THE STRUCTURE OF IDEALS IN A EUCLIDEAN SEMIRING

By Louis Dale and Dorothy L. Hanson

1. Introduction

It is well known that a Euclidean ring is a generalization of the ring of ordinary integers and their properties. It is equally well known that every ideal in a Euclidean ring is a principal ideal, i.e. a Euclidean ring is a principal ideal ring. The purpose of this paper is to generalize the semiring of nonnegative integers, Z^+ , and their properties by defining a Euclidean Semiring. Since Z^+ is not a principal ideal semiring, it is not expected that a Euclidean semiring will be a principal ideal semiring. The structure of ideals in a Euclidean semiring E is closely related to the function ϕ associated with E. It will be shown that if E is a basis for an ideal in E, then Φ restricted to E is bounded. Some interesting consequences can be derived from this fact.

2. Fundamentals

There are different definitions of semiring appearing in the literature. However, the following definition will be used throughout this paper:

DEFINITION. A set S together with two binary operation called addition (+) and multiplication (\cdot) will be called a *semiring* provided (S, +) is an abelian semigroup with a zero, (S, \cdot) is a semigroup, and multiplication distributes over addition from the left and from the right.

A semiring is said to be commutative if (S, \cdot) is a commutative semigroup. A semiring S is said to have an identity if there exists $1 \in S$ such that $1 \cdot x = x \cdot 1 = x$ for each $x \in S$.

DEFINITION. A subset T of a semiring S is called a *subsemiring* of S if T is also a semiring with respect to the binary operations defined in S.

DEFINITION. A subset I of a semiring S will be called an *ideal* in S if I is an additive subsemigroup of (S, +), $IS \subset I$ and $SI \subset I$.

Let S be a semiring with identity e. Then it is clear that the set $\{ne \mid n \in Z^+\}$ is a subsemiring. With this in mind we give the following definition:

DEFINITION. Let S be a commutative semiring with an identity e. The set

 $S_p = \{x \in S \mid \text{ there exists } y \in S \text{ such that } x = y + e\} \cup \{0\} \text{ will be called the principal part of } S$.

It is to be noted here that the identity e may or may not belong to S_p . However, as indicated, the additive identity $0 \subseteq S_p$.

THEOREM 1. If S is a commutative semiring with an identity e, then S_p is a subsemiring of S.

PROOF. Let x_1 , $x_2 \in S_p$. Then there are elements y_1 , $y_2 \in S_p$ such that $x_1 = y_1 + e$ and $x_2 = y_2 + e$ and it follows that

$$x_1+x_2=(y_1+e)+(y_1+e)=(y_1+y_2+e)+e \in S$$
.

Also,

$$x_1x_2=(y_1+e)(y_2+e)=(y_1y_2+y_1e+y_2e)+e \in S_b$$

Hence, S_b is a subsemiring of S.

DEFINITION. Let S be a commutative semiring with an identity. Then S will be called a principal semiring if $S=S_b$.

The semiring Z^+ is a principal semiring as will be shown in the following examples. This important property is a generalization of a similar property of Euclidean rings. it is easy to see that all Euclidean rings are principal semirings.

EXAMPLES. (1) Z^+ is a principal semiring. Let $x \in Z^+$. Since $0 \in Z_p^+$ by definition and $1=0+1 \in Z_p^+$, assume that $x \neq 1$, $x \neq 0$. Since x is a non-identity, by Peano's Postulates, there exists $y \in Z^+$ such that x=y+1. Hence, Z^+ is a principal semiring.

