Real reduced multirings and multifields[☆]

M. Marshall[1]

Department of Computer Science, University of Saskatchewan, Saskatoon, SK Canada, S7N 5E6

Abstract

We work in the big category of commutative multirings with 1. A multiring is just a ring with multivalued addition. We show that certain key results in real algebra (parts of the Artin–Schreier theory for fields and the Positivstellensatz for rings) extend to the corresponding objects in this category. We also show how the space of signs functor $A \rightsquigarrow Q_{\mathrm{red}}(A)$ defined in [C. Andradas, L. Bröcker, J. Ruiz, Constructible Sets in Real Geometry, Springer, Berlin, 1996; M. Marshall, Spaces of Orderings and Abstract Real Spectra, Springer, Berlin, 1996] extends to this category. The proofs are no more difficult than in the ring case. In fact they are easier. This simplifies and clarifies the presentation in [C. Andradas, L. Bröcker, J. Ruiz, Constructible Sets in Real Geometry, Springer, Berlin, 1996; M. Marshall, Spaces of Orderings and Abstract Real Spectra, Springer, Berlin, 1996]. As a corollary we obtain a first-order description of a space of signs as a multiring satisfying certain additional properties. This simplifies substantially the description given in [M. Dickmann, A. Petrovich, Real semigroups and abstract real spectra I, Cont. Math. 344 (2004) 99–119].
© 2005 Published by Elsevier B.V.

MSC: Primary 14P10

Spaces of signs [1, Chapter 3], also called abstract real spectra in [7, Chapters 6–8], arise naturally in the study of semialgebraic sets, more generally, in the study of constructible sets in the real spectrum of a commutative ring with 1.

Spaces of signs are obtained by 'patching together' other more basic structures called spaces of orderings [1, Chapter 4; 7, Chapters 2–4], reduced special groups [4] or reduced quadratic form schemes [9]. These structures arise in the study of the reduced theory of quadratic forms over a real field.

Let V be an algebraic set in R^n where R is a real closed field, e.g., $R = \mathbb{R}$, and let A denote coordinate ring of V, i.e., the ring of all polynomial functions $f : V \to R$. Consider $f, g \in A$ to be equivalent if f and g have the same sign at each point of V. The space of signs of A, denoted $Q_{\text{red}}(A)$, can be viewed as the set of all equivalence classes of elements of A equipped with the structure inherited from the ring structure on A.

In this paper we work in the big category of multirings (commutative with 1) and show how certain well-known results in real algebra (part of the Artin–Schreier theory for fields and the Positivstellensatz for rings [3]) extend to the corresponding objects in this category. We also show how the space of signs functor $A \rightsquigarrow Q_{\text{red}}(A)$ extends to multirings. The proofs are no more difficult than in the ring case. In fact they are easier, because everything takes place in a single category. As a corollary we obtain an elementary description of spaces of signs as multirings satisfying certain additional properties. This is the goal of the paper.

A multiring is just a ring with multivalued addition. The idea of a multiring is very natural, although there seems to be no reference to it in the literature. Some basic properties of multigroups and multirings are established in Sections 1 and 2.

The simplest example of a real reduced multifield is $Q_2 := \{-1, 0, 1\}$. Here addition and multiplication are defined in the obvious way, by interpreting 1 to mean 'positive', -1 to mean 'negative', and 0 to mean 'zero', i.e., $0 \cdot x = x \cdot 0 = 0$, $(1)(1) = (-1)(-1) = 1$, $(1)(-1) = (-1)(1) = -1$, $x + 0 = 0 + x = x$, $1 + 1 = 1$, $(-1) + (-1) = -1$, and $1 + (-1) = (-1) + 1 = \{-1, 0, 1\}$ (since 'positive plus negative' is indeterminate).

An ordering on a multiring A is just a multiring homomorphism $\sigma : A \to Q_2$. A multiring A has an ordering iff $-1 \notin \sum A^2$. The real spectrum of A, denoted $\text{Sper}(A)$, is the set of all orderings of A. This has a natural topology giving it the structure of a spectral space. Each $a \in A$ determines a function $\bar{a} : \text{Sper}(A) \to Q_2$ defined by $\bar{a}(\sigma) = \sigma(a)$. The mapping $a \mapsto \bar{a}$ defines a multiring homomorphism from A into $Q_2^{\text{Sper}(A)}$. Copying what is done in the ring case in [7, Chapter 5], we develop a version of the Positivstellensatz for multirings, and use this to show that the image of A in $Q_2^{\text{Sper}(A)}$, denoted $Q_{\text{red}}(A)$,[2] is itself a multiring, and is strongly embedded in $Q_2^{\text{Sper}(A)}$. Actually, we prove a more general result; see Proposition 7.3.

A multiring A with $-1 \notin \sum A^2$ is called real reduced if the natural multiring homomorphism from A onto $Q_{\text{red}}(A)$ is an isomorphism. Corollary 7.6 provides a simple characterization of real reduced multirings. The functor $A \rightsquigarrow Q_{\text{red}}(A)$ is a reflection[3] from the cate-

---

[2] If A is the coordinating ring of an algebraic set $V \subseteq R^n$, R real closed, then V is embedded in $\text{Sper}(A)$ via $x \mapsto \sigma_x$ where $\sigma_x \in \text{Sper}(A)$ is defined by $\sigma_x(f) = \text{sgn}(f(x))$. Applying a suitable version of Lang's homomorphism theorem, e.g., [7, Theorem 5.3.1], we see that $\text{sgn}(f(x)) = \text{sgn}(g(x))$ holds for all $x \in V$ iff $\sigma(f) = \sigma(g)$ holds for all $\sigma \in \text{Sper}(A)$. This shows that the definition of $Q_{\text{red}}(A)$ coincides with the previous one in this case.

[3] A functor F from a category $\mathscr{C}$ to a subcategory $\mathscr{C}'$ of $\mathscr{C}$ is a reflection if F is left adjoint to the inclusion functor.

gory of multirings with $-1 \notin \sum A^2$ onto the (full) subcategory of real reduced multirings. A space of signs is nothing more or less than a real reduced multiring.

Simplifications occur when the multiring in question is a multifield, so we consider this case first. In Sections 3 and 4 we show that part of the standard Artin–Schreier theory holds for real multifields, extend the functor $F \rightsquigarrow Q_{\mathrm{red}}(F)$ to real multifields, characterize real reduced multifields, and explain how these objects axiomatize spaces of orderings.

We remark that other first-order descriptions of a space of orderings are known, see [4,9]. Just recently, a first-order description of a space of signs was also given in [5]. At the same time, it seems that the descriptions given here are the most natural and the most easily understood.

One would expect many of the results presented here to extend to non-commutative multirings and to orderings of higher level. The (non-reduced) special groups [4], called quadratic form schemes in [9], provide additional examples of multifields. We do not consider these topics in the present paper.

1. Multigroups

Multigroups are a natural generalization of groups.

1.1. Definition. A *multigroup* is a quadruple $(G, \Pi, r, \imath)$ where G is a non-empty set, Π is a subset of $G \times G \times G$, $r : G \to G$ is a function and $\imath$ is an element of G satisfying:

(1) If $(x, y, z) \in \Pi$ then $(z, r(y), x) \in \Pi$ and $(r(x), z, y) \in \Pi$.
(2) $(x, \imath, y) \in \Pi$ iff $x = y$.
(3) If $\exists \, p \in G$ such that $(u, v, p) \in \Pi$ and $(p, w, x) \in \Pi$ then $\exists \, q \in G$ such that $(v, w, q) \in \Pi$ and $(u, q, x) \in \Pi$.
   A multigroup is said to be *commutative* if
(4) $(x, y, z) \in \Pi$ iff $(y, x, z) \in \Pi$.

1.2. Example. Suppose $(G, \cdot, \imath)$ is a group. Define $\Pi := \{(x, y, z) \in G \times G \times G : z = xy\}$, $r(x) := x^{-1}$, the inverse of x. Then $(G, \Pi, r, \imath)$ is a multigroup. (1) asserts that $z = xy \Rightarrow x = zy^{-1}$ and $y = x^{-1}z$. (2) asserts that $y = x\imath$ iff $x = y$. (3) asserts that if $p = uv$ and $x = pw$ [i.e., $x = (uv)w$], then there exists q such that $q = vw$ and $x = uq$, [i.e., $x = u(vw)$], i.e., that the group operation is associative.

A multigroup is nothing more or less than a group with multivalued group operation. See [2] for the more general notion of multigroupoid. We record basic properties.

