COLLOQUIUM MATHEMATICUM

VOL. 83 2000 NO. 1

ORDERINGS AND PREORDERINGS IN RINGS WITH INVOLUTION

BY

ISMAIL M. IDRIS (CAIRO)

Abstract. The notions of a preordering and an ordering of a ring R with involution are investigated. An algebraic condition for the existence of an ordering of R is given. Also, a condition for enlarging an ordering of R to an overring is given. As for the case of a field, any preordering of R can be extended to some ordering. Finally, we investigate the class of archimedean ordered rings with involution.

1. Introduction, definitions and basic facts. The notion of an ordering of a field was studied by Artin and Schreier. This notion was extended to division rings with involution in [1], [2] and [3]. One can ask now if this can be generalized to noncommutative rings with involution. In this paper, the notions of a preordering and an ordering of a ring R with involution are investigated. An algebraic condition for the existence of an ordering of R is given. Also, a condition for enlarging an ordering of R to an overring is given. As for the case of a field, any preordering of R can be extended to some ordering. Finally, we investigate the class of archimedean ordered rings with involution. We should remark that the orderings as defined in this work can only exist for rings without zero-divisors.

Now, we state some definitions and basic facts that will be needed in this paper. Hereafter R will be a not necessarily commutative ring with involution * (an anti-automorphism of period 2). By a *norm* in R we mean an element of the form xx^* for some $x \in R$. Let $S = \{s \in R : s = s^*\}$ be the set of all symmetric elements of R. For $x_1, \ldots, x_r \in R$ we shall write $(x_1x_1^*, \ldots, x_rx_r^*)$ to denote the set of products of the $2r$ elements x_i and x_i^* $(i = 1, \ldots, r)$ in some arbitrary but fixed order. Let X denote the union of the sets $(x_1x_1^*, \ldots, x_rx_r^*)$ $(x_i \in R,\ i = 1, \ldots, r;\ r$ any positive integer$)$, and we write P for the subset of R consisting of sums of elements of X. Then P is called the *-*core* of R. This generalizes the notion of a *-core given in [1] for the case of a ring with involution.

Clearly X contains the set of all products of norms of R, and P contains the set of all sums of products of norms, in particular $X \subset P$. Also, it is clear that X is *-closed, multiplicatively closed and contains 1; and P is

2000 *Mathematics Subject Classification*: Primary 16K40, 16W10.

*-closed and closed under sums and products. If * = identity, then R is commutative and P will be the set of all sums of products of squares of R. Our goal is to show that R has an ordering if and only if $0 \notin P$. First, we give the definition of an ordering.

DEFINITION 1.1. A *-closed subset $M \subseteq R$ is called a *preordering* of R if:

(a) $M + M \subseteq M$;
(b) $M \cdot M \subseteq M$;
(c) $0 \notin M$, $1 \in M$; and
(d) $a_1, \ldots, a_t \in M$ and $x_1, \ldots, x_r \in R$ implies that any product of the $2r + t$ elements a_j, x_i, x_i^* in some arbitrary but fixed order belongs to M (where $x_i \neq 0$).

A preordering M is called an *ordering* of R if:

(e) For $0 \neq s = s^* \in R$, $s \in M \cup -M$, i.e. S is a totally ordered (additive) group.

If R is commutative, then condition (d) above is equivalent to the condition

$$a \in M,\ x \in R \Rightarrow axx^* \in M.$$

The above definition of an ordering of R generalizes the notion of a strong ordering of a division ring with involution given in [2]. Also, $M \cap S$ will be a Jordan ordering in the sense given in [3] in the case of a division ring with involution. If * = identity, then R is commutative, and the definition of an ordering reduces to that of the classical Artin–Schreier ordering.

PROPOSITION 1.2. *Let M be an ordering on R. Then*

$$M \cap -M = \emptyset,$$

and R is a domain of characteristic zero.