- (ii) Let $Q^+ = \{x \in Q \mid x \ge 0\}$. Suppose $x \in Q^+$ and 0 < x < 1. Then $x = \frac{p}{q}$ where p, $q \in Z^+$ and p < q. If there exists $\frac{s}{r} \in Q^+$ such that $\frac{b}{q} = \frac{s}{r} + 1 = \frac{r+s}{r}$, then s + r < r, which is a contradiction. Hence, for 0 < x < 1, $x \notin Q_p^+$. Now, suppose $x \ge 1$. Then $(x-1) \in Q^+$ and $x = (x-1) + 1 \in Q_p^+$. Hence, $Q_p^+ = \{x \in Q \mid x \ge 1\}$, and Q^+ is not a principal semiring.
- (iii) Let $a, b \in R$, b > a and S = [a, b]. In S, define $x + y = \max\{x, y\}$ and $xy = \min\{x, y\}$. Clearly, under the two operations, addition and multiplication, S is closed, commutative and associative. Also, for each $x \in S$, $a + x = \max\{a, x\} = x$ and $xb = \min\{x, b\} = x$. So S has an additive identity a, and a multiplicative identity b. Hence S is a commutative semiring with an identity. Now let $x \neq b \in S$

and suppose there exist $y \in S$ such that x=y+b. But $x=y+b=\max\{y,b\}=b$, which is a contradiction. Hence $S_p=\{b\} \cup \{a\}=\{b,a\}$, and S is not a principal semiring.

The above examples indicate that the principal part of a semiring may be trivial or non-trivial. For our purpose here we will be interested in the case where $S=S_p$, i.e. principal semirings.

Throughout this paper, unless otherwise stated, the semirings will be commutative semirings with an identity.

3. Euclidean semirings

The problem of generalizing the nonnegative integers and their properties is an interesting one. In an ordinary Euclidean ring the function defined on the ring satisfies certain properties relating to the product of two elements and the division algorithm. No relationship is defined regarding the sum of two elements. To study ideals in a Euclidean semiring it is necessary to impose a condition on the function that relates to the sum of two elements. This condition will be derived from the fact that, in Z^+ , we have $|a+b|=|a|+|b|\geq |a|$. By taking the usual definition of a Euclidean ring and adding this property, we define a Euclidean semiring as follows:

DEFINITION. A Euclidean semiring, E, is a principal semiring, free of divisors of zero, with a function $\phi \colon E \to Z^+$ satisfying the following properties:

- (i) for $a \in E$, $\phi(a)=0$ if and only if a=0,
- (ii) for all a, $b \in E$, if $a+b\neq 0$ then $\phi(a+b) \ge \phi(a)$,
- (iii) for all $a, b \in E$, then $\phi(ab) = \phi(a)\phi(b)$,
- (iv) for all a, $b\neq 0 \in E$, there exists p, $r\in E$ such that a=pb+r where r=0 or $\phi(r)<\phi(b)$.

Recall that any two integers a and b have a greatest common divisor d, for which there are integers s and t such that d=sa+tb. However, if a, $b \in Z^+$, then we have either sa=tb+d or tb=sa+d. We wish to extend this property to Euclidean semirings.

DEFINITION. Let E be a Euclidean semiring and $a\neq 0$, $b\in E$. An element $d\in E$ will be called the *greatest common divisor* of a and b if:

- (i) d is a common divisor of both a and b.
- (ii) If c is a common divisor of both a and b, then $\phi(c) \leq \phi(d)$.

It is well known and easy to prove that in a Euclidean ring, the greatest common divisor d of any two elements a and b can be written in the form d =

sa+tb, where s and t are elements in the ring. Consequently, for our Euclidean semirings, we will assume that either sa=tb+d or tb=sa+d. The general form of the division algorithm is indispensable in the study of Euclidean rings. It will be seen that this is true also for the study of Euclidean semirings.

EXAMPLES. (i) The set of nonnegative integers, Z^+ , is a Euclidean semiring. To see this, let $\phi(n)=n$ for all $n\in Z^+$. It is clear that the four properties of a Euclidean semiring are satisfied.

