RESEARCH ARTICLE

Orderings on semirings

Thomas C. Craven
Communicated by Boris M. Schein

1. Introduction

Though more general definitions are sometimes used, for this paper a semiring will be defined to be a set $S$ with two operations $+$ (addition) and $\cdot$ (multiplication); with respect to addition, $S$ is a commutative monoid with $0$ as its identity element. With respect to multiplication, $S$ is a (generally noncommutative) monoid with $1$ as its identity element. Connecting the two algebraic structures are the distributive laws,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

for all $a, b, c \in S$, and the requirement $a \cdot 0 = 0 \cdot a = 0$ for every $a \in S$. The reader is referred to [3] and [4] for an introduction to the theory of semirings.

Semirings have proven to be useful in theoretical computer science, in particular for studying automata and formal languages. Several authors have considered total order relations on semirings (e.g. [8, 9]). In this paper, we begin by looking at special classes of semirings which arise naturally in the theory of formally real (not necessarily commutative) fields and in the study of (commutative) real algebraic geometry. In the second section of the paper, we give characterizations of the semirings which arise in this way. Using this work as motivation, the third section of the paper suggests a new notion of ordering for commutative semirings which generalizes the concepts found in real algebraic geometry. In the most general case, these orderings turn out to have a somewhat weaker connection with total order relations than in the case of rings.

2. Semirings which are orderings

To maintain as much generality as possible, we begin by looking at orderings in skew fields (i.e. division rings). When we shift our attention to rings, we shall assume commutativity since there is as yet no established noncommutative version of real algebraic geometry.
By a preordering of a skew field $K$, we shall mean a subset $T$ of $K$ satisfying $T + T \subseteq T$, $T \cdot T \subseteq T$, $-1 \notin T$, and $K^2 \subseteq T$, where $K^2 = \{ x^2 \mid x \in K \}$ (see [11]). When we also have $T \cup -T = K$, the set $T$ is called an ordering. The first example of an ordered skew field was given by Hilbert. Széle [10] generalized the Artin-Schreier theory from formally real fields to show that a skew field $K$ can be ordered iff $-1$ is not in $\Sigma K^2$, the set of sums of products of squares in $K$. In this context, an ordering $P$ induces a total order relation defined by $a \leq b \iff b - a \in P$. Tschimmel [11] has shown that maximal preorderings are orderings.

We note here that preorderings are semirings and they induce a partial order relation on the skew field. In fact, a preordering in a skew field is a positive semiring [3, p. 125]: that is, it is nontrivial ($0 \neq 1$), $x + y = 0 \Rightarrow x = 0 = y$, and $xy = 0 \Rightarrow x = 0$ or $y = 0$. It will be interesting to observe how these latter two conditions fit into our theory later.

The next proposition is completely trivial, following immediately from the definitions. We state it in order to motivate the succeeding examples which show that it cannot be strengthened.

**Proposition 2.1.** Let $S$ be a semiring contained in a skew field $K$. Let $T$ be the semiring generated by $S \cup K^2$. Then $T$ is a preordering iff $-1 \notin T$.

The condition $-1 \notin T$ may seem a bit unwieldy. It would be nice to have a condition more intrinsic to $S$. Using the fact that $T$ contains $K^2$, it is easily shown that $-1 \notin T$ is equivalent to $-S \cap T = \{0\}$. In the examples below we consider the weaker conditions on $S$: $-1 \notin S$ and $-S \cap \Sigma K^2 = \{0\}$.

**Examples 2.2.** (i) Let $K$ be the rational function field $\mathbb{R}(x)$ in one variable over the real numbers and let $S$ be the semiring in $K$ generated by the set $\{x, -x\}$. That is, $S = \{\sum a_i x^i \mid a_i \in \mathbb{Z}, a_0 \geq 0\}$. Then $-1$ is not in $S$; however, for $T$ as defined in Proposition 2.1, we have $-1 = x(-x) \cdot x^{-2} \in T$.

(ii) Let $K = \mathbb{R}(x, y)$ be the field of rational functions in two variables and let $S$ be the semiring generated by $\{x^3, -x - y^2\}$. Then $-1 = [y^2 + (-x - y^2)] \cdot x^3 \cdot x^{-4} \in T$. On the other hand, we shall sketch a rather technical argument to show that $-S \cap \Sigma K^2 = \{0\}$. Any element of $S$ can be written in the form $\sum_{i=0}^n f_i(x^3)(-x - y^2)^i$, where each $f_i$ is a polynomial with nonnegative integer coefficients. Assume that $\phi$ is such a polynomial with $n > 0$ minimal such that $\phi \in -\Sigma K^2$. Since $\phi(x, y) \leq 0$ for all $x, y \in \mathbb{R}$, the high order term in $y$ must have a negative coefficient; i.e. $n$ must be odd. Now a sum of squares (and in particular $\phi$) must have even value with respect to every real valuation. Since the degree is minimal and the lowest order term has even degree (consider the $(x+y^2)$-adic valuation), we have $f_0 \neq 0$. Dividing $\phi$ by the square $(-x - y^2)^{n+1}$, we obtain an element of value 1 in the $(x+y^2)^{-1}$-adic valuation, a contradiction.

