ORDERED $*$-RINGS

Thomas C. Craven and Tara L. Smith

Abstract. Marshall has generalized the notion of $*$-ordering to the setting of a ring with involution. In this paper we analyze the ways in which a given $*$-ordering (on the set of symmetric elements) can be extended to a multiplicatively closed ordering on a larger set of elements. A complete answer is given for Ore domains.

1. Introduction and notation.

Considerable work has been done on the topic of orderings on skew fields with involution ($*$-fields), with several different generalizations of the usual ordering on a commutative field being considered (see the survey article [Cr3] for references). Recently Marshall [M] has extended the theory of $*$-orderings on $*$-fields to the case of general rings with involution ($*$-rings). He develops the notion of an extended $*$-ordering on a $*$-ring and shows that every $*$-ordering has such an extension, as in the skew field case. The algebraic theory of quadratic forms for commutative fields carries over extremely well to hermitian forms over $*$-fields in the context of orderings (see [C2]). There is reason to hope that real algebraic geometry will work as well for $*$-rings. The ring-theoretic terminology in this paper will follow that of Lam's books [L1, L2].

In this paper we consider the problem of characterizing all extensions of a given $*$-ordering on a $*$-ring R. In order to extend the elegant valuation-theoretic characterization of $*$-orderings for $*$-fields, we first must slightly strengthen the definition of an extended $*$-ordering as given by Marshall [M, Definition 2.1]. The added condition is automatically satisfied when inverses exist. In Section 2 we provide a complete characterization of all extensions of a given $*$-ordering with support $\{0\}$ on an Ore domain R containing 2^{-1}. In Section 3 we construct a class of extensions of a given $*$-ordering with support $\{0\}$ on any $*$-domain R. We also construct an example of a $*$-ring which is not an Ore domain but has a $*$-ordering with support $\{0\}$.

For any subset $A \subseteq R$, we set $A^{\times} = A \setminus \{0\}$. We define $S(R)$ to be the set of all symmetric elements in R, that is, $S(R) = \{r \in R \mid r^* = r\}$.

2000 *Mathematics Subject Classification.* Primary 13J25; Secondary 16U20, 16W10.
Key words and phrases. $*$-ordering, valuation, Ore domain.

Definition 1.1 [M, Definition 1.2]**.** A $*$-*ordering* is a subset $P \subseteq S(R)$ satisfying

(1) $1 \in P, -1 \notin P$,
(2) $P + P \subseteq P$,
(3) $rPr^* \subseteq P$ for any $r \in R$,
(4) $P \cup -P = S(R)$,
(5) for any $a, b \in S(R)$, if $aba \in P \cap -P$ then $a \in P \cap -P$ or $b \in P \cap -P$,
(6) if $a, b \in P$ then $ab + ba \in P$.

The set $P \cap -P$ is called the *support* of P.

The operation $a \mapsto rar^*$ seen above in (3) occurs so often and is so fundamental that we shall give it the name of $*$-*conjugation*. Marshall shows that the support generates a $*$-closed completely prime ideal $\mathfrak{p}$ in R (i.e. $R/\mathfrak{p}$ is a domain with an induced involution, which we again denote by $*$), in the sense that $\mathfrak{p} = \{r \in R \mid rr^* \in P \cap -P\}$ and $\mathfrak{p} \cap S(R) = P \cap -P$. In the case when R is a division ring, Definition 1.1 is equivalent to the usual definition of $*$-ordering [Cr1]. As is usual in real algebraic geometry, here we use $P \cap -P = \{0\}$ rather than the empty set in the earlier definitions which exclude zero from orderings.

It is crucial to many proofs in this subject (as we shall see in the next section) that one deal with a multiplicatively closed set. For this purpose, one extends a $*$-ordering to a larger set containing some of the nonsymmetric elements and closed under multiplication.

Definition 1.2 [M, Definition 2.1]**.** A *weak extended* $*$-*ordering* of a $*$-ring R is a subset Q of R satisfying

(1) $Q + Q \subseteq Q$,
(2) $QQ \subseteq Q$,
(3) $Q^* = Q$,
(4) $rQr^* \subseteq Q$ for all $r \in R$,
(5) $Q \cap S(R)$ is a $*$-ordering P of R.

If the additional condition

(6) $rxr^* \in Q \implies x \in Q$ for any r not in the ideal generated by $Q \cap -Q$

also holds, we shall call Q an *extended* $*$-*ordering*.

Marshall proves the existence of a weak extension of any $*$-ordering [M, Theorem 2.2]; we shall strengthen this to include condition (6) in Theorem 1.8. Condition (6) holds for all extended $*$-orderings on $*$-fields. It is needed in Section 2 to obtain the correspondence between extensions of a $*$-ordering on an Ore domain and extended $*$-orderings on its field of fractions. We shall see in Example 2.11 that there exist weak extended $*$-orderings of a ring which are not extended $*$-orderings (that is, condition (6) fails to hold). Condition (6) has very strong implications as we shall see below; it essentially guarantees the commutativity that arises from having all multiplicative commutators $sds^{-1}d^{-1}$, $s \in S(D)^\times$, $d \in D^\times$, in extended $*$-orderings of a skew field D [Ho]. Furthermore the appropriate modification of

(6) also holds for all $*$-orderings as shown in Proposition 1.4. We next demonstrate the (nonobvious, though elementary) power of condition (6). Note that the elements b and c in the next proposition may not have any nice properties; they may even be skew units, and so not be orderable in any sense.