(ii) The principal part of the set of nonnegative rational numbers Q_p^+ is a Euclidean semiring. Let $\phi(0)=0$ and $\phi(q)=1$ for all $q\neq 0$. Properties (i)-(iii) of a Euclidean semiring are clearly satisfied. If $q, p\neq 0 \in Q^+$, then it is well-known that there is an $r\in Q$ such that q=rp. Consequently, property (iv) follows. The principal part of the set of nonnegative real numbers R_p^+ is a Euclidean semiring.

4. Ideals in a Euclidean semiring

Since Z^+ is a Euclidean semiring, it is easy to see that a Euclidean semiring is not a principal ideal ring. However, the ideals in a Euclidean semiring can be characterized. Let E be a Euclidean semiring, $a \in E$ and $T_a = \{x \in E | \phi(x) \ge \phi(a)\} \cup \{0\}$.

THEOREM 2. If E is a Ecuclidean ring and $a \in E$, then T_a is an ideal in E.

PROOF. Let $x, y \in T_a$ and $k \in E$ such that $k \neq 0$. Then $\phi(x) > \phi(a)$ and $\phi(y) \ge \phi(a)$. Consequently, $\phi(x+y) \ge \phi(x) \ge \phi(a)$ and $\phi(kx) = \phi(k)\phi(x) \ge \phi(x) \ge \phi(a)$, therefore $x+y \in T_a$, $kx \in T_a$ and it follows that T_a is an ideal in E.

Since $\phi(a)=0$ if and only if a=0 and $\phi(e)=1$, it is clear that $T_0=T_1=E$. Some of the properties of ideals of the form T_a are given in the following theorem.

THEOREM 3. Let E be a Euclidean semiring and a, $b \in E$. Then

- (i) $T_a \subset T_b$ if and only if $\phi(a) \ge \phi(b)$,
- (ii) $T_a \cup T_b = T_c$, where $\phi(c) = \min\{\phi(a), \phi(b)\}$.
- (iii) $T_a \cap T_b = T_{c'}$, where $\phi(c') = \max\{\phi(a), \phi(b)\}$,
- (iv) If $\{a_i\}$ is a sequence of elements in E such that $\phi(a_i) < \phi(a_{i+1})$, then $\bigcap T_{a_i} = 0$.

PROOF. (i) If $T_a \subset T_b$, then from the definition of T_b it follows that $\phi(a) \ge \phi(b)$. Conversely, if $\phi(a) \ge \phi(b)$ it is clear that $T_a \subset T_b$.

(ii) and (iii) Since a, $b \in E$, it follows that $\phi(a) \ge \phi(b)$ or $\phi(b) \ge \phi(a)$. Conseq-

uently, $T_a \subset T_b$ or $T_b \subset T_a$ and (ii) and (iii) follow.

(iv) Suppose $x \in T_{a_i}$ and $\phi(x) = n$. Since $\{\phi(a_i)\}$ is an increasing sequence of positive integers, there is an a_j such that $\phi(a_j) > n = \phi(x)$. Consequently, $x \notin \bigcap T_{a_i}$ and it follows that $\bigcap T_{a_i} = \phi$.

Let T_a be an ideal in E and $B_a = \{x \in T_a | x = a + y \text{ where } \phi(y) < \phi(a)\}$. For a, $b \in E$, let $S[a,b) = \{x \in E | \phi(a) \le \phi(x) < \phi(b)\}$. We wish to show that $B_a = S[a, 2a)$. First, to show that $\phi(B_a)$ is bounded, let $x = a + y \in B_a$. Then $\phi(y) < \phi(a)$ and by the division algorithm, a = qy + r where r = 0 or $\phi(r) < \phi(y)$. Since E is a principal semiring, $q = q' + \varepsilon$ for some $q' \in E$. Consequently,