Now we turn our attention to rings. It is clear that for a semiring to be contained in a ring, a necessary condition is that a cancellation law hold: $x + a = y + a \Rightarrow x = y$. In fact, this is sufficient. This result can be found in [12,
Proposition 2.3. Let \( S \) be a semiring with cancellation. Then there exists a ring \( R \) containing \( S \) and generated by it.

Proof. Consider the set of formal differences \( \{s - t \mid s, t \in S\} \). We define \( R \) to be this set modulo the equivalence relation

\[
(a - b) \sim (c - d) \quad \iff \quad a + d = b + c \text{ in } S.
\]

(Note that the cancellation law is used here to show that the relation is transitive.) We define operations on \( R \) in the obvious way:

\[
(a - b) + (c - d) = (a + c) - (b + d) \\
(a - b) \cdot (c - d) = (ac + bd) - (ad + bc).
\]

Since the elements 0, 1 and the distributive laws are inherited from \( S \), the only thing left to prove is that the operations are well-defined. This is very easy for addition. We do only the somewhat tricky case of multiplication. Assume \((a_1 - b_1) \sim (a_2 - b_2)\) and \((c_1 - d_1) \sim (c_2 - d_2)\). Then, for \( i = 1, 2 \), we have \((a_i - b_i)(c_i - d_i) = (a_ic_i + b_id_i) - (a_id_i + b_ic_i)\). We must show that

\[
a_1c_1 + b_1d_1 + a_2d_2 + b_2c_2 = a_2c_2 + b_2d_2 + a_1d_1 + b_1c_1.
\]

From \( a_1 + b_2 = a_2 + b_1 \), we obtain

\[
a_1c_1 + b_2c_1 = a_2c_1 + b_1c_1 \\
a_2d_1 + b_1d_1 = a_1d_1 + b_2d_1.
\]

And from \( c_1 + d_2 = c_2 + d_1 \), we obtain

\[
a_2c_1 + a_2d_2 = a_2c_2 + a_2d_1 \\
b_2c_2 + b_2d_1 = b_2c_1 + b_2d_2.
\]

Adding the four displayed equations and cancelling yields the desired equality. \( \blacksquare \)

From now on our rings and semirings will all be commutative. We follow the excellent exposition in Lam [5] in extending the concept of ordering to rings. A subset \( T \) of a ring \( R \) is called a preorder if the same conditions hold as before: \( T + T \subseteq T \), \( T \cdot T \subseteq T \), \( -1 \notin T \), and \( R^2 \subseteq T \). A preorder \( T \) is called an order if \( T \cup -T = R \) and the center \( \mathfrak{p} = T \cap -T \) is a prime ideal of \( R \). Some of the major results that we shall wish to consider generalizing to semirings in the next section are that a maximal preorder is an ordering; a ring has an ordering iff \(-1\) is not a sum of squares; and if \( P \) is an ordering with center \( \mathfrak{p} \), then the image \( \hat{P} \) of \( P \) in the integral domain \( R/\mathfrak{p} \) induces an ordering of its field of fractions.

Theorem 2.4. Let \( S \) be a commutative semiring. \( S \) generates a ring \( R \) which contains an ordering \( P \supseteq S \) iff

1. \( S \) satisfies the cancellation law;
(2) For all \( a, b, c \in S \), we have \( 2 \sum a_ib_i c_i \neq 1 + \sum a_i(b_i^2 + c_i^2) \).

\textbf{Proof.} By Proposition 2.3, condition (1) is necessary and sufficient for \( S \) to be contained in a ring. Let \( R \) be the ring generated by \( S \) and set \( T \) equal to the semiring generated by \( S \cup R^2 \). Then \( T \) is a preordering (or equivalently, \( S \) is contained in an ordering) iff \(-1 \notin T \). But \(-1 \in T \) iff \(-1 = \sum a_ir_i^2 \), for some \( a_i \in S \) and \( r_i \in R^2 \). Writing \( r_i = b_i - c_i \), \( b_i, c_i \in S \), we see that this yields (2).