Proof. If $a \in M \cap -M$, then $0 = a + (-a) \in M + M \subseteq M$, contradicting (c) above. Since $1 \in M$, it follows that, for any natural number n,

$$n \cdot 1 = 1 + \ldots + 1 \in M.$$

Therefore, $\operatorname{char} R = 0$. Finally, if $x, y \in R \setminus \{0\}$ and $xy = 0$, then $0 = x^*xyy^* \in M$, a contradiction. This shows that R is a domain. ■

PROPOSITION 1.3. *Let M be a preordering. Then*

(a) *$s = s^* \in M$, s invertible $\Rightarrow s^{-1} \in M$.*
(b) *$s \in R$, s invertible $\Rightarrow sMs^{-1} \subset M$.*

Proof. (a) We note that $s^{-1} = s(s^{-1}s^{-1*}) \in M$.
(b) $sMs^{-1} = sMs^{-1}(s^{-1*}s^*) \subset M$ (by Definition 1.1(d)). ■

If we are given an ordering M of R, then M defines a partial order relation on R by:

$$b \geq a \Leftrightarrow b - a \in M \cup \{0\}.$$

The ring $\mathbb{Z}$ of integers, the field $\mathbb{Q}$ of rational numbers and the field $\mathbb{R}$ of real numbers, with their usual orderings and the identity as involution, are examples of ordered commutative rings. The field $\mathbb{C}$ of complex numbers with conjugation as involution is ordered by the set $M = \mathbb{R}^+$ (the positive real numbers).

An example of a noncommutative ordered ring is the Weyl algebra generated over $\mathbb{R}$ by x and y with the relation $xy - yx = 1$, i.e., $R = \mathbb{R}\langle x, y\rangle/(xy - yx - 1)$, relative to the involution, making x symmetric and y skew. Elements of R have the canonical form

$$r = r_0(x) + r_1(x)y + \ldots + r_n(x)y^n,$$

where each $r_i(x) \in \mathbb{R}[x]$, $r_n(x) \neq 0$. Let $M \subseteq R$ be the set of all nonzero elements $r \in R$ as above for which $r_n(x)$ has a positive leading coefficient. One can show that M is an ordering of R.

2. Existence of orderings. For a preordering M and $0 \neq s = s^* \in R$ we define $M(s)$ to be the set of all sums of products of elements of M, elements x_i, x_i^* of R and s in some arbitrary but fixed order (where $x_i \neq 0$). If R is commutative, then clearly $M(s) = Ms$. For $R = D$ a division ring, also $M(s) = Ms$.

LEMMA 2.1. *$M \cup M(s) \cup M + M(s)$ is a preordering iff $0 \notin M + M(s)$.*

Proof. Let $M' = M \cup M(s) \cup M + M(s)$. Then clearly $M' + M' \subset M'$. By the definition of $M(s)$ and property (d) of a preordering, we have

$$\begin{aligned} M' \cdot M' &= M \cdot M(s) + M(s) \cdot M + M \cdot M + M(s) \cdot M(s) \\ &\subset M(s) + M(s) + M + M \subset M + M(s) \subset M'. \end{aligned}$$

Also M' has property (d) and $1 \in M'$. Since $0 \notin M \cup M(s)$, M' is a preordering iff $0 \notin M + M(s)$. ∎

LEMMA 2.2. *If M is a preordering and $0 \neq s = s^* \in R$, then either*

$$M_1 = M \cup M(s) \cup M + M(s) \quad \textit{or} \quad M_2 = M \cup M(-s) \cup M + M(-s)$$

is a preordering containing M.

