.6.5.) *Let G be a RS. For $a, b, x, y \in G$ we have:*

(1) *The relation $\leq$ is a partial order on G such that $a \leq b \Leftrightarrow -b \leq -a$.*

(2) *For all $a \in G$, $1 \leq a \leq -1$.*

(3) $a \leq 0 \Leftrightarrow a = a^2 \in \mathrm{Id}(G)$,[7]
$0 \leq a \Leftrightarrow a = -a^2 \in -\mathrm{Id}(G)$.

(4) *Let X_G be the character space of G. For $a, b \in G$,*

$$\begin{aligned} a \leq_G b \quad &\Leftrightarrow \quad \forall h \in X_G \ (h(a) \leq_{\mathbf{3}} h(b)) \quad \Leftrightarrow \\ &\Leftrightarrow \quad \forall h \in X_G \ [(h(b) = 1 \Rightarrow h(a) = 1) \wedge (h(b) = 0 \Rightarrow h(a) \in \{0, 1\})]. \end{aligned}$$

(5) *The following are equivalent:*
(i) $a^2 \leq b \leq -a^2$; (ii) $Z(a) \subseteq Z(b)$; (iii) $b = a^2 b$.

In particular,

(6) $a^2 \leq ab \leq -a^2$ *(hence* $a^2 \leq \pm a \leq -a^2$*).*

(7) *If* $a^2 \leq b \leq -a^2$ *and* b *is invertible, then* a *is invertible.*

(8) $a \leq x, y \Rightarrow a \leq -xy$. *Hence,* $x, y \leq a \Rightarrow xy \leq a$.

(9) *For all $a \in G$, the infimum and the supremum of a and $-a$ for the representation partial order $\leq$ exist, and $a \wedge -a = a^2$, $a \vee -a = -a^2$. In particular,*

(10) $a \wedge -a \leq 0 \leq b \vee -b$ *for all* $a, b \in G$.[8] □

The following notion will be of constant use in the sequel:

Definition 1.6 (Saturation) A subset S of a RS, G, is called **saturated** iff for every pair a, b of elements of G, $a, b \in S \Rightarrow D_G(a, b) \subseteq S$. □

2 The main results and some consequences.

The first order of business is to work out the explicit form of the representation relations corresponding to the notion of "q-fan". Given $X \subseteq \mathbf{3}^G$, ternary relations D_X and D^t_X are defined by the following clauses: for $a, b, c \in G$,

[R] $a \in D_X(b, c)$ iff $\forall h \in X\, [h(a) = 0 \vee (h(a) \neq 0 \ \wedge (h(a) = h(b) \vee h(a) = h(c)))]$.

[TR] $a \in D^t_X(b, c)$ iff $\forall h \in X\, [(h(a) = 0 \wedge h(b) = -h(c)) \vee (h(a) \neq 0 \ \wedge$
$\wedge\, (h(a) = h(b) \vee h(a) = h(c)))]$.

(See [M], § 6.1, p. 99.)

---

[7] $\mathrm{Id}(G) = \{a^2 \mid a \in G\}$ is the set of *idempotents* of G.

[8] Called the *Kleene inequality*; cf. [DP2], Rmk. 1.2 (b), p. 55.

A. Main theorems.

Theorem 2.1 *Let G be a ternary semigroup verifying*
[Z] $\forall a, b \in G\,(a^2b^2 = a^2$ *or* $a^2b^2 = b^2)$.
Let $X \subseteq \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$ be such that $(X, G) \models$ q-fan. With $D = D_X$ and $D^t = D^t_X$ denoting the representation relations defined by [R] and [TR] above, for $a, b \in G$ we have:

$$[D^t] \quad D^t(a,b) = \begin{cases} \{a\} & \text{if } a^2b^2 = b^2 \text{ and } a^2b^2 \neq a^2 \\ \{b\} & \text{if } a^2b^2 = a^2 \text{ and } a^2b^2 \neq b^2 \\ \{a,b\} & \text{if } a^2 = b^2 \text{ and } b \neq -a \\ \{a^2x \mid x \in G\} & \text{if } b = -a. \end{cases}$$

[D] $\quad D(a,b) = a \cdot \mathrm{Id}(G) \cup b \cdot \mathrm{Id}(G) \cup \{x \in G \mid xa = -xb \wedge x = a^2x\}$. □

Theorem 2.2 *Let G be a ternary semigroup verifying condition [Z] of Theorem* 2.1. *Then, conditions [D] and $[D^t]$ in* 2.1 *are interdefinable in the following sense:*

(1) *Assuming that a ternary relation D on G is defined as in [D] and the corresponding transversal representation is given by the clause*

$$a \in D^t(b,c) \Leftrightarrow a \in D(b,c) \wedge -b \in D(-a,c) \wedge -c \in D(b,-a),$$

then D^t verifies condition $[D^t]$ of 2.1.

(2) *Conversely, if D^t is defined as in $[D^t]$ and the associated ternary representation relation D is defined by the stipulation $a \in D(b,c) \Leftrightarrow a \in D^t(a^2b, a^2c)$, then D verifies clause [D] of* 2.1.□

Theorem 2.3 *Let G be a ternary semigroup verifying condition [Z] of Theorem 2.1. With the ternary relation D defined as in* 2.1, *(G, D) is a real semigroup.* □

The proof of these results is long and delicate but they are very fruitful.

B. Some consequences.

Corollary 2.4 *Let G be a TS verifying condition [Z] of Theorem* 2.1 *and let $X \subseteq \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$. The following are equivalent:*

(1) $(X, G) \models \mathrm{fan}_1$ (*i.e.*, $X = \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$).

(2) *(X, G) is a q-fan and verifies: for every subsemigroup S of G such that $S \cup -S = G$ and $S \cap -S$ is a (proper) prime ideal, there is $h \in X$ such that $S = h^{-1}[0, 1]$.*

(3) $(X, G) \models \mathrm{fan}_2$. □

Definition and Notation 2.5 (Fan) Henceforth we call **ARS-fan** either of the equivalent notions $\mathbf{fan}_1$ or $\mathbf{fan}_2$. In using the notation "$(X, G) \models$ ARS-fan" we implicitly assume that the underlying ternary semigroup G verifies condition [Z] in Theorem 2.1; this assumption is crucial and, in fact, distinguishes fans from most other classes of ARSs. We shall also say "G is a **RS-fan**", tacitly assuming that its representation relations are those given in Theorem 2.1. If the category under use is clear from context, we may simply write **fan** instead of **ARS**-fan or **RS**-fan. □

Corollary 2.6 *Let G be a TS verifying condition [Z] of Theorem 2.1. Let H be a real semigroup, and let $f : G \longrightarrow H$ be a homomorphism of ternary semigroups. Then, f preserves the representation relation D defined by clause [D] of* 2.1, *and hence it is a RS-homomorphism from (G, D) into H. In other words,* $\mathrm{Hom}_{\mathrm{RS}}((G, D), H) = \mathrm{Hom}_{\mathrm{TS}}(G, H)$. □

In particular we have:

Corollary 2.7 *Let G be a TS verifying condition $[Z]$ of Theorem 2.1. Then,*

(1) $\mathrm{Hom}_{\mathrm{RS}}((G, D), \mathbf{3}) = \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$.

Hence,

(2) *The ARS dual to the real semigroup (G, D) is $(\mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3}), \overline{G})$.*[9]

(3) $(\mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3}), \overline{G})$ *is a* fan_1 *(hence an ARS-fan, see 2.5).*

(4) (G, D) *is a RS-fan.* □

Corollary 2.8 *Let (G, D) be a RS-fan. Then, the set $G^\times = \{a \in G \,|\, a^2 = 1\}$ of invertible elements of G with representation induced by restriction of D to $G^\times$, is a RSG-fan, i.e., a fan in the category of reduced special groups.* □

Corollary 2.9 *Let G be a TS verifying condition $[Z]$ of Theorem 2.1 and let D be the ternary relation on G defined by clause $[D]$ therein. Then,*

(1) *Every TS-ideal of G is a saturated prime ideal of the real semigroup (G, D) (cf. 1.6).*

(2) *A TS-subsemigroup S of G is saturated in (G, D) iff it contains* $\mathrm{Id}(G) = \{x^2 \,|\, x \in G\}$ *and $S \cap -S$ is an ideal.* □

C. Characterisation of q-fans.

It is easy to give examples of q-fans that are not fans. The following theorem gives a topological characterization of q-fans.

Theorem 2.10 *Let G be a ternary semigroup and let $X \subseteq X_G = \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$ be a non-empty set of TS-characters closed under product of any three of its members. Then,*

$$(X, G) \text{ is a q-fan } \Leftrightarrow X \text{ is dense for the constructible topology of } X_G.$$

In particular, if X is proconstructible, i.e., closed in the constructible topology, then $X = X_G$, and hence (X, G) is a fan. □

3 Examples.

With the aim of illustrating the notions introduced above, we present in this section some examples of (alas, finite) fans based on ternary semigroups with up to three generators. For each example we shall draw both the root-system of an ARS-fan ordered under specialization and the representation partial order of its dual real semigroup.

We already know that $\mathbf{3}$ is a fan. Recall that condition $[Z]$ in Theorem 2.1, $\forall ab\,(a^2b^2 \in \{a^2, b^2\})$, is necessary to obtain a fan. With this condition fulfilled, the representation relations defined in 2.1 turn the underlying ternary semigroup into an RS-fan (2.3 and 2.5).

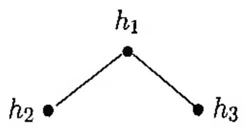
Example A. Ternary semigroups on one generator.

Call x the generator. We treat first the case where there are no additional relations ("free" case). The corresponding TS is:

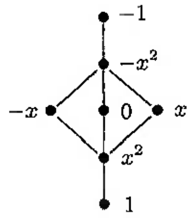
$$F_1 = \{1, 0, -1, x, -x, x^2, -x^2\}.$$

The necessary condition [Z] is trivially verified. Characters are determined by their value on x, and any value 1, 0 and -1 is possible; hence the dual ARS, X_{F_1}, consists of three characters given by: $h_1(x) = 0$, $h_2(x) = 1$, $h_3(x) = -1$. Clearly, $h_1 = h_1^2 \cdot h_i$, whence $h_i \rightsquigarrow h_1$, for $i = 2, 3$ (Lemma 1.1). So we get the specialization root-system below left.

[9] Recall that $\overline{G} = \{\overline{a} \,|\, a \in G\}$, where $\overline{a} \in \mathbf{3}^{\mathrm{Hom_{TS}}(G,\mathbf{3})}$ is the map "evaluation at a": for $\sigma \in \mathrm{Hom}_{\mathrm{TS}}(G, \mathbf{3})$, $\overline{a}(\sigma) := \sigma(a)$.



Specialization root-system of X_{F_1}



Representation partial order of F_1

Figure 1

The representation partial order of the real semigroup F_1 —illustrated in Figure 1, right— is computed straightforwardly from Theorem 1.5 (4).

Remark. Barring the case where the generator x becomes invertible (i.e., $x^2 = 1$, which gives a four element RSG-fan with an added 0), the only possible additional relation is $x^2 = x$, which eliminates the character h_3. Thus, we get the following diagrams for the specialization order (left) and the representation order (right):

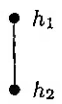


Figure 2

A more interesting example is:

Example B. Ternary semigroups on three generators.

Generators: x, y, z. Condition [Z] gives raise to the following possible relations:

1. $x^2 = y^2 = z^2$. ([Z] is automatically verified in this case.)

2. $x^2 = y^2 \neq z^2$ and $x^2z^2 = y^2z^2 \in \{x^2, z^2\}$.

The two identities obtained from the last clause give raise to non-isomorphic cases, and, upon permutation, all cases where two of the three generators have equal squares (i.e., equal zero-sets) are isomorphic to these.

3. x^2, y^2, z^2 are different, and $x^2y^2 \in \{x^2, y^2\}$, $x^2z^2 \in \{x^2, z^2\}$, $y^2z^2 \in \{y^2, z^2\}$.

A case-by-case analysis of all eight combinations of these values shows that, up to isomorphism by permutation, the only surviving case is $x^2y^2 = x^2z^2 = x^2$ and $y^2z^2 = y^2$.

As an illustration we analyze the following configuration:

(a) $x^2 = y^2 \neq z^2$ and $x^2z^2 = y^2z^2 = x^2$.

This amounts to $Z(z) \subset Z(x) = Z(y)$. We focus on two alternatives:

i) No relations other than the above.

Routine checking shows that the following are all possible characters:

— h_1 sends all three generators to 0;

— h_2, h_3 send x, y to 0 and, say, $h_2(z) = 1$, $h_3(z) = -1$;

— $h_4, \ldots, h_{11}$ assign to the generators all possible combinations of values ± 1, with, say, $h_4, \ldots, h_7$ sending z to 1, and $h_8, \ldots, h_{11}$ sending z to -1.

Call F_2 the TS corresponding to this case. Using Lemma 1.1 one sees at once that the specialization root-system of the ARS dual to F_2 looks as in Figure 3.

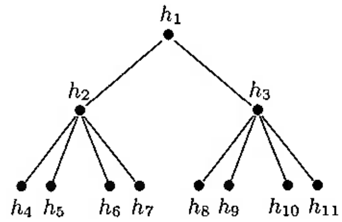


Figure 3. Specialization root-system of X_{F_2}

Since X_{F_2} has 11 elements, we must have $\mathrm{card}\,(F_2) = 23$ [10] the reader is invited to check that:

$$F_2 = \{1, 0, -1, x, -x, y, -y, z, -z, x^2, -x^2, z^2, -z^2, xy, -xy, xz, -xz, yz, -yz, x^2z, -x^2z, xyz, -xyz\}.$$

The Hasse diagram of the representation partial order of F_2 is drawn in Figure 4.

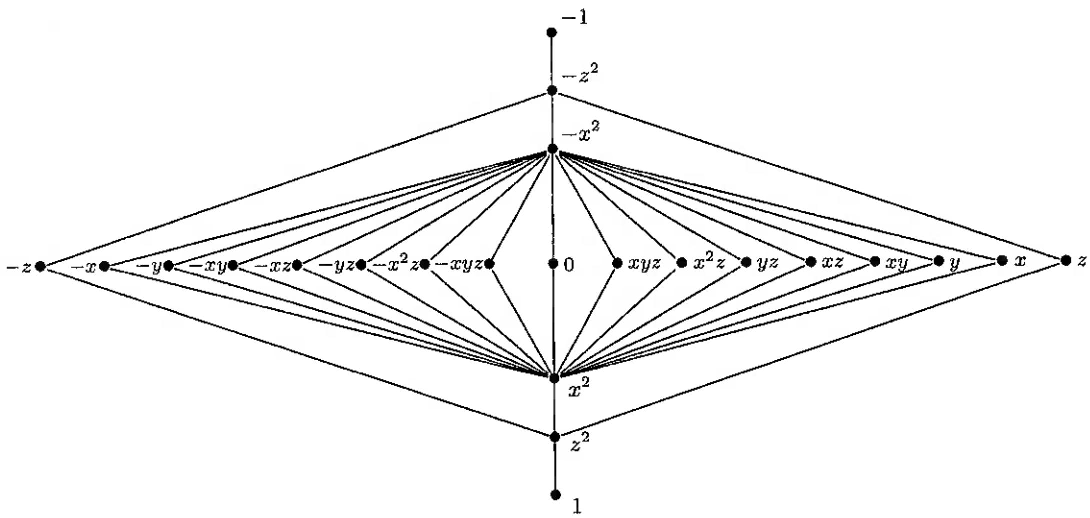


Figure 4. Representation partial order of F_2.

Theorem 1.5 is used in the computation of this diagram.

One may also consider fans arising by adding relations between generators; as an example we describe the fan obtained from the preceding one by adding:

ii) <u>The relations $xz = x$ and $z^2 = 1$.</u>

The additional relation $z^2 = 1$ makes z invertible and hence excludes the character h_1 sending z to 0. This makes the characters h_2, h_3 to become "disconnected"; we obtain a "two-component" root-system:

[10] For finite RS-fans, F, one has $\mathrm{card}(F) = 2{\cdot}\mathrm{card}(X_F) + 1$; this is proved employing the tools described in § 7 below.

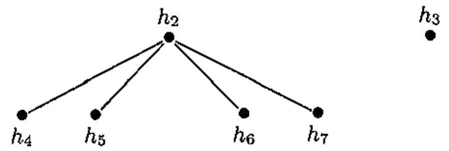


Figure 5. Specialization root-system of X_{F_4}

The dual RS-fan is: $F_4 = \{1, 0, -1, x, -x, y, -y, z, -z, x^2, -x^2, xy, -xy\}$, with the representation partial order:

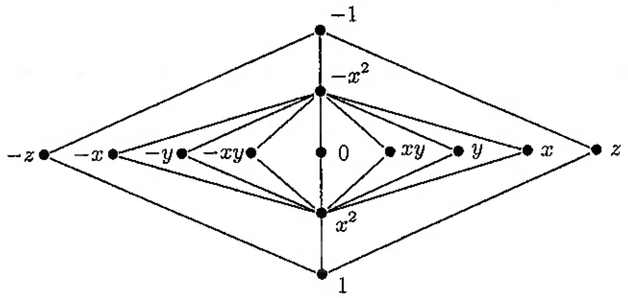
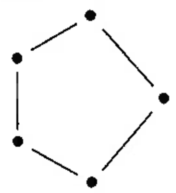


Figure 6. Representation partial order of F_4

A common feature of these examples is that, under the representation partial order $\leq$ every RS-fan is a bounded lattice:

Theorem 3.1 *Let F be a RS-fan and let $\leq$ denote its representation partial order* (1.4). *Then, $(F, \leq)$ is a lattice with smallest element* 1 *and largest element* -1. □

Remarks 3.2 (a) A closer look at the examples presented above shows that the lattices $(F, \leq)$ are not modular —hence not distributive either— except in very special cases. In fact, most of these lattices contain the configuration



as a sublattice (cf. [B], Ch. V, § 2, Thm. 2, p. 66). For instance, in Figures 4 and 6 above, the sublattices $\{z^2 < x^2 < -x^2 < -z^2; z\}$ and $\{1 < x^2 < -x^2 < 1; z\}$, respectively, form such a pentagon. Example 3. A is modular but not distributive. Note that a RSG-fan (i.e., a reduced special group that is a fan, cf. [RSG-fan], Introduction) *is a modular lattice* under the order $a \leq b \Leftrightarrow a \in D(1, b)$.