1.3. Lemma. *For any multigroup G:*

(5) $r(\imath) = \imath$.
(6) $r(r(x)) = x$.
(7) $(x, y, z) \in \Pi$ *iff* $(r(y), r(x), r(z)) \in \Pi$.
(8) $(\imath, x, y) \in \Pi$ *iff* $x = y$.
(9) *If* $\exists \, q \in G$ *such that* $(v, w, q) \in \Pi$ *and* $(u, q, x) \in \Pi$ *then* $\exists \, p \in G$ *such that* $(u, v, p) \in \Pi$ *and* $(p, w, x) \in \Pi$.
(10) *For each* $a, b \in G$ *there exists* $c \in G$ *such that* $(a, b, c) \in \Pi$.

Proof.

(5) $(\iota, \iota, \iota) \in \Pi \Rightarrow (r(\iota), \iota, \iota) \in \Pi \Rightarrow r(\iota) = \iota.$

(6) $(x, \iota, x) \in \Pi \Rightarrow (r(x), x, \iota) \in \Pi \Rightarrow (r(r(x)), \iota, x) \in \Pi \Rightarrow r(r(x)) = x.$

(7) $(x, y, z) \in \Pi$ iff $(z, r(y), x) \in \Pi$ iff $(r(z), x, r(y)) \in \Pi$ iff $(r(y), r(x), r(z)) \in \Pi.$

(8) $(\iota, x, y) \in \Pi \Leftrightarrow (r(x), \iota, r(y)) \in \Pi \Leftrightarrow r(x) = r(y) \Leftrightarrow x = y.$

(9) This follows from (3), by applying r, using (6) and (7).

(10) $(a, \iota, a) \in \Pi$ and $(b, r(b), \iota) \in \Pi$ so by the associative property, there exists $c \in G$ such that $(a, b, c) \in \Pi$ and $(c, r(b), a) \in \Pi.$ $\quad\square$

2. Multirings

A multiring is a ring with multivalued addition. Every ring is a multiring. Here, we only consider multirings which are commutative with 1.

2.1. Definition. A *multiring* is a system $(A, \Pi, \cdot, -, 0, 1)$ satisfying:

(1) $(A, \Pi, -, 0)$ is a commutative multigroup.

(2) $(A, \cdot, 1)$ is a commutative monoid, i.e., $\cdot$ is a binary operation on A which is commutative and associative and $a1 = a$ for all $a \in A$.

(3) $a0 = 0$ for all $a \in A$.

(4) $(a, b, c) \in \Pi \Rightarrow (ad, bd, cd) \in \Pi.$

Property (4) is the distributive property; more precisely, it is the first half of the distributive property. The second half is $(ad, bd, e) \in \Pi \Rightarrow \exists \, c$ such that $(a, b, c) \in \Pi$ and $e = cd$. We do not assume the second half. For a ring, the second half is automatic from the first half.

Since $(A, \Pi, -, 0)$ is a commutative group, we have $-0 = 0$, $-(-a) = a$. We also have $a(-b) = (-a)b = -(ab)$ and $(-a)(-b) = ab.$

Proof: $(b, 0, b) \in \Pi$ so $(-b, b, 0) \in \Pi$ so $(a(-b), ab, a0) \in \Pi$ so $(-(ab), a0, a(-b)) \in \Pi$. Since $a0 = 0$ this implies $a(-b) = -(ab).$

Note: For a ring, (3) is a consequence of (4). It is not clear if this is true in general.

2.2. Definition. If A and B are multirings, a mapping $f : A \to B$ is called a *multiring homomorphism* if, for all $a, b, c \in A$,

(1) $(a, b, c) \in \Pi_A \Rightarrow (f(a), f(b), f(c)) \in \Pi_B,$

(2) $f(-a) = -f(a),$

(3) $f(0) = 0,$

(4) $f(ab) = f(a)f(b)$ and

(5) $f(1) = 1.$

For multirings, there are various sorts of 'substructure' that one can consider. For rings, these all coincide. If A, B are multirings, we say A is *embedded* in B by the multiring homomorphism $i : A \to B$ if i is injective. We say A is *strongly embedded* in B if A is embedded in B and, for all $a, b, c \in A$, $(i(a), i(b), i(c)) \in \Pi_B \Rightarrow (a, b, c) \in \Pi_A$. We

say A is a *submultiring* of B if A is strongly embedded in B and, for all $a, b \in A$ and all $c \in B$, $(i(a), i(b), c) \in \Pi_B \Rightarrow c \in i(A)$.

Given a multiring A and subsets S and T of A it is convenient to define $S + T$ to be the set $\{c \in A : \text{ there exists } a \in S, b \in T \text{ such that } (a, b, c) \in \Pi\}$. This satisfies $S + T = T + S$, $(S + T) + U = S + (T + U)$ and $(S + T)U \subseteq SU + TU$. We also define $S - T := S + (-T)$ where $-T := \{-a : a \in T\}$. $\sum S$ denotes the union of the sets $S + \cdots + S$ (k times), $k \geqslant 1$.

Note: In particular, $a + b = \{c \in A : (a, b, c) \in \Pi\}$. A submultiring of A is a subset S of A satisfying $S - S \subseteq S$, $SS \subseteq S$, and $1 \in S$.

Many concepts available in the category of rings extend naturally to the category of multirings. We describe some of these now.

If A_i, $i \in I$ are multirings then the product $\prod_{i \in I} A_i$ is a multiring in the natural (componentwise) way.

An *ideal* of A is a non-empty subset $\mathfrak{a}$ of A such that $\mathfrak{a} + \mathfrak{a} \subseteq \mathfrak{a}$ and $A\mathfrak{a} \subseteq \mathfrak{a}$. The kernel of a multiring homomorphism $f : A \to B$ is an ideal of A. The smallest ideal of A containing the elements $a_1, \ldots, a_k$ of A is $\sum Aa_1 + \cdots + \sum Aa_k$. If the second half of the distribute property holds, then $\sum Aa = Aa$. An ideal $\mathfrak{p}$ of A is said to be *prime* if $1 \notin \mathfrak{p}$ and $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. The *prime spectrum* of A, denoted $\mathrm{Spec}(A)$, is defined to be the set of prime ideals of A. As in the ring case we have the following:

2.3. Proposition. *For any multiring A, $\mathrm{Spec}(A)$ has a natural topology giving it the structure of a spectral space* [6]. *Basic open sets have the form $D(a) := \{\mathfrak{p} \in \mathrm{Sper}(A) \mid a \notin \mathfrak{p}\}$, $a \in A$.*

Proof. The standard argument in the ring case carries over. Consider the embedding $\Phi : \mathrm{Spec}(A) \to \{0, 1\}^A$ defined by $\mathfrak{p} \mapsto f_{\mathfrak{p}}$ where

$$f_{\mathfrak{p}}(a) = \begin{cases} 0 & \text{if } a \in \mathfrak{p}, \\ 1 & \text{if } a \notin \mathfrak{p}. \end{cases}$$

The topology on $\mathrm{Spec}(A)$ induced by Φ (giving $\{0, 1\}$ the discrete topology and $\{0, 1\}^A$ the product topology) is the so-called patch topology, i.e., the topology with subbasis consisting of the sets $D(a)$, $\mathrm{Spec}(A) \backslash D(b)$, $a, b \in A$. It suffices to show that $\mathrm{Spec}(A)$ with the patch topology is a Boolean space or, equivalently, that the image of Φ is closed in $\{0, 1\}^A$. This is easy to check. $\square$

2.4. Proposition. *For any multiring A, the intersection of the set of prime ideals of A is the ideal of nilpotent elements of A.*

Proof. Again, the argument in the ring case carries over. Suppose $a \in A$, $a^n \neq 0$ for all $n \geqslant 0$. Let $S = \{a^n \mid n \geqslant 0\}$. Use Zorn's lemma to pick an ideal $\mathfrak{p}$ of A maximal subject to the condition $\mathfrak{p} \cap S = \emptyset$. Suppose $b, c \in A$, $bc \in \mathfrak{p}$, $b, c \notin \mathfrak{p}$. Consider the ideals $\mathfrak{p} + \sum Ab$, $\mathfrak{p} + \sum Ac$. Thus, $a^k \in \mathfrak{p} + \sum Ab$, $a^\ell \in \mathfrak{p} + \sum Ac$, for some integers $k, \ell \geqslant 0$. Then $a^{k+\ell} \in (\mathfrak{p} + \sum Ab)(\mathfrak{p} + \sum Ac) \subseteq \mathfrak{p}$ (using $bc \in \mathfrak{p}$), a contradiction. This proves the ideal $\mathfrak{p}$ is prime. $\square$

For any ideal $\mathfrak{a}$ and any multiplicative set S, $A/\mathfrak{a}$ and $S^{-1}A$ are again multirings and the natural maps $A \to A/\mathfrak{a}$, $A \to S^{-1}A$ are multiring homomorphisms.