Proof. We first note that any element of $M(-s)$ is of the form $-x$ where $x \in M(s)$ and hence every element of $M + M(-s)$ is of the form $t - x$, where $t \in M$, $x \in M(s)$. Assume now that the lemma is false. Then by Lemma 2.1, $0 \in M + M(s)$ and $0 \in M + M(-s)$. Hence $t_1 + x_1 = 0 = t_2 - x_2$ where $t_1, t_2 \in M$, $x_1, x_2 \in M(s)$, and $x_1 = -t_1$, $x_2 = t_2$. Since $x_1x_2 \in M(s) \cdot M(s) \subset M$

and $t_1t_2 \in M$ and $t_1t_2 = -x_1x_2$, it follows that $0 = x_1x_2 + t_1t_2 \in M$, which is a contradiction. Thus M_1 or M_2 is a preordering. ∎

PROPOSITION 2.3. *If M is a maximal preordering with respect to inclusion, then M is an ordering.*

Proof. We need to show that $S \subset M \cup -M$. For $0 \neq s = s^* \in S$, either

$$M_1 = M \cup M(s) \cup M + M(s) \quad \text{or} \quad M_2 = M \cup M(-s) \cup M + M(-s)$$

is a preordering containing M. But M is maximal, so $M = M_1$ or $M = M_2$ and hence M contains s or $-s$ as desired. ∎

THEOREM 2.4. *Let R be a ring with involution. Then R has an ordering if and only if $0 \notin P$.*

Proof. If R has an ordering M, then $P \subset M$ and $0 \notin P$. Conversely, if $0 \notin P$, then P is a preordering. By Zorn's Lemma, we have a maximal preordering M. By Proposition 2.3, M is an ordering of R.

THEOREM 2.5. *Any preordering M_0 of R can be extended to some ordering M.*

Proof. By Zorn's Lemma, the set of all preorderings extending M_0 contains some maximal preordering M. By Proposition 2.3, M is an ordering containing M_0. ∎

We note that any intersection of orderings of R is a preordering of R. If R is orderable, i.e., $0 \notin P$, then the *-core P is a preordering with the following features: $P \subset M$ and $M \cdot P = P \cdot M = M$ for each preordering M. Throughout the rest of this section, we will assume that $0 \notin P$. By $\mathrm{Sym}(A)$ we mean the subset of symmetric elements of A.

COROLLARY 2.6. $\mathrm{Sym}(P) = \mathrm{Sym}(\bigcap_i M_i)$, *where the intersection is over all orderings M_i of R.*

Proof. Clearly $\mathrm{Sym}(P) \subseteq \mathrm{Sym}(\bigcap_i M_i)$. Conversely, we show that $s = s^* \notin P$ implies $s \notin M$ for some ordering M. Since P is a preordering, Lemma 2.2 shows that $M_1 = P \cup P(-s) \cup P + P(-s)$ is a preordering containing P and $-s$. By Theorem 2.5, M_1 can be extended to some ordering M. Since $-s \in M_1 \subset M$ and M is an ordering, it follows that $s \notin M$. ∎

COROLLARY 2.7. *Let M_0 be any preordering. Then we have* $\mathrm{Sym}(M_0) = \mathrm{Sym}(\bigcap_i M_i)$, *where the intersection is over all orderings M_i containing M_0.*

LEMMA 2.8. *Let M_1 and M_2 be two orderings of R. If $M_1 \subset M_2$, then*

$$\mathrm{Sym}(M_1) = \mathrm{Sym}(M_2).$$

Proof. If there is $s = s^* \in M_2 - M_1$, then $s \notin M_1$ implies $-s \in M_1 \subset M_2$, so both s and $-s$ are in M_2, which is absurd. ∎

THEOREM 2.9. *Let $R \subseteq R'$ be rings with involution. Let M be an ordering of R. Let M' be the set of all sums of products of $2r+t$ elements a_j, x_i, x_i^* in some arbitrary but fixed order, where $a_1, \ldots, a_t \in M$ and $x_1, \ldots, x_r \in R' - \{0\}$. If $0 \notin M'$, then M can be enlarged to some ordering of R'.*

Proof. Since $0 \notin M'$, it follows that $0 \notin P'$ (the *-core of R') and R' is ordered. It is easy to show that M' is a preordering of R'. By Theorem 2.5, M' can be enlarged to some ordering $M_1 \supset M' \supset M$. ∎

It is known that any archimedean ordered ring is commutative. In the rest of this work, we shall investigate the class of archimedean ordered rings with involution. Let $s = s^*$ be a positive element in an ordered ring R with involution. We say that s is *infinitely large* if $s > n$ for any integer $n \geq 1$, and that s is *infinitely small* if $n \cdot s < 1$ for any integer $n \geq 1$.