(b) Since $\mathrm{Id}(F) \cup -\mathrm{Id}(F)$ is a totally ordered subset of $(F, \leq)$, the proof of Theorem 3.1 shows that the lattice operations in $(F, \leq)$ satisfy the following identities:

$$a \wedge b = \begin{cases} \min_{\leq}\{a^2, b^2\} & \text{if } a \perp b \\ \min_{\leq}\{a, b\} & \text{if } a, b \text{ are } \leq\text{-comparable,} \end{cases}$$

and

$$a \vee b = \begin{cases} \max_{\leq}\{-a^2, -b^2\} & \text{if } a \perp b \\ \max_{\leq}\{a, b\} & \text{if } a, b \text{ are } \leq\text{-comparable.} \end{cases}$$

Note that, if $a \perp b$, then $a \wedge b$, $a \vee b \in \mathrm{Id}(F) \cup -\mathrm{Id}(F)$.

(c) The operation $x \mapsto -x$ $(x \in F)$ *is not* a complement in the lattice-theoretic sense, but it verifies:

— The Kleene inequality $a \wedge -a \leq 0 \leq b \vee -b$. (A special case of Theorem 1.5 (10).)

— The De Morgan laws. □

4 Quotients of fans

A. Reminder. Congruences of ternary semigroups and of real semigroups.

Definition 4.1 A congruence of ternary semigroups (abbreviated **TS-congruence**) is an equivalence relation $\equiv$ on a TS, G, compatible with the semigroup operation and such that the induced quotient structure $G/\equiv$ is a ternary semigroup. [This is equivalent to require $\equiv$ to be proper, i.e. $\equiv \subset G \times G$, and for $x \in G$, $\;x \equiv -x \;\Rightarrow\; x \equiv 0$.] □

Remarks 4.2 (a) Since the axioms for TSs are universal, the quotient map $\pi_{\equiv} : G \longrightarrow G/\equiv$ is automatically a TS-homomorphism.

(b) For each non-empty set $\mathcal{H} \subseteq X_G$, the relation

$(\dagger)_{\mathcal{H}}$ $\qquad a \equiv_{\mathcal{H}} b \;\Leftrightarrow\;$ For all $h \in \mathcal{H}$, $h(a) = h(b)$, $\;(a, b \in G)$,

defines a TS-congruence of G (straightforward checking). We shall write $G/\mathcal{H}$ for the quotient TS $G/\equiv_{\mathcal{H}}$. □

Definition 4.3 A **(RS-)congruence** of a real semigroup G is an equivalence relation $\equiv$ satisfying the following requirements:

(i) $\equiv$ is a congruence of ternary semigroups (4.1).

(ii) There is a ternary relation $D_{G/\equiv}$ in the quotient *ternary semigroup* $(G/\equiv, \cdot, -1, 0, 1)$ so that $(G/\equiv, \cdot, D_{G/\equiv}, -1, 0, 1)$ is a real semigroup, and the canonical projection $\pi : G \longrightarrow G/\equiv$ is a RS-morphism.

(iii) (Factoring through π.) For every RS-morphism $f : G \longrightarrow H$ into a real semigroup H such that $a \equiv b$ implies $f(a) = f(b)$ for all $a, b \in G$, there exists a RS-morphism (necessarily unique), $\widehat{f} : G/\equiv \longrightarrow H$, such that $\widehat{f} \circ \pi = f$, i.e. the following diagram commutes

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \nearrow_{\widehat{f}} & \\ G/\equiv & & \end{array}$$

Remark 4.4 With notation as in 4.2, if G is a RS, we define a ternary relation $D_{G/\mathcal{H}}$ on $G/\mathcal{H}$ as follows: for $a, b, c \in G$,

$(\dagger\dagger)_{\mathcal{H}}$ $\qquad \pi(a) \in D_{G/\mathcal{H}}(\pi(b), \pi(c)) \;\Leftrightarrow\;$ For all $h \in \mathcal{H}$, $h(a) \in D_3(h(b), h(c))$.

Obviously $D_{G/\mathcal{H}}$ is well-defined and it can be proved that every RS-congruence of real semigroups is obtained in this way. □

B. Congruences of fans. The main result concerning congruences of RS-fans is:

Proposition 4.5 *Let F be a RS-fan and let $\mathcal{H}$ be a non-empty proconstructible subset of X_F which is 3-closed (i.e., stable under product of any three of its elements). Then the quotient $F/\mathcal{H}$ is a RS-fan (and $\equiv_{\mathcal{H}}$ is a RS-congruence).* □

In fact, all RS-congruences of a fan are obtained in the way given by the preceding Proposition:

Corollary 4.6 *Let F be a RS-fan and let $\equiv$ be a RS-congruence of F. Then:*

(a) $\equiv\, = \,\equiv_{\mathcal{H}}$ for some proconstructible, 3-closed set $\mathcal{H} \subseteq X_F$. Hence,

(b) $F/\!\equiv$ is a RS-fan.

(c) The correspondence $\mathcal{H} \longmapsto \equiv_{\mathcal{H}}$ establishes an inclusion-reversing bijection between proconstructible 3-closed subsets of X_F and the set of RS-congruences of F. □

Remark. Quotients of fans have a much stronger property called *transversal 2-regularity*, introduced and studied in [DP4], Ch. III, § 3, and proved for fans in [DP4], Thm. VI.11.3. □

C. Quotients modulo ideals. As a last point in this section we address the special case of quotients of RS-fans modulo ideals. Amongst the outstanding cases of congruences of a RS ([DP4], Ch. II, § 3, [M], §§ 6.5, 6.6) one considers those determined by saturated prime ideals.

A saturated prime I ideal of a RS, G, cf. 1.6, determines the set of characters $\mathcal{H}_I := \{h \in X_G \mid Z(h) = I\}$. The congruence $\equiv_{\mathcal{H}_I}$ induced by $\mathcal{H}_I$ will be denoted by $\sim_I$, and the corresponding quotient set by G/I.[11] In [DP4], Thm. II.3.15, we characterize the congruence $\sim_I$ and both representation relations of G/I solely in terms of the data carried by G. We also prove that the representation relation $D_{G/I}$ induces on the set $G_I := (G/I) \setminus \{\pi(0)\}$, obtained from G/I by omitting zero, the structure of a *reduced special group*. The proof of these results for arbitrary RSs is rather lengthy; however, in the special case of RS-fans this follows from Proposition 4.5. Recall (2.9) that the ideals of a RS-fan are automatically prime and saturated.

The following Lemma is used in the proof and elsewhere in this paper:

Lemma 4.7 *Let I be an ideal of a RS-fan F. Then, for $a, b \in F \setminus I$:*

$$a \sim_I b \Leftrightarrow \exists z \notin I\,(az = bz).$$ □

Proposition 4.8 *Let F be a RS-fan. Let I be a proper ideal of F. Let $\pi = \pi_I : F \longrightarrow F/I$ denote the canonical quotient map. Then, $F_I = (F/I) \setminus \{\pi(0)\}$ is a RSG-fan.* □

5 Characterizations of fans

The main result of this section is the following characterization of RS-fans:

Theorem 5.1 *For a real semigroup G, the following are equivalent:*

(1) G is a RS-fan.

(2) G satisfies the following conditions:

(i) $\forall a, b \in G\,(a^2b^2 = a^2$ or $a^2b^2 = b^2)$.

(ii) Given $g, h \in X_G$ such that $Z(g) \subseteq Z(h)$, there is $h' \in X_G$ such that $Z(h) = Z(h')$ and $g \rightsquigarrow h'$.

(iii) For every saturated prime ideal I of G, the quotient reduced special group (G_I, D_{G_I}) is a RSG-fan. □

The proof of (2) $\Rightarrow$ (1) is rather delicate.

Remarks. (a) There are examples satisfying conditions (2.i) and (2.iii) of Theorem 5.1 but not condition (2.ii).

[11] Quotients of this type have been considered by Marshall in the dual category of abstract real spectra; cf. [M], p. 102 and Cor. 6.6.9.

(b) The real semigroup $G_{C(X)}$ associated to the ring $C(X)$ of continuous, real-valued functions on a topological space X satisfies conditions (2.ii) and (2.iii) of Theorem 5.1 but, in general, not (2.i); cf. [M], 5.2 (6), p. 87. □

The next two corollaries of Theorem 5.1 give stylized (abstract) versions of the notion of a *trivial fan*, a basic concept in the theory of (pre-)orders on fields (see [La], Prop. 5.3, p. 39). Their translation in the case of preordered rings is given in Theorem 6.10 below, where it will be obvious that in the case of fields they boil down to the notion of a trivial fan.

Corollary 5.2 *Let G be a real semigroup such that the character space X_G is totally ordered under specialization. Then, G is a RS-fan.* □

Corollary 5.3 *Let G be a real semigroup satisfying the following requirements:*
(1) *Condition* [Z] *in* 2.1.
(2) *The character space X_G of G is the union of two maximal specialization chains, $\mathcal{C}_0, \mathcal{C}_1$.*
(3) *For every saturated prime ideal I of G and for $i = 0, 1$, there is $h_i \in \mathcal{C}_i$ such that $Z(h_i) = I$.*
Then, G is a RS-fan. □

Remark. The specialization chains in item (2) may not be disjoint, and the characters h_0, h_1 in (3) may be identical.

Remark 5.4 (Chain length) There is a well-known characterization of fans in the categories **AOS** and **RSG** in terms of *chain length*, i.e., the size of longest strict inclusion chain of non-empty subbasic opens $[\![a = 1]\!]$ of X_G $(a \in G)$, cf. [DMP] 1.5 (b.2): an AOS is a fan if and only if its chain length is ≤ 2, see [ABR], Prop. 3.11, p. 74, or [M], Thm. 4.2.1 (2), p. 65. This notion of chain length also makes sense for ARSs, cf. [M], p. 167. However, this characterization is no longer valid for ARS-fans or RS-fans; an easy computation shows that the RS-fan F_2 in Example 3. B.(i), see Figure 4, has chain length 4. The integer $2 \cdot \mathrm{card}(\mathrm{Spec}(F))$ is an upper bound on chain length of a RS-fan, F, with a finite spectrum (7.1 (b.i)); this is easily proved using Theorem 5.1; see also [M], Thm. 8.5.3, p. 167. □

6 Fans and preordered rings

A natural question in the context of this paper is that of characterizing those preordered rings (**p-rings**)$\langle A, T\rangle$ whose associated RS, $G_{A,T}$, is a RS-fan. At present we are far from being able to offer a satisfactory answer. So, we only comment on some partial results and examples.

A. Extending to rings the Becker-Köpping definition of a fan. Recall, [La], Def. 5.1, p. 39, that a preorder T of a field K is called a **fan** iff for every set $S \supseteq T$ such that $-1 \notin S$ and $S^\times = S \setminus \{0\}$ is a subgroup of $K^\times$ of index 2, S is closed under addition (i.e., S is an order of F). This is the original definition of fans in fields, due to Becker and Köpping, [BK]; many equivalent characterizations exist in the field case, cf. [La], Ch. 5.

In § 6 of [DP5] we extend this definition to the world of preordered rings by imposing suitable requirements on the set S; namely, conditions that embody the notion of a TS-character of the ternary semigroup $G_{A,T}$. We omit detais but mention the following:

Corollary 6.1 *Let K be a field and T be a preorder of K which is a fan. Let A be a subring of K whose field of fractions is K. Then, the real semigroup $G_{A,T \cap A}$ is a fan. In particular, if $A = A_v$ is the valuation ring of a T-compatible valuation v of K, the real semigroup $G_{A_v, T \cap A_v}$ is a fan.* □

B. Total preorders and trivial fans in rings.

Notation 6.2 Let $\langle A, T\rangle$ be a p-ring.

(i) Recall ([BCR], Def. 4.2.3, p. 87) that an ideal I of A is called **T-convex** iff for all $t_1, t_2 \in T, t_1 + t_2 \in I \Rightarrow t_1, t_2 \in I$.

(ii) For a T-convex prime ideal I of A, we let

- A_I denote the localization of A at I,
- $M_I = I \cdot A_I$ denote the maximal ideal of A_I, and
- $T_I = T \cdot (A \setminus I)^{-2}$ denote the preorder induced by T on A_I,

and recall:

Fact. T_I/M_I is a proper preorder of the field A_I/M_I. □

Definition 6.3 A **total preorder** in a ring A is a (proper) preorder T such that $T \cup -T = A$. □

Fact 6.4 *For a total preorder T of a ring A, $T \cap -T$ is a proper T-convex ideal of A. Any T-convex ideal of A contains $T \cap -T$.* □

Remarks 6.5 (i) The ideal $T \cap -T$ *may not* be prime (see Example 6.6). When it is, the notion of "total preorder" coincides with "prime cone", i.e., element of Sper(A).

(ii) When $T \cap -T = \{0\}$ the total preorders are just the total orders of A. □

Example 6.6 Let $A := \mathbb{R}[X]/(X^2)$; the elements of A are uniquely representable in the form $aX + b$ with $a, b \in \mathbb{R}$. Clearly, the zero ideal of A is not radical, hence not prime either: $X \neq 0$ but $X^2 = 0$. We define a total (pre)order T in A by the stipulation:

$$aX + b \in T \text{ iff } b > 0 \text{ or } (b = 0 \text{ and } a \geq 0).$$

Checking that T is a total (pre)order of A is routine, left to the reader. However, the ideal $T \cap -T = \{0\}$ is not prime. □

We register that total preorders are preserved by localization at, and lifting by convex prime ideals.

Proposition 6.7 *Let T be a total preorder of a ring A, let I be a T-convex prime ideal of A, and let $T_I = T \cdot (A \setminus I)^{-2}$ be the preorder induced by T on the localization of A at I. Then, T_I is a total preorder of A_I.* □

Proposition 6.8 *Let I be a prime ideal of a ring A and let Q be a total preorder of A_I. With $\iota_I : A \longrightarrow A_I$ denoting the canonical map $a \mapsto \frac{a}{1}$ $(a \in A)$, we have:*

(i) $T := \iota_I^{-1}[Q]$ *is a total preorder of A.*

(ii) $T_I = Q$.

(iii) If the maximal ideal M_I of A_I is Q-convex, then I is T-convex. □

Remark 6.9 Even if Q is a total <u>order</u> of A_I, T *may not* be a total order of A. In fact,

$$T \cap -T = \iota_I^{-1}[Q \cap -Q] = \iota_I^{-1}[0],$$

which, in general is not $\{0\}$. Note that, for $x \in A$,

$$x \in \iota_I^{-1}[0] \Leftrightarrow \iota_I(x) = 0 \text{ (in } A_I) \Leftrightarrow \exists z \notin I\, (zx = 0);$$

in particular, x is a zero-divisor. Thus, T <u>is</u> a total order when A is an integral domain. □

The following result exhibits two outstanding examples in which total preorders in a p-ring give rise to fans in the associated RS.

Theorem 6.10 *(i) Let T be a total preorder of a ring A. Then, the real semigroup $G_{A,T}$ is a fan.*

(ii) Let T_0, T_1 be total preorders of a ring A, and let $T = T_0 \cap T_1$. Assume that the set of T-convex prime ideals of A is totally ordered under inclusion. Then, the real semigroup $G_{A,T}$ is a fan. □

Remark 6.11 (i) In case the ring A is a field, K, a total preorder is just a (total) order of K. Thus, Theorem 6.10 is a ring-theoretic analog of the well-known fact that the intersection of at most two total orders of a field is a fan, namely the *trivial fans*, cf. [La], Prop. 5.3, p. 39. □

(ii) The following example shows that the requirement in item (ii) of Theorem 6.10 does not hold automatically. Let $A = C(\mathbb{R})$ be the ring of real-valued continuous functions on the reals. For $i = 0, 1$, let $T_i = \{f \in A \mid f(i) \geq 0\}$ and $M_i = \{f \in A \mid f(i) = 0\}$. The (maximal) ideal M_i is T_i-convex; hence, with $T = T_0 \cap T_1$, both M_0 and M_1 are T-convex; however, M_0 and M_1 are incomparable under inclusion. □

7 Involutions of ARS-fans

A. Levels of a ARS-fan

The saturated prime ideals of a real semigroup induce a partition of its character space. The pieces are called *levels*: the level corresponding to a saturated prime ideal I of G is the set $L_I(G)$ of all $g \in X_G$ such that $Z(g) = I$; i.e., with the notation of § 4.C, $L_I(G) = \mathcal{H}_I$. In the case of RS-fans, (proper) ideals —automatically prime (1.3) and saturated (2.9)— are totally ordered under inclusion, a fact that of much help in studying the relationship between its levels.

Notation 7.1 (a) With notation as in § 4.C, every character $h \in \mathcal{H}_I$ induces a map $\widehat{h} : G_I \longrightarrow \{\pm 1\}$ defined by $\widehat{h} \circ \pi_I = h$. The correspondence $h \mapsto \widehat{h}$ is a bijection between the set $L_I(G) = \mathcal{H}_I$ of **I-th levels** and the space of orders X_{G_I} of the reduced special group G_I. Thus, we can identify the set $L_I(G) \subseteq X_G$ with the AOS (X_{G_I}, G_I). We shall systematically use this identification in the sequel, and unambiguously refer to the <u>AOS structure</u> of the set $L_I(G)$. In case G is a RS-fan, Proposition 4.8 shows that $L_I(G)$ is an <u>AOS-fan</u>.

(b) Let F be a RS-fan. We denote by Spec (F) the set of all (necessarily prime (1.3 (3)) and saturated (2.9)) proper ideals of F.

(c) (AOS- and ARS-morphisms; [M], § 2, pp. 23-24, and § 6, p. 103)

(i) Let $(X, G), (Y, H)$ be ARS's. A map $F : X \longrightarrow Y$ is an **ARS-morphism** iff for all $a \in H$ there is $b \in G$ so that $\widehat{a} \circ F = \widehat{b}$. Here, for $x \in G$, $\widehat{x} : X \longrightarrow \mathbf{3}$ denotes the map "evaluation at x": $\widehat{x}(\sigma) := \sigma(x)$, for $\sigma \in X$, and similarly for H.

(ii) The definition of an **AOS-morphism** is similar, with $(X, G), (Y, H)$ AOS's, and the evaluation maps taking values in $\{\pm 1\}$. □

Clearly, if $f : G \longrightarrow H$ is a RS-morphism (resp. RSG-morphism), the dual map $f^* : X_H \longrightarrow X_G$ defined by $f^*(\gamma) := \gamma \circ f$ for $\gamma \in X_H$, is an ARS-morphism (resp., AOS-morphism).

Proposition 7.2 *Let F be a RS-fan and let $I \subseteq J$ be ideals of F. With notation as in 7.1,*

(1) The rule $a/J \mapsto a/I$ $(a \in F \setminus J)$ defines a homomorphism of special groups $\iota_{JI} : F_J \longrightarrow F_I$.

(2) The map $\kappa_{IJ} : L_I(F) \longrightarrow L_J(F)$ assigning to each $g \in L_I(F)$ the unique element $h \in L_J(F)$ such that $g \rightsquigarrow h$ is an AOS-morphism. □

B. Involutions of ARS-fans

We introduce now a class of involutions of RS-fans that will have a crucial role in analyzing their fine structure and that of their spaces of characters.