Proposition 1.3. *Let Q be an extended $*$-ordering on a ring R with $P = Q \cap S(R)$. Let $\mathfrak{p}$ be the (completely prime) ideal generated by $Q \cap -Q$. Let a and bc be elements of Q with $abc \notin \mathfrak{p}$. Then cb and bac also lie in Q. In particular, $bac + c^*a^*b^* \in P$. For any $s \in P \setminus -P$ and $r \in R$, if $sr \in Q$, then $r \in Q$.*

Proof. Since $bc \in Q$ and $bb^* \in Q$, the product $bcbb^* \in Q$, whence $cb \in Q$ by condition (6). Now $a, cb \in Q$, so $acb \in Q$ and hence $(ac)(bac)(ac)^* = (acb)[(ac)(ac)^*] \in Q$. Another application of condition (6) gives $bac \in Q$. For the final statement, $sr \in Q$ and $s \in P$ implies that $srs = srs^* \in Q$ and $s \notin \mathfrak{p}$, so (6) again can be used to conclude that $r \in Q$. $\square$

Proposition 1.4. *Let P be a $*$-ordering on a ring R and set $\mathfrak{p}$ equal to the ideal generated by $P \cap -P$. Let $r \in R$, $r \notin \mathfrak{p}$ and $x \in S(R)$. If $rxr^* \in P$, then $x \in P$.*

Proof. Assume $rxr^* \in P$ but $x \notin P$. Since the element x is symmetric, it lies in $P \cup -P$. Therefore $-x \in P$ and hence $-rxr^* \in P$. Thus $rxr^* \in P \cap -P \subseteq \mathfrak{p}$. By hypothesis, r and hence r^* are not in $\mathfrak{p}$. Since $x \notin P$, we also have $x \notin \mathfrak{p}$. Since $\mathfrak{p}$ is a completely prime ideal, this is a contradiction. $\square$

Upon reflection, one sees that this proof could have been simplified by immediately reducing to the domain $R/\mathfrak{p}$ with the $*$-ordering induced by P. For the remainder of this paper, we shall assume that R is a domain and that the support of any $*$-ordering P under consideration is $\{0\}$. All results can be pulled back to arbitrary $*$-rings.

In order to prove the existence of an extension (in the strong sense) of any $*$-ordering, we need some understanding of the valuation theory involved. Marshall [M, Section 3] defines a valuation-like mapping on $*$-ordered $*$-rings associated to a given $*$-ordering P as follows. For $a, b \in S(R)^\times$, we write $a \sim b$ if there exists an integer $n \geq 1$ such that $n|a| \geq |b|$ and $n|b| \geq |a|$, where $\geq$ is the ordering on $S(R)$ induced by P. We extend the relation $\sim$ to $R^\times$ by defining $a \sim b$ if $aa^* \sim bb^*$. We let $v(a)$ denote the equivalence class of a with respect to $\sim$ and let $\Gamma_v = \{\, v(a) \mid a \in R^\times \,\}$. Also set $v(0) = \infty$. We call v the *natural $*$-valuation* associated to P. The set Γ_v is a totally ordered cancellation semigroup under the ordering given by $v(a) \geq v(b)$ if $nbb^* \geq aa^*$ for some positive integer n and the operation $+$ defined by $v(a) + v(b) = v(ab)$. Moreover, we have

Proposition 1.5 [M, Theorem 3.3]**.**

(1) *v is $*$-invariant.*
(2) *For $a, b \in R$, $v(a + b) \geq \min\{v(a), v(b)\}$.*
(3) *If $a, b \in S(R)^\times$, then $v(ab - ba) > v(ab) = v(ba)$.*

Marshall proves very little about how much his mapping v behaves like a valuation. We fill in some of those gaps with lemmas for later reference.

Lemma 1.6. *Let R be a $*$-ring with $*$-ordering P and let v be the natural $*$-valuation associated to P. If $0 \neq a, b \in S(R)$, then $v(ab+ba) = v(ab) = v(a) + v(b)$.*

Proof. By the preceding proposition, we have that $v(ab+ba) \geq \min(v(ab), v(ba)) = v(ab)$. Since it does not affect the values to change an element to its negative, we may assume that $a, b \in P$. With respect to a weak extended $*$-ordering $Q \supseteq P$ (which exists by [M, Theorem 2.2]), we have $0 < ab < ab+ba$, which implies that $(ab)(ab)^* < (ab+ba)(ab+ba)^*$, which by definition of the ordering of the set of values gives $v(ab) \geq v(ab+ba)$. Therefore they are equal. □

Lemma 1.7. *Let R be a $*$-ring with $*$-ordering P and let v be the natural $*$-valuation associated to P. If $a \in P$ and $b \in S(R)$ with $v(b) > v(a)$, then $a + b \in P$.*

Proof. By definition, $v(b) > v(a)$ means $a^2 = aa^* > nbb^* = nb^2$ for all integers n; since a and b are symmetric, we must have either $a > b$ or $b > a$. The relation between the squares implies we cannot have $b > a$, so in particular, $a \pm b \in P$. □

As noted earlier, Marshall [M, Theorem 2.2] shows that every $*$-ordering P is contained in some weak extended $*$-ordering whose intersection with the symmetric elements is again P. His proof is based on the theory for skew fields and, as we shall see, actually gives an extended $*$-ordering. This will be carried still further in Theorem 3.1, where an entire family of extensions is constructed.