Let $\mathfrak{a}$ be an ideal in A. Elements of $A/\mathfrak{a}$ are the cosets $\bar{a} = a + \mathfrak{a}$, $a \in A$. $\bar{\Pi}$ consists of all triples $(\bar{a}, \bar{b}, \bar{c})$ such that $(a, b, c) \in \Pi$. $-: A/\mathfrak{a} \to A/\mathfrak{a}$ is defined by $-\bar{a} = \overline{-a}$. The zero element of $A/\mathfrak{a}$ is $\bar{0}$. Multiplication on $A/\mathfrak{a}$ is defined by $\bar{a}\bar{b} = \overline{ab}$.

Let S be a multiplicative set in A. Elements of $S^{-1}A$ have the form a/s, $a \in A$, $s \in S$. $a/s = b/t$ iff $atu = bsu$ for some $u \in S$. $(a/s)b/t = ab/st \cdot ((a/s, b/t, c/u) \in S^{-1}\Pi$ iff $(atuv, bsuv, cstv) \in \Pi$ for some $v \in S$.

A *multifield* is a multiring F with $1 \neq 0$ such that every non-zero element has a multiplicative inverse.

Note: For multifields, the second half of the distributive property does hold. If D is a *multidomain*, i.e., $\{0\}$ is a prime ideal of D, then one can form the multifield of fractions $\mathrm{ff}(D) := (D\backslash\{0\})^{-1}D$. Unlike what happens in the domain case, the natural homomorphism $D \to \mathrm{ff}(D)$ need not be injective.

The theory of multirings is more complicated than the theory of rings. Every multiring homomorphism $f : A \to B$ factors through $A/\mathfrak{a}$ where $\mathfrak{a}$ is the kernel of f but the induced multiring homomorphism $\bar{f} : A/\mathfrak{a} \to B$ need not be injective. Even if $\bar{f}$ is injective, the embedding $A/\mathfrak{a} \hookrightarrow B$ need not be a strong embedding.

2.5. Example. (1) Let A be the coordinate ring of an algebraic set V in R^n, R real closed, and consider the multiring $Q_{\mathrm{red}}(A)$ mentioned in the introduction. Denote by $\bar{f} \in Q_{\mathrm{red}}(A)$ the image of $f \in A$ under the natural homomorphism $A \to Q_{\mathrm{red}}(A)$. By definition, $\bar{f} = \bar{g}$ iff $\mathrm{sgn}(f(p)) = \mathrm{sgn}(g(p))$ holds for all $p \in V$. Addition in $Q_{\mathrm{red}}(A)$ is defined by $\bar{f} \in \bar{g} + \bar{h}$ iff there exist $f_1, g_1, h_1 \in A$ such that $\bar{f} = \bar{f_1}$, $\bar{g} = \bar{g_1}$, $\bar{h} = \bar{h_1}$ and $f_1 = g_1 + h_1$. Multiplication is defined by $\bar{f}\bar{g} = \overline{fg}$. For the proof that $Q_{\mathrm{red}}(A)$ is indeed a multiring see [7, Chapter 5] or (which is no harder) look ahead to the general result in Section 7. The homomorphism $A \to Q_{\mathrm{red}}(A)$ has kernel zero but is obviously not injective. For example, $\bar{f}^3 = \bar{f}$, but $f^3 \neq f$ in general.

(2) Suppose now that V is irreducible. Then A is a domain and $D := Q_{\mathrm{red}}(A)$ is a multidomain. The natural homomorphism $D \to \mathrm{ff}(D)$ is not injective in general. For example, suppose V is the elliptic curve $y^2 = x(x+1)^2$ in R^2. Since $(x+1)x$ and $(x+1)x^2$ have the same sign on V, $\overline{x+1} \cdot \bar{x} = \overline{x+1} \cdot \bar{x}^2$ in D. Since $\overline{x+1} \neq 0$ in D this implies $\bar{x} = \bar{x}^2$ in $\mathrm{ff}(D)$. But $\bar{x} \neq \bar{x}^2$ in D (since x and x^2 have different signs at the isolated point). Suppose now that $V = R$ (so A is the polynomial ring $R\lfloor x \rfloor$). In this case the homomorphism $D \to \mathrm{ff}(D)$ is injective. Since $1 \in 1 + 1$ holds in D and $\bar{x}^2 = 1$ holds in $\mathrm{ff}(D)$ (since $\bar{x}^3 = \bar{x}$ holds in D and $\bar{x} \neq 0$), we see that $\bar{x}^2 \in 1 + 1$ holds in $\mathrm{ff}(D)$. But $\bar{x}^2 \in 1 + 1$ cannot hold in D (because x vanishes at the origin but 1 is positive at the origin). Thus, the embedding $D \to \mathrm{ff}(D)$ is not a strong embedding.

We make frequent use of the following construction.

2.6. Example. Fix a multiring A and a multiplicative subset S of A. Define an equivalence relation $\sim$ on A by $a \sim b$ iff $as = bt$ for some $s, t \in S$. Denote by $\bar{a}$ the equivalence class of a and set $A/_m S = \{\bar{a} \mid a \in A\}$. $A/_m S$ is given the structure of a multiring by defining $\bar{\Pi} = \{(\bar{a}, \bar{b}, \bar{c}) \mid (as, bt, cu) \in \Pi$ for some $s, t, u \in S\}$, $-\bar{a} = \overline{-a}$ and $\bar{a}\bar{b} = \overline{ab}$.

$(A/_m S, \bar{\Pi}, -, \bar{0}, \cdot, \bar{1})$ is a multiring and the map $a \mapsto \bar{a}$ from A to $A/_m S$ is a multiring homomorphism.

Note: If $0 \in S$ then $A/_m S = \{0\}$.

A special case of this construction appears already in quadratic form theory. Let F be a field of characteristic $\neq 2$, $F \neq \mathbb{F}_3, \mathbb{F}_5$, and consider the multifield $Q(F) := F/_m F^{*2}$ where F^{*2} denotes the subgroup $\{a^2 \mid a \in F^*\}$ of the multiplicative group $F^* = F\backslash\{0\}$ of F. ($Q(\mathbb{F}_3)$ and $Q(\mathbb{F}_5)$ are also defined, but the definition is not quite the same.) $Q(F)$ is nothing more or less than the special group of F [4] (also called the quadratic form scheme of F [9]) with zero adjoined. If $a_i \in Q(F)$, $a_i \neq 0$, $i = 1, \ldots, n$ then $a_1 + \cdots + a_n$ is precisely the value set of the associated diagonal quadratic form. If F^{*2} has finite index in F^* then $Q(F) = F^*/F^{*2} \cup \{0\}$ has order $2^n + 1$ where $2^n = (F^* : F^{*2})$. The possible structures of $Q(F)$ (as F varies) have been computed for $n \leqslant 5$; see [9]. For $n = 0$ there is just one possibility, namely $Q_1 := \{0, 1\}$ with addition and multiplication defined by $x \cdot 0 = 0 \cdot x = 0$, $1 \cdot 1 = 1$, $0 + x = x + 0 = x$, $1 + 1 = \{0, 1\}$. For $n = 1$ there are three possibilities (the multifield Q_2 defined earlier and 2 others). For $n = 2$ (resp., 3, 4, 5), there are six (resp., 17, 51, 155) possibilities.

If the field F is real, i.e., -1 is not a sum of squares in F, one can also form the multifield $Q_{\mathrm{red}}(F) := F/_m \sum F^{*2}$ which is the reduced special group of F [4] (also called the reduced quadratic form scheme of F [9]) with zero adjoined. $Q_{\mathrm{red}}(F)$ is a rather complicated object even in relatively simple cases (e.g., if F is the rational function field $R(x)$, R real closed) but, at the same time, it is better understood than $Q(F)$. Reduced special groups play an important role in real algebraic geometry; see [1,7].

2.7. Example. Suppose V is an irreducible algebraic set in R^n, R real closed, A is the coordinate ring of V, and F is the function field of V, i.e., $F = \mathrm{ff}(A)$. The reduced special group $Q_{\mathrm{red}}(F)$ is naturally identified with the multifield of fractions of the multidomain $Q_{\mathrm{red}}(A)$. (But to obtain a better understanding of $Q_{\mathrm{red}}(A)$ it is also necessary to consider reduced special groups of function fields of irreducible algebraic subsets of V.)

In [1,7] the space of signs $Q_{\mathrm{red}}(A)$ is defined for an arbitrary ring A with $-1 \notin \sum A^2$. Again, this is a multiring. Abstract versions of spaces of signs, special groups and reduced special groups are also defined; see [1,4,7,9]. These objects provide additional examples of multirings and multifields.

2.8. Remarks. (1) For any multiring A, prime ideals $\mathfrak{p}$ of A correspond bijectively to multiring homomorphisms $\alpha : A \to Q_1$, where Q_1 is defined as above. The correspondence is given by $\mathfrak{p} = \ker(\alpha)$.