Definition 7.3 (Involutions) Let F be a RS-fan, let $g_1, g_2 \in X_F$, and fix $I \in \text{Spec}(F)$ so that $Z(g_1), Z(g_2) \subseteq I$. We define a map $\varphi_I^{g_1,g_2} : L_I(F) \longrightarrow L_I(F)$ as follows: for $h \in L_I(F)$,

$$\varphi_I^{g_1,g_2}(h) = h\,g_1 g_2. \qquad \square$$

Note. Since $Z(g_i) \subseteq I = Z(h)$ $(i = 1,2)$, we have $Z(h\,g_1 g_2) = I$, whence $h\,g_1 g_2 \in L_I$. In Definition 7.3 we may assume $Z(g_1) = Z(g_2)$. $\square$

Theorem 7.4 *With notation as in Definition 7.3, we have:*

(a) $\varphi_I^{g_1,g_2}$ *is an AOS-automorphism of* L_I.

(b) $\varphi_I^{g_1,g_2}$ *is an involution: for* $h \in L_I$, $\varphi_I^{g_1,g_2}(\varphi_I^{g_1,g_2}(h)) = h$.

(c) For $i = 1,2$, *let* h_i *be the unique* $\rightsquigarrow$*-successor of* g_i *in* L_I. *Then,* $\varphi_I^{g_1,g_2}(h_1) = h_2$.

In particular,

(d) If g_1, g_2, *have a common* $\rightsquigarrow$ *- upper bound* h *at some level* $I \supseteq Z(g_1), Z(g_2)$, *then* h *is a fixed point of* $\varphi_I^{g_1,g_2}$.

(e) Let $J \subseteq I$ *be in Spec(F). Assume* $Z(g_1), Z(g_2) \subseteq J$, *and let* $h_1 \in L_J$, $h_2 \in L_I$. *Then,*

$$h_1 \rightsquigarrow h_2 \;\;\Rightarrow\;\; \varphi_J^{g_1,g_2}(h_1) \rightsquigarrow \varphi_I^{g_1,g_2}(h_2). \qquad \square$$

Use of these involutions yields a number of regularity results concerning the order structure of ARS-fans. These are based on analyzing the way these involutions move certain sets of characters, namely:

Notation 7.5 For $J \subseteq I$ in Spec(F) we define the sets:

$$S_J^I = \{\, h \in L_I \mid \exists g \in X_F \,(\, g \rightsquigarrow h \wedge Z(g) = J\,)\}.$$

$$C_J^I = \{\, h \in L_I \mid \exists g \in X_F \,(\, g \rightsquigarrow h \wedge Z(g) = J\,) \wedge \forall g' \in X_F \,(\, g' \rightsquigarrow h \Rightarrow J \subseteq Z(g'))\}.$$

That is, S_J^I *consists of those elements of level* I *having predecessors of level* J *or lower in the specialization partial order;* C_J^I *is the set of elements in* L_I *having predecessors at level* J *but not lower.* $\square$

Corollary 7.6 *Let* F *be a RS-fan, and let* $J \subseteq I$ *be in* Spec(F). *The set* S_J^I *is an AOS-fan. Indeed, it is a sub-fan of* $L_I(F)$, *when the latter is endowed with its structure of AOS-fan, as indicated in* 7.1. *More generally, if* $\mathcal{F} \subseteq L_J(F)$ *is an AOS-fan, the set* $S_J^I(\mathcal{F}) = \{\, h \in L_I \mid \exists g \in \mathcal{F}\,(\, g \rightsquigarrow h)\}$ *is an AOS-subfan of* $L_I(F)$. $\square$

Proposition 7.7 *Let* F *be a RS-fan. For* $J \subseteq J_1 \subseteq J_2 \subseteq I$ *in* Spec(F), *and* $h \in S_J^I$ *set:*

$$B^{J_1,J_2}(h) = \{\, g \in S_{J_1}^{J_2} \mid g \rightsquigarrow h\,\}, \quad \textit{and} \quad A^{J_1,J_2}(h) = \{\, g \in C_{J_1}^{J_2} \mid g \rightsquigarrow h\,\}.$$

Then,

(a) For $h_1, h_2 \in S_J^I$, *we have* $\text{card}\,(B^{J_1,J_2}(h_1)) = \text{card}\,(B^{J_1,J_2}(h_2))$.

(b) For $h_1, h_2 \in C_J^I$, *we have* $\text{card}\,(A^{J_1,J_2}(h_1)) = \text{card}\,(A^{J_1,J_2}(h_2))$.

(c) For $g_1, g_2 \in X_F$ *such that* $Z(g_i) \subseteq J$ $\;(i = 1,2)$, *the map* $\varphi_I^{g_1,g_2}$ *is a permutation of* S_J^I *and of* C_J^I. $\square$

Remark. The assumptions of the Proposition guarantee that the sets $B^{J_1,J_2}(h)$ are non-empty. The sets $A^{J_1,J_2}(h)$ may be empty for some choices of h and the J_i's. However, if $h \in C_J^I$ and $J_1 = J$, we have $A^{J_1,J_2}(h) \neq \emptyset$. $\square$

C. Connected components of ARS-fans. For a RS-fan, F, and $h \in X_F$, we denote by $P_h = \{ g \in X_F \mid g \rightsquigarrow h \}$ the root-system of predecessors of h under specialization.

Recall:

Definition 7.8 Let $(X, \preceq)$ be a root-system[12], and let $g_1, g_2 \in X$. Define:

$$g_1 \equiv_C g_2 \quad \text{iff} \quad g_1, g_2 \text{ have a common } \preceq\text{-upper bound.}$$

$\equiv_C$ is an equivalence relation; its classes are called **connected components** of $(X, \preceq)$. □

Note. If (X, F) is an ARS-fan, the connected components of X are precisely the sets of the form P_g, where g is a $\rightsquigarrow$-maximal element of X, i.e., an element such that $Z(g)$ is the (unique) maximal ideal of F. □

We register:

Proposition 7.9 (1) *P_h is an ARS-fan.*

In particular,

(2) *Any connected component of an ARS-fan is an ARS-fan.* □

Further, we have:

Theorem 7.10 *Let F be a RS-fan and let $J \subseteq I$ be in* Spec(F). *Let $h_1 \in C^I_J$, $h_2 \in S^I_J$. For $i = 1, 2$, we write P_i for P_{h_i}. Then,*

(1) *There is an ARS-embedding φ of P_1 into P_2. Further, $\varphi[P_1] = \{ u \in P_2 \mid J \subseteq Z(u) \}$. In particular, φ is an order-embedding of $(P_1, \rightsquigarrow)$ into $(P_2, \rightsquigarrow)$.*

(2) *If, in addition, $h_2 \in C^I_J$, then φ is an isomorphism of ARSs.* □

Proposition 7.7 and Theorem 7.10 provide significant information on the structure of the connected components of ARS-fans; see Definition 7.8.

Remark. Since every connected component of an ARS-fan is itself an ARS-fan, 7.9 (2), the zero-sets of its elements attain a lowest level, which can be explicitly determined, cf. Proposition 7.11 below. However, different components may have different lowest levels, see Corollary 7.13. □

Notation. The sets L_I, S^I_J and C^I_J defined in 7.1 and 7.5 relativize in an obvious way to the connected components of a fan (X, F); if K is such a component and $J \subseteq I$ are in Spec(F) we set:

$$L_I(K) = L_I \cap K, \quad S^I_J(K) = S^I_J \cap K, \quad \text{and} \quad C^I_J(K) = C^I_J \cap K.$$

Note that some (or all) of these sets may be empty, depending on I, J and the component K. $L_I(K) \neq \emptyset$ just means that K "reaches at least" the I-th level of X (possibly lower). □

Proposition 7.11 *Let K be a connected component of an ARS-fan (X, F). Let h_0 be the $\rightsquigarrow$-top element of K, and let $T = h_0^{-1}[1]$. Then, the lowest level of K (i.e., the smallest ideal I of F such that $L_I(K) \neq \emptyset$) is $I = \Gamma \cap -\Gamma$, where Γ is the saturated subsemigroup of F generated by* Id$(F) \cdot T$. □

Proposition 7.7 implies:

Corollary 7.12 *Let (X, F) be an ARS-fan and let K_1, K_2 be connected components of (X, F). Then,*

(1) *Let $I \in$ Spec(F); if $L_I(K_i) \neq \emptyset$ for $i = 1, 2$, then* card$(L_I(K_1)) =$ card$(L_I(K_2))$.

(2) *Let $J \subseteq J'$ be in* Spec(F), *and assume $L_J(K_i) \neq \emptyset$ $(i = 1, 2)$. Then,* card$(S^{J'}_J(K_1)) =$ card$(S^{J'}_J(K_2))$. □

[12] I.e., a partially ordered set such that the set of successors of every element is totally ordered.

Theorem 7.10 gives:

Corollary 7.13 *Let K_1, K_2 be connected components of the ARS-fan (X, F). Let $I_1, I_2 \in$ Spec(F) be the lowest levels of K_1, K_2, resp. (cf. 7.11). Then,*

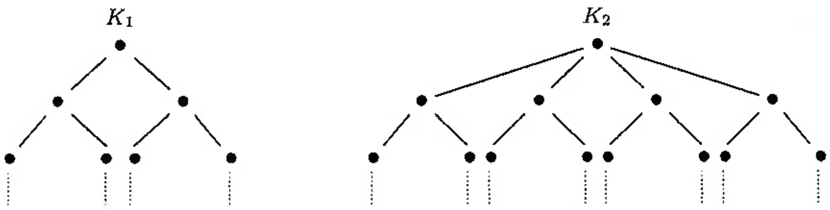
(1) If $I_2 \subseteq I_1$, then K_1 endowed with the specialization order is (order-) isomorphic to the root-system obtained by deleting all levels $I \subset I_1$ in K_2.

(2) If $I_1 = I_2$, then K_1, K_2 are order-isomorphic. □

7.14 Some impossible configurations.

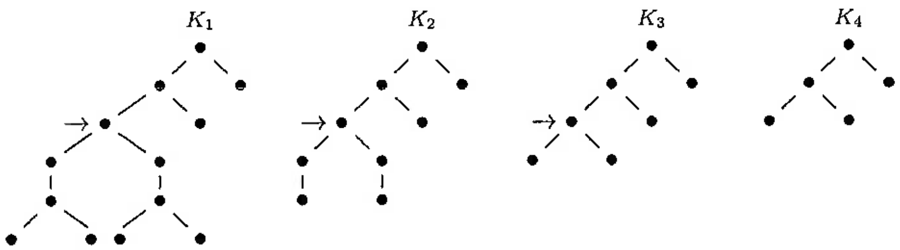
The preceding results show that there are strong constraints on the order structure of ARS-fans, especially when there is more than one connected component. We include a few examples to help the reader visualize the extent of those restrictions.

(1) A configuration like



contradicts Corollary 7.12 (1).

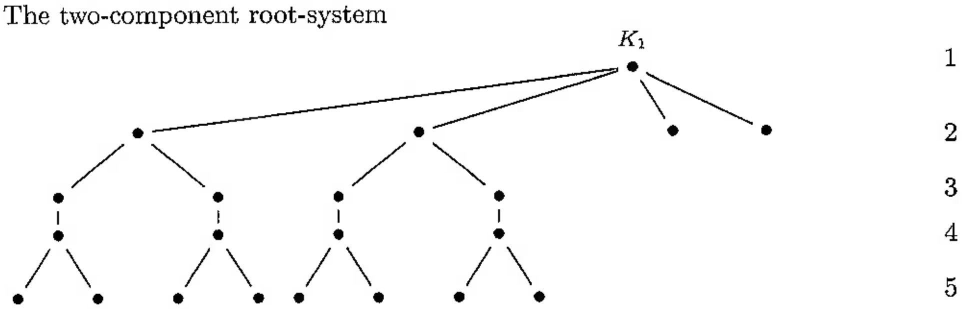
(2) The four-component configuration

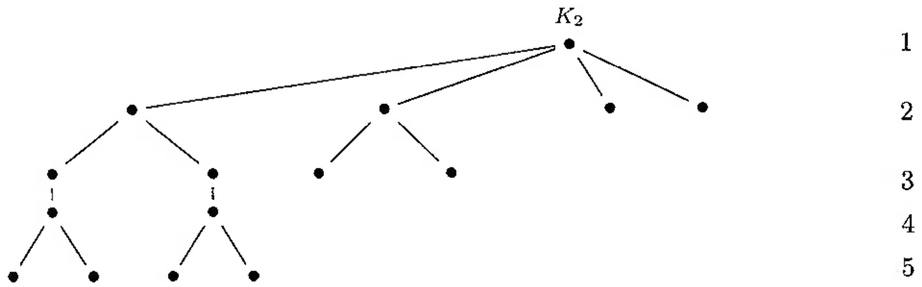


(where the components pairwise verify the conclusion of 7.12 (2)) is also impossible: card (S_4^3) = 3 is not a power of 2, and hence S_4^3 (shown with arrows) cannot be an AOS-fan (see Corollary 7.6). However, the same configuration with K_3 replaced by another copy of K_4 does not clash with either 7.12 or 7.13.

Note. Our notation here (and below) follows the standard convention for finite fans. Thus, S_4^3 stands for the set $S_{I_4}^{I_3}$, see 7.5 and 8.1.

(3) The two-component root-system





contradicts both Corollary 7.12 (2) (card $(S^3_4(K_1)) = 4$, but card $(S^3_4(K_2)) = 2$) and Corollary 7.13 (K_1 and K_2 have the same "length" but are not order-isomorphic). □

8 The specialization root-system of finite ARS-fans

In this section we mostly deal with finite fans in the categories **ARS** and **RS**. Our main result is Theorem 8.2 —the isomorphism theorem for finite ARS-fans— which proves that, in this case, the order of specialization alone determines the isomorphism type. The proof depends on the notion of a "standard generating system" which we introduce in 8.4. □

8.1 Reminder. Recall that the AOSs have a combinatorial geometric (matroid) structure; it was introduced in [D1] and [D2] for spaces of orders of fields, and later generalized to abstract order spaces in [Li]. In general, ARSs do not possess such a structure. Thus, combinatorial geometric notions such as *dependent set, independent set, basis, closed set, closure, dimension,* etc., will always refer to the above-mentioned combinatorial geometric structure, and apply only to AOSs. For the definition and the mutual relationships, in the general context of matroid theory, of combinatorial notions such as those just mentioned, the reader is referred to [Wh].

Since the combinatorial geometric structure of any AOS is isomorphic to that of a set of vectors in a (possibly infinite-dimensional) vector space over the two-element field $\mathbb{F}_2$ with the structure induced by linear dependence (cf. [D1], Thm. 3.1, p. 618), the notions above coincide with the corresponding notions over vector spaces. For example, a subset $A \subseteq X$ of an AOS $(X, G, -1)$ (G a group of exponent 2) is dependent iff there are pairwise distinct elements $g, g_1, \ldots, g_r \in A\,(r \geq 2)$, such that $g = g_1 \cdot \ldots \cdot g_r$ (as characters of G). Since functions in X send -1 to -1, this functional identity can only hold if r is odd. Likewise, A is closed iff the product of any odd number of members of A belongs to A. □

Warning. In this section the words *closed set* and *closure* are used only in the combinatorial geometric sense just defined. □

The main result in this section is:

Theorem 8.2 (The isomorphism theorem for finite ARS-fans.)
Let (X_1, F_1), (X_2, F_2) be finite ARS-fans and let $\underset{1}{\rightsquigarrow}$, $\underset{2}{\rightsquigarrow}$ denote their respective specialization orders. If $(X_1, \underset{1}{\rightsquigarrow})$ and $(X_2, \underset{2}{\rightsquigarrow})$ are order-isomorphic, then X_1 and X_2 are isomorphic ARSs. □

The main ingredients of the proof are:

Proposition 8.3 (Choice of basis). *Let (X, F) be a finite ARS-fan; let $1 \leq k < n = \ell(X)$. Let $\mathcal{G}$ be an arbitrary AOS-subfan of $L_{k+1} = L_{k+1}(X)$. Let $\mathcal{F} = \{ h \in L_k \mid$ There is $g \in \mathcal{G}$ such that $g \rightsquigarrow h) \}$ be the AOS-fan consisting of the depth-k successors of elements of $\mathcal{G}$ (cf. 7.6).*

<u>*Assume:*</u>

$(*)$ $\forall h, h' \in \mathcal{F}$, $\mathrm{card}(\{g \in \mathcal{G} \mid g \rightsquigarrow h\}) = \mathrm{card}(\{g \in \mathcal{G} \mid g \rightsquigarrow h'\})$.

Let $\mathcal{B} = \{h_1, \ldots, h_r\}$ be a basis of $\mathcal{F}$ (as an AOS), and let $\mathcal{C}$ be a basis of the AOS-fan $\{g \in \mathcal{G} \mid g \rightsquigarrow h_1\}$. For $i = 2, \ldots, r$, let $g_i \in \mathcal{G}$ be such that $g_i \rightsquigarrow h_i$.

<u>*Then*</u>*, $\mathcal{C} \cup \{g_2, \ldots, g_r\}$ is a basis of $\mathcal{G}$.* □

8.4 Standard generating systems.

For any finite ARS-fan, (X, F), by induction on k, $1 \le k \le n = \ell(X)$, we construct a class of bases $\mathcal{B}_k$ of the AOS-fan $L_k(X)$. Each basis $\mathcal{B}_k$ will be required to satisfy the additional condition:

$(*)$ For $k \le j \le n$, $\mathcal{B}_k \cap S_j^k$ is a basis of the AOS-fan S_j^k.

This additional requirement guarantees that the inductive construction of the $\mathcal{B}_k$'s does not get interrupted before the n-th (and last) step. The construction uses Proposition 8.3 and the results from §7 above. The set $\mathcal{B} = \bigcup_{k=1}^{n} \mathcal{B}_k$ is called a **standard generating system** for (X, F). □

References

[ABR] C. Andradas, L. Bröcker, J. Ruiz, **Constructible Sets in Real Geometry**, *A Series of Modern Surveys in Mathematics* **33**, Springer-Verlag, Berlin, Heidelberg, New York (1996).

[AR] C. Andradas, J. Ruiz, **Algebraic and Analytic Geometry of Fans**, Memoirs Amer. Math. Soc. **553** (1995), 117 pp.

[B] G. Birkhoff, **Lattice Theory**, AMS, Revised Ed., 1960.

[BCR] J. Bochnak, M. Coste, M.-F. Roy, **Real Algebraic Geometry**, Springer-Verlag, Berlin, Heidelberg, New York (1998). [English version of **Géométrie algébrique réelle**, *Ergeb. Math.* **12**, Springer-Verlag, Berlin, Heidelberg, New York (1987).]