Theorem 1.8. *Let P be a $*$-ordering on a $*$-ring R in which 2 is a unit. There exists an extended $*$-ordering Q with $Q \cap S(R) = P$.*

Proof. We follow Marshall [M, Proof of Theorem 2.2] in immediately factoring out the ideal generated by $P \cap -P$ so that we may assume R is a domain and $P \cap -P = \{0\}$. Marshall shows that

$$Q = \{\, p + k \mid p \in P,\ k^* = -k,\ v(k) > v(p) \,\}$$

is a weak extended $*$-ordering with $Q \cap S(R) = P$. Thus we only need to check that Q satisfies condition (6) of Definition 1.2. Assume that $rxr^* \in Q$ with $r \neq 0$. We can write $x = s + j$, where $s \in S(R)$ and $j^* = -j$ (use $s = (x + x^*)/2,\ j = (x - x^*)/2$). Then $rxr^* = p + k$ where $p = rsr^*$ is symmetric and $k = rjr^*$ is skew. Since $rxr^* \in Q$, we have $p \in P$ and $v(k) > v(p)$. But then $s \in P$ by Proposition 1.4, and $v(j) = v(k) - 2v(r) > v(p) - 2v(r) = v(s)$, so $x = s + j \in Q$. □

This theorem remains true if 2 is not a unit in R, but the definition of Q no longer works. In this case, one must form $R \otimes_{\mathbb{Z}} \mathbb{Z}[1/2]$, apply the theorem and then intersect the extended $*$-ordering obtained with the ring R. The trouble one encounters with the definition of Q given in the proof of the theorem is demonstrated in Example 2.10.

In the case when the $*$-ring under consideration is a $*$-field D, Craven [Cr4, Theorem 2.3] has provided a complete description of all extended $*$-orderings containing a given $*$-ordering P of D. In this case the set Γ_v is a group. We remark here that the set Γ_v^+ defined in [Cr4, Section 2] should correctly be defined as

$$\Gamma_v^+ = \{\, v(k) \in \Gamma_v \mid k \in D^\times, v(k) > 0, k^* = -k \,\} \cup \{\infty\}.$$

Theorem 1.9 [Cr4, Theorem 2.3]**.** *Let D be a $*$-field with a $*$-ordering P and let v be the associated order valuation with value group Γ_v. Then there is a one-to-one correspondence between extended $*$-orderings Q containing P and convex subsets $A \subseteq \Gamma_v^+$ containing $\{\, v(s_1 s_2 s_1^{-1} s_2^{-1} - 1) \mid s_1, s_2 \in S(D)^\times \,\}$ defined by $Q_A = \{\, s + k \mid s \in P,\ k^* = -k,\ v(k) - v(s) \in A \,\}$ and $A_Q = \{\, v(k) \mid 1 + k \in Q \,\}$.*

In the definition of Q_A, we think of $k = 0$ as giving $v(k) - v(s) = \infty \in A$, since it occurs for $s_1 = s_2 = 1$. We shall see in Theorem 2.8 that this result generalizes to Ore domains and $*$-orderings with support $\{0\}$.

2. Ore domains.

Let R be an Ore domain with field of fractions D (see [Co, Chap. 1]). We assume throughout this section that 2 is a unit in R; this condition is needed in Theorem 2.8.

If D has an involution $*$, it restricts to an involution of R. Conversely, we wish to know that an involution $*$ of R extends to an involution of D.

Lemma 2.1. *Let R be a $*$-ring satisfying the right Ore condition. Then R also satisfies the left Ore condition.*

Proof. Recall that the left Ore condition says that for all $x, y \in R^\times$, there exist $x_1, y_1, u \in R^\times$ such that $u y_1 x = u x_1 y$. So let $x, y \neq 0$. Set $a = x^*, s = y^*$. Then by the right Ore condition there exist $s_1, a_1, t \in R^\times$ such that $x^* s_1 t = y^* a_1 t$. Therefore $t^* s_1^* x = t^* a_1^* y$. Set $x_1 = a_1^*, y_1 = s_1^*, u = t^*$ for the conclusion. $\square$

Lemma 2.2. *Let R be an Ore domain with an involution $*$ and field of fractions D. Then the involution extends uniquely to D.*

Proof. If $*$ extends to D, it must be defined so that $(ab^{-1})^* = (b^*)^{-1} a^*$. Thus we must check that this is well defined. Suppose $ab^{-1} = cd^{-1}$. Then there exist $u, v \in R$ such that