LEMMA 2.10. *For any ordered ring R, the following two properties are equivalent*:

(a) *For any positive elements $s = s^*$, $d = d^*$ in R, there exists an integer $n \geq 1$ such that $n \cdot s > d$.*

(b) *R has neither infinitely large nor infinitely small elements.*

Proof. Assume (b) holds and consider $s, d > 0$. By (b), there exist integers $m, n \geq 1$ such that $d < n$ and $m \cdot s > 1$. Then $m \cdot n \cdot s > n > d$ as desired. Now, assume (a) holds, and $s = s^* > 0$. Since $1, s > 0$, by (a) there exist integers $m, n \geq 1$ such that $m = m \cdot 1 > s$ and $n \cdot s > 1$, so that s is neither infinitely large nor infinitely small. ∎

An ordered ring with involution is called *archimedean* if it satisfies any of the two conditions of Lemma 2.10. We note that if $R = D$ is an ordered division ring, then for $s = s^* > 0$, s is infinitely large if and only if s^{-1} is infinitely small. Thus D is archimedean if and only if D has no infinitely large elements, if and only if D has no infinitely small elements.

THEOREM 2.11. *Let R be an archimedean ordered ring with involution. Then all symmetric elements in R mutually commute.*

Proof. Let b, d and s be three symmetric elements of R. Let k be the skew symmetric element $[b, d] = bd - db$ and form the symmetric element $[k, s] = [[b, d], s]$. From $(s-k)^*(s-k) \geq 0$ and $(s-k)(s-k)^* \geq 0$ one can get the inequality $0 \leq |[k, s]| \leq s^2 - k^2$ where $|[k, s]|$ means the absolute value symbol in its usual sense. We assume that $s > 0$ (if $s < 0$ we replace s by $-s$). Since R is archimedean, for each $n \geq 1$ there exists an integer m such that $1 > ns - m \geq 0$ so that $(ns - m)^2 < 1$. Now, replace s by $ns - m$ in the above inequality to get $0 \leq n|[k, s]| \leq 1 - k^2$, $n = 1, 2, \ldots$; this implies $[k, s] = 0$ (since both $|[k, s]|$ and $1 - k^2$ are positive symmetric elements), i.e. $k = [b, d]$ commutes with s for all symmetric b, d, and s. This says that all commutators $[b,d]$, $b,d \in S$, commute with all symmetric elements. From the identity

$$2b[b,d] = [b^2,d] + [b,[b,d]] = [b^2,d],$$

$2b[b,d]$ also commutes with all symmetric elements, for $b,d \in S$. Thus both $[b,d]$ and $2b[b,d]$ commute with all symmetric elements. As R is a domain, b must commute with all symmetric elements. Hence all symmetric elements mutually commute. ■

COROLLARY 2.12. *Let R be an archimedean ordered ring with involution where the set S of symmetric elements generates R. Then R is a commutative domain.*

In the case of a division ring R with involution, it is known that S generates R, unless R is of dimension 4 over its centre. Hence we get

COROLLARY 2.13. *If R is an archimedean ordered division ring with involution, then R is commutative or of dimension 4 over its centre.*

REFERENCES

[1] M. Chacron, *C-orderable division rings with involution*, J. Algebra 75 (1982), 495–521.
[2] S. S. Holland, *Strong ordering of *-fields*, J. Algebra 101 (1986), 16–46.
[3] I. M. Idris, *Jordan ordering of a division ring with involution*, Arabian J. Sci. Engrg. 14 (1989), 527–535.

Mathematics Department
Faculty of Science
Ain-Shams University
Cairo, Egypt
E-mail: idris@asunet.shams.enn.eg

Received 23 March 1999;
revised 28 July 1999 (3718)