[BK] E. Becker, E. Köpping, *Reduzierte quadratische Formen und Semiordnungen reeller Körper*, Abh. Math. Sem. Univ. Hamburg **46** (1977), 143-177.

[Br] L. Bröcker, *Abstract Real Spectra*, in Séminaire de Structures Algébriques Ordonnées 1992–1993, Univ. Paris VII (F. Delon, M. Dickmann, D. Gondard, eds.), Prépublication No. 49 (1994), 4 pp.

[D1] M. Dickmann, *A Combinatorial Geometric Structure on the Space of Orders of a Field. I*, *Europ. J. Combinatorics* **18** (1997), 613-634.

[D2] M. Dickmann, *A Combinatorial Geometric Structure on the Space of Orders of a Field. II*, in **Real Algebraic Geometry and Quadratic Forms** (B. Jacob, T. Y. Lam and R. Robson, eds.), *Contemporary Math.* **155** (1994), AMS, 119-140.

[DM1] M. Dickmann, F. Miraglia, **Special Groups. Boolean-Theoretic Methods in the Theory of Quadratic Forms**, Memoirs Amer. Math. Soc. **689** (2000), 247 pp.

[DMP] M. Dickmann, F. Miraglia, A. Petrovich, *Constructions in the Category of Real Semigroups: A Summary of Results*, this volume, 9 pp.

[DP1] M. Dickmann, A. Petrovich, *Real Semigroups and Abstract Real Spectra. I*, Contemporary Math. **344** (2004), 99-119, Amer. Math. Soc.

[DP2] M. Dickmann, A. Petrovich, *The Three-Valued Logic of Quadratic Form Theory over Real Rings*, in **"Andrzej Mostowski and Foundational Studies"** (A. Ehrenfeucht, V. W. Marek, M. Srebrny, eds.), IOS Press, Amsterdam, 2008, 49-67.

[DP3] M. Dickmann, A. Petrovich, *Spectral Real Semigroups*, Annales de la Faculté des Sciences de Toulouse (Série 6, **21**) (2012), 359-412.

[DP4] M. Dickmann, A. Petrovich, **Real Semigroups, Real Spectra and Quadratic Forms over Rings**, monograph, approx. 250 pp. (in preparation).

[DP5] M. Dickmann, A. Petrovich, *Fans in the Theory of Real Semigroups*, 59 pp., submitted, May 2015.

[DST] M. Dickmann, N. Schwartz, M. Tressl, **Spectral Spaces** (in preparation; to appear, Cambridge Univ. Press, 2017).

[La] T. Y. Lam, **Orderings, valuations and quadratic forms**, Regional conference series in mathematics **52**, Amer. Math. Soc. (1983).

[Li] A. Lira, *Les groupes spéciaux*, Ph. D. thesis, Univ. of Paris VII (1995), unpublished.

[M] M. Marshall, **Spaces of Orderings and Abstract Real Spectra**, *Lecture Notes Math.* **1636**, Springer-Verlag, Berlin, (1996).

[Wh] N. White (ed.), **The Theory of Matroids**, *Encyclopedia of Mathematics and its Applications*, vol. **26**, Cambridge Univ. Press (1986).

M. Dickmann
Institut de Mathématiques de Jussieu – Paris Rive Gauche
Universités Paris 6 et 7
Paris, France
e-mail: dickmann@math.univ-paris-diderot.fr

A. Petrovich
Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
1428 Buenos Aires, Argentina
e-mail: apetrov@dm.uba.ar

Constructions in the Category of Real Semigroups: A Summary of Results

M. Dickmann F. Miraglia A. Petrovich

February, 2016

We present here a summary of results, together with some of the pertinent background, of certain constructions in the category of Real Semigroups (RS). Proofs will appear elsewhere.

1 Real Semigroups. Duality

Definition 1.1 A **ternary semigroup (TS)** is a structure $S = \langle S, 1, 0, -1, \cdot \rangle$, such that $\forall$ $x \in S$:

[TS1] S is a commutative semigroup with unit 1;

[TS2] $x^3 = x$;

[TS3] $-1 \neq 1$ and $(-1)(-1) = 1$;

[TS4] $x \cdot 0 = 0$;

[TS5] $x = (-1) \cdot x \;\Rightarrow\; x = 0$.

Write $-x$ for $(-1) \cdot x$.

Definition 1.2 *A* **real semigroup (RS)** *is a ternary semigroup G, together with a ternary relation D on G, to be written $a \in D(b,c)$, called* **binary representation**, *and with* **transversal binary representation**, *D^t, defined by*

[t-rep] $\quad a \in D^t(b,c) \;\Leftrightarrow\; a \in D(b,c)$ *and* $-b \in D(-a,c)$ *and* $-c \in D(b,-a)$,

satisfying, for all a, b, d, e $\in G$:

[RS0] $c \in D(a,b) \;\Leftrightarrow\; c \in D(b,a)$;

[RS 1] $a \in D(a,b)$;

[RS 2] $a \in D(b,c) \;\Rightarrow\; ad \in D(db,dc)$;

[RS 3] (Strong associativity) $a \in D^t_G(b,c)$ *and* $c \in D^t_G(d,e) \;\Rightarrow\; \begin{cases} \exists\, x \in D^t_G(b,d) \text{ s.t.} \\ a \in D^t_G(x,e). \end{cases}$

[RS 4] $e \in D(c^2a, d^2b) \;\Rightarrow\; e \in D(a,b)$;

[RS 5] $ad = bd$, $ae = be$ *and* $c \in D(d,e) \;\Rightarrow\; ac = bc$;

[RS 6] $c \in D(a,b) \;\Rightarrow\; c \in D^t(c^2a, c^2b)$;

[RS 7] (Reduction) $D^t(a,-b) \cap D^t(b,-a) \neq \emptyset \;\Rightarrow\; a = b$.

[RS 8] $a \in D(b,c) \;\Rightarrow\; a^2 \in D(b^2,c^2)$.

If G is a RS, $G^\times := \{a \in G : a^2 = 1\}$ is the multiplicative **group of units** of G.

Representation and t-representation are extended, by induction, to forms of dimension $n \geq 3$, by:

If $\varphi = \langle a_1, \ldots, a_n \rangle$ is a form over a RS G, and $x \in G$,

$$x \in D_G(\varphi) \;\Leftrightarrow\; \exists\, u \in D_G(a_2, \ldots, a_n) \text{ s. t. } x \in D_G(a_1, u).$$

Similarly, for $D_G^t(\varphi)$: $\quad x \in D_G^t(\varphi) \;\Leftrightarrow\; \exists\, u \in D_G^t(a_2, \ldots, a_n)$ s. t. $x \in D_G^t(a_1, u)$.

Example 1.3 a) The TS $\mathbf{3} = \{1, 0, -1\}$ has a unique structure of RS, with representation and t-representation determined by the axioms for RS. For instance,

$$D_{\mathbf{3}}(0, 1) = D_{\mathbf{3}}(1, 1) = \{0, 1\} \text{ and } D_{\mathbf{3}}^t(0, 1) = D_{\mathbf{3}}^t(1, 1) = \{1\}.$$

b) Let K be a reduced special group (RSG) and let $K^* = K \cup \{0\}$ ($0 \notin K$); define $0 \cdot z = 0$ for all $z \in K^*$. Then, K^* is a TS. Extend the binary representation of K to K^* by

$$D_{K^*}(a, b) = \begin{cases} \{a, b\} & \text{if } a = 0 \text{ or } b = 0 \\ D_K(a, b) \cup \{0\} & \text{if } a, b \in G. \end{cases}$$

Then, K^* is a RS, and representation and t-representation in K^* coincide on binary forms with entries in K. There is also a converse: cf. Cor. I.2.6, [DP2]. ■

1.4 RS-morphisms. a) If G, H are RSs, a map $f : G \longrightarrow H$, is a **RS-morphism** if it is semigroup morphism, preserving 0, 1, -1, and representation, i.e.,

[mor] $$a \in D_G(b, c) \;\Rightarrow\; f(a) \in D_H(f(b), f(c)).$$

We register that in [mor], D_G may be replaced by D_G^t. Moreover, if $\varphi = \langle a_1, \ldots, a_n \rangle$ is a form over G, $x \in G$ and $G \xrightarrow{f}$ is an RS-morphism, then

$$x \in D_G(\varphi) \text{ implies } f(x) \in D_H(f \star \varphi),$$

where $f \star \varphi = \langle f(a_1), \ldots, f(a_n) \rangle$.

b) If $\varphi = \langle a_1, \ldots, a_n \rangle$, $\psi = \langle b_1, \ldots, b_m \rangle$ are forms over a RS, G, write $\varphi \cong \psi$ iff for all $\sigma \in X_G$

$$\textstyle\sum_{k=1}^{n} \sigma(a_k) \;=\; \sum_{j=1}^{m} \sigma(b_j) \qquad \text{(sum in } \mathbb{Z}).$$

c) A RS-morphism, $f : G \longrightarrow H$, is a **complete embedding** if for all forms φ, ψ over G,

$$\varphi \cong \psi \;\Leftrightarrow\; f \star \varphi \cong f \star \psi.$$

It is straightforward that any complete embedding is injective.

d) A RS morphism, $f : G \longrightarrow H$, is a **pure embedding** if it reflects all positive existential formulas in the first-order language with equality of RSs, $\mathcal{L}_{RS} = \langle \cdot, 0, 1 - 1, D \rangle$, where D stand for the representation relation. Every pure embedding is injective and, in fact, a complete embedding. ■

1.5 The Space of RS-characters of an RS. If G is a RS, X_G is the set of RS-morphisms from G to $\mathbf{3}$, called the **space of RS-characters** of G.

a) Important Properties of X_G:

- X_G separates points in G; in particular, $X_G \neq \emptyset$.
- (Separation) For all $a, b, c \in G$, $a \in D_G(b, c) \;\Leftrightarrow\; \forall\, \sigma \in X_G,\; \sigma(a) \in D_{\mathbf{3}}(\sigma(b), \sigma(a))$, with a similar equivalence holding with D_G^t in place of D_G.
- The existence of the Post and Spectral hulls of G, whose definition and basic properties are can be found in Chapters IV and V of [DP2].

b) Topologies on X_G: (1) Recall that a T_0 topological space, Y, carries a partial order, **specialization**, defined for $x, y \in Y$, by

$$x \rightsquigarrow y \quad \text{iff} \quad y \in \overline{\{x\}}.$$

Y is **a root system** if for all $x \in Y$, $\{y \in Y : x \rightsquigarrow y\}$ is *linearly ordered* by specialization.

(2) For $g \in G$ and $j \in \mathbf{3}$, define $[\![g = j]\!] = \{\sigma \in X_G : \sigma(g) = j\}$. The family

$$\{[\![a = 1]\!] \subseteq X_G : a \in G\}$$

is a sub-basis of a root system spectral topology on X_G. The associated constructible topology has as basis of clopens

$$\{[\![z = 0]\!] \cap \bigcap_{k=1}^{n} [\![a_k = 1]\!] : n \geq 0 \text{ and } z, a_1, \ldots, a_n \in G.\}$$

It can be shown that just one set of the form $[\![z = 0]\!]$ suffices.

(3) An RS-morphism, $f : G \longrightarrow H$, induces a spectral map, $f^* : X_H \longrightarrow X_G$, given by $\tau \in X_H \longmapsto (\tau \circ f) \in X_G$. ■

1.6 Duality and Isomorphism. We have the following important results:

- By Theorem 4.1 in [DP1] (cf. also Theorem I.5.1, [DP2]), the category **RS** is **isomorphic** to **ARS**$^{\mathbf{op}}$, where **ARS** is the category of abstract real spectra in the sense of M. Marshall (cf. [M]).

- Marshall shows in [M] that the category **ARS** is **isomorphic** to that of spaces of signs, as defined by L. Bröcker (cf. [ABR]).

Remark that the category **RS** is Horn-geometrically axiomatizable, while **ARS** and that of Spaces of Signs are not. Clearly, the strong duality and isomorphism results stated above provide a means to transfer statements from one category to any of the others. ■

1.7 The Post and Spectral Hulls of a RS. Let G be a RS.

(I) By Theorem IV.4.2 of [DP2], G has a **Post hull**, P_G, a Post algebra of order 3, consisting of all continuous maps from X_G to **3**; here, X_G has the constructible topology and **3**, the discrete topology. We have a complete embedding,

$$\varepsilon_P : G \longrightarrow P_G, \text{ given by } g \longmapsto ev_g = \sigma(g),$$

i.e., ev_g is the evaluation map at $\sigma \in X_G$.

Clearly, the construction of P_G depends on the knowledge of the constructible topology of X_G. Interesting properties of representation and of morphisms are obtained through the Post hull construction. As examples, we mention (Theorem IV.4.5 in [DP2]):

- A SG-morphism, $G \xrightarrow{f} H$, is a complete embedding iff for every Pfister form $\mathcal{P}$ over G and $a \in G$, $f(a) \in D_H(f \star \mathcal{P}) \Rightarrow a \in D_G(\mathcal{P})$.
- Any pure SG-embedding is a complete embedding.

Example. Let H be a RS. There is a *unique* RS-morphism, $\iota_H : \mathbf{3} \longrightarrow H$, taking $1, 0, -1$ to $1, 0, -1$ in H. For any $\sigma \in X_G$, we have $\sigma \circ \iota_H = Id_{\mathbf{3}}$ and so **3** is a retract of H. In particular, ι_H is a pure SG-embedding and hence a complete embedding. □

Employing the Post hull, this example can be considerably generalized: any injective SG-morphism from a Post algebra of order 3 to a RS is pure (whence, complete).

(II) Endow **3** with the spectral topology, wherein the only opens are $\emptyset$, $\{1\}$, $\{-1\}$ and **3**. Let $\mathbf{Sp}(X_G)$ be the set of all spectral maps from X_G to **3**. Then, $\mathbf{Sp}(X_G)$ is a RS and there is a complete embedding, $\eta_G : G \longrightarrow \mathbf{Sp}(X_G)$, with the properties of a hull, called the **spectral hull** of G. It is introduced in [DP3] (see also Chapter V in [DP2]), wherein its properties are discussed and developed.

The point to be made here is the following: in introducing a new construction in the category **RS**, it is important to achieve some understanding – characterize if possible –, the space of RS-characters of that construction, to make available the resources coming from its Post and Spectral hulls. ■

1.8 The RS associated to a p-ring. A **p-ring**, $\langle A, T \rangle$, is pair where A is a commutative unitary ring ($1 \neq 0$) and T is a proper preorder of A.

Let $\mathrm{Sper}(A,T)$ be the **real spectrum** of $\langle A, T \rangle$ it is a root system spectral space when endowed with the topology having as a sub-basis the Harrison sets

$$H(a_1, \ldots, a_n) = \{\alpha \in \mathrm{Sper}(A,T) : a_k \in \alpha \setminus (-\alpha),\, n \geq 1,\, a_1, \ldots, a_n \in A\}.$$

For $w \in A$, set $Z(w) = \{\alpha \in \mathrm{Sper}(A,T) : w \in \mathrm{supp}(\alpha)\}$, where $\mathrm{supp}(\alpha) = \alpha \cap (-\alpha)$, a T-convex prime ideal of A.

Each $a \in A$ gives rise to a spectral map, $\overline{a}_T : \mathrm{Sper}(A,T) \longrightarrow 3 = \{-1, 0, 1\}$, given by

$$\overline{a}_T(\alpha) = \begin{cases} 1 & \text{if } a \in \alpha \setminus -\alpha; \\ 0 & \text{if } a \in \mathrm{supp}(\alpha) = \alpha \cap -\alpha; \\ -1 & \text{if } a \in -\alpha \setminus \alpha. \end{cases}$$

If T is clear from context, write $\overline{a}$ for $\overline{a}_T$.

Let $G_{A,T} = \{\overline{a}_T : a \in A\}$. With the product induced by A, $G_{A,T}$ is a TS with identity 1 and distinguished elements 0 and -1 (the corresponding constant-valued maps).

Define $D_{G_{A,T}}$ (representation) by : for $a, b, c \in A$,

$$\overline{a} \in D_{G_{A,T}}(\overline{b}, \overline{c}) \Leftrightarrow \exists\, t, t_1, t_2 \in T, \text{ s.t. } \overline{at} = \overline{a} \text{ and } ta = t_1 b + t_2 c.$$

The corresponding t-representation is given by

$$\overline{a} \in D^t_{G_{A,T}}(\overline{b}, \overline{c}) \Leftrightarrow \exists\, a', b', c' \in A \text{ s.t. } \overline{a} = \overline{a'}, \overline{b} = \overline{b'}, \overline{c} = \overline{c'} \text{ and } a' = b' + c'.$$

With these representation relations,

- $G_{A,T}$ is a RS;
- $X_{G_{A,T}}$ is the spectral space $\mathrm{Sper}(A,T)$. ■

In the present setting, the following result, due to M. Marshall, is important:

Theorem 1.9 (Cor. 5.4.3 in [M]) *Let $\langle A, T \rangle$ be a p-ring. For $a, b \in A$:*

$$\overline{a_T} = \overline{b_T} \text{ iff there are } s, t \in T \text{ and } k \geq 0 \text{ so that } sab = (a^2 + b^2)^k + t. \quad ■$$

We now describe a natural functor, $\boldsymbol{G}$, from the category of p-rings, **p-Rings**, to the category of RSs, **RS**.

If $\langle A, T \rangle \xrightarrow{f} \langle A', T' \rangle$ is a p-ring morphism, define

$$G(f) : G_{A,T} \longrightarrow G_{A',T'}, \text{ given by } \overline{a_T} \longmapsto \overline{f(a)_{T'}}.$$

Employing Theorem 1.9, one shows that $G(f)$ is a well-defined RS-morphism. The maps

$$\begin{cases} \langle A, T \rangle & \longmapsto & G_{A,T} \\ \langle A, T \rangle \xrightarrow{f} \langle A', T' \rangle & \longmapsto & G_{A,T} \xrightarrow{G(f)} G_{A',T'}, \end{cases}$$

yield a covariant functor, $\boldsymbol{G}$, from **p-Rings** to **RS**.

2 A Summary of Results

2.1 Real Semigroups of Continuous Functions

Let Z be a topological space and let K be a real semigroup. Endow K with the discrete topology (all points are open). Let

$$\mathbb{C}(Z,K) \;=\; \{g : Z \longrightarrow K : g \text{ is continuous}\},$$

called the **Boolean power** of K by Z. $\mathbb{C}(Z,\, K)$ has a natural structure of TS, under pointwise product and constants 0, 1, -1 given by the corresponding constant-valued functions.

For $f,\, g,\, h \in \mathbb{C}(Z,\, K)$, define representation and t-representation in $\mathbb{C}(Z,\, K)$ by

$f \in D_{Z,K}\,(g,\, h) \;\Leftrightarrow\; \forall\, z \in Z,\;\; f(z) \in D_K(g(z),\, h(z))$;

$f \in D^t_{Z,K}(g,\, h) \;\Leftrightarrow\; \forall\, z \in Z,\;\; f(z) \in D^t_K(g(z),\, h(z))$.