Let \( S \) be the semiring of Example 2.2 (generated by \( \{ x, -x \} \)). The ring generated by \( S \) is the polynomial ring \( \mathbb{Z}[x] \). If we view \( S \) as a subset of \( R(x) \) as in Example 2.2, the semiring \( T \) of Proposition 2.1 is no longer a preordering since it contains both \( x \) and its negative. The work with rings suggests a way to improve Proposition 2.1 to handle such situations. Condition (2) of Theorem 2.4 must be strengthened considerably to allow for quotients. Following the theorem, we give an example to illustrate why this is so.

\textbf{Theorem 2.5.} Let \( S \) be a semiring contained in a (commutative) field \( F \). Let \( R \) be the ring generated by \( S \) inside \( F \). Assume (as in the conclusion of Theorem 2.4) that \( S \) is contained in an ordering \( P_0 \) of \( R \) with center \( p \). Let \( T_0 = (P_0 \setminus p) \cup \{ 0 \} \) and \( T = \{ \sum t_i z_i \mid t_i \in T_0, \ z_i \in F^2 \} \). If \(-1 \notin T \), then there exists a valuation on \( F \) such that the finite elements of \( S \) map into an ordering of the residue class field.

\textbf{Proof.} We first that claim that \( T_0 \) is a semiring. Indeed, it contains 1 and it is closed under multiplication because \( p \) is prime; to check closure under addition, let \( x, y \in T_0 \). If \( x + y \notin T_0 \), then \( x + y \in -P_0 \); and then \( x = -y + (x + y) \in P_0 \cap -P_0 = p \), a contradiction. By Proposition 2.1, \( T \) is a preordering of \( F \), and thus it is contained in an ordering \( P \) of \( F \).

Consider the valuation ring \( A(P) = \{ a \in F \mid a < n, \text{ for some } n \in \mathbb{Z} \} \) of elements finite over \( \mathbb{Q} \) with respect to \( P \) (see [6] for details). Set \( A \) equal to the valuation ring generated by \( R \) and \( A(P) \), and let \( m \) be its maximal ideal. We claim that \( p \subseteq m \); indeed, assume that \( x \in p \), but \( x \notin m \). Replacing \( x \) by \(-x \) if necessary, we may assume that there exists a positive rational number \( q \) such that \( x - q > 0 \) with respect to \( P \) (i.e., \( x - q \in P \)). Write \( q = m/n \), with \( m, n \in \mathbb{Z}^+ \). We may replace \( x \) by \( nx \), so that \( x - m \in P \). But \( x - m \in R \), hence lies in \( P_0 \) which contains \( P \cap R \). Now \(-x \in p \subseteq P_0 \), so \(-m \in P_0 \), a contradiction. Therefore \( (A, m) \) dominates \( (R, p) \) and is a valuation ring with formally real residue class field. Furthermore, \( S \subseteq P_0 \) maps into the ordering \( P \) of the residue class field \( A/m \).

The difficulty in extending \( S \), or at least some portion of \( S \), to an ordering of \( F \) in the previous proof is best illustrated by the fact that there exist integral domains with (necessarily not total) orderings such that the field of fractions is not even formally real. An example is given by \( R = \mathbb{R}[x, y]/(x^2 + y^2) \). It contains the ordering \( P \) generated by \( \mathbb{R}^+ \) and the maximal ideal \( (x, y) \). The residue field is isomorphic to the real numbers. But the field of fractions has no orderings since \(-1 = (x/y)^2 \).

We conclude this section by mentioning that there are other semirings, very similar to those considered above, contained in skewfields and rings. These are known as higher level preorderings and orderings. They arise by replacing
the requirement that products of squares be contained in the semiring, with
the weaker requirement that $2n$-th powers and multiplicative commutators be
contained in it [2], [7].

3. Orderings for semirings

Taking our motivation from real algebraic geometry and the results of
the previous section, we now set the foundation for a theory of orderings of
commutative semirings which contains within it the theory for commutative rings
mentioned above. One difference which we shall encounter from more classical
theories is that knowing the positive cone of an ordering does not determine a
total order relation, even in the case of a semifield (a semiring which is a group
under multiplication). We give merely the beginnings of a theory to motivate
further research. We do only enough work to attempt to convince the reader
that our definitions are the “correct” ones for a generalization of real algebraic
geometry.