(2) If A is a ring, $A \neq \{0\}$, the prime subring of A is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/(m)$ for some positive integer m. One can similarly define the prime submultiring of a multiring A to be the smallest submultiring of A, but this is a very complicated object in general. For example, if F is a field of characteristic $\neq 2$, $F \neq \mathbb{F}_3, \mathbb{F}_5$, then the subset $1 + (-1)$ of $Q(F)$ is all of $Q(F)$, i.e., the prime submultiring of the multifield $Q(F)$ is all of $Q(F)$. Similarly, for any ring A (more generally, for any multiring A) with $-1 \notin \sum A^2$, the prime submultiring of the multiring $Q_{\mathrm{red}}(A)$ is all of $Q_{\mathrm{red}}(A)$.

(3) Every ring is expressible as a factor ring of a polynomial ring over $\mathbb{Z}$ in suitably many variables. There is no known analog of this result for multirings. It is not even known if a multiring homomorphism $\mathbb{Z} \to A$ exists, for a general multiring A.

3. Artin–Schreier theory

We show how part of the standard Artin–Schreier theory for fields extends to multifields.

Let F be a multifield. A subset P of F is called an *ordering* if $P + P \subseteq P$, $PP \subseteq P$, $P \cup -P = F$ and $P \cap -P = \{0\}$. Orderings on a field F correspond to order relations on F defined by $a \leqslant b$ iff $b - a \in P$. For multifields this is not true in general. The *real spectrum* of a multifield F, denoted $\mathrm{Sper}(F)$, is defined to be the set of all orderings of F.

3.1. Proposition. $\mathrm{Sper}(F)$ *has a natural topology giving it the structure of a Boolean space. The sets* $U(a) := \{P \in \mathrm{Sper}(A) \mid a \notin -P\}$, $a \in F$, *are a subbasis for the topology.*

Proof. The proof is the same as the proof of Proposition 2.3, except that now the patch topology and the spectral topology coincide:

$$\mathrm{Sper}(F) \backslash U(a) = \begin{cases} U(-a) & \text{if } a \neq 0, \\ U(1) & \text{if } a = 0. \end{cases} \quad \square$$

A *preordering* of F is defined to be a subset T of F satisfying $T + T \subseteq T$, $TT \subseteq T$ and $F^2 \subseteq T$. Here, $F^2 := \{a^2 \mid a \in F\}$. Every ordering is a preordering. $\sum F^2$ is the unique smallest preordering of F. For any preordering T, $T^* := T \backslash \{0\}$ is a subgroup of F^* (using $1 = 1^2$ and $1/t = (1/t)^2 t$). A multifield F is said to be *real* if $-1 \notin \sum F^2$. If F is real, then $-1 \neq 1$. A preordering T of F is said to be *proper* if $-1 \notin T$.

3.2 Lemma. *Suppose F is a multifield with $-1 \neq 1$. For a preordering T of F, the following are equivalent*:

(1) *T is proper.*
(2) *$T \neq F$.*

Proof. Suppose $-1 \in T$. Let $a \in F$. If $a = 0$, then $a \in T$. Suppose $a \neq 0$. Fix $b \in 1 + a$. Then $b^2 \in 1 + a + a + a^2$, so $b^2 \in 1 + u + a^2$, $u \in a + a$. Then $u \in b^2 - 1 - a^2 \in T$. $u/a \in 1 + 1$, so $u/a \in T$, $u \neq 0$ (since $-1 \neq 1$) and $a = (a/u)u \in T$. $\quad \square$

3.3. Lemma. *A preordering which is maximal proper is an ordering. F has ordering iff F is real.*

Proof. The second assertion follows from the first by Zorn's lemma. Let P be a preordering of the multifield F which is maximal proper. Let $a \in F$. Consider the preordering $P - aP$. If $-1 \in P - aP$, then $-1 \in s - at$, $s, t \in P$. If $t = 0$, then $-1 = s \in T$, a contradiction. Thus $t \neq 0$. Then $at \in 1 + s$, so $a \in 1/t + s/t \subseteq P$. If $-1 \notin P - aP$, then by maximality

of P, $-a \in P$. This proves $P \cup -P = F$. If $s \in P \cap -P$, $s \neq 0$, then $s = -t$, $t \in P$, so $-1 = s/t \in P$, a contradiction. This proves $P \cap -P = \{0\}$. $\quad \square$

For a preordering T of F, denote by X_T the set of all orderings P of F with $T \subseteq P$.

3.4. Proposition. *For any proper preordering* T, $T = \bigcap_{P \in X_T} P$.

Proof. One inclusion is clear. For the other, fix $a \in F$, $a \notin T$. $T - aT$ is a preordering of F and the argument in the proof of Lemma 3.3 show that $-1 \notin T - aT$. Use Zorn's lemma to pick a maximal proper preordering P lying over $T - aT$. By Lemma 3.3, P is an ordering, and $-a \in P$, so $a \notin P$. $\quad \square$

4. Real reduced multifields

Suppose F is a real multifield. For any proper preordering T of F, we can build the multifield $Q_T(F) := F/_m T^*$, see Example 2.6. In particular, we can build $Q_{\sum F^2}(F)$ which we denote simply by $Q_{\mathrm{red}}(F)$. If T_1, T_2 are preorderings with $T_1 \subseteq T_2$ then the multiring homomorphism $F \to Q_{T_2}(F)$ factors through $Q_{T_1}(F)$.

Consider the multifield Q_2 defined earlier. $\{0, 1\}$ is an ordering of Q_2. For any ordering P of a multifield F, $Q_P(F) \cong Q_2$ by a unique multiring isomorphism. Orderings of a multifield F correspond bijectively to multiring homomorphisms $\sigma: F \to Q_2$ via $P = \sigma^{-1}(\{0, 1\})$. $\mathrm{Sper}(Q_{\mathrm{red}}(F))$ is naturally identified with $\mathrm{Sper}(F)$. $\mathrm{Sper}(Q_T(F))$ is naturally identified with X_T. This is clear.

4.1. Proposition. *For a real multifield F the following are equivalent*:

(1) *The multiring homomorphism* $F \to Q_{\mathrm{red}}(F)$ *is an isomorphism.*
(2) $\sum F^2 = \{0, 1\}$.
(3) *For all* $a \in F$, $a^3 = a$ *and, for all* $a \in F$, $(1, 1, a) \in \Pi \Rightarrow a = 1$.

Proof. Assume (3). Then $a^2 = 1$ if $a \neq 0$ and, by induction on n, 1 is the only element of $1 + \cdots + 1$ (n times) for any $n \geqslant 1$. It follows that $\sum F^2 = F^2 = \{0, 1\}$. Everything else is clear. $\quad \square$

A *real reduced* multifield is defined to be a real multifield satisfying the equivalent conditions of Proposition 4.1.

4.2. Corollary. *A multifield F is a real reduced multifield iff the following conditions hold (for all* $a \in F$):

(1) $a^3 = a$.
(2) $(1, 1, a) \in \Pi \Rightarrow a = 1$.

Proof. Assume (1) and (2). As explained above, this implies $\sum F^2 = \{0, 1\}$. If $-1 \in \{0, 1\}$, then $-1 = 0$, so $1 = 0$, or $-1 = 1$, so $0 \in 1 + 1$ which, by (2), implies $1 = 0$. This contradicts

$1 \neq 0$. Thus $-1 \notin \sum F^2$, so F is real, and F is a real reduced multifield by Proposition 4.1. The converse is clear. $\square$

For any proper preordering T of a real multifield F, $Q_T(F)$ is a real reduced multifield. In particular, $Q_{\mathrm{red}}(F)$ is a real reduced multifield. If $p : F_1 \to F_2$ is a multiring homomorphism of real multifields, then $p(\sum F_1^2) \subseteq \sum F_2^2$, so p induces a multifield homomorphism $Q_{\mathrm{red}}(F_1) \to Q_{\mathrm{red}}(F_2)$. In this way, Q_{red} defines a functor (a reflection) from the category of real multifields onto the subcategory of real reduced multifields.