With notation as above, we have

Theorem 2.1 *Let Z be a topological space and let K be a RS.*

a) $G := \mathbb{C}(Z,K)$ is a RS.

b) If Z is a Boolean space, the map $\gamma : Z \times X_K \longrightarrow X_G$, given by

$$\langle z, \tau \rangle \longmapsto \gamma(z,\tau) \;:=\; \tau \circ ev_z,$$

is a homeomorphism of spectral spaces, where ev_z is the evaluation at $z \in Z$. ■

Remark: For any **compact** Z, X_G is spectrally homeomorphic to $S(B(Z)) \times X_K$, where $S(B(Z))$ is the Stone space of the BA of clopens in Z.

The preceding result yields

Corollary 2.2 *Let $G_1, \ldots, G_n$ be RSs and let G be their product. The map*

$$\eta : \textstyle\bigoplus_{i=1}^n X_{G_i} \longrightarrow X_G, \text{ defined by } \eta(\langle \tau, i\rangle)(\langle g_1, \ldots, g_n\rangle) \;=\; \tau(g_i),$$

is a homeomorphism of spectral spaces, where $\bigoplus_{i=1}^n X_{G_i}$ is the topological sum of the X_{G_i}. ■

The situation of **arbitrary products** is considerably more complicated; we shall have something to say about it below.

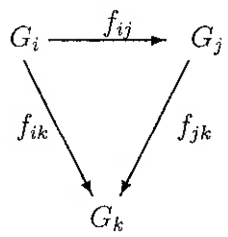
2.2 Inductive Limits

As remarked in 1.5.(3), a SG-morphism, $H \xrightarrow{f} G$, yields a spectral map, $f^* : X_G \longrightarrow X_H$, given by $f^*(\sigma) \;=\; \sigma \circ f$.

Let $\langle I, \leq \rangle$ be a right-directed poset and let

$$\mathcal{S} = \langle G_i;\; \{G_i \xrightarrow{f_{ij}} G_j : i \leq j \in I\}\rangle$$

be an inductive system of RSs over I, i.e., $f_{ii} = Id_{G_i}$ and for $i \leq j \leq k$, $f_{ik} = f_{jk} \circ f_{ij}$.



Theorem 2.3 *With notation as above,*

a) The inductive limit of $\mathcal{S}$ exists in **RS**. *Let* $\langle G; \{f_i : G_i \longrightarrow G\} \rangle = \varinjlim \mathcal{S}$.

b) If for all $i \leq j$, f_{ij} is a complete embedding, then each f_i is a complete embedding, $i \in I$.

c) If for all $i \leq j$, f_{ij} is a pure embedding, then each f_i is a pure embedding, $i \in I$.

d) $\mathcal{S}$ gives rise to a <u>*projective system*</u> *of spectral root systems and spectral maps:*

$$\mathfrak{X}(\mathcal{S}) \quad = \quad \langle X_{G_i}; \{X_{G_j} \xrightarrow{f_{ij}^*} X_{G_i} : i \leq j \in I\} \rangle.$$

Then, X_G is homeomorphic, as a spectral space, to the projective limit of the system $\mathfrak{X}(\mathcal{S})$. ∎

2.3 RS-sums

The category of RSs, in general, does not have coproducts because this is the case for the category of reduced special groups (cf. Definition 5.27, p. 93ff, in [DM1]). In this section we show that there is a construction, the **RS-sum**, coming as close as it seems possible to a coproduct in the category **RS**.

As in the case of special groups, if G, H are RSs, there is no canonical way to define a RS-morphism from G to $G \times H$. It is an entirely different matter if we add a component **3** :

Let I be a non-empty set and let G_i, $i \in I$, be RSs. Let $G = \prod_{i \in I} G_i$ be their product, endowed with the natural coordinate-wise product structure.

For each <u>proper</u> subset J of I, let

$$G_J^\flat \quad = \quad \left(\textstyle\prod_{j \in J} G_j\right) \times \mathbf{3},$$

Write $\langle s, d \rangle$ for an element of $G_J^\flat$, where $s \in \prod_{j \in J} G_j$ and $d \in \mathbf{3}$. Then,

a) If $J \subsetneq I$ there is a <u>*pure embedding*</u>,

$$\iota_J : G_J^\flat \longrightarrow G,$$

given by the product of the identity on $\prod_{j \in J} G_j$ and the unique pure embedding of **3** into $\prod_{i \notin J} G_i$:

$$\iota_J(s, d)(i) \quad = \quad \begin{cases} s(i) & \text{if } i \in J; \\ d & \text{if } i \notin J. \end{cases}$$

b) Similarly, if $\emptyset \neq K \subseteq J \subsetneq I$, we get a *pure embedding*, $\mathfrak{t}_{KJ} : G_K^\flat \longrightarrow G_J^\flat$, the product of the identity map on $\prod_{k \in K} G_k$ with the unique pure embedding of **3** into $\prod_{j \in (J \setminus K)} G_j \times \mathbf{3}$.

Note that:

- $\mathfrak{t}_{KK} = Id_{G_K^\flat}$;
- For $K \subsetneq J \subsetneq I$, the diagram (I) commutes:

- For $\emptyset \neq K \subseteq J \subseteq J' \subsetneq I$, $\mathfrak{t}_{KJ'} = \mathfrak{t}_{JJ'} \circ \mathfrak{t}_{KJ}$, i.e., diagram (II) commutes.

Definition 2.4 *Let $I \neq \emptyset$ be a set and let G_i, $i \in I$, be RSs. Define*

$$\bigoplus_{i\in I} G_i \;=\; \left\{ s \in \prod_{i\in I} G_i : \begin{array}{l} \exists\ \underline{\text{finite}}\ F \subseteq I, \text{ such that for all } j \notin F, \\ s(j) \text{ is constant and belongs to } \mathbf{3} \end{array} \right\},$$

endowed with the representation relations induced by $\prod_{i\in I} G_i$ and with 0, 1 and -1 being the corresponding constant-valued I-sequences.

Clearly, if I is finite, then $\bigoplus_{i\in I} G_i = \prod_{i\in I} G_i$.

Theorem 2.5 *Let I be an infinite set and let G_i, $i \in I$, be RSs.*

a) Let $\mathfrak{F}(I)$ be the poset (under inclusion) *of* non-empty *finite subsets of I. Let*

$$\mathcal{S} \;:=\; \{\langle G_F^\flat; \mathfrak{t}_{FF'}\rangle : \emptyset \neq F \subseteq F' \in \mathfrak{F}(I)\}$$

be the inductive system of pure embeddings over $\mathfrak{F}(I)$ (as above). *Then, $\bigoplus_{i\in I} G_i = \varinjlim \mathcal{S}$.*

b) $\bigoplus_{i\in I} G_i$ is a RS and its canonical embedding into $\prod_{i\in I} G_i$ is pure.

c) Let $G^\flat := \bigoplus_{i\in I} G_i$. Then, $X_{G^\flat}$ is spectrally homeomorphic to the projective limit of the system

$$\mathfrak{X}^\flat \;=\; \langle X_{G_F^\flat}; \{X_{G_{F'}^\flat} \xrightarrow{\mathfrak{t}^*_{FF'}} X_{G_F^\flat} : F \subseteq F' \text{ in } \mathfrak{F}(I)\}\rangle,$$

where the connecting maps $\mathfrak{t}^*_{FF'}$ are all surjective. ■

2.4 The space of RS-characters of Products

We start by recalling the notions of ideal, multiplicative set, saturated and transversally saturated sets in a real semigroup.

Definition 2.6 *Let H be a RS and S be a subset of S.*

a) S is an **ideal** *in H, if for all $x \in S$ and $a \in H$, we have $ax \in S$.*

b) S is **multiplicative** *if it is closed under products.*

c) S is **transversally saturated (t-saturated)** *if for all $a \in H$ and $s, t \in S$, $a \in D_H^t(s,t)$ implies $a \in S$. Similarly one defines* **saturated**, *replacing D_G^t by D_G.*

We can now state:

Theorem 2.7 *Let H be a real semigroup. If I is a saturated ideal of G and T is a multiplicative t-saturated set in H, containing 1 and disjoint from I, there is a RS-character $\sigma \in X_H$ such that $\sigma \upharpoonright I = 0$ and $\sigma \upharpoonright T = 1$.* ■

Let $\{G_\lambda : \lambda \in \Lambda\}$ be a non-empty family of real semigroups and let $G = \prod_{\lambda\in\Lambda} G_\lambda$ be their product. Write $\mathbb{0}$, $\mathbb{1}$ and $-\mathbb{1}$ for the elements of G whose entries are all equal to 0, 1, -1, respectively. Endow G with the product RS-structure, i.e., the constants are $\mathbb{0}$, $\mathbb{1}$, $-\mathbb{1}$, product is defined coordinatewise, and for $a = \langle a_\lambda \rangle$, $b = \langle b_\lambda \rangle$, $c = \langle c_\lambda \rangle$ in G, set

$$a \in D_G(b, c) \quad \Leftrightarrow \quad \text{for all } \lambda \in \Lambda, \quad a_\lambda \in D_{G_\lambda}(b_\lambda, c_\lambda),$$

with an analogous relation holding for transversal representation in G. The canonical coordinate projections, π_λ: $G \longrightarrow G_\lambda$, $\lambda \in \Lambda$, are then SG-morphisms.

For $\lambda \in \Lambda$, the projection $\pi_\lambda : G \longrightarrow G_\lambda$ induces a spectral embedding (cf. 1.5.(3)), $\pi_\lambda^* : X_{G_\lambda} \longrightarrow X_G$, given by $\pi_\lambda^*(\sigma) = \sigma \circ \pi_\lambda$. The image of X_{G_λ} by π_λ^* in X_G will be written X_λ. If $\sigma \in X_{G_\lambda}$, then $\pi_\lambda^*(\sigma)$ is the SG-character of G satisfying,

$$[\pi_\lambda^*] \qquad \text{For all } a \in G, \quad \pi_\lambda^*(\sigma)(a) \;=\; \sigma(a_\lambda).$$

Clearly, if $\lambda \neq \lambda'$ in Λ, then $X_\lambda \cap X_{\lambda'} = \emptyset$ [1]. Hence, the disjoint union, $\coprod_{\lambda\in\Lambda} X_\lambda$, is a subset of X_G.

With notation as above, we have

Theorem 2.8 *$\coprod_{\lambda\in\Lambda} X_\lambda$ is dense in X_G, endowed with its constructible topology.* ■

Let $\beta\Lambda$ be the Stone-Čech compactification of the discrete space Λ.

Proposition 2.9 *Let $G = \prod_{\lambda\in\Lambda} G_\lambda$.*

a) Each $\tau \in X_G$ gives rise to an ultrafilter $\mathcal{U}(\tau)$ on Λ.

b) The map $\mathcal{U} : X_G \longrightarrow \beta\Lambda$, given by $\tau \longmapsto \mathcal{U}(\tau)$ is a spectral surjection.

c) If X_G is endowed with its constructible topology, then there is continuous $s : \beta\Lambda \longrightarrow X_G$ so that $\mathcal{U} \circ s = Id_{\beta\Lambda}$, i.e., $\beta\Lambda$ is a retract of X_G. ■

2.5 The Functor from p-Rings to RS

Recall that a p-ring, $\langle R, P \rangle$, is a **bounded inversion ring (BIR)** if the multiplicative set $1 + P$ is contained in $R^\times$, the multiplicative group of units of R. In [DM2] we show that the RS associated to a p-ring $\langle A, T \rangle$ (cf. 1.8 above), is isomorphic to the RS of a BIR canonically associated to $\langle A, T \rangle$. Complementing these results, we have, with notation as 1.8:

Theorem 2.10 *The functor **G** from **p-Rings** to **RS** preserves finite products and arbitrary filtered colimits.* ■

In general, **G** <u>does not</u> preserve infinite products. If $R := \mathbb{C}([0,1])$ is the ring of continuous real valued functions on the real unit interval, partially ordered by squares, it can be shown that $G(R^\omega)$ is not isomorphic to $G(R)^\omega$.

[1] If $x = 1\lceil\{\lambda\}$, then $\tau(x) = 1$ for all $\tau \in X_\lambda$, while $\tau'(x) = 0$, for all τ' in $X_{\lambda'}$.

References

[ABR] C. Andradas, L. Bröcker, J. Ruiz, **Constructible Sets is Real Geometry**, Modern Surveys in Math **33**, Springer, 1996.

[DM1] M. Dickmann, F. Miraglia, **Special Groups : Boolean-Theoretic Methods in the Theory of Quadratic Forms**, Memoirs Amer. Math. Soc. **689**, Providence, R.I., 2000.

[DM2] M. Dickmann, F. Miraglia, *Rings and Real Semigroups*, Tribute Series **17**, College Publications, 23-51, London, 2011.

[DP1] M. Dickmann, A. Petrovich, *Real Semigroups and Abstract Real Spectra, I*, Contemp. Math. **344**, p. 99-119 (2004).

[DP2] M. Dickmann, A. Petrovich, **Real Semigroups, Real Spectra and Quadratic Forms over Rings**, February, 2015, in preparation.

[DP3] M. Dickmann, A. Petrovich, *Spectral Real Semigroups*, Annales de la Faculté des Sciences de Toulouse, Mathématiques, Série 6, Vol. XXI (2012), 359-412.

[M] M. Marshall, **Spaces of Orderings and Abstract Real Spectra**, Lect. Notes in Math. **1636**, Springer, 1996.

M. Dickmann
Équipe de Logique Mathématique,
Institut de Mathématiques de Jussieu
Paris Rive Gauche
Universités de Paris VI et VII
e-mail: dickmann@math.univ-paris-diderot.fr

F. Miraglia
Departamento de Matemática
Instituto de Matemática e Estatística
Universidade de São Paulo
São Paulo, Brazil
e-mail: miraglia@ime.usp.br

A. Petrovich
Departamento de Matemáticas
Faculdad de Cs. Exatas y Naturales
Universidad de Buenos Aires
Ciudad Universitária
1428 Buenos Aires, Argentina
e-mail: apetrov@dm.uba.ar

WITT EQUIVALENCE OF FUNCTION FIELDS OVER GLOBAL FIELDS

PAWEŁ GŁADKI AND MURRAY MARSHALL

ABSTRACT. Witt equivalent fields can be understood to be fields having the same symmetric bilinear form theory. Witt equivalence of finite fields, local fields and global fields is well understood. Witt equivalence of function fields of curves defined over archimedean local fields is also well understood. In the present note we communicate our recent results, where Witt equivalence of general function fields over global fields is studied. For any two such fields K, L, any Witt equivalence $K \sim L$ induces a cannonical bijection $v \leftrightarrow w$ between Abhyankar valuations v on K having residue field not finite of characteristic 2 and Abhyankar valuations w on L having residue field not finite of characteristic 2. The main tool used in the proof is a method for constructing valuations due to Arason, Elman and Jacob [1]. The method of proof does not extend to non-Abhyankar valuations. The result is applied to study Witt equivalence of function fields over number fields. For example, if k, ℓ are number fields and $k(x_1, \dots, x_n) \sim \ell(x_1, \dots, x_n)$, $n \geq 1$, then $k \sim \ell$ and the 2-ranks of the ideal class groups of k and ℓ are equal. The proofs are omitted.

1. INTRODUCTION

Let K be a field. Denote by $W(K)$ the Witt ring of (non-degenerate) symmetric bilinear forms over K; see [27], [29] or [48] for the definition in case $\text{char}(K) \neq 2$ and [19], [20] or [33] for the definition in the general case. Denote by $Q(K)$ the quadratic hyperfield of K; roughly speaking this is the same thing as the quadratic form scheme of K [26] [27]; see Section 3 for the definition. We say two fields K, L are *Witt equivalent,* denoted $K \sim L$, if $Q(K) \cong Q(L)$ as hyperfields, equivalently, if $W(K) \cong W(L)$ as rings; see Proposition 3.2 below. Witt equivalent fields can be understood as fields having the same symmetric bilinear form theory.

Witt equivalence of finite fields and local fields is well understood. Witt equivalence of global fields is considered in [5], [36], [42], [43], [44]. Witt equivalence of function fields of curves defined over local and global fields is considered in [13], [21], [22]. (Note, however, that there is a serious error in the proof of Theorem 1.3 in [21], in the proof of (1.3.1) $\Rightarrow$ (1.3.2).)

It is well-known that any hyperfield isomorphism $\alpha : Q(K) \to Q(L)$ carries orderings of K to orderings of L in the sense that if $P \subsetneq K^*$ is the positive cone of an ordering of K then

$$Q = \{s \in L^* : \overline{s} = \alpha(\overline{t}) \text{ for some } t \in P\}$$

2000 *Mathematics Subject Classification.* Primary 11E81, 12J20 Secondary 11E04, 11E12.

Key words and phrases. symmetric bilinear forms, quadratic forms, Witt equivalence of fields, function fields, global fields, valuations, Abhyankar valuations.

The research of the second author was supported in part by NSERC of Canada.

is the positive cone of an ordering of L. Here, $\overline{x}$ denotes the image of x under the canonical map $K^* \to K^*/K^{*2}$. This correspondence can also be deduced from the fact that orderings on K correspond to ring homomorphisms from $W(K)$ to $\mathbb{Z}$.

It is natural to wonder if a similar result holds for valuations, i.e., if the valuations of a field K can be detected by looking at the quadratic hyperfield $Q(K)$. At this level of generality the result is false. E.g., $\mathbb{C} \sim \mathbb{F}_2$ and $\mathbb{C}((x)) \sim \mathbb{F}_5$. In each of these examples, the first field has lots of non-trivial valuations, but the second field has only the trivial valuation. At the same time, there is a detection procedure which works for certain sorts of fields. E.g., if K, L are global fields of characteristic $\neq 2$, then any hyperfield isomorphism $\alpha : Q(K) \to Q(L)$ induces in a cannonical way a bijection $v \leftrightarrow w$ between valuations v of K and valuations w of L; see [5], [36], [42], [43], [44]. The main tool for setting up this bijection is a method of constructing valuations described in [1], which is based, in turn, on earlier constructions, of a similar sort, described in [15] and [46].

In the present paper we extend the above-mentioned result for global fields, proving that if K, L are function fields over global fields then any hyperfield isomorphism $\alpha : Q(K) \to Q(L)$ induces in a canonical way a bijection $v \leftrightarrow w$ between Abhyankar valuations v of K having residue field not finite of characteristic 2 and Abhyankar valuations w of L having residue field not finite of characteristic 2; see Theorem 7.5.