$$\phi(2a) = \phi(a+a) = \phi(a+qy+r)$$

$$= \phi(a+(q'+e)y+r)$$

$$= \phi(a+y+q'y+r) \ge \phi(a+y) = \phi(x).$$

Therefore $\phi(B_a)$ is bounded by $\phi(2a)$ and it follows that $B_a \subset S[a, 2a)$. Now suppose that $z \in S[a, 2a)$. Then $\phi(a) \leq \phi(z) < \phi(2a)$. The division algorithm gives z = pa + r where r = 0 or $\phi(r) < \phi(a)$. If $p \neq e$, then there is a p' such that p = p' + e. Consequently, z = pa + r = (p' + e)a + r = p'a + a + r. If p' = e, then $\phi(z) = \phi(a + a + r) \geq \phi(a + a) = \phi(2a)$, a contradiction. If $p' \neq e$, then p' = p'' + e for some $p'' \in E$. Consequently, z = p'a + a + r = p''a + a + a + r and $\phi(z) = \phi(p''a + a + a + r) \geq \phi(a + a) = \phi(2a)$, a contradiction. Therefore p = e and $z = a + r \in B_a$. Thus $S[a, 2a) \subset B_a$ and it follows that $B_a = S[a, 2a)$.

THEOREM 4. S[a, 2a) is a basis for T_a .

PROOF. Let $Z \in T_{a^*}$ Then Z = qa + r where r = 0 or $\phi(r) < \phi(a)$. If r = 0 or q = e the proof is complete. Suppose $r \neq 0$ and $q \neq e$. Since E is a principal semiring, q = q' + e for some $q' \in E$. Then z = qa + r = q'a + (a + r), where $a + r \in S[a, 2a)$, and it follows that S[a, 2a) is a basis for T_a .

Now if A is an ideal in E and $S[a, 2a) \subset A$ for some $a \in A$ it is clear that $T_a \subset A$. We want to find some other conditions which will guarantee that $T_a \subset A$ for some $a \in A$. These conditions are given in the following three lemmas.

LEMMA 5. Let A be an ideal in a Euclidean semiring E. If $a \in A$ and $S[ma, (m+e)a] \subset A$ for some $m \in A$, then $T_{ma} \subset A$.

*

PROOF. Suppose $x \in S[ma, 2ma) - S[ma, (m+e)a]$. Then $\phi(ma+a) < \phi(x) < \phi(2ma)$. Applying the division algorithm gives x = p(m+e)a + r where r = 0 or $\phi(r) < \phi(ma+a)$. Now r = sa + t where t = 0 or $\phi(t) < \phi(a)$. Since E is a principal semi-

ring, there is an element $q \in E$ such that p = q + e. All of this gives

$$x = p(m+e)a+r$$

$$= (q+e)(ma+a)+(sa+t)$$

$$= q(ma+a)+(ma+a)+(sa+t)$$

$$= q(ma+a)+(sa+a)+(ma+t)$$

$$= q(ma+a)+(s+e)a+(ma+t).$$

Now $q(ma+a) \in A$, $(s+e)a \in A$, and $ma+t \in A$ since $\phi(t) < \phi(ma)$. Consequently, $x \in A$ and it follows that $S[ma, 2ma) \subset A$. An application of theorem 4 assures that $T_{ma} \subset A$.

LEMMA 6. Let A be an ideal in a Euclidean semiring E. If there exists $a \in A$ such that $a+e \in A$, then $T_{a^2} \subset A$.

PROOF. Suppose a, $a+e \in A$ and $x \in S(a^2, a^2+a)$. Then $x=a^2+z$ where $\phi(z) < \phi(a)$. Now a=pq+r where r=0 or $\phi(r) < \phi(z)$. Since E is a principal semiring, p=q+e for some $q \in E$. Thus,

$$x=a^{2}+z$$

$$=(pz+r)a+z$$

$$=pza+ra+z$$

$$=z(pa+e)+ra$$

$$=z[(q+e)a+e]+ra$$

$$=z[qa+(a+e)]+ra \in A.$$

Consequently, $S[a^2, a^2+a) \subset A$ and it follows from Lemma 5 that $T_{a^2} \subset A$.

LEMMA 7. Let A be an ideal in a Euclidean semiring E. If $a,b \in A$ and a and b are relative prime, then there exist $c \in A$ such that $T \subset A$.