4.3. Lemma. *Let F be a real reduced multifield, $T = \sum F^2$. For any $a, b \in F^*$,*

$$(a + b)^* = (Ta + Tb)^* = \{c \in F^* \mid \forall \sigma \in \mathrm{Sper}(F), \sigma(c) = \sigma(a) \text{ or } \sigma(c) = \sigma(b)\}.$$

Proof. Since F is a real reduced multifield, $T = \{0, 1\}$, so $Ta + Tb = \{0, a, b\} \cup (a + b)$. In particular, $F = T - T = \{0, 1, -1\} \cup (1 - 1)$. To prove $(a + b)^* = (Ta + Tb)^*$, it remains to show $a, b \in a + b$. By symmetry, it suffices to show $a \in a + b$. If $a \neq \pm b$, then $b/a \neq \pm 1$ so $b/a \in 1 - 1$, i.e., $b \in a - a$, i.e., $a \in a + b$. Suppose $a = b$. Since $1 \in 1 + 1$, $a \in a + a = a + b$. Suppose $a = -b$. Since $-b \in -b - b$, $a \in a - b$, i.e., $a \in a + b$. This proves $(a + b)^* = (Ta + Tb)^*$. If $c \in Ta + Tb$ then $\sigma(a) = \sigma(b) \Rightarrow \sigma(c) = \sigma(a)$. Thus, $\sigma(c) = \sigma(a)$ or $\sigma(c) = \sigma(b)$ for any $\sigma \in \mathrm{Sper}(F)$. Conversely suppose this holds for any σ. Then $\sigma(b/a) = 1 \Rightarrow \sigma(c/a) = 1$ for any σ, so by Proposition 3.4, $c/a \in T + T(b/a)$. Multiplying by a, this yields $c \in Ta + Tb$ as required. $\square$

Real reduced multifields have a natural representation in terms of functions.

4.4. Corollary. *For any real reduced multifield F, the natural embedding $F \hookrightarrow Q_2^{\mathrm{Sper}(F)}$ is a strong embedding.*

Proof. It follows from Proposition 3.4 that the multiring homomorphism from F to $Q_2^{\mathrm{Sper}(F)}$ defined by $a \mapsto (\sigma(a))_{\sigma \in \mathrm{Sper}(F)}$ is injective. It remains to show that if $(\sigma(a), \sigma(b), \sigma(c)) \in \Pi_\sigma$ for all $\sigma \in \mathrm{Sper}(F)$ then $(a, b, c) \in \Pi$. If $a = 0$ then $\sigma(b) = \sigma(c)$ for all $\sigma \in X_T$ so by Proposition 3.4, $b = c$. Similarly, if $b = 0$ then $c = a$ and if $c = 0$ then $b = -a$. Suppose now that a, b, c are not zero. Then $(a, b, c) \in \Pi$ by Lemma 4.3. $\square$

Real reduced multifields and spaces of orderings are essentially the same thing: if F is a real reduced multifield, then the pair $(\mathrm{Sper}(F), F^*)$ is a space of orderings in the terminology of [7, Section 2.1], and every space of orderings is of this form, for some unique multifield F. This is clear. It follows from the theory of spaces of orderings that finite real reduced multifields (more generally, real reduced multifields having finite chain length) are completely classified recursively [7, Theorem 4.22].

Suppose F is an arbitrary real reduced multifield. For each proper preordering T of F we have a natural multiring homomorphism from F to the real reduced multifield $Q_T(F)$. In view of the above-mentioned result, we are especially interested in the T such that $Q_T(F)$ is finite, i.e., T^* has finite index in F^*. A major question is the following: which positive primitive formulas in the language of multifields with parameters in F have the property

that they hold in F iff they hold in $Q_T(F)$ for each preordering T of F such that T^* has finite index in F^* [8]?

5. The Positivstellensatz

We define the real spectrum of a multiring and prove an abstract version of the Positivstellensatz.

Let A a multiring. A subset P of A is an *ordering* if $P + P \subseteq P$, $PP \subseteq P$, $P \cup -P = A$ and $P \cap -P$ is a prime ideal of A (called the *support* of A). Orderings of a multiring A correspond bijectively to multiring homomorphisms $\sigma : A \to Q_2$ via $P = \sigma^{-1}(\{0, 1\})$. For a prime ideal $\mathfrak{p}$ of A, orderings on A having support contained in $\mathfrak{p}$ (resp., containing $\mathfrak{p}$, resp., equal to $\mathfrak{p}$) correspond bijectively to orderings on the localization of A at $\mathfrak{p}$ (resp., on $A/\mathfrak{p}$, resp., on $\mathrm{ff}(A/\mathfrak{p})$). The *real spectrum* of A, denoted $\mathrm{Sper}(A)$, is the set of all orderings of A.

5.1. Proposition. $\mathrm{Sper}(A)$ *is endowed with a natural topology making it a spectral space. The sets* $U(a) := \{\sigma \in \mathrm{Sper}(A) \mid \sigma(a) = 1\}$, $a \in A$, *are a subbasis for the topology.*

A *preordering* of a multiring A is a subset T of A satisfying $T + T \subseteq T$, $TT \subseteq T$ and $A^2 \subseteq T$, where $A^2 := \{a^2 \mid a \in A\}$. A preordering T of A is said to be *proper* if $-1 \notin T$. Every ordering is a proper preordering. $\sum A^2$ is a preordering, and is the unique smallest preordering of A. A multiring A is said to be *semireal* if $-1 \notin \sum A^2$.

Fix a preordering T of A. Define $X_T := \{\sigma \in \mathrm{Sper}(A) : \sigma(T) = \{0, 1\}\}$. A *T-module* in A is defined to be a subset M of A satisfying $M + M \subseteq M$, $TM \subseteq M$, and $1 \in M$ (so $T \subseteq M$).

5.2. Proposition. *Suppose T is a proper preordering of A and M is a T-module in A which is maximal subject to $-1 \notin M$. Then $M \cap -M$ is a prime ideal of A, and $M \cup -M = A$.*

Proof. First we show that $\mathfrak{p} = M \cap -M$ is an ideal. Let $M' = \{a \in A \mid (a+a) \cap M \neq \emptyset\}$. Then $M' \supseteq M$ and M' is a T-module. If $-1 \in M'$, then $(-1-1) \cap M \neq \emptyset$, say $a \in (-1-1) \cap M$. Then $-1 \in 1 + a \subseteq M$, a contradiction. Thus $-1 \notin M'$. By maximality of M, $M' = M$. Clearly $\mathfrak{p} + \mathfrak{p} \subseteq \mathfrak{p}$, $-\mathfrak{p} = \mathfrak{p}$, and $T\mathfrak{p} \subseteq \mathfrak{p}$. Suppose $a \in A$, $b \in \mathfrak{p}$ are given. Fix $c \in 1 + a$. Then $c^2 \in 1 + a + a + a^2$, so $c^2 \in 1 + d + a^2$ for some $d \in a + a$. Then $d \in c^2 - 1 - a^2$, so $db \in c^2 b - b - a^2 b \subseteq \mathfrak{p} \subseteq M$. At the same time, $db \in (a+a)b \subseteq ab + ab$. This proves $ab \in M' = M$. A similar argument shows that $ab \in -M$. Thus $ab \in M \cap -M = \mathfrak{p}$. This proves that $\mathfrak{p}$ is an ideal of A. Next we show $\mathfrak{p}$ is prime. Suppose $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$, $b \notin \mathfrak{p}$. Replacing a by $-a$ and b by $-b$ if necessary, we can assume $a \notin M$, $b \notin M$. Thus -1 lies in the T-module $M + \sum aT$ and also in the T-module $M + \sum bT$. Then $-b^2 \in Mb^2 + \sum ab^2 T \subseteq M$ (using the fact that $ab \in \mathfrak{p}$), so $b^2 \in \mathfrak{p}$. Writing $-1 \in q + c$, $q \in M$, $c \in \sum bt_i$, $t_i \in T$, we have $-c \in 1 + q$, so $c^2 \in 1 + q + q + q^2$. On the other hand, $c^2 \in \sum b^2 t_i t_j \subseteq \mathfrak{p}$. This implies $-1 \in -c^2 + q + q + q^2 \subseteq M$, a contradiction. This proves that $\mathfrak{p}$ is a prime ideal. Suppose now that $a \in A$, $a \notin M$, $a \notin -M$. Then $-1 \in M + \sum aT$, $-1 \in M - \sum aT$. Multiplying by a^2, and noting that $a(\sum aT) \subseteq T$, this yields $-a^2 \in M + t_1 a$, $-a^2 \in M - t_2 a$, $t_1, t_2 \in T$.