Our results are applied to study Witt equivalence of function fields over number fields; see Corollary 8.2, Theorem 8.6 and Corollary 8.8. It is proved, for example, that if $k(x_1, \dots, x_n) \sim \ell(x_1, \dots, x_n)$, where $n \geq 1$ and k and ℓ are number fields, then $k \sim \ell$ and the 2-ranks of the ideal class groups of k and ℓ are equal.

In Sections 2 and 3 we recall basic terminology which is used throughout the paper. In Section 4 we establish basic connections between quadratic hyperfields and valuations. In Section 5 we apply the result in [1] to understand the behavior of valuations under Witt equivalence; see Theorem 5.3. In Section 6 we recall the terminology of function fields, global fields and Abhyankar valuations, and we introduce the idea of nominal transcendence degree.

The main new results in the paper are found in Sections 5,7 and 8.

The authors would like to express their thanks to the annonymous referee for his careful reading and useful improvements that made the presentation more comprehensible.

2. HYPERFIELDS

A hyperfield is an object like a field, but where the addition is allowed to be multivalued. Hyperfields were introduced by Krasner [23], [24], in connection with his work on valuations. Hyperfields were also introduced independently in [31] where they were called multifields.

A *hyperfield* is a system $(H, +, \cdot, -, 0, 1)$ where H is a set, $+$ is a multivalued binary operation on H, i.e., a function from $H \times H$ to the set of all subsets of H, $\cdot$ is a binary operation on H, $- : H \to H$ is a function, and $0, 1$ are elements of H such that

I. $(H, +, -, 0)$ is a canonical hypergroup, terminology as in Mittas [35], i.e.,

(1) $c \in a + b \Rightarrow a \in c + (-b)$,

(2) $a \in b + 0$ iff $a = b$,

(3) $(a + b) + c = a + (b + c)$, and

(4) $a + b = b + a$; and

II. $(H, \cdot, 1)$ is a commutative monoid, i.e., $(ab)c = a(bc)$, $ab = ba$, and $a1 = a$ for all $a, b, c \in A$; and

III. $a0 = 0$ for all $a \in H$; and

IV. $a(b + c) \subseteq ab + ac$; and

V. $1 \neq 0$ and every non-zero element has a multiplicative inverse.

Hyperfields form a category. A *morphism* from H_1 to H_2, where H_1, H_2 are hyperfields, is a function $\alpha : H_1 \to H_2$ which satisfies $\alpha(a + b) \subseteq \alpha(a) + \alpha(b)$, $\alpha(ab) = \alpha(a)\alpha(b)$, $\alpha(-a) = -\alpha(a)$, $\alpha(0) = 0$, $\alpha(1) = 1$.

Here are some elementary consequences of the hyperfield axioms: (i) $-0 = 0$ (ii) $-(-a) = a$ (iii) $a + b \neq \emptyset$ (iv) $a(-b) = -(ab)$ (v) $(-a)(-b) = ab$.

Every field is a hyperfield. The simplest non-trivial examples of hyperfields are the quotient hyperfields. If T is a subgroup of H^*, where H is a field or hyperfield, the *quotient hyperfield* $H/_mT = (H/_mT, +, \cdot, -, 0, 1)$ is defined as follows: $H/_mT$ is the set of equivalence classes with respect to the equivalence relation $\sim$ on H defined by $a \sim b$ iff $as = bt$ for some $s, t \in T$. The operations on $H/_mT$ are the obvious ones induced by the corresponding operations on H: Denote by $\overline{a}$ the equivalence class of a. Then $\overline{a} \in \overline{b} + \overline{c}$ iff $as \in bt + cu$ for some $s, t, u \in T$, $\overline{a}\overline{b} = \overline{ab}$, $-\overline{a} = \overline{-a}$. Also, $0 = \overline{0}$, and $1 = \overline{1}$. The group of non-zero elements of $H/_mT$ is H^*/T. The subscript m here is used to indicate that $H/_mT$ is a quotient modulo a multiplicative subgroup T and was introduced in [31]: although we call $H/_mT$ a quotient, its construction really resembles more that of a localisation, and the authors believe that denoting it simply by H/T might be somewhat misleading.

The hyperfield associated to an ordered abelian group $\Gamma := (\Gamma, \cdot, 1, \leq)$ is $\Gamma \cup \{0\} := (\Gamma \cup \{0\}, +, \cdot, -, 0, 1)$, where

$$a + b := \begin{cases} b \text{ if } a < b \\ a \text{ if } b < a \\ [0, a] \text{ if } a = b \end{cases},$$

$a \cdot 0 = 0 \cdot a := 0$ and $-a := a$. Convention: $0 < a$ for all $a \in \Gamma$.

A valuation on a field K is just a morphism $v : K \to \Gamma \cup \{0\}$, for some ordered abelian group $\Gamma := (\Gamma, \cdot, 1, \leq)$. If Γ is the value group of v, i.e., if v is surjective, then v induces an isomorphism $\overline{v} : K/_mU \to \Gamma \cup \{0\}$, where U is the unit group of v.[1]

See [32] for an example of a hyperfield which is not realizable as a quotient hyperfield of a field.

We are mostly interested in one special example of a quotient hyperfield, namely the hyperfield $K/_mK^{*2}$, for a fixed field K, and its particular connection to symmetric bilinear forms over K. Observe that, for a field K, and for $z, a, b \in K$ the following equivalence holds true:

$$z = ax^2 + by^2 \text{ for some } x, y \in K^* \text{ if and only if } \overline{z} \in \overline{a} + \overline{b} \text{ in } K/_mK^{*2}.$$

[1]The foregoing example notwithstanding, in what follows we will always use the more standard additive notation for valuations, i.e., a valuation is a function $v : K \to \Gamma \cup \{\infty\}$, for some ordered abelian group $\Gamma := (\Gamma, +, 0, \geq)$.

It turns out that, in fact, a slightly more general equivalence holds true, at least when $K \neq \mathbb{F}_2, \mathbb{F}_3$, $\mathrm{char}(K) \neq 2$ (see Proposition 3.1 below for details), namely:

$$z = ax^2 + by^2 \text{ for some } x, y \in K \text{ if and only if } \overline{z} \in \overline{a} + \overline{b} \text{ in } K/_m K^{*2}.$$

This equivalence fails to hold without these additional assumptions. Here it is necessary to modify the definition of addition in $K/_m K^{*2}$, defining $\overline{a} + \overline{b}$, for $a, b \neq 0$, "by hand". Fortunately enough, this can be also done more conceptually, by defining a new addition on any given hyperfield.

If $H = (H, +, \cdot, -, 0, 1)$ is a hyperfield, the *prime addition* on H is defined by

$$a +' b = \begin{cases} a + b & \text{if one of } a, b \text{ is zero} \\ a + b \cup \{a, b\} & \text{if } a \neq 0,\ b \neq 0,\ b \neq -a \\ H & \text{if } a \neq 0,\ b \neq 0,\ b = -a \end{cases}.$$

In the next section we use the following result:

Proposition 2.1. For any hyperfield $H := (H, +, \cdot, -, 0, 1)$, $H' := (H, +', \cdot, -, 0, 1)$ is also a hyperfield.

We refer to H' as the *prime* of the hyperfield H. Observe that if T is a subgroup of H^* then $H'/_m T = (H/_m T)'$.

3. Quadratic hyperfields and Witt equivalence

Let K be a field. The *quadratic hyperfield* of K, denoted $Q(K)$, is defined to be the prime of the hyperfield $K/_m K^{*2}$.[2] Note that $Q(K)^* = K^*/K^{*2}$.

Proposition 3.1. Assume $\overline{a} \in Q(K)^*$. Then
(1) $\overline{a}^2 = \overline{1}$.
(2) If $\overline{a} \neq -\overline{1}$ then $\overline{1} + \overline{a}$ is a subgroup of $Q(K)^*$.[3]
(3) If $K \neq \mathbb{F}_3, \mathbb{F}_5$ and $\mathrm{char}(K) \neq 2$ then $Q(K) = K/_m K^{*2}$.

The interest in $Q(K)$ stems from its connection to symmetric bilinear forms over K. One is mainly interested in the characteristic $\neq 2$ case. In this case, symmetric bilinear forms and quadratic forms are the same thing.

Denote by $W(K)$ the Witt ring of non-degenerate symmetric bilinear forms over K; see [27], [29] or [48] for the definition in case $\mathrm{char}(K) \neq 2$ and [19], [20] or [33] for the definition in the general case.

---

[2]This is the same object referred to in [31, page 458]. Roughly speaking, it is the quadratic form scheme of K, terminology as in [26] or [27], with zero adjoined.

[3]If $G = (G, -1, V)$ is an (abstract) quadratic form scheme, terminology as in [26], then $H = (H, +, \cdot, -, 0, 1)$, where $H := G \cup \{0\}$,

$$a + b := \begin{cases} a \text{ if } b = 0 \\ b \text{ if } a = 0 \\ a \cdot V(ab) \text{ if } a, b \neq 0, b \neq -a \\ H \text{ if } a, b \neq 0, b = -a \end{cases},$$

$a \cdot 0 = 0 \cdot a := 0$ and $-a := (-1) \cdot a$, is hyperfield satisfying (1) and (2) of Proposition 3.1, i.e., for all $a \in H^*$ (1) $a^2 = 1$ and (2) if $a \neq -1$ then $1 + a$ is a subgroup of H^*. Conversely, every hyperfield H satisfying (1) and (2) arises in this way, from some unique quadratic form scheme G. See [26, Theorem 1.4] for some equivalent descriptions of quadratic form schemes. The question of whether every quadratic form scheme is realized as the quadratic form scheme of a field appears to be still open.

A (non-degenerate diagonal) *binary form* over K is just an ordered pair $\langle \overline{a}, \overline{b} \rangle$, $\overline{a}, \overline{b} \in K^*/K^{*2}$. The *value set* of such a form, denoted by $D_K\langle \overline{a}, \overline{b} \rangle$, is the set of non-zero elements of $\overline{a} + \overline{b}$, i.e., $D_K\langle \overline{a}, \overline{b} \rangle$ is the image under $K^* \to K^*/K^{*2}$ of the subset $D_K\langle a, b \rangle$ of K^* defined by

$$D_K\langle a, b \rangle := \begin{cases} K^* \text{ if } -ab \in K^{*2} \\ \{z \in K^* : z = ax^2 + by^2, x, y \in K\} \text{ otherwise} \end{cases}.$$

Two binary forms $\langle \overline{a}, \overline{b} \rangle$ and $\langle \overline{c}, \overline{d} \rangle$ are considered to be *equivalent*, denoted $\langle \overline{a}, \overline{b} \rangle \approx \langle \overline{c}, \overline{d} \rangle$, if $\overline{c} \in D_K\langle \overline{a}, \overline{b} \rangle$ and $\overline{a}\overline{b} = \overline{c}\overline{d}$.

In terms of generators and relations, $W(K)$ is the integral group ring $\mathbb{Z}[K^*/K^{*2}]$ factored by the ideal generated by $[1] + [-1]$ and all elements

$$[a] + [b] - [c] - [d] \text{ such that } \overline{a}, \overline{b}, \overline{c}, \overline{d} \in K^*/K^{*2},\ \langle \overline{a}, \overline{b} \rangle \approx \langle \overline{c}, \overline{d} \rangle.$$

See [20, Theorem 1.16 (iv) and Corollary 1.17] for the proof. Here, $[x]$ denotes the image of $\overline{x}$ under the canonical embedding $K^*/K^{*2} \hookrightarrow \mathbb{Z}[K^*/K^{*2}]$.

A hyperfield isomorphism $\alpha : Q(K) \to Q(L)$, where K, L are fields, can be viewed as a group isomorphism $\alpha : K^*/K^{*2} \to L^*/L^{*2}$ such that $\alpha(-\overline{1}) = -\overline{1}$ and

$$\alpha(D_K\langle \overline{a}, \overline{b} \rangle) = D_L\langle \alpha(\overline{a}), \alpha(\overline{b}) \rangle \text{ for all } \overline{a}, \overline{b} \in K^*/K^{*2},$$

or, equivalently, as a group isomorphism $\alpha : K^*/K^{*2} \to L^*/L^{*2}$ which induces a ring isomorphism between $W(K)$ and $W(L)$. We say two fields K and L are *Witt equivalent*, denoted $K \sim L$, to indicate that $Q(K)$ and $Q(L)$ are isomorphic as hyperfields. For completeness and clarity we record the following:

Proposition 3.2. *$K \sim L$ iff $W(K)$ and $W(L)$ are isomorphic as rings.*

For fields of characteristic $\neq 2$, Witt equivalence is also characterized in terms of Galois groups; see [34, Theorem 3.8].

It is well-known that the Witt ring of a field K encodes the theory of symmetric bilinear forms over K. Witt equivalent fields can be understood as fields having the same symmetric bilinear form theory. The quadratic hyperfield $Q(K)$ encodes exactly the same information as the Witt ring $W(K)$. At the same time, it is a much simpler and easier object to deal with.

Hyperfields provide a first-order axiomatization of the algebraic theory of quadratic forms. Although other first-order descriptions have been already known for some time (see [9] and [30]), it seems that the theory of hyperfields is the most natural and the most easily understood. All the results presented in what follows can be "translated" to the traditional notion of Witt rings, and, as of today, the authors are not familiar with any results in the algebraic theory of quadratic forms that can be proven with the use of hyperfields, but can not be proven without them. Still, the authors believe that hyperfields make the exposition easier to read and to understand.

4. Quadratic hyperfields and valuations

Let H_1, H_2 be hyperfields. Each morphism $\iota : H_1 \to H_2$ induces a morphism $\overline{\iota} : H_1/_m\Delta \to H_2$ where $\Delta := \{x \in H_1^* : \iota(x) = 1\}$. The morphism ι is said to be a *quotient morphism* if $\overline{\iota}$ is an isomorphism, equivalently, if ι is surjective, and $\iota(c) \in \iota(a) + \iota(b)$ iff $cs \in at + bu$ for some $s, t, u \in \Delta$. A morphism $\iota : H_1 \to H_2$

is said to be a *group extension* if ι is injective, every $x \in H_2^* \setminus \iota(H_1^*)$ is *rigid* in the sense that $1 + x \subseteq \{1, x\}$,[4] and $y \in H_1$, $y \neq -1 \Rightarrow \iota(1+y) = 1 + \iota(y)$.

We assume now that K is a field. For a valuation v on K, Γ_v denotes the value group, A_v denotes the valuation ring, M_v the maximal ideal, U_v the unit group, and K_v the residue field. $\pi = \pi_v : A_v \to K_v$ denotes the canonical homomorphism, i.e., $\pi(a) = a + M_v$. We say v is *discrete rank one* if $\Gamma_v = \mathbb{Z}$. See [10], [12], [37] for background material on valuations.

We will be interested in the subgroup $T = (1 + M_v)K^{*2}$ of K^*.

Proposition 4.1. Suppose v is non-trivial and $T = (1 + M_v)K^{*2}$. Then:
(1) $T \cup xT \subsetneq T + xT$ for all $x \in K^*$;
(2) $T - T = K$;
(3) The map $Q(K) \to K/_mT$ defined by $\overline{x} \mapsto xT$ is a quotient morphism.

Propositions 4.2 and 4.3 below are variants of old results of Springer [40], [41] couched in the language of quadratic hyperfields. Consider the canonical group isomorphism $\alpha : U_vK^{*2}/(1+M_v)K^{*2} \to K_v^*/K_v^{*2}$ induced by $x \in U_v \mapsto \pi(x) \in K_v^*$. Define $\iota : Q(K_v) \to K/_mT$ by $\iota(0) = 0$ and $\iota(a) = \alpha^{-1}(a)$ for $a \in K_v^*/K_v^{*2}$.

Proposition 4.2. Suppose v is non-trivial and $T = (1 + M_v)K^{*2}$. Then:
(1) ι is a morphism;
(2) ι is a group extension.

Note: The cokernel of the group embedding $\alpha^{-1} : K_v^*/K_v^{*2} \to K^*/T$ is equal to $K^*/U_vK^{*2} \cong \Gamma_v/2\Gamma_v$. For this reason we sometimes say that $K/_mT$ is a *group extension of* $Q(K_v)$ *by the group* $\Gamma_v/2\Gamma_v$.

Proposition 4.3. Suppose v is non-trivial, $\text{char}(K_v) \neq 2$, and $T = (1 + M_v)K^{*2}$. Then $K/_mT$ is naturally identified with $Q(\tilde{K}_v)$, where $\tilde{K}_v$ denotes the henselization of (K, v).

Note: The conclusions of Propositions 4.1, 4.2 and 4.3 also hold when v is trivial, provided $K \neq \mathbb{F}_3, \mathbb{F}_5$ and $\text{char}(K) \neq 2$.

If v is discrete rank one, one can replace henselization by completion in Proposition 4.3. The assumption in Proposition 4.3 that $\text{char}(K_v) \neq 2$ is crucial. One says that v is *dyadic* if $\text{char}(K) = 0$, $\text{char}(K_v) = 2$. The structure of $Q(\tilde{K}_v)$ when v is dyadic is complicated; see [27] or [29] for the case where K is a number field and [16] and [17] for the case where K is arbitrary.

Remark 4.4. Suppose v, v' are valuations on K with $v \preceq v'$, i.e., v' is a coarsening of v, i.e., $A_v \subseteq A_{v'}$. Then $M_{v'} \subseteq M_v$ so $(1 + M_{v'})K^{*2} \subseteq (1 + M_v)K^{*2}$. Denote by $\overline{v}$ the valuation on $K_{v'}$ induced by v, i.e., $\overline{v}(\pi_{v'}(a)) = v(a)$, for $a \in U_{v'}$. Note that $\overline{v}$ and v have the same residue field. See [37, Chapter C] for background. Assume now that v, v' are non-trivial and that v' is a proper coarsening of v. Then $K/_m(1 + M_v)K^{*2}$ is a group extension of the hyperfield $K_{v'}/_m(1 + M_{\overline{v}})K_{v'}^{*2}$ in a natural way, and the following diagram of hyperfields and hyperfield morphisms is

[4]We are interested here in the case where the groups H_1^*, H_2^* have exponent 2. In this situation, $1 + x \subseteq \{1, x\} \Leftrightarrow 1 + x = \{1, x\}$.

commutative:

$$
\text{(4.1)} \qquad \begin{array}{ccccc}
Q(K) & \longrightarrow & K/_m(1+M_{v'})K^{*2} & \longrightarrow & K/_m(1+M_v)K^{*2} \\
 & & \uparrow & & \uparrow \\
 & & Q(K_{v'}) & \longrightarrow & K_{v'}/_m(1+M_{\overline{v}})K_{v'}^{*2} \\
 & & & & \uparrow \\
 & & & & Q(K_v)
\end{array}
$$

Here, the horizontal arrows are quotient morphisms and the vertical arrows are group extensions.