PROOF. If a and b are relative prime, then their greatest common divisor is e. Hence there exist s, $t \in E$ such that either sa=tb+e or tb=sa+e. Suppose sa=tb+e. Now $tb \in A$, and $tb+e=sa \in A$. Consequently, lemma 6 assures that $T_{tb} \subset A$. Similarly, if tb=sa+e it follows that $T_{sa} \subset A$. In either case, there exist c such that $T_c \subset A$.

If $\phi(a)\neq\phi(b)$ it is easy to see that $\phi(T_a)$ and $\phi(T_b)$ can differ by only a finite number of nonnegative integers. Consequently, if A is an ideal containing T_a , then $E\supset A\supset T_a$ and it follows that $\phi(E)$ and $\phi(A)$ can differ by only finitely many integers.

THEOREM 8. Let A be an ideal in a Euclidean semiring E such that $T_a \subset A$ for

some $a \in A$. Then there exists $x \in A$ such that T_x is maximal in A and $A = K \cup T_x$ where $K = \{y \in A \mid 0 < \phi(y) < \phi(x)\}$.

PROOF. Let $S = \{\phi(u) | T_u \subset A\}$. It is clear that S is a non-empty subset of Z^+ and by the Well-Ordering Principle, S contains a least element, say $\phi(x)$. Now $\phi(x) \leq \phi(u)$ for all $\phi(u) \in S$ and it follows from theorem 3 that T_x is maximal in A. If $K = \{y \in A | 0 < \phi(y) < \phi(x)\}$ then it follows that $A = K \cup T_x$. It is clear that any basis for A is contained in $K \cup S[x, 2x)$.

Not every ideal A in E contains an ideal of the form T_a . For example, if $a \in A$ such that $\phi(a) > 1$, then the principal ideal (a) contains no ideal of the form T_x for any x. This is clear since $(a) = \{ax | x \in E\}$ and $\phi(ax) = \phi(a)\phi(x)$. Thus, $\phi\{(a)\}$ consists only of multiples of $\phi(a)$. In this case, $(a) = aT_e$. We want to generalize this case by considering ideals of the form bT_a . It is easy to show that if T_a is an ideal in E and $b \in E$, then bT_a is an ideal in E. Also it follows from theorem 3 that $bT_a \subset bT_c$ if and only if $\phi(a) \ge \phi(b)$. Our aim now is to show that if A is an ideal in E such that A contains no ideal of the form T_a , then A contains an ideal of the form bT_a . To do this we will need to derive some properties of ideals of this type.

THEOREM 9. bS(a, 2a) is a basis for bT_a .

PROOF. Since S[a, 2a) is a basis for T_a , it follows that bS[a, 2a) is a basis for bT_a .

Now it is clear that for any $b \in A$ the ideal $(b)=bT_e \subset A$. We are interested in ideals of the form bT_a where $a \neq e$ and conditions which will insure that an ideal A will contain bT_a .

Since $S[a, 2a] = B_a = \{y | y = a + r \text{ where } \phi(r) < \phi(a)\}$, it follows that $dS[a, 2a] = \{y | y = da + r \text{ where } \phi(r) < \phi(da) \text{ and } d \text{ divides } r\}$.

Consequently, the proof of the following lemma follows directly from the proof of lemma 5.

LEMMA 10. Let A be an ideal in E. If $a \in A$ and dS [ma, (m+e)a] $\subset A$, then $dT_{ma} \subset A$.

This lemma is necessary for the following theorem.

THEOREM 11. Let A be an ideal in E and $a \in A$. If d divides a and $a+d \in A$, then $dT_a \subset A$.