Then $-t_1a \in a^2 + M \subseteq M$ and $t_2a \in a^2 + M \subseteq M$, so $t_1t_2a \in \mathfrak{p}$. This is not possible. If either of t_1 or t_2 is in $\mathfrak{p}$, then $-a^2 \in M$, so $a \in \mathfrak{p}$. If $a \in \mathfrak{p}$, then $a \in M$ (and also $a \in -M$) which contradicts our assumption. This proves $A = M \cup -M$. $\square$

5.3. Corollary. $\mathrm{Sper}(A) \neq \emptyset$ iff $-1 \notin \sum A^2$. *For a preordering T of A, $X_T \neq \emptyset$ iff T is proper.*

Proof. The first assertion follows from the second. If $X_T \neq \emptyset$ then clearly T is proper. Suppose now that T is proper. Use Zorn's lemma to choose a maximal proper preordering P in A with $T \subseteq P$, and a P-module M of A maximal subject to $-1 \notin M$. If $P \neq M$ then for any $a \in M \setminus P$, $P + \sum aP$ is a preordering and $P + \sum aP \subseteq M$, so $P + \sum aP$ is proper. This contradicts the maximality of P. It follows that $P = M$. Proposition 5.2 implies that P is an ordering. $\square$

For a fixed preordering T of A we have a multiring homomorphism $a \mapsto \bar{a}$ from A to the product multiring $Q_2^{X_T}$ defined by $\bar{a}(\sigma) = \sigma(a)$ for each $\sigma \in X_T$.

5.4. Proposition. *Suppose $c, d \in A$. Then $\bar{c} \geqslant 0 \Rightarrow \bar{d} = 0$ holds on X_T (i.e., $\forall \sigma \in X_T$, $\sigma(c) \geqslant 0 \Rightarrow \sigma(d) = 0$) iff $-d^{2k} \in T + \sum A^2c$ for some integer $k \geqslant 0$.*

Proof. Let $B = S^{-1}A$, $T' = S^{-1}T$, where $S := \{d^{2k} \mid k \geqslant 0\}$, and consider the T-module $T + \sum A^2c$ and the T'-module $T' + \sum B^2c$. If $-S \cap (T + \sum A^2c) = \emptyset$, then $-1 \notin T' + \sum B^2c$, so there is a T'-module M in B containing $T' + \sum B^2c$ and maximal subject to $-1 \notin M$. By Proposition 5.2, $\mathfrak{p} := M \cap -M$ is a prime ideal. Also, $T' \subseteq M$, so $(T' + \mathfrak{p}) \cap -(T' + \mathfrak{p}) = \mathfrak{p}$. It follows that the preordering $T'' := \{(a + \mathfrak{p})/(b + \mathfrak{p}) \mid a, b \in T', b \notin \mathfrak{p}\}$ is a proper preordering in the multifield $F := \mathrm{ff}(A/\mathfrak{p})$. Since $d \notin \mathfrak{p}$ (d is invertible in B), it follows from our assumption that $c + \mathfrak{p} \notin P$ for all orderings P of F containing T''. According to Proposition 3.4, this implies that $c + \mathfrak{p} \in -T''$. This yields elements $s, t \in T' + \mathfrak{p}$ with $s, t, \notin \mathfrak{p}$ such that $-sc = t$. Then $st \in T' + \mathfrak{p} \subseteq M$ and $-st = s^2c \in \sum B^2c \subseteq M$, so $st \in M \cap -M = \mathfrak{p}$, a contradiction. $\square$

5.5. Corollary.

(1) $\bar{a} = 0$ on X_T iff $-a^{2k} \in T$ for some $k \geqslant 0$.
(2) $\bar{a} = 1$ on X_T iff $-1 \in T - \sum A^2a$.
(3) $\bar{a} \geqslant 0$ on X_T iff $-a^{2k} \in T - \sum A^2a$ for some $k \geqslant 0$.
(4) Fix $a \in b^2 + c^2$. Then $\bar{b} = \bar{c}$ on X_T iff $-a^{2k} \in T - \sum A^2bc$ for some $k \geqslant 0$.

Proof. Apply Proposition 5.4 as follows: (1) take $c = 0$, $d = a$. (2) Take $c = -a$, $d = 1$. (3) Take $c = -a$, $d = a$. (4) Take $c = -bc$, $d = a$. $\square$

6. Real ideals

We indicate briefly how the theory of real ideals and real prime ideals extends to multirings. An ideal $\mathfrak{a}$ in a multiring A is said to be *real* if $(\sum a_i^2) \cap \mathfrak{a} \neq \emptyset \Rightarrow a_i \in \mathfrak{a}$

for each i. Every real ideal is *radical* in the sense that $a^2 \in \mathfrak{a} \Rightarrow a \in \mathfrak{a}$, i.e., $\mathfrak{a}$ is the intersection of prime ideals of A. The converse is not true, in general.

6.1. Proposition. *For a prime ideal $\mathfrak{p}$ in a multiring A, the following are equivalent*:

(1) $\mathfrak{p}$ *is real*.
(2) *The residue multifield ff$(A/\mathfrak{p})$ is real*.
(3) $\mathfrak{p}$ *is the support of some ordering of A*.

Proof. This is clear. $\square$

The *real radical* of an ideal $\mathfrak{a}$ in A is

$$\sqrt[R]{\mathfrak{a}} := \left\{ a \in A \mid \exists \ b_i \in A \text{ and } k \geqslant 0 \text{ such that } \left(a^{2k} + \sum b_i^2 \right) \cap \mathfrak{a} \neq \emptyset \right\}.$$

6.2. Proposition. $\sqrt[R]{\mathfrak{a}}$ *is the intersection of all real prime ideals of A containing $\mathfrak{a}$*.

Proof. One inclusion is clear. For the other inclusion, use Corollary 5.5(1). Suppose $a \in \mathfrak{p}$ for each real prime $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p}$. Consider $T = \sum A^2 + \mathfrak{a}$ (the preordering in A generated by $\mathfrak{a}$). Then $\bar{a} = 0$ on X_T so, by Corollary 5.5(1), $-a^{2k} \in T$ for some $k \geqslant 0$. Then $(a^{2k} + \sum b_j^2) \cap \mathfrak{a} \neq \emptyset$ for some b_j, so $a \in \sqrt[R]{\mathfrak{a}}$. $\square$

6.3. Proposition. *For an ideal $\mathfrak{a}$ of a multiring A, the following are equivalent*:

(1) $\mathfrak{a}$ *is real*,
(2) $\sqrt[R]{\mathfrak{a}} = \mathfrak{a}$.
(3) $\mathfrak{a}$ *is the intersection of real prime ideals*.
(4) $\mathfrak{a}$ *is radical and every minimal prime ideal over $\mathfrak{a}$ is real*.

Proof. Clearly (1) $\Leftrightarrow$ (2). (2) $\Leftrightarrow$ (3) by Proposition 6.2. If $\mathfrak{a}$ is radical, then $\mathfrak{a}$ is the intersection of the minimal prime ideals over $\mathfrak{a}$, so (4) $\Rightarrow$ (3). It remains to show (3) $\Rightarrow$ (4). Suppose $\mathfrak{q}$ is a minimal prime ideal over $\mathfrak{a}$ which is not real. Thus, for every real prime $\mathfrak{p}$ of A with $\mathfrak{a} \subseteq \mathfrak{p}$, there exists $a_\mathfrak{p} \in \mathfrak{p}$, $a_\mathfrak{p} \notin \mathfrak{q}$. By the compactness of $\mathrm{Sper}(A)$ in the patch topology, there exist finitely many elements $a_1, \dots, a_n$ of A such that $a_i \notin \mathfrak{q}$ for each i, and for each real prime $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p}$, $a_i \in \mathfrak{p}$, for some i. Let $a = a_1, \dots, a_n$. Then $a \in \mathfrak{p}$ for each real prime $\mathfrak{p}$ containing $\mathfrak{a}$ so, by (3), $a \in \mathfrak{a}$. This contradicts $a \notin \mathfrak{q}$. $\square$

A multiring A (with $1 \neq 0$) is said to be *real* if the ideal $\{0\}$ is real. If $\mathfrak{a}$ is a real proper ideal of A, then $A/\mathfrak{a}$ is real. In particular, if $-1 \notin \sum A^2$, then $A/\sqrt[R]{\{0\}}$ is real.

7. Real reduced multirings

We assume that A is a multiring with $-1 \notin \sum A^2$ and T is a proper preordering of A. We use the notation introduced in Section 5. We prove that the image of A in $Q_2^{X_T}$ is a multiring

which is strongly embedded in $Q_2^{X_T}$. We develop a first-order axiomatization of the spaces of signs (also called abstract real spectra) introduced in [1,7].

We introduce notation as in [7]: For $a_1, \ldots, a_n \in A$, define the *value set* of $\phi = (\overline{a_1}, \ldots, \overline{a_n})$ to be

$$D(\phi) = D(\overline{a_1}, \ldots, \overline{a_n}) = \left\{ \bar{b} \,\middle|\, b \in \sum Ta_1 + \cdots + \sum Ta_n \right\}.$$

We say $\bar{b}$ is *represented* by ϕ if $\bar{b} \in D(\phi)$.