$au = cv$ and $bu = dv$. Applying the involution, we obtain $u^*a^* = v^*c^*$ and $v^*d^* = u^*b^*$. Since R is a left Ore domain by Lemma 2.1, we have $b^{*-1}a^* = d^{*-1}c^*$. $\square$

Theorem 2.3. *Let Q be an extended $*$-ordering with support $\{0\}$ on the Ore $*$-domain R with field of fractions D. Define $Q_D = \{ ab^{-1} \in D \mid ab^* \in Q \}$. Then Q_D is an extended $*$-ordering on D and $Q_D \cap R = Q$.*

Proof. We first check that Q_D is well defined. Assume that $ab^{-1} = cd^{-1}$ with $ab^* \in Q$. We must show that $cd^* \in Q$. From the equality of the fractions, we know that there exist $b_1, d_1 \in R$ such that $ad_1 = cb_1$ and $db_1 = bd_1$. Now $ab^* \in Q$ implies that $ad_1d_1^*b^* \in Q$ by Proposition 1.3. Using the previous two equations, we obtain $(cb_1b_1^*)d^* = (cb_1)(db_1)^* = (ad_1)(d_1^*b^*) \in Q$, from which we obtain $d^*cb_1b_1^* \in Q$ using Proposition 1.3 to switch the order of the factors. Then we obtain $cd^* \in Q$ as desired using Proposition 1.3 twice more, first to cancel the norm and then to switch the order of the factors.

Closure under addition. Assume that $ab^{-1}, cd^{-1} \in Q_D$, which means $ab^*, cd^* \in Q$. Then the sum is $ab^{-1} + cd^{-1} = (ad_1 + cb_1)(bd_1)^{-1}$ where $db_1 = bd_1$, $b_1, d_1 \in R$. But then $(ad_1 + cb_1)(bd_1)^* = ad_1d_1^*b^* + cb_1(db_1)^* = ad_1d_1^*b^* + cb_1b_1^*d^*$ lies in Q since each summand does by Proposition 1.3, and therefore $ab^{-1} + cd^{-1} \in Q_D$.

Closure under multiplication. Again we assume that $ab^{-1}, cd^{-1} \in Q_D$. Then the product is $(ab^{-1})(cd^{-1}) = (ac_1)(db_1)^{-1}$, where $bc_1 = cb_1$, $b_1, c_1 \in R$. Now $(ac_1)(db_1)^*$ lies in Q if and only if its product with b^*b lies in Q, which is true if and only if $a(b^*b)c_1b_1^*d^* = ab^*b(b^{-1}cb_1)b_1^*d^* = ab^*c(b_1b_1^*)d^*$ lies in Q. However the final element is known to be in Q by Proposition 1.3.

Closure under $*$-conjugation. Since $*$-conjugating by cd^{-1} is the same as $*$-conjugating first by d^{-1} and then $*$-conjugating by c, we may do them as separate cases to simplify notation. First assume that $c \in R$, $ab^{-1} \in Q_D$. Then $c(ab^{-1})c^* = cac_1b_1^{-1}$, where $c^*b_1 = bc_1$, $b_1, c_1 \in R$. The last equation gives us $bc_1b_1^* = c^*b_1b_1^*$. Since $c(ab^*)c^* \in Q$, so is $cab^*c^*(b_1b_1^*) = cab^*bc_1b_1^*$, from which we obtain $cac_1b_1^* \in Q$ as desired. Next we work with $d^{-1}(ab^{-1})d^{-1*}$ for $d \in R$. This can be written as $a_1d_1^{-1}(d^*b)^{-1} = a_1(d^*bd_1)^{-1}$ where $ad_1 = da_1$, $a_1, d_1 \in R$. Now $d^*(ab^*)d \in Q$ and we can multiply by the norm $a_1a_1^*$ to obtain $a_1a_1^*d^*ab^*d = a_1(d_1^*a^*)ab^*d = a_1d_1^*(a^*a)b^*d$ in Q, and hence $a_1d_1^*b^*d = a_1(d^*bd_1)^* \in Q$, and so $a_1(d^*bd_1)^{-1} \in Q_D$.

Closure under $*$. Assume that $ab^{-1} \in Q_D$. Since Q is closed under the involution, we have $ab^* \in Q$, which implies $ba^* \in Q$, and so $ba^{-1} \in Q_D$. But then $(ab^{-1})^* = (ab^{-1})^*(ba^{-1})(ab^{-1})$, which lies in Q_D by closure under $*$-conjugation.

$S(D) \subseteq Q_D \cup -Q_D$. Assume that $ab^{-1} \in S(D)$. Then we also have $b^*a = b^*(ab^{-1})b \in S(D) \cap R = S(R)$. Hence either $b^*a \in Q$ (which implies $bb^*(ab^*) = b(b^*a)b^* \in Q$, hence $ab^{-1} \in Q_D$) or $b^*a \in -Q$ (which implies $bb^*(ab^*) = b(b^*a)b^* \in -Q$, hence $ab^{-1} \in -Q_D$).