Let T be a subgroup of K^*. We say $x \in K^*$ is *T-rigid* if $T + Tx \subseteq T \cup Tx$.

$$B(T) := \{x \in K^* : \text{ either } x \text{ or } -x \text{ is not } T\text{-rigid}\}.$$

Elements of $B(T)$ are said to be *T-basic*. Note that if $x \in K^*$ is T-rigid and $y = tx$, $t \in T$, then y is T-rigid. Consequently, $B(T)$ is a union of cosets of T. -1 is not T-rigid (because $0 \in T - T$), so $\pm T \subseteq B(T)$. We say that T is *exceptional* if $B(T) = \pm T$ and either $-1 \in T$ or T is additively closed.

We recall the result of Arason, Elman and Jacob alluded to in the introduction:

Theorem 4.5. *Let $T \subseteq K^*$ be a subgroup and $H \subseteq K^*$ be a subgroup containing $B(T)$. Then there exists a subgroup $\hat{H}$ of K^* such that $H \subseteq \hat{H}$ and $(\hat{H} : H) \leq 2$ and a valuation v of K such that $1 + M_v \subseteq T$ and $U_v \subseteq \hat{H}$. Moreover, $\hat{H} = H$ works, unless T is exceptional.*

We will apply Theorem 4.5 to study Witt equivalence of function fields over global fields. We make frequent use of the following:

Proposition 4.6.

(1) $B(K^{*2})$ is a subgroup of K^*.

(2) Suppose $T = (1 + M_v)K^{*2}$ for some non-trivial valuation v of K. Then $B(T) \subseteq U_vK^{*2}$ and

$$B(T) = \{x \in K^* : \overline{x} = \iota(\overline{y}) \text{ for some } y \in B(K_v^{*2})\},$$

where $\iota : Q(K_v) \hookrightarrow K/_mT$ is the morphism in Proposition 4.2. $B(T)$ is a group and the group isomorphism $\iota : K_v^*/K_v^{*2} \to U_vK^{*2}/T$ induces a group isomorphism $B(K_v^{*2})/K_v^{*2} \to B(T)/T$. T is exceptional iff K_v^{*2} is exceptional.

5. Matching valuations

For any abelian group Γ, the *rational rank* of Γ, denoted $\mathrm{rk}_{\mathbb{Q}}(\Gamma)$, is defined to be the dimension of the $\mathbb{Q}$-vector space $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$.

We apply Theorem 4.5 to obtain useful results concerning the behaviour of valuations under Witt equivalence; refer to Theorem 5.3 below. We begin with two lemmas.

Lemma 5.1. *If Γ is a torsion free abelian group and $|\Gamma/2\Gamma| = 2^r$, then $\mathrm{rk}_{\mathbb{Q}}(\Gamma) \geq r$.*

This is well known. Observe that if $\Gamma \cong \mathbb{Z} \times \cdots \times \mathbb{Z}$ (r factors) then $|\Gamma/2\Gamma| = 2^r$, so $\mathrm{rk}_{\mathbb{Q}}(\Gamma) = r$ holds in this case. On the other hand, if $\Gamma = \mathbb{Q}$ for example then $\mathrm{rk}_{\mathbb{Q}}(\Gamma) = 1$, $r = 0$.

Lemma 5.2. *Suppose v, w are non-comparable valuations on a field K and Γ_v is finitely generated as an abelian group. Then $(1+M_w)K^{*2} \not\subseteq (1+M_v)K^{*2}$.*

Note: Since the abelian group Γ_v is torsion free, the assumption that Γ_v is finitely generated is equivalent to $\Gamma_v \cong \mathbb{Z} \times \cdots \times \mathbb{Z}$, r times, for some $r \geq 0$.

Theorem 5.3. *Suppose K, L are fields, $\alpha : Q(K) \to Q(L)$ is a hyperfield isomorphism and v is a valuation on K such that Γ_v is finitely generated as an abelian group. Suppose either (i) the basic part of $(1+M_v)K^{*2}$ is U_vK^{*2} and $(1+M_v)K^{*2}$ is unexceptional, or (ii) the basic part of $(1+M_v)K^{*2}$ is $(1+M_v)K^{*2}$ and $(1+M_v)K^{*2}$ has index 2 in U_vK^{*2}. Then there exists a valuation w on L such that the image of $(1+M_v)K^{*2}/K^{*2}$ under α is $(1+M_w)L^{*2}/L^{*2}$ and $(L^* : U_wL^{*2}) \geq (K^* : U_vK^{*2})$. If (i) holds, then the image of U_vK^{*2}/K^{*2} under α is U_wL^{*2}/L^{*2}.*

Proposition 5.4.

(1) Suppose K, L are fields and $\alpha : Q(K) \to Q(L)$ is a hyperfield isomorphism such that the image of $(1+M_v)K^{*2}/K^{*2}$ under α is $(1+M_w)L^{*2}/L^{*2}$. Then α induces a hyperfield isomorphism $K/_m(1+M_v)K^{*2} \to L/_m(1+M_w)L^{*2}$ such that the obvious diagram

$$\begin{array}{ccc} Q(K) & \longrightarrow & Q(L) \\ \downarrow & & \downarrow \\ K/_m(1+M_v)K^{*2} & \longrightarrow & L/_m(1+M_w)L^{*2} \end{array} \tag{5.1}$$

commutes.

(2) If, in addition, the image of U_vK^{*2}/K^{*2} under α is U_wL^{*2}/L^{*2}, then α induces a hyperfield isomorphism $Q(K_v) \to Q(L_w)$ and a group isomorphism $\Gamma_v/2\Gamma_v \to \Gamma_w/2\Gamma_w$ such that the obvious diagrams

$$\begin{array}{ccc} K/_m(1+M_v)K^{*2} & \longrightarrow & L/_m(1+M_w)L^{*2} \\ \uparrow & & \uparrow \\ Q(K_v) & \longrightarrow & Q(L_w) \end{array} \tag{5.2}$$

and

$$\begin{array}{ccc} Q(K)^* & \longrightarrow & Q(L)^* \\ \downarrow & & \downarrow \\ \Gamma_v/2\Gamma_v & \longrightarrow & \Gamma_w/2\Gamma_w \end{array} \tag{5.3}$$

commute. We are assuming here that v, w are non-trivial.

6. Abhyankar valuations on function fields over global fields

Suppose K and k are fields. We say K is a *function field* over k if K is a finitely generated field extension of k. If $\text{trdeg}(K : k) = n$ we say K is a *function field in n variables* over k. The *field of constants* of K over k (i.e., the algebraic closure of k in K) is a finite extension of k [28, Chapter 10, Proposition 3]. We do not require that k is the field of constants of K over k. If K is a function field over k and v is a valuation on K, the *Abhyankar inequality* asserts that

$$\text{trdeg}(K : k) \geq \text{rk}_{\mathbb{Q}}(\Gamma_v/\Gamma_{v|k}) + \text{trdeg}(K_v : k_{v|k}),$$

where $v|k$ denotes the restriction of v to k. We will say the valuation v is *Abhyankar* (relative to k) if

$$\operatorname{trdeg}(K:k) = \operatorname{rk}_{\mathbb{Q}}(\Gamma_v/\Gamma_{v|k}) + \operatorname{trdeg}(K_v : k_{v|k}).$$

In this case it is well known that $\Gamma_v/\Gamma_{v|k}$ is finitely generated and K_v is a function field over $k_{v|k}$. For a proof of these assertions see [25, Corollary 26].

A *global field* is a field which is either a number field, i.e., a finite extension of $\mathbb{Q}$, or a function field of transcendence degree 1 over a finite field.

We are interested here in function fields over global fields, equivalently, function fields of transcendence degree ≥ 0 over $\mathbb{Q}$ or function fields of transcendence degree ≥ 1 over $\mathbb{F}_p$ for some prime p. If K is any field we define the *nominal transcendence degree* of K to be

$$\operatorname{ntd}(K) := \begin{cases} \operatorname{trdeg}(K:\mathbb{Q}) & \text{if } \operatorname{char}(K)=0 \\ \operatorname{trdeg}(K:\mathbb{F}_p)-1 & \text{if } \operatorname{char}(K)=p\neq 0 \end{cases}.$$

Thus, if K is a function field over a global field k, then $\operatorname{ntd}(K) = \operatorname{trdeg}(K:k)$. In this situation, for any valuation v of K,

$$\operatorname{rk}_{\mathbb{Q}}(\Gamma_v) := \begin{cases} \operatorname{rk}_{\mathbb{Q}}(\Gamma_v/\Gamma_{v|k}) & \text{if } v|k \text{ is trivial} \\ \operatorname{rk}_{\mathbb{Q}}(\Gamma_v/\Gamma_{v|k})+1 & \text{if } v|k \text{ is discrete rank 1} \end{cases},$$

and

$$\operatorname{ntd}(K_v) := \begin{cases} \operatorname{trdeg}(K_v:k_{v|k}) & \text{if } v|k \text{ is trivial} \\ \operatorname{trdeg}(K_v:k_{v|k})-1 & \text{if } v|k \text{ is discrete rank 1} \end{cases}.$$

It follows, for any valuation v of K, the Abhyankar inequality implies

$$\operatorname{ntd}(K) \geq \operatorname{rk}_{\mathbb{Q}}(\Gamma_v) + \operatorname{ntd}(K_v),$$

and v is Abhyankar (relative to k) iff

$$\operatorname{ntd}(K) = \operatorname{rk}_{\mathbb{Q}}(\Gamma_v) + \operatorname{ntd}(K_v).$$

Moreover, if v is Abhyankar (relative to k) then

$$\Gamma_v \cong \mathbb{Z}\times\cdots\times\mathbb{Z}$$

(with $\operatorname{rk}_{\mathbb{Q}}(\Gamma_v)$ factors) and K_v is either a function field over a global field (if $\operatorname{ntd}(K_v)\geq 0$) or a finite field (if $\operatorname{ntd}(K_v)=-1$).

7. Witt equivalence of function fields over global fields

The main result in this section is Theorem 7.5 which explains how a Witt equivalence of function fields over global fields induces a natural bijection between Abhyankar valuations.

It is important to point out that the bijection between Abhyankar valuations of function fields over global fields is very special. In general, Witt equivalence of two fields does not imply any bijection between valuations whatsoever, as shown in the following simple example:

Example 7.1. Let $F = k((t))$, where k is an algebraically closed field, $\operatorname{char} k \neq 2$. Denote by v the natural valuation on F, i.e.,

$$v(\sum_{i=n}^{\infty} a_i t^i) := \min\{i : a_i \neq 0\} \text{ if } \sum_{i=n}^{\infty} a_i t^i \neq 0.$$

The residue field of (F, v) is k, the value group is $\mathbb{Z}$. Applying Proposition 4.2, we see that $Q(F)$ is a group extension of $Q(k) = \{0,1\}$ by a cyclic group of order 2, so $Q(F) = \{0,1,p\}$, $p \in Q(F)\backslash Q(k)$, $a+0=a$, $1+1=p+p=\{0,1,p\}$, $1+p=\{1,p\}$, $a \cdot 0 = 0$, $1 \cdot 1 = p \cdot p = 1$, $1 \cdot p = p$. It is not difficult to check that exactly the same identities hold true for $Q(\mathbb{F}_5)$, so that $Q(F) \cong Q(\mathbb{F}_5)$ and thus $F \sim \mathbb{F}_5$. At the same time, F has lots of non-trivial valuations, whereas $\mathbb{F}_5$ has only the trivial one.

We begin with some preliminary results.

Lemma 7.2. *Suppose K is a function field over a global field. Then*

(1) There are infinitely many discrete rank one Abhyankar valuations v on K.

(2) The group K^*/K^{*2} is infinite.

(3) For any $x \in K^*$, $\exists\ y \in K^{*2} + xK^{*2}$, $y \notin K^{*2} \cup xK^{*2}$. If $\operatorname{char}(K) \neq 2$ or $x \notin K^{*2}$ one can choose $y \neq 0$.

(4) $B(K^{*2}) = K^*$.

All of this seems to be well-known. Anyway, here is a proof.

Theorem 7.3. *Suppose K is a function field over a global field and v is an Abhyankar valuation on K. Then:*

(1) $(K^* : U_v K^{*2}) = 2^{\operatorname{rk}_{\mathbb{Q}}(\Gamma_v)}$.

(2)
$$(U_vK^{*2} : (1+M_v)K^{*2}) = \begin{cases} \infty & \text{if } \operatorname{ntd}(K_v) \geq 0 \\ 2 & \text{if } K_v \text{ is finite, } \operatorname{char}(K_v) \neq 2 \\ 1 & \text{if } K_v \text{ is finite, } \operatorname{char}(K_v) = 2 \end{cases}.$$

(3) The basic part of $T := (1+M_v)K^{*2}$ is
$$\begin{cases} U_vK^{*2} & \text{if } \operatorname{ntd}(K_v) \geq 0 \\ \pm T = U_vK^{*2} & \text{if } K_v \text{ is finite, } \operatorname{char}(K_v) \neq 2, -1 \notin K_v^{*2} \\ T & \text{if } K_v \text{ is finite, } \operatorname{char}(K_v) \neq 2, -1 \in K_v^{*2} \\ T = U_vK^{*2} & \text{if } K_v \text{ is finite, } \operatorname{char}(K_v) = 2 \end{cases}.$$

Lemma 7.4. *Suppose K is a function field over a global field, L is a field, and $\alpha : Q(K) \to Q(L)$ is a hyperfield isomorphism. Then $\operatorname{ntd}(L) \geq \operatorname{ntd}(K)$.*

Theorem 7.5. *Suppose K, L are function fields over global fields and $\alpha : Q(K) \to Q(L)$ is a hyperfield isomorphism. Then:*

(1) $\operatorname{ntd}(K) = \operatorname{ntd}(L)$.

(2) For each Abhyankar valuation v of K with K_v not finite of characteristic 2 there exists a unique Abhyankar valuation w of L such that α maps $(1+M_v)K^{*2}/K^{*2}$ onto $(1+M_w)L^{*2}/L^{*2}$. L_w is also not finite of characteristic 2, $\operatorname{rk}_{\mathbb{Q}}(\Gamma_v) = \operatorname{rk}_{\mathbb{Q}}(\Gamma_w)$ and $\operatorname{ntd}(K_v) = \operatorname{ntd}(L_w)$.

(3) α maps U_vK^{*2}/K^{*2} onto U_wL^{*2}/L^{*2} except possibly when K_v is finite, $\operatorname{char}(K_v) \neq 2$ and $-1 \in K_v^{*2}$.

(4) For v, w non-trivial, α induces a hyperfield isomorphism $K/_m(1+M_v)K^{*2} \to L/_m(1+M_w)L^{*2}$ such that diagram (5.1) commutes. If, in addition, α maps U_vK^{*2}/K^{*2} onto U_wL^{*2}/L^{*2} then α induces a hyperfield isomorphism $Q(K_v) \to Q(L_w)$ and a group isomorphism $\Gamma_v/2\Gamma_v \to \Gamma_w/2\Gamma_w$ such that diagrams (5.2) and (5.3) commute.

(5) If v corresponds to w and v' corresponds to w' then v' is coarser than v iff w' is coarser than w.

Note: One can show that $Q(K_v) \cong Q(L_w)$ as hyperfields, and $\Gamma_v/2\Gamma_v \cong \Gamma_w/2\Gamma_w$ as groups, even in the case where α does not map U_vK^{*2}/K^{*2} onto U_wL^{*2}/L^{*2}.

The next two lemmas allow one to distinguish the characteristic 2 case from the characteristic $\neq 2$ case. Denote by $\bar{t} \in K^*/K^{*2}$ the image of $t \in K^*$.

Lemma 7.6. *Suppose K is a field,* $\operatorname{char}(K) = 2$*, $\bar{x}, \bar{y} \in K^*/K^{*2}$, $\bar{x}, \bar{y} \neq 1$ and $\bar{y} \in D_K\langle 1, \bar{x}\rangle$. Then $D_K\langle 1, \bar{y}\rangle = D_K\langle 1, \bar{x}\rangle$.*

Lemma 7.7. *Suppose K is a function field over a global field,* $\operatorname{char}(K) \neq 2$*. Then there exists $\bar{x}, \bar{y} \in K^*/K^{*2}$, $\bar{x}, \bar{y} \neq 1$ such that $\bar{y} \in D_K\langle 1, \bar{x}\rangle$, $D_K\langle 1, \bar{y}\rangle \not\subseteq D_K\langle 1, \bar{x}\rangle$.*

Corollary 7.8. *Let K, L be function fields over global fields and $K \sim L$. Then*

(1) $\operatorname{char}(K) = 0$ *iff* $\operatorname{char}(L) = 0$,

(2) $\operatorname{char}(K) = 2$ *iff* $\operatorname{char}(L) = 2$.

Remark 7.9. (1) For a global field K the square of the fundamental ideal of its Witt ring of non-singular symmetric bilinear forms vanishes, if K has characteristic 2 ([33, Theorem III.5.10]) and does not vanish for global fields of any other characteristic (see [33, Chapter III]). Hence, if K and L are Witt equivalent global fields and one field has characteristic 2, the other does also. Corollary 7.8 can be viewed as a certain generalization of this observation.

(2) Any two quadratically closed fields are Witt equivalent, regardless of their characteristics, their Witt ring being just $\mathbb{Z}/2\mathbb{Z}$ ([27, Proposition 3.1], [33, Remark III.3.4]). Therefore it is, in principle, possible to provide an example of two Witt equivalent fields K and L with $\operatorname{char} K = 2$ and $\operatorname{char} L \neq 2$. However, the authors are not aware of any other examples.

Lemma 7.10. *If K is a function field over a field k,* $\operatorname{char}(k) = 2$*, then*

$$[K : K^2] = 2^{\operatorname{trdeg}(K:k)} \cdot [k : k^2].$$

Remark 7.11.

(1) It follows from results in [4] (specifically, from [4, Theorem 2.9 and Proposition 2.10]) that (i) if K, L are global fields of characteristic 2 then $K \sim L$, and (ii) if K, L are function fields over global fields of characteristic 2 of nominal transcendence degree 1 or more then $K \sim L$ iff $K \cong L$. One obtains these results by applying Lemma 7.10, taking $k = \mathbb{F}_2$.

(2) For K, L global fields of characteristic $\neq 2$ the meaning of $K \sim L$ is well understood; see for example [5, Theorem 3.1 and Corollary 3.2].

The relationship between Abhyankar valuations v on K with K_v finite, $\operatorname{char}(K_v) = 2$ and Abhyankar valuations w on L with L_v finite, $\operatorname{char}(L_w) = 2$ seems to be not very well understood.

Remark 7.12.

(1) If K and L are number fields and $\alpha : Q(K) \to Q(L)$ is a hyperfield isomorphism the arguments in [42] show that for each dyadic valuation v of K there exists a unique dyadic valuation w of L such that α maps $(1 + 4M_v)K^{*2}/K^{*2}$ onto $(1 + 4M_w)L^{*2}/L^{*2}$.