7.1. Lemma.

(1) $D(\bar{a}) = \{\bar{b}^2\bar{a} \mid b \in A\} = \{\bar{t}\bar{a} \mid t \in A, \bar{t} \geqslant 0\} = \{\bar{b} \mid \text{for each } \sigma \in X_T \text{ either } \bar{b}(\sigma) = 0 \text{ or } \bar{a}(\sigma)\bar{b}(\sigma) > 0\}$.
(2) $D(\bar{a}, \bar{b}) = \{\bar{c} \mid \text{for each } \sigma \in X_T, \text{ either } \bar{c}(\sigma) = 0 \text{ or } \bar{a}(\sigma)\bar{c}(\sigma) > 0 \text{ or } \bar{b}(\sigma)\bar{c}(\sigma) > 0\}$.
(3) If $n \geqslant 3$, $D(\overline{a_1}, \ldots, \overline{a_n}) = \bigcup_{\bar{c} \in D(\overline{a_2}, \ldots, \overline{a_n})} D(\overline{a_1}, \bar{c})$.
(4) $D(\overline{a_1}, \ldots, \overline{a_n})$ depends only on $\overline{a_1}, \ldots, \overline{a_n}$ (not on the particular representatives $a_1, \ldots, a_n$).

Proof. See [7, Proposition 5.5.1]. (1) is clear. (2) If $c \in \sum Ta + \sum Tb$, then $c^2 \in \sum Tac + \sum Tbc$. It is clear from this that for any $\sigma \in X_T$, either $\bar{c}(\sigma) = 0$ of one of $\bar{a}(\sigma)\bar{c}(\sigma), \bar{b}(\sigma)\bar{c}(\sigma)$ is strictly positive, so $\bar{c}$ belongs to the second set. Now pick c such that $\bar{c}$ belongs to the second set. Denote by A', the localization of A and the multiplicative set $S = \{c^{2k} \mid k \geqslant 0\}$ and let T' be the preordering in A' defined by $T' = \{t/c^{2k} \mid k \geqslant 0\}$. Let $a' = ac$, $b' = bc$. On $X_{T' - \sum T'a'}$, $\overline{b'} > 0$so, by Corollary 5.5(2), $-1 \in T' - \sum T'a' - \sum A'^2 b'$. Multiplying by c^{2m+1}, m sufficiently large, $-c^{2m+1} \in Tc - \sum Ta - \sum Tb$. This yields $c_1 \in \left(\sum Ta + \sum Tb \right) \cap \left(c^{2m+1} + Tc \right)$. It follows that $\bar{c} = \overline{c_1} \in D(\bar{a}, \bar{b})$. (3) This follows from (2).

Note: by (2), $D(\overline{a_1}, \bar{c})$ depends only on $\bar{c}$, not on the particular representative c. (4) For $n = 1$ and 2, this is immediate from (1) and (2). For $n \geqslant 3$, it follows by induction on n, using (3). $\square$

7.2. Lemma. *For $a_0, \ldots, a_n \in A$, the following are equivalent:*

(1) *There exist $a_i' \in A$ such that $\overline{a_i'} = \overline{a_i}$ and $0 \in a_0' + \cdots + a_n'$.*
(2) $\overline{-a_i} \in D(\overline{a_0}, \ldots, \overline{a_{i-1}}, \overline{a_{i+1}}, \ldots, \overline{a_n})$ *for $i = 0, \ldots, n$.*

Proof. See [7, Proposition 5.5.3] (1) $\Rightarrow$ (2). By symmetry, it suffices to show $-\overline{a_0} \in D(\overline{a_1}, \ldots, \overline{a_n})$. Since $0 \in a_0' + \cdots + a_n'$, $-a_0' \in a_1' + \cdots + a_n'$, so $-\overline{a_0} = -\overline{a_0'} \in D(\overline{a_1'}, \ldots, \overline{a_n'}) = D(\overline{a_1}, \ldots, \overline{a_n})$, using Lemma 7.1(3). (2) $\Rightarrow$ (1). We have a_i' with $\overline{a_i'} = \overline{a_i}$ such that $0 \in a_i' + \sum_{j \neq i} \sum Ta_j$. Then $0 \in 0 + \cdots + 0 \subseteq \sum_{i=0}^{n} (a_i' + \sum_{j \neq i} \sum Ta_j) = \sum_{i=0}^{n} (a_i' + \sum Ta_i)$, so there exist $a_i'' \in a_i' + \sum Ta_i$ such that $0 \in a_0'' + \cdots + a_n''$. Clearly, $\overline{a_i''} = \overline{a_i}$. $\square$

Denote the image of A in $Q_2^{X_T}$ by $Q_T(A)$. Addition on $Q_T(A)$ is defined by $\bar{\Pi} = \{(\bar{a}, \bar{b}, \bar{c}) \mid a, b, c \in A, (a, b, c) \in \Pi\}$. $\bar{a}\bar{b} := \overline{ab}$, $-\bar{a} := \overline{-a}$. The zero element of $Q_T(A)$ is $\bar{0}$.

7.3. Proposition. *Suppose T is a proper preordering of A. Then*

(1) $Q_T(A)$ *is a multiring.*
(2) $Q_T(A)$ *is strongly embedded in* $Q_2^{X_T}$.

Proof. (1) Everything is clear except the associativity of $\bar{\Pi}$. Suppose $x, u, v, w, p \in A$ are such that $(\bar{u}, \bar{v}, \bar{p}) \in \bar{\Pi}$ and $(\bar{p}, \bar{w}, \bar{x}) \in \bar{\Pi}$. Then $\bar{x} \in D(\bar{p}, \bar{w})$ and $\bar{p} \in D(\bar{u}, \bar{v})$, so $\bar{x} \in D(\bar{u}, \bar{v}, \bar{w})$. Also $(-\bar{x}, \bar{p}, -\bar{w}) \in \bar{\Pi}$ so $-\bar{w} \in D(-\bar{x}, \bar{p})$, i.e., $-\bar{w} \in D(-\bar{x}, \bar{u}, \bar{v})$. Also $(-\bar{p}, \bar{v}, -\bar{u}) \in \bar{\Pi}$ and $(-\bar{x}, \bar{w}, -\bar{p}) \in \bar{\Pi}$, so $-\bar{u} \in D(-\bar{p}, \bar{v})$ and $-\bar{p} \in D(-\bar{x}, \bar{w})$, i.e., $-\bar{u} \in D(-\bar{x}, \bar{v}, \bar{w})$. Similarly, $(\bar{u}, -\bar{p}, -\bar{v}) \in \bar{\Pi}$ and $(-\bar{x}, \bar{w}, -\bar{p}) \in \bar{\Pi}$, so $-\bar{v} \in D(-\bar{x}, \bar{u}, \bar{w})$. According to Lemma 7.2 this implies there exist $x', u', v', w' \in A$ such that $\overline{x'} = \bar{x}, \overline{u'} = \bar{u}, \overline{v'} = \bar{v}, \overline{w'} = \bar{w}$, and $x' \in u' + v' + w'$. Pick $q \in v' + w'$ such that $x' \in u' + q$. Then $(\bar{v}, \bar{w}, \bar{q}) \in \bar{\Pi}$ and $(\bar{u}, \bar{q}, \bar{x}) \in \bar{\Pi}$. This completes the proof of (1).

(2) Let $a, b, c \in A$. According to Lemma 7.2, $(\bar{a}, \bar{b}, \bar{c}) \in \bar{\Pi}$ iff $\bar{c} \in D(\bar{a}, \bar{b})$, $-\bar{a} \in D(-\bar{c}, \bar{b})$ and $-\bar{b} \in D(-\bar{c}, \bar{a})$. According to Lemma 7.1(2), this occurs iff for all $\sigma \in X_T$, $\bar{c}(\sigma)\bar{a}(\sigma) > 0$ or $\bar{c}(\sigma)\bar{b}(\sigma) > 0$ or $\bar{a}(\sigma)\bar{b}(\sigma) < 0$ or $\bar{a}(\sigma) = \bar{b}(\sigma) = \bar{c}(\sigma) = 0$, i.e., iff for all $\sigma \in X_T$, $(\bar{a}(\sigma), \bar{b}(\sigma), \bar{c}(\sigma)) \in \Pi_\sigma$. This completes the proof of (2). $\square$

The real spectrum of $Q_T(A)$ is naturally identified with X_T. Now that we know that addition is a well-defined associative operation on subsets of $Q_T(A)$, we have another more intrinsic description of value sets.

7.4. Corollary. *Let* $\bar{T} = \{\bar{t} \mid t \in T\} = \{\bar{t} \mid t \in A, \bar{t} \geqslant 0\}$. *Then*

(1) $\bar{T}\overline{a_1} + \cdots + \bar{T}\overline{a_n} = \{\bar{b} \mid b \in \sum Ta_1 + \cdots + \sum Ta_n\}$.
(2) $\bar{0} \in \overline{a_0} + \cdots + \overline{a_n} \Leftrightarrow -\overline{a_i} \in \sum_{j \neq i} \bar{T}\overline{a_j}$ *for* $i = 0, \ldots, n \Leftrightarrow \exists\, a'_0, \ldots, a'_n$ *such that* $0 \in a'_0 + \cdots + a'_n$ *and* $\overline{a'_i} = \overline{a_i}, i = 0, \ldots, n$.