$Q_D \cap R = Q$. Assume that $ab^{-1} \in Q_D \cap R$. Then we also have $ab^* = (ab^{-1})(bb^*) \in Q$, so $ab^{-1} \in Q$ by Proposition 1.3. $\square$

Remark 2.4. Keeping the notation above, we also have $Q_D = \{\, ab^{-1} \in D \mid b^*a \in Q \,\}$. For since Q_D is closed under $*$-conjugation, we have $ab^{-1} \in Q_D$ if and only if $b^*ab^{-1}b = b^*a \in Q_D \cap R = Q$.

Corollary 2.5. *Let P be a $*$-ordering with support $\{0\}$ on the Ore $*$-domain R with field of fractions D. Define $P_D = \{\, ab^{-1} \in S(D) \mid b^*a \in P \,\}$. Then P_D is a $*$-ordering on D and $P_D \cap R = P$. Moreover, this process gives a one-to-one correspondence between $*$-orderings on R and $*$-orderings on D.*

Proof. Let Q be the extended $*$-ordering given by Theorem 1.8. Let Q_D be the extension to D defined in Theorem 2.3. We claim that

$$P_D = \{\, ab^{-1} \in S(D) \mid b^*a \in P \,\} = Q_D \cap S(D).$$

If true, this will verify the first claim of the corollary. It is clear that $P_D \subseteq Q_D \cap S(D)$ since $b^*a \in P$ implies $b^*a \in Q$, so that $ab^{-1} \in Q_D \cap S(D)$. Conversely, if $ab^{-1} \in Q_D \cap S(D)$, then $b^*a = b^*(ab^{-1})b \in Q_D \cap S(D) \cap R = P$, so that $ab^{-1} \in P_D$.

To show that this process gives a one-to-one correspondence, we need to show that for a given $*$-ordering P' on D with $P = P' \cap R$, we have $P' = P_D$. Let $ab^{-1} \in P'$; closure under $*$-conjugation shows that $b^*a \in P' \cap R = P$, so $ab^{-1} \in P_D$. Conversely, if $ab^{-1} \in P_D$, then $b^*a \in P \subseteq P'$ and closure of P' under $*$-conjugation gives $ab^{-1} \in P'$. $\square$

Proposition 2.6. *Let R be an Ore $*$-domain with field of fractions D. There is a one-to-one correspondence between extended $*$-orderings on R with support equal to $\{0\}$ and extended $*$-orderings on D.*

Proof. Given an extended $*$-ordering Q on R, form Q_D as in Theorem 2.3. Then $Q_D \cap R = Q$. Conversely, let Q' be an extended $*$-ordering on D and let $Q = Q' \cap R$. We must show $Q' = Q_D = \{\, ab^{-1} \mid ab^* \in Q \,\}$. Let $ab^{-1} \in Q_D$; then $ab^{-1} = ab^*b^{*-1}b^{-1} \in Q'$ since $ab^* \in Q \subseteq Q'$ and Q' is closed under multiplication by norms. Conversely, let $ab^{-1} \in Q'$. Then $ab^{-1}bb^* \in Q' \cap R = Q$, so $ab^{-1} \in Q_D$. $\square$

We next check that the order valuations defined by Marshall for $*$-orderings on R extend to the order valuations as defined by Holland [Ho] for the associated $*$-orderings on D. Let v be such an order valuation associated with a $*$-ordering P and let Γ_v be its associated semigroup. Since Γ_v is a cancellation semigroup, we can form the Grothendieck group $\widetilde{\Gamma}_v$. The next proposition shows that v extends to a $*$-valuation on D associated with the $*$-ordering P_D and having value group $\widetilde{\Gamma}_v$.

Proposition 2.7. *Let v be the order valuation associated with the $*$-ordering P on the Ore domain R. Let D and P_D be as above. Extend v to D by defining $\tilde{v}(ab^{-1}) = v(a) - v(b)$ in $\widetilde{\Gamma}_v$. This gives a well-defined valuation on D which is the associated order valuation for P_D.*

Proof. To check that $\tilde{v}$ is well defined, we need to see that if $ab^{-1} = cd^{-1}$, then $v(a)+v(d) = v(c) + v(b)$. Since $ab^{-1} = cd^{-1}$, there exist d_1, b_1 such that $ad_1 = cb_1$ and $db_1 = bd_1$. Then $v(a) + v(d_1) = v(c) + v(b_1)$ and $v(b_1) + v(d) = v(b) + v(d_1)$. Adding these and canceling we see $v(a) + v(d) = v(c) + v(b)$. For the order valuation, the valuation ring is $A(P_D) = \{\, ab^{-1} \in D \mid nbb^* - aa^* \in P_D$ for some positive integer $n \,\}$. But $\tilde{v}(ab^{-1}) \geq 0$ if and only if $v(a) \geq v(b)$, which is defined to mean $nbb^* \geq aa^*$ for some positive integer n. □

Henceforth we shall use v to denote both the valuation on R and its unique extension to D. We are finally in a position to give the valuation-theoretic characterization of all extensions of a given $*$-ordering. We define

$$\widetilde{\Gamma}_v^+ = \{\, v(k) - v(s) \in \widetilde{\Gamma}_v \mid k, s \in R^\times,\ v(k) > v(s),\ k^* = -k,\ s^* = s \,\} \cup \{\infty\}.$$

The difference between this and the $*$-field case prior to Theorem 1.9 is primarily a technicality; if R is a skew field, the two definitions yield the same set (see the proof of Theorem 1.9). Thus, when R is a $*$-field, this yields Theorem 1.9.