(2) Suppose v is a dyadic valuation on a number field K. Denote by $\tilde{K}_v$ the completion of K at v. The natural embedding $K \hookrightarrow \tilde{K}_v$ induces a hyperfield isomorphism $K/_mT \cong Q(\tilde{K}_v)$, where $T := (1 + 4M_v)K^{*2}$. The structure of $Q(\tilde{K}_v)$ is described in [29, Section 3.6] for example.

(3) Suppose K is a function field over $\mathbb{Q}$ and v' is an Abhyankar valuation on K such that the residue field $K_{v'}$ is a number field. Suppose also that v is a valuation of K such that $v \preceq v'$ and the induced valuation $\overline{v}$ on $K_{v'}$ is dyadic. Then $M_{v'} \subseteq M_v$ and $4M_{v'} = M_{v'}$ (so $1 + M_{v'} \subseteq 1 + 4M_v$), $K/_m(1+4M_v)K^{*2}$ is a group extension of the hyperfield $K_{v'}/_m(1+4M_{\overline{v}})K_{v'}^{*2}$ in a natural way, and the following diagram of hyperfields and hyperfield morphisms is commutative:

$$\begin{array}{ccccc} Q(K) & \longrightarrow & K/_m(1+M_{v'})K^{*2} & \longrightarrow & K/_m(1+4M_v)K^{*2} \\ & & \uparrow & & \uparrow \\ & & Q(K_{v'}) & \longrightarrow & K_{v'}/_m(1+4M_{\overline{v}})K_{v'}^{*2} \end{array} \tag{7.1}$$

Here, the horizontal arrows are quotient morphisms and the vertical arrows are group extensions.

(4) It follows from (1), (2) and (3) that if K, L are function fields over global fields and $\alpha : Q(K) \to Q(L)$ is a hyperfield isomorphism, then there is a well-defined bijection $v \leftrightarrow w$ such that α maps $(1+4M_v)K^{*2}/K^{*2}$ onto $(1+4M_w)L^{*2}/L^{*2}$ between Abhyankar valuations v of K with K_v finite, $\mathrm{char}(K_v) = 2$ such that there exists an Abhyankar valuation v' with $v \preceq v'$ and $K_{v'}$ is a number field and Abhyankar valuations w of L with L_w finite, $\mathrm{char}(L_w) = 2$ such that there exists an Abhyankar valuation w' with $w \preceq w'$ and $L_{w'}$ is a number field. The proof is omitted.

The relationship between non-Abhyankar valuations v on K and non-Abhyankar valuations w on L is not very well understood. It is known, by results in [25], that the Abhyankar valuations are dense in the spectral space consisting of all valuations, but this does not seem to help very much.

8. Further applications

Let K be a function field in n variables over a global field. For $0 \le i \le n$ denote by $\nu_{K,i}$ the set of Abyankar valuations v on K with $\mathrm{ntd}(K_v) = i$. Observe that

$$\nu_{K,i} = \nu_{K,i,0} \cup \nu_{K,i,1} \cup \nu_{K,i,2} \text{ (disjoint union)}$$

where

$$\nu_{K,i,j} := \begin{cases} \{v \in \nu_{K,i} : \mathrm{char}(K_v) = 0\} \text{ if } j = 0 \\ \{v \in \nu_{K,i} : \mathrm{char}(K_v) \ne 0, 2\} \text{ if } j = 1 \\ \{v \in \nu_{K,i} : \mathrm{char}(K_v) = 2\} \text{ if } j = 2 \end{cases}.$$

Of course, some of the sets $\nu_{K,i,j}$ may be empty. Specifically, if $\mathrm{char}(K) = p$ for some odd prime p then $\nu_{K,i,j} = \emptyset$ for $j \in \{0, 2\}$, and if $\mathrm{char}(K) = 2$ then $\nu_{K,i,j} = \emptyset$ for $j \in \{0, 1\}$.

Corollary 8.1. *Suppose K, L are function fields in n variables over global fields which are Witt equivalent via a hyperfield isomorphism $\alpha : Q(K) \to Q(L)$. Then for each $i \in \{0, 1, \dots, n\}$ and each $j \in \{0, 1, 2\}$ there is a uniquely defined bijection between $\nu_{K,i,j}$ and $\nu_{L,i,j}$ such that, if $v \leftrightarrow w$ under this bijection, then α maps $(1+M_v)K^{*2}/K^{*2}$ onto $(1+M_w)L^{*2}/L^{*2}$ and U_vK^{*2}/K^{*2} onto U_wL^{*2}/L^{*2}.*

Corollary 8.2. *Let $K \sim L$ be function fields over number fields, with fields of constants k and ℓ respectively. If there exists $v \in \nu_{K,0,0}$ with $K_v = k$ and $w \in \nu_{L,0,0}$ with $L_w = \ell$ then $k \sim \ell$.*

Remark 8.3.

(1) Suppose K is the function field of an irreducible k-variety which has a non-singular k-rational point. (This is always the case, for example, if K is purely transcendental over k.) Then there exists $v \in \nu_{K,0,0}$ with $K_v = k$. To prove this one uses the fact that if A is a regular local ring of dimension n with maximal ideal $\mathfrak{m} = (x_1, \dots, x_n)$ and residue field k, then $A/(x_n)$ is a regular local ring of dimension $n-1$, and the localization of A at the prime ideal (x_n) is a discrete valuation ring with residue field equal to the field of quotients of $A/(x_n)$; e.g., see [3, Chapter 11]. Iterating this procedure yields a chain of Abhyankar valuations $v_1 \succeq \cdots \succeq v_n$ on K with $\mathrm{trdeg}(K_{v_i} : k) = n - i$, $i = 1, \dots, n$ and $K_{v_n} = k$.

(2) If K and L are function fields over global fields of characteristic $\neq 0$, with fields of constants k and ℓ, respectively, then $K \sim L \Rightarrow k \sim \ell$. If k, ℓ have characteristic 2 then $[k : k^2] = [\ell : \ell^2] = 2$, by Lemma 7.10, so $k \sim \ell$, by [4, Proposition 2.10]. Suppose k, ℓ each have characteristic different from 0 and 2. Then k, ℓ each have level 1 or 2. If k has level 1 then K and consequently also L has level 1. Since ℓ is algebraically closed in L this implies ℓ has level 1. This proves k and ℓ have the same level, so $k \sim \ell$, by [5, Corollary 3.2].

(3) Combining Corollary 8.2 with (1) and (2) we see that, in particular, [21, Proposition 3.2] is indeed true (even though the proof of [21, Proposition 3.2] given in [21] is based on the erroneous argument in [21, Theorem 1.3]).

Suppose now that k is a number field. Then every ordering of k is archimedean, i.e., corresponds to a real embedding $k \hookrightarrow \mathbb{R}$. Let r_1, respectively r_2 be the number of real embeddings of k, respectively the number of conjugate pairs of complex embeddings of k. Thus $[k : \mathbb{Q}] = r_1 + 2r_2$. Let

$$V_k := \{r \in k^* : (r) = \mathfrak{a}^2 \text{ for some fractional ideal } \mathfrak{a} \text{ of } k\}.$$

Here, (r) denotes the fractional ideal of k generated by r. Clearly V_k is a subgroup of k^* and $k^{*2} \subseteq V_k$.

Lemma 8.4. *The 2-rank of V_k/k^{*2} is $r_1 + r_2 + 2\text{-rk}(C_k)$, where C_k denotes the ideal class group of k.*

Lemma 8.5. *Suppose $K = k(x_1, \dots, x_n)$ and v is a discrete rank 1 valuation on k. There exists an Abhyankar extension v' of v to K such that $\Gamma_{v'} = \Gamma_v$.*

Theorem 8.6. *Suppose $K = k(x_1, \dots, x_n)$ and $L = \ell(x_1, \dots, x_n)$ where $n \geq 1$ and k and ℓ are number fields, and $\alpha : Q(K) \to Q(L)$ is a hyperfield isomorphism. Then*

(1) $r \in k^*/k^{*2}$ iff $\alpha(r) \in \ell^*/\ell^{*2}$.

(2) The map $r \mapsto \alpha(r)$ defines a hyperfield isomorphism between $Q(k)$ and $Q(\ell)$.

(3) α maps V_k/k^{*2} to V_ℓ/ℓ^{*2}.

(4) The 2-ranks of the ideal class groups of k and ℓ are equal.

Remark 8.7. (1) The fact that Witt rings of number fields carry some data on the parity of class numbers was first noticed in [43], and then some additional results were given in [18]. A deeper study of the relations between Witt equivalence of number fields and 2-ranks of ideal class groups can be found in [7].

(2) One can extend Theorem 8.6 a bit: Let V_k^1 denote the set of all $r \in k^*$ such that $v(r)$ is even for all non-dyadic valuations v of k. By Lemma 8.5,

$$V_k^1/k^{*2} = \{r \in k^*/k^{*2} : r \in U_v K^{*2}/K^{*2} \ \forall v \in \nu_{K,n-1,1}\},$$

so α maps V_k^1/k^{*2} to V_ℓ^1/ℓ^{*2}. Applying this in conjunction with the generalization of Lemma 8.4 given in [6, Lemma 2.4] or [45, Proposition 1], we see that the S-class groups of k and ℓ have the same 2-rank, where S consists of all primes which are infinite or dyadic.

Questions:

(1) In Theorem 8.6, is the hypothesis that K and L are purely transcendental over k and ℓ really necessary?

(2) For arbitrary fields K and L is it true that $K(x) \sim L(x) \Rightarrow K \sim L$?

(3) For fixed integers $n \geq 1$, $m \geq 2$, are there infinitely many Witt inequivalent fields $k(x_1, \ldots, x_n)$, k a number field, $[k : \mathbb{Q}] = m$?

Question 3 is interesting because, for given m, there are only finitely many Witt inequivalent number fields k with $[k : \mathbb{Q}] = m$. For $m = 1, 2, 3$ and 4 these numbers are $1, 7, 8$ and 29 respectively; see [7] and [18].

It is proved in [45] that if ℓ is a number field, $[\ell : \mathbb{Q}]$ even, and $\ell \neq \mathbb{Q}(\sqrt{-1})$, then, for each integer $t \geq 1$, there exists a number field k such that $k \sim \ell$ and the 2-rank of the class group of k is $\geq t$. This extends an earlier result in [7].

Corollary 8.8. *For fixed $n \geq 1$ and fixed number field ℓ, $[\ell : \mathbb{Q}]$ even, $\ell \neq \mathbb{Q}(\sqrt{-1})$, there are infinitely many Witt inequivalent fields of the form $k(x_1, \ldots, x_n)$, k a number field, $k \sim \ell$.*

For odd degree extensions Question 3 remains open. Table 2 in [45] shows that each of the 8 Witt equivalence classes of cubic extensions contains fields with 2-rank of the class group equal to $0, 1$, and 2. Results in [11] [38] [39] [47] show that $0, 1, 2, 3, 4, 5, 7$ can occur as the 2-rank of the class group of a cubic field.

References

[1] J.K. Arason, R. Elman, W. Jacob, Rigid elements, valuations, and realization of Witt rings. *J. Algebra* **110** (1987) 449–467.

[2] J.K. Arason, A. Pfister, Beweis des Krullschen Durchschnittsatzes für den Wittring. *Invent. Math.* **12** (1971), 173–176.

[3] M.F Atiyah, I.G. Macdonald, Introduction to commutative algebra. *Addison-Wesley Publishing Co.*, Reading, Mass.-London-Don Mills, Ont. 1969.

[4] R. Baeza, R. Moresi, On the Witt-equivalence of fields of characteristic 2. *J. Algebra* **92** (1985), no. 2, 446–453.

[5] J. Carpenter, Finiteness theorems for forms over global fields. *Math. Z.* **209** no. 1 (1992) 153–166.

[6] P.E. Conner, J. Hurrelbrink, The 4-rank of $K_2(O)$. *Canad. J. Math.* **41** (1989), no. 5, 932–960.

[7] P.E. Conner, R. Perlis, K. Szymiczek, Wild sets and 2-ranks of class groups. *Acta Arith.* 79 (1997), no. 1, 83–91.

[8] A. Czogała, On reciprocity equivalence of quadratic number fields. *Acta Arith.* 58 (1991), no. 1, 27-46.

[9] M. Dickmann, F. Miraglia, Special groups: Boolean-theoretic methods in the theory of quadratic forms, *Mem. Amer. Math. Soc.* **145**, American Mathematical Society, Providence, RI, 2000.

[10] I. Efrat, Valuations, orderings, and Milnor K-theory. *Mathematical Surveys and Monographs*, **124**. American Mathematical Society, Providence, RI, 2006.

[11] H. Eisenbeis, G. Frey, B. Ommerborn. Computation of the 2-rank of pure cubic fields. *Math. Comp.* **32** (1978), no. 142, 559–569.

[12] A.J. Engler, A. Prestel, Valued fields. *Springer Monographs in Mathematics.* Springer-Verlag, Berlin, 2005.

[13] N. Grenier-Boley, D.W. Hoffmann, Isomorphism criteria for Witt rings of real fields. With appendix by Claus Scheiderer. *Forum Math.* **25** (2013) 1–18.

[14] D.K. Harrison, Witt rings. *University of Kentucky Notes*, Lexington, Kentucky (1970).
[15] W. Jacob, On the structure of Pythagorean fields. *J. Algebra* **68** (1981), no. 2, 247–267.
[16] W. Jacob, Quadratic forms over dyadic valued fields. I. The graded Witt ring. *Pacific J. Math.* **126** no. 1, (1987), 21–79.
[17] W. Jacob, Quadratic forms over dyadic valued fields. II. Relative rigidity and Galois cohomology. *J. Algebra* **148** (1992), no. 1, 162–202.
[18] S. Jakubec, F. Marko, K. Szymiczek, Parity of class numbers and Witt equivalence of quartic fields. *Math. Comp.* 64 (1995), no. 212, 1711–1715.
[19] J.L. Kleinstein, A. Rosenberg, Succinct and representational Witt rings. *Pacific J. Math.* **86** (1980) 99–137.
[20] M. Knebusch, A. Rosenburg, R. Ware, Structure of Witt rings and quotients of Abelian group rings. *Amer. J. Math.* **94** (1972), 119–155.
[21] P. Koprowski, Local-global principle for Witt equivalence of function fields over global fields. *Colloq. Math.* **91** (2002) 293–302.
[22] P. Koprowski, Witt equivalence of algebraic function fields over real closed fields. *Math. Z.* **242** (2002) 323–345.
[23] M. Krasner, Approximation des corps valués complets de caractéristique $p \neq 0$ par ceux de caractéristique 0. 1957 Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956 pp. 129–206 Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain; Librairie Gauthier-Villars, Paris.
[24] M. Krasner, A class of hyperrings and hyperfields, *Internat. J. Math. and Math. Sci.* **6** (1983) 307–312.
[25] F.-V. Kuhlmann, On places of algebraic function fields in arbitrary characteristic. *Advances in Math.* **188** (2004) 399–424.
[26] M. Kula, L. Szczepanik, K. Szymiczek, Quadratic form schemes and quaternionic schemes. *Fund. Math.* **130** (1988), no. 3, 181–190.
[27] T.-Y. Lam, Introduction to quadratic forms over fields. *Graduate Studies in Mathematics* **67** American Mathematical Society, Providence, RI, 2005.
[28] S. Lang, Algebra. *Addison-Wesley Publishing Co.*, Reading, Mass. 1965
[29] M. Marshall, Abstract Witt rings, *Queen's Papers in Pure and Applied Math.* **57**, Queen's University, Kingston, Ontario (1980).
[30] M. Marshall, The elementary type conjecture in quadratic form theory, *Cont. Math* **344** (2004), 275–293.
[31] M. Marshall, Real reduced multirings and multifields, *J. Pure and Appl. Alg.* **205** (2006) 452–468.
[32] Ch.G. Massouros, Methods of constructing hyperfields. *Internat. J. Math. Math. Sci.* **8** no. 4 (1985) 725–728.
[33] J. Milnor, D. Husemoller, Symmetric bilinear forms. *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Band **73**. Springer-Verlag, New York-Heidelberg, 1973.
[34] J. Mináč, M. Spira, Witt rings and Galois groups. *Ann. of Math.* (2) 144 (1996), no. 1, 35–60.
[35] J. Mittas, Sur une classe d'hypergroupes commutatifs. *C. R. Acad. Sci. Paris Sér. A-B* **269** 1969 A485–A488.
[36] R. Perlis, K. Szymiczek, P.E. Conner, R. Litherland, Matching Witts with global fields. *Contemp. Math.* **155** (1994) 365–378.
[37] P. Ribenboim, Théorie des valuations. Deuxième édition multigraphié. Séminaire de Mathématiques Supérieures, No. 9 (Été, 1964) *Les Presses de l'Université de Montréal*, Montreal, Que. 1968.
[38] U. Schneiders, Estimating the 2-rank of cubic fields by Selmer groups of elliptic curves. *J. Number Theory* **62** (1997), no. 2, 375–396.
[39] D. Shanks, The simplest cubic fields. *Math. Comp.* **28** (1974), 1137–1152.
[40] T.A. Springer, Quadratic forms over fields with a discrete valuation. I. Equivalence classes of definite forms. *Indag. Math.* **17**, (1955) 352–362.
[41] T.A. Springer, Quadratic forms over fields with a discrete valuation. II. *Indag. Math.* **18** (1956) 238–246.
[42] K. Szymiczek, Matching Witts locally and globally. *Math. Slovakia* **41** (1991) 315–330.
[43] K. Szymiczek, Witt equivalence of global fields. *Comm. Algebra* **19** (1991) 1125–1149.
[44] K. Szymiczek, Witt equivalence of global fields. II. Relative quadratic extensions. *Trans. Amer. Math. Soc.* **343** (1994) 277–303.

[45] K. Szymiczek, 2-ranks of class groups of Witt equivalent number fields. Number theory (Cieszyn, 1998). *Ann. Math. Sil.* No. 12 (1998), 53–64.
[46] R. Ware, Valuation rings and rigid elements in fields. *Canad. J. Math.* **33** (1981), no. 6, 1338–1355.
[47] L.C. Washington, Class numbers of the simplest cubic fields. *Math. Comp.* **48** (1987), no. 177, 371–384.
[48] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern. *Journal für die reine und angewandte Mathematik* **176** (1937) 31–44.

Institute of Mathematics, University of Silesia,
ul. Bankowa 14, 40-007 Katowice, Poland
and
Department of Computer Science, AGH University of Science and Technology,
al. Mickiewicza 30, 30-059 Kraków, Poland
E-mail address: pawel.gladki@us.edu.pl

Department of Mathematics and Statistics, University of Saskatchewan,
106 Wiggins Rd., Saskatoon, SK S7N 5E6, Canada
E-mail address: marshall@math.usask.ca