Proof. (1) follows from Lemma 7.1, by induction on n. (2) is clear from Lemma 7.2. $\square$

We restrict our attention now to the case where $T = \sum A^2$ and consider the multiring homomorphism $a \mapsto \bar{a}$ from A into $Q_2^{\text{Sper}(A)}$. We denote $Q_{\sum A^2}(A)$ by $Q_{\text{red}}(A)$ which we refer to as the *real reduced* multiring associated to A. The multirings A such that the multiring homomorphism $a \mapsto \bar{a}$ from A onto $Q_{\text{red}}(A)$ is an isomorphism are obviously of special interest.

7.5. Proposition. *For a multiring A with* $-1 \notin \sum A^2$, *the map* $a \mapsto \bar{a}$ *from A onto* $Q_{\text{red}}(A)$ *is an isomorphism iff A satisfies the following three properties (for all* $a, b \in A$):

(1) $a^3 = a$.
(2) $a + ab^2 = \{a\}$.
(3) $a^2 + b^2$ *contains a unique element.*

Proof. If $c \in a^2 + b^2$, then $c^2 \in (a^2 + b^2)(a^2 + b^2) \subseteq a^4 + a^2b^2 + a^2b^2 + b^4 = (a^2 + a^2b^2) + (b^2 + a^2b^2)$. Since a^2 is the unique element of $a^2 + a^2b^2$, and b^2 is the unique element

of $b^2 + a^2b^2$, this implies $c^2 \in a^2 + b^2$. Consequently, $c^2 = c$, i.e., the unique element of $a^2 + b^2$ is necessarily a square. It follows by induction that, for any $a_1, \ldots, a_n \in A$, $a_1^2 + \cdots + a_n^2$ contains a unique element, which is a square. In particular, $\sum A^2 = A^2$.

Let $T = \sum A^2 = A^2$. Suppose $\bar{a} = \bar{b}$. Let $c \in a^2 + b^2$. Thus $-c^{2k} \in A^2 - \sum A^2 ab$. Since $c^3 = c$, $c^{2k} = c^2$. Thus, there exists $d \in \sum A^2 ab$ with $d \in c^2 + A^2$. $ac \in a(a^2 + b^2) \subseteq a^3 + ab^2 = a + ab^2 = a$, so $ac = a$. Similarly, $bc = b$ and $cd = c$. Thus, $ad = (ac)d = a(cd) = ac = a$ and, similarly, $bd = b$. Say $d \in \sum e_i^2 ab$. Then $ab = abd \in \sum e_i^2 a^2 b^2 \subseteq A^2$. This implies $ab \in A^2$, so $ab = a^2b^2$. Thus, $a^2 = a^2 d \in \sum e_i^2 a^3 b = \sum e_i^2 ab = \sum e_i^2 a^2 b^2$ and, similarly, $b^2 \in \sum e_i^2 a^2 b^2$. Since $\sum e_i^2 a^2 b^2$ is a singleton set, this implies $a^2 = ab = b^2$. Finally, $a = a^3 = aa^2 = ab^2 = (ab)b = b^2b = b^3 = b$, as required. $\quad\square$

A multiring satisfying $-1 \notin \sum A^2$ and the equivalent conditions of Proposition 7.5 will be called a *real reduced multiring*.

7.6. Corollary. *A multiring A is a real reduced multiring iff the following properties hold (for all $a, b, c, d \in A$):*

(1) $1 \neq 0$.
(2) $a^3 = a$.
(3) $(a, ab^2, c) \in \Pi \Rightarrow c = a$.
(4) $(a^2, b^2, c) \in \Pi$ *and* $(a^2, b^2, d) \in \Pi \Rightarrow c = d$.

Proof. As noted above, (2), (3), (4) imply $\sum A^2 = A^2$. If $-1 \in \sum A^2$, then $-1 = a^2$ for some a, so $0 \in 1 + a^2$. By (3), $0 = 1$. This contradicts (1). Thus, $-1 \notin \sum A^2$. Now apply Proposition 7.5 to conclude that A is a real reduced multiring. The converse is obvious. $\quad\square$

Real reduced multirings and spaces of signs are the same thing: if A is a real reduced multiring, then the pair $(\mathrm{Sper}(A), A)$ is an space of signs in the terminology of [7, Section 6.1], and every space of signs is of this form. This is clear.

If A is a multiring such that $-1 \notin \sum A^2$, then for each proper preordering T of A, $Q_T(A)$ is a real reduced multiring. In particular, $Q_{\mathrm{red}}(A)$ is a real reduced multiring. If A_1, A_2 are two such multirings, then any multiring homomorphism $A_1 \to A_2$ induces a multiring homomorphism $Q_{\mathrm{red}}(A_1) \to Q_{\mathrm{red}}(A_2)$. In this way, Q_{red} is a functor (a reflection) from the category of all such multirings onto the subcategory of real reduced multirings.

For a multiring A with $-1 \notin \sum A^2$, and a proper preordering T of A, the primes of $Q_T(A)$ are the images under $A \to Q_T(A)$ of the supports of orderings in X_T, equivalently, the images under $A \to Q_T(A)$ of the primes $\mathfrak{p}$ in A such that $(T + \mathfrak{p}) \cap -(T + \mathfrak{p}) = \mathfrak{p}$. In particular, the primes in $Q_{\mathrm{red}}(A)$ are the images under $A \to Q_{\mathrm{red}}(A)$ of the real primes of A. If $\mathfrak{p}$ is a real prime of A such that $(T + \mathfrak{p}) \cap -(T + \mathfrak{p}) = \mathfrak{p}$ and $\bar{\mathfrak{p}}$ denotes the image of $\mathfrak{p}$ in $Q_T(A)$, and T' denotes the preordering in $\mathrm{ff}(A/\mathfrak{p})$ induced by T, then $\mathrm{ff}(Q_T(A)/\bar{\mathfrak{p}})$ is identified with the real reduced multifield $Q_{T'}(\mathrm{ff}(A/\mathfrak{p}))$. In particular, if $\mathfrak{p}$ is a real prime of A and $\bar{\mathfrak{p}}$ is the image of $\mathfrak{p}$ in $Q_{\mathrm{red}}(A)$, then $\mathrm{ff}(Q_{\mathrm{red}}(A)/\bar{\mathfrak{p}})$ is identified with the real reduced multifield $Q_{\mathrm{red}}(\mathrm{ff}(A/\mathfrak{p}))$.

In a real reduced multiring A every ideal is real. Moreover, for each prime ideal $\mathfrak{p}$ in A, the residue multifield $\mathrm{ff}(A/\mathfrak{p})$ is a real reduced multifield. As explained in [1,7], considerable

information concerning the real reduced multiring A can be read off from the structure of the real reduced multifields $ff(A/\mathfrak{p})$, $\mathfrak{p} \in \mathrm{Spec}(A)$. Additional information concerning A is obtained from certain multiring homomorphisms (relating the residue multifields $ff(A/\mathfrak{p})$ and $ff(A/\mathfrak{q})$ in case $\mathfrak{p} \subseteq \mathfrak{q}$) that arise from the specialization relation on $\mathrm{Sper}(A)$. In case A is finite (or, more generally, has finite chain length), this local information suffices to determine A completely [7, Section 8.5].

References

[1] C. Andradas, L. Bröcker, J. Ruiz, Constructible Sets in Real Geometry, Springer, Berlin, 1996.
[2] M. El Bachraoui, Relation algebras, multigroupoids, and degree, Ph.D. Thesis, University of Amsterdam, 2002.
[3] J. Bochnak, M. Coste, M.-F. Roy, Géométrie Algébrique Réelle, Springer, Berlin, 1987.
[4] M. Dickmann, F. Miraglia, Special groups: Boolean-theoretic methods in the theory of quadratic forms, Mem. Amer. Math. Soc. 145 (2000).
[5] M. Dickmann, A. Petrovich, Real semigroups and abstract real spectra I, Cont. Math. 344 (2004) 99–119.
[6] M. Hochster, Prime ideal structure in commutative rings, Trans. Amer. Math. Soc. 142 (1969) 43–60.
[7] M. Marshall, Spaces of Orderings and Abstract Real Spectra, Springer, Berlin, 1996.
[8] M. Marshall, Open questions in the theory of spaces of orderings, J. Symbolic Logic 67 (2002) 341–352.
[9] M. Marshall, The elementary type conjecture in quadratic form theory, Cont. Math. 344 (2004) 275–293.