Theorem 2.8. *Let P be a $*$-ordering with support $\{0\}$ on an Ore $*$-domain R. Assume that 2 is a unit in R. There is a bijective correspondence between the extended $*$-orderings which intersect $S(R)$ in P and convex subsets of $\widetilde{\Gamma}_v^+$ containing*

$$\{\, v(ab - ba) - v(a) - v(b) \mid a, b \in S(R) \,\}.$$

First note that this is reasonable: Using Proposition 1.5 and Lemma 1.6, we see that $\{\, v(ab - ba) - v(a) - v(b) \mid a, b \in S(R) \,\} \subseteq \widetilde{\Gamma}_v^+$. Let D be the field of fractions of R. Let A be a convex subset of $\widetilde{\Gamma}_v^+$ containing $\{\, v(ab-ba) - v(a) - v(b) \mid a, b \in S(R) \,\}$. With inverses available, we can write $v(ab - ba) - v(a) - v(b) = v(aba^{-1}b^{-1} - 1)$. As noted following Theorem 1.9, we have $\infty \in A$, so convexity of A means that it contains all elements greater than any given element in the set. The main step in the proof of Theorem 2.8 is the following lemma concerning the set A which may be of independent interest.

Lemma 2.9. *Let A be a convex subset of $\widetilde{\Gamma}_v^+$ containing $\{\, v(ab - ba) - v(a) - v(b) \mid a, b \in S(R) \,\}$. Then A contains all elements $v(xyx^{-1}y^{-1} - 1)$ for $x, y \in S(D)^\times$.*

Proof. (1) The set A contains $v([x, y] - 1)$ for x, y either symmetric elements in R or their inverses. This is because

$$\begin{aligned} v([x,y^{-1}]-1) &= v(xy^{-1}x^{-1}y-1) \\ &= v(xy^{-1}-y^{-1}x)-v(x)-v(y^{-1}) \\ &= v(y(xy^{-1}-y^{-1}x)y)-2v(y)-v(x)-v(y^{-1}) \\ &= v(yx-xy)-v(x)-v(y) \end{aligned}$$

and similarly, $v([x^{-1},y^{-1}]-1)=v(yx-xy)-v(x)-v(y)$.

(2) If A contains $v([a,b]-1)$ and $v([a,c]-1)$, then A contains $v([a,bc]-1)$. Indeed, we have

$$\begin{aligned} v([a,bc]-1) &= v(ab[c,a^{-1}]a^{-1}b^{-1}-1) \\ &= v(ab([c,a^{-1}]-[b^{-1},a^{-1}])a^{-1}b^{-1}) \\ &= v([c,a^{-1}]-1+1-[b^{-1},a^{-1}]) \\ &\geq \min(v([c,a^{-1}]-1),\ v([b^{-1},a^{-1}]-1)) \\ &= \min(v(ac-ca)-v(a)-v(c),\ v(ab-ba)-v(a)-v(b)), \end{aligned}$$

from which the claim follows by the convexity of A.

Working in D, we write $x=ab^{-1},\ y=cd^{-1}\in S(D)^{\times},\ a,b,c,d\in R$ and form the commutator $[x,y]=[ab^{-1},cd^{-1}]=[a,b^{-1}][b^{-1},acd^{-1}][a,cd^{-1}]$. Since $ab^{-1}\in S(D)$, we have $b^*(ab^{-1})b=b^*a=a^*b\in S(R)$. Thus we can write

$$ab^{-1}=(ab^*ba^*)(bb^*)[(bb^*)(ba^*bb^*)]^{-1},$$

showing that

(3) In any fraction $ab^{-1}\in S(D)$, we may assume that a and b are products of symmetric elements in $S(R)$.

(4) If $v(s-1),\ v(t-1)\in A$, then $v(st-1)\in A$. To see this, note that $v(st-1)=v((s-1)(t-1)+(s-1)+(t-1))\geq\min(v(s-1),v(t-1))$ (where we have used the fact that all such expressions are positive in the value group) to see that the product st also yields a value in A by convexity.