Let $S$ be a commutative semiring. For any semiring $P$ with $S^2 \subseteq P \subseteq S$,
we write

$$N_P = \{x \in P \mid x + y = 0, \text{ for some } y \in P\}$$

Note that $N_P + N_P = N_P$ and $P \cdot N_P = N_P$. A subsemiring $P$ of $S$ containing
$S^2$ is called a preordering of $S$ if $1 \notin N_P$. A preordering is called an ordering if

1. $s \in S$ and $s \notin P$ implies there exists $t \in P$ such that $s + t = 0$; and
2. $ab \in N_P$ implies $a \in P$ or $b \in P$.

It should be noted that (2) is not an obvious generalization from rings,
where $N_P = P \cap -P$ is required to be a prime ideal. To require that $a$ or $b$ lie
in $N_P$ would be too strong a condition for semirings. Using the characterization
of ordering given in [5, Theorem 3.2], one can show that the conditions are
equivalent for rings. To see that they are different for semirings, consider $S = P = \mathbb{N}[x,y]/(xy)$; i.e., polynomials with nonnegative integer coefficients in the
ring of polynomials in two variables over the integers modulo the ideal generated
by $xy$. In this case, $N_P = 0$ and $P$ is a preordering satisfying condition (1) for
an ordering; but condition (2) holds only in the weaker form.

Proposition 3.1. Let $P$ be an ordering of $S$ and $a, b \in S$. If there exists
$p \in P$ such that $ab + p = 0$, then $a \in P$ or $b \in P$.

Proof. Assume neither $a$ nor $b$ lies in $P$. Then there exist elements $s, t \in P$
such that $a + s = 0 = b + t$. Thus $ab + sb + st = (a + s)b + st = st$ and
$ab + sb + st = ab + s(b + t) = ab$, which yields $ab = st \in P$. But then $ab + p = 0$
implies $ab \in N_P$, so that $a \in P$ or $b \in P$.

For rings, the concluding statement of the previous proposition is suf-
ficient to imply that a preordering $P$ is an ordering. It is not sufficient for
semirings, as shown by the example $S = \mathbb{N}[x]$ with $P$ equal to the set of sums
of squares in $S$. 49
**Theorem 3.2.** A maximal preordering is an ordering.

**Proof.** Let \( P \) be a maximal preordering in a semiring \( S \). We claim first that the concluding condition of the previous proposition holds. Otherwise, there exist elements \( a \notin P, b \notin P \) and \( p \in P \) such that \( ab + p = 0 \). Consider the semirings \( Q_a = P + aP \) and \( Q_b = P + bP \). The maximality of \( P \) implies that \( 1 \in N_{Q_a} \) and \( 1 \in N_{Q_b} \); i.e., there exist elements \( p_i \in P, i = 1, \ldots, 4 \), such that \( 1 + p_1 + a p_2 = 0 \) and \( 1 + p_3 + b p_4 = 0 \). Multiplying these equations and adding \((1 + p_1)(1 + p_3) + pp_2 p_4\) to both sides yields \( 0 = (1 + p_1)(1 + p_3) + pp_2 p_4 = 1 + (p_1 + p_3 + p_1 p_3 + pp_2 p_4) \), so that \( 1 \in N_p \), a contradiction.

For condition (1) of an ordering, assume \( s \notin P \). By maximality, the semiring \( P + sP \) is not a preordering, so there exist elements \( p_1, p_2 \in P \) such that \( 1 + p_1 + sp_2 = 0 \). Multiplying by \( s \) yields \( s + s^2 = 0 \). Setting \( t = sp_1 + s^2 p_2 \), we have \( s + t = 0 \). Then \( st + s^2 = 0 \), with \( s^2 \in P \), so that \( t \in P \) by the previous paragraph.

For condition (2), assume \( ab \in N_P \). Then there exists \( p \in P \) such that \( ab + p = 0 \) by definition of \( N_P \), and so \( a \in P \) or \( b \in P \) by the first paragraph of the proof. 

As in rings, orderings may be contained in other orderings. Since Zorn's lemma can be used to enlarge any preordering to an ordering, the maximal orderings are the same as the maximal preorderings. One consequence of the previous theorem is a generalization of the Artin-Schreier theorem which states that a field has an ordering iff \(-1\) is not a sum of squares.

**Theorem 3.3.** A semiring \( S \) has an ordering iff the subset \( P = \Sigma S^2 \) of sums of squares in \( S \) is a preordering; that is, iff \( 1 \notin N_P \), or equivalently, there do not exist elements \( s_i \in S \) satisfying \( 1 + \sum s_i^2 = 0 \).

**Proof.** Since any ordering must contain \( P \), the condition is clearly necessary. Conversely, if \( P \) is a preordering, it can be enlarged to a maximal one, so \( S \) has at least one ordering by Theorem 3.2.