We have seen above that the commutator $[ab^{-1},cd^{-1}]$ becomes a product of commutators of the form $[r,z]$ or $[r^{-1},z]$, where $r\in S(R)$ and z is a product of symmetric elements of $S(R)$ and their inverses by (3). Using (2) (with induction) along with (1), we see that each individual value $v([r,z]-1)$ and $v([r^{-1},z]-1)$ is in A. Then (4) shows that the product also yields a value $v([x,y]-1)\in A$. $\square$

Proof of Theorem 2.8. The set A gives rise to a unique extended $*$-ordering Q_A defined by $Q_A=\{\,s+k\mid s\in P,k^*=-k,v(k)-v(s)\in A\,\}$ as proved in Theorem 3.1 below. In view of Lemma 2.9, we can apply Theorem 1.9 to see that the set A corresponds uniquely to an extended $*$-ordering Q_D of D. Clearly $Q_D \cap R$ contains Q_A. To get equality, assume that $s + k \in Q_D \cap R$, where $s \in P_D = Q_D \cap S(D)$ and $k^* = -k \in D$. But then $2s = (s+k) + (s+k)^* \in R$, whence $s, k \in R$ since 2 is a unit in R. Since $v(k) - v(s) \in A$, we have $s + k \in Q_A$. $\square$

Example 2.10. The condition that 2 be a unit in R is genuinely needed in this theorem. To see this, consider the commutative $*$-field $D = \mathbb{Q}(x)$ with involution defined via $x^* = -x$. Let $P_D \subseteq S(D) = \mathbb{Q}(x^2)$ be the $*$-ordering in which $-x^2 = xx^*$ is infinitesimal and positive. Consider the subring $R = \mathbb{Z}[2x, \frac{1}{2} \pm x]$. Note that there is a homomorphism $R \to \mathbb{Z}$ defined by $x \mapsto \frac{1}{2}$; thus $\frac{1}{2}$ cannot be in R and hence neither can x. Letting $\frac{1}{2} + x$ play the role of $s + k$ in the last paragraph of the previous proof, we see that while $\frac{1}{2} + x$ lies in the maximal extended $*$-ordering of R containing $P = P_D \cap R$ (since it is in $Q_D = \{\, s + k \in D \mid v(k) > v(s), s \in P_D, k^* = -k \,\}$), it cannot lie in any Q_A since $\frac{1}{2}$ and x do not lie in R.

The following example shows that weak extended $*$-orderings need not be extended $*$-orderings.

Example 2.11. Let $D = \mathbb{R}((x))$ be the field of Laurent series in one variable over the real numbers. The involution is given by $x^* = -x$. Let P_D be the ordering of $S(D) = \mathbb{R}((x^2))$ in which $x^2 = -xx^*$ is negative. This set is a $*$-ordering of $(D, *)$, and the extended $*$-orderings containing it are described in [C3, Example 2.10]. The maximal one is $Q_D = \{\, \sum_{i=2n}^{\infty} a_i x^i \in D \mid (-1)^n a_{2n} > 0 \,\}$. Now let $R = \mathbb{R}[[x]] \subseteq D$. The induced extended $*$-ordering $Q_{max} = Q_D \cap R$ is an extended $*$-ordering containing the $*$-ordering $P = P_D \cap R$. Set $Q = \{\, \sum_{i=2n}^{\infty} a_i x^i \in R \mid (-1)^n a_{2n} > 0,\ a_1 = 0 \,\}$. One easily checks that Q is a weak extended $*$-ordering, but it does not satisfy the stronger condition. Indeed, $-x^2 + x^3 = xx^*(1-x) \in Q$, but $1 - x \notin Q$.

3. General domains.

When R is not an Ore domain, it is far more difficult to determine what transpires. Indeed, until now there were no known examples of non-Ore domains with $*$-orderings of support $\{0\}$. In this section we shall see that such domains exist. The construction shown in Section 2 to give all extensions of a $*$-ordering on an Ore domain, is shown in the general case to give a family of extensions.

Theorem 3.1. *Let R be a $*$-domain in which 2 is a unit. Let P be a $*$-ordering with support $\{0\}$. Let A be a convex subset of $\widetilde{\Gamma}_v^+$ containing $\{v(ab - ba) - v(a) - v(b) \mid a, b \in S(R)\,\}$. Define*

$$Q = Q_A = \{\, s + k \mid s \in P, k^* = -k, v(k) - v(s) \in A \,\}.$$

Then Q is an extended $*$-ordering which intersects the symmetric elements in P.

Proof. We check the six conditions of Definition 1.2. Clearly $Q^* = Q$, $rQr^* \subseteq Q$ for all $r \in R$ and $Q \cap S(R) = P$, the last because $k = 0$ gives $v(k) - v(s) = \infty \in A$. The fact that Q satisfies condition (6) of the definition is proved in a similar manner as the corresponding result in Theorem 1.8 since the value $v(k) - v(s)$ is unchanged by $*$-conjugation.
Closure under addition. Let $s_i + k_i \in Q$, $i = 1, 2$, where $0 \neq s_i \in P$, $k_i^* = -k_i$. Since $0 < s_1 < s_1 + s_2$, we have $s_1 s_1^* < (s_1 + s_2)(s_1 + s_2)^*$, which implies that $v(s_1) \geq v(s_1 + s_2)$ by definition of v. Similarly $v(s_2) \geq v(s_1 + s_2)$, so that $v(s_1 + s_2) \leq \min(v(s_1), v(s_2))$. By Proposition 1.5, v behaves as an ordinary valuation giving $v(s_1 + s_2) \geq \min(v(s_1), v(s_2))$, so that $v(s_1 + s_2) = \min(v(s_1), v(s_2))$. But then $v(k_1 + k_2) \geq \min(v(k_1), v(k_2)) > \min(v(s_1), v(s_2)) = v(s_1 + s_2)$ so that $(s_1 + s_2) + (k_1 + k_2) \in Q$.
Closure under multiplication. Letting s_i, k_i be as before, we write the product $(s_1+k_1)(s_2+k_2) = s + k$, where