**Example 3.4.** Let \( S = \mathbb{N}[x] \) be the semiring of polynomials in one variable over the nonnegative integers. Let \( P \) be the set of sums of squares in \( S \). Since \( S \) has no negative elements, \( N_P = 0 \) and \( P \) is a preordering. But \( x \) is not in \( P \) and \(-x\) is not even in \( S \), so \( P \) is not an ordering. \( S \) itself is the only ordering. In fact, \( P \) is the minimal preordering and any semiring \( Q \subseteq S \) containing \( P \) is a preordering, again with \( N_Q = 0 \).

Taking \( P = S \), this example shows how an ordering, even with \( N_P = 0 \), fails to determine an order relation. There are uncountably many order relations inherited from the rational function field \( \mathbb{R}(x) \), in each of which \( P \) is contained in the positive elements [1]. For an ordering of a semifield with this same property, one can take \( P = S \) to be the subset of \( \mathbb{R}(x) \) of rational functions with only nonnegative coefficients.

More generally, the situation of Example 3.4 occurs whenever \( S \) is a preordering of a field \( F \). All semirings \( P \) between \( \Sigma F^2 \) and \( S \) are preorderings of \( S \) with \( N_P = 0 \).
Our next goal is to show that, as in the case of rings, if \( P \) is an ordering with \( N_P \neq 0 \), we can factor out \( N_P \) to obtain a quotient semiring with the pushdown ordering \( \bar{P} \) having \( N_P = 0 \). Because of the weaker form of (2) in the definition of ordering, the quotient semiring may have zero divisors, as shown by the example following that definition.

**Lemma 3.5.** Let \( P \) be a subset of a semiring \( S \).

1. If \( P \) is a preordering, then \( x \in N_P \) and \( x + y \in N_P \) imply \( y \in N_P \).
2. If \( P \) is an ordering, then \( S \cdot N_P \subseteq N_P \).

**Proof.**
1. Since \( x \in N_P \), there exists \( p \in P \) (and hence in \( N_P \)) such that \( x + p = 0 \). Since \( x + y \in N_P \), we obtain \( y = (x + p) + y = p + (x + y) \in N_P \).

2. Let \( s \in S \). If \( s \in P \), the result is clear from the definition of \( N_P \). If \( s \notin N_P \), then there exists \( t \in P \) such that \( s + t = 0 \). Let \( n \in N_P \). Then \( t \in P \) implies \( tn \in N_P \); since we also have \( sn + tn = (s + t)n = 0 \in N_P \), we obtain \( sn \in N_P \) by (1), as desired.

**Theorem 3.6.** Let \( P \) be an ordering of a semiring \( S \). Then \( N_P \) can be used to define an equivalence relation on \( S \) such that the quotient \( S_0 = S/N_P \) is a semiring. The image \( \bar{P} \) of \( P \) in \( S_0 \) is an ordering with \( N_P = 0 \).

**Proof.** Define a relation on \( S \) by \( s_1 \sim s_2 \) if there exist elements \( n_i \in N_P \), \( i = 1, 2 \), such that \( s_1 + n_1 = s_2 + n_2 \). Using the properties of \( N_P \) from the definition and Lemma 3.5, a standard argument shows that \( S_0 \) is a well-defined quotient semiring, as claimed. For \( s \in S \), we write \( \bar{s} \) for its image in \( S_0 \).

The set \( \bar{P} = \{ \bar{s} \in S_0 \mid s \in P \} \) is a semiring, just as \( S_0 \) is. We have \( S_0^2 \subseteq \bar{P} \) since \( S^2 \subseteq P \). By definition, the set \( N_P \) equals \( \{ \bar{x} \in \bar{P} \mid \bar{x} + \bar{y} = 0, \text{ for some } \bar{y} \in \bar{P} \} \). Let \( \bar{x} \in N_P \) with \( \bar{y} \in \bar{P} \) such that \( \bar{x} + \bar{y} = 0 \); then there exist \( n_1, n_2 \in N_P \) such that \( x + y + n_1 = n_2 \). Since \( n_2 \in N_P \), there exists \( n_3 \in N_P \) such that \( n_2 + n_3 = 0 \). Therefore, \( x + (y + n_1 + n_3) = 0 \), so that \( x \in N_P \). Thus \( N_P = 0 \). The remaining two conditions to check that \( \bar{P} \) is an ordering are now easily seen to follow from the fact that \( P \) is an ordering.

**References**


CRAVEN


Department of Mathematics
University of Hawaii
Honolulu, HI 96822

Received January 29, 1990