$$s = (s_1 s_2 + s_2 s_1 + k_1 k_2 + k_2 k_1 + k_1 s_2 - s_2 k_1 + s_1 k_2 - k_2 s_1)/2$$

and

$$k = (s_1 s_2 - s_2 s_1 + k_1 k_2 - k_2 k_1 + k_1 s_2 + s_2 k_1 + s_1 k_2 + k_2 s_1)/2,$$

where $s^* = s$ and $k^* = -k$. By Lemma 1.6 $v(s_1 s_2 + s_2 s_1) = v(s_1) + v(s_2)$, which, in turn, equals $v(s)$ since the remainder of s has larger value. Furthermore, we know $s_1 s_2 + s_2 s_1 \in P$, whence $s \in P$ by Lemma 1.7. Now $v(k) \geq \min[v(s_1 s_2 - s_2 s_1), v(s_i) + v(k_j)\ (i \neq j)]$. If $v(k) \geq v(s_i) + v(k_j)$, then $v(k) - v(s) \geq v(s_i) + v(k_j) - v(s) = v(k_j) - v(s_j) \in A$. Then $s + k \in Q$ by the convexity of A. On the other hand, if $v(k) \geq v(s_1 s_2 - s_2 s_1)$, then $v(k) - v(s) \geq v(s_1 s_2 - s_2 s_1) - v(s_1) - v(s_2) \in A$ by hypothesis. $\square$

Example 3.2. Let $R = \mathbb{Z}\langle x, y\rangle$ be the free algebra on two variables over the integers. This is the simplest possible domain for us to consider which is not an Ore domain [L2, Proposition 10.25]. Define $*$ on R via $x^* = y$, $y^* = x$. We claim that $(R, *)$ has a $*$-ordering with support $\{0\}$. Using the notation of [M], we write T_0 for the set of all finite sums of permuted products of elements $b_1, b_1, b_2, b_2, \ldots, b_m, b_m \in S(R), r_1, r_1^*, \ldots, r_n, r_n^* \in R$ $(m, n \geq 0)$, which are nested with respect to each r_i, r_i^*. That is, r_j appears between r_i and r_i^* if and only if r_j^* also appears between r_i and r_i^*. By [M, Corollary 4.8] applied to the zero ideal, $(R, *)$ has a $*$-ordering with support $\{0\}$ if and only if $t, -t \in T_0 \cap S(R)$ implies that $t = 0$. Now assume that t is an element such that $t, -t \in T_0 \cap S(R)$. Let $(D, *)$ be any $*$-ordered $*$-field. For any $d \in D$, we have an induced $*$-homomorphism $\phi_d \colon R \to D$ defined via $\phi_d(x) = d$. Since $(D, *)$ has a $*$-ordering, the image of t must be zero in D, for any symmetric element of D which is a finite sum of permuted products of doubled symmetric elements and nested $*$-conjugates would otherwise be positive. Since this holds for every $d \in D$, we actually have a polynomial $t = f(x, x^*)$ which is identically zero on D. It is known from work by Herstein [He, Theorems 1 and 2] that this forces D to be finite dimensional over its center. However, D was arbitrary and several examples which are infinite dimensional are given in [Cr2, §7]. It follows that t must be identically zero in R and thus R has $*$-orderings with support $\{0\}$.

We remark that although we can show that the ring R above must have $*$-orderings, the construction of an explicit $*$-ordering P on R seems far more difficult.

References

[Co] P. M. Cohn, *Skew Fields*, Encyclopedia Math. Appl. vol. 57, Cambridge Univ. Press, London, 1995.

[Cr1] T. Craven, *Orderings and valuations on $*$-fields*, Rocky Mountain J. Math. **19** (1989), 629–646.

[Cr2] T. Craven, *Witt groups of hermitian forms over $*$-fields*, J. Algebra **147** (1992), 96–127.

[Cr3] T. Craven, *Orderings, valuations and hermitian forms over $*$-fields*, Proc. Symposia Pure Math. **58.2** (1995), 149–160.

[Cr4] T. Craven, *Extension of orderings on $*$-fields*, Proc. Amer. Math. Soc. **124** (1996), 397–405.

[He] I. N. Herstein, *Special simple rings with involution*, J. Algebra **6** (1967), 369–375.

[Ho] S. Holland, Jr., *Strong orderings of $*$-fields*, J. Algebra **101** (1986), 16–46.

[L1] T. Y. Lam, *A First Course in Noncommutative Rings*, Springer Verlag, New York, 1991.

[L2] T. Y. Lam, *Lectures on Modules and Rings*, Springer Verlag, New York, 1999.

[M] M. Marshall, *$*$-orderings on a ring with involution*, Comm. Algebra **28** (2000), 1157–1173.

Department of Mathematics, University of Hawaii, Honolulu, HI 96822–2273

E-mail address: tom@math.hawaii.edu

Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221–0025

E-mail address: tsmith@math.uc.edu