PROOF. Let a=dm and $x \in dS[a, a+d]$. Then dS[a, a+d]=dS[dm, (m+e)d] and it follows that $x=d^2m+z$ where $\phi(z)<\phi(dm)$ and d divides z. Hence z=kd for some $k \in E$. Now d=pz+r where $\phi(r)<\phi(z)$ and since E is a principal semiring, we have both d=f+e and p=q+e. All of this gives

$$x=d^{2}m+z$$

$$=dm(pz+r)+z$$

$$=(apz+z)+ar$$

$$=k(apd+d)+ar$$

$$=k[a(q+e)(f+e)+d]+ar$$

$$=k[a(qf+q+f)+(a+d)]+ar.$$

Since $a \in A$ and $a+d \in A$, it follows that $x \in A$. Consequently, $dS[a, a+d] \subset A$ and it follows from Lemma 10 that $dT_a \subset A$.

COROLLARY 12. Let A be an ideal in E and a, $b \in A$. If d is the greatest common divisor of a and b, then $dT_{b} \subset A$ for some $p \in A$.

PROOF. Since d is the greatest common divisor of a and d it follows that either sa=tb+d or tb=sa+d for some s, $t \in A$. Suppose sa=tb+d. Then $tb \in A$ and it follows from theorem 11 that $dT_{tb} \subset A$. Similarly, if tb=sa+d, then $dT_{sa} \subset A$.

LEMMA 13. Let $p,q,c, d \in E$. (i) If p divides q, then $dT_q \subset dT_p$. (ii) If c divides d, then $dT_p \subset cT_p$.

PROOF. (i) If p divides q, then q=pk for some $k \in E$. If $x \in dT_q$, then x=dq' for some $q' \in E$ with $\phi(q') \ge \phi(q)$. But $\phi(q') \ge \phi(q) = \phi(pk) \ge \phi(p)$. Consequently, $x \in dT_p$ and $dT_q \subset dT_p$. (ii) If c divides d, then d=cm for some $m \in E$. Consequently, $dT_p = cmT_p = c(mT_p) \subset cT_p$.

Now suppose that A is an ideal in E such that A contains no ideals of the form T_a for $a \in A$. Let $a, b \in A$ and d be the greatest common divisor of a and b. It is clear that $d \neq e$. Otherwise, lemma 7 would assure that $T_c \subset A$ for some $c \in A$, a contradiction. Consequently, it follows from corollary 12 that $dT_p \subset A$ for some $p \in A$. Now let $W = \{d \mid d \text{ is the greatest common divisor of some } a, b \in A\}$ and $k \in W$ such that $\phi(k)$ is minimum. Let $V = \{p \mid dT_p \subset A\}$ and $q \in V$ such that $\phi(q)$ is minimum. It is clear that k divides k for all k we applying lemma 13 and theorem 3 we obtain that kT_q is maximal in k. Now letting $k \in A$ where k where k where k where k where k where k of k where k of k where k of k of

for kT_q . Consequently, $L \cup kS(q, 2q)$ is a basis for A and it follows that this basis is bounded by $\phi(2kq)$. These remarks and theorem 8 prove the following structure theorem for ideals in a Euclidean semiring.

THEOREM 14. Let A be an ideal in a Euclidean semiring E. Then $A=L\cup dT_p$, where dT_p is maximal in A, $L=\{t\in A|\phi(t)<\phi(dp)\}$ and $L\cap dT_p=\{0\}$. Moreover, $L\cup dS[p,2p)$ is a basis for A whose images are bounded by $\phi(2dp)$.

An immediate consequence of this structure theorem is that if E is a Euclidean semiring with the property that $\phi^{-1}(n)$ is finite or empty for each $n \in Z^+$, then every ideal in E has a finite basis. This is clear since the basis $L \cup dS[p, 2p)$ would be a finite set. The set of integers Z^+ is such a semiring. It can be concluded from this structure theorem that every ideal A in Z^+ is "almost principal", i.e. A is a principal ideal except for a finite number of elements. To see this, note that in Z^+ , dT_p is a principal ideal if p=1. Consequently, if p>1, then dT_p is a principal ideal with only a finite number of elements missing and it is obvious that L is a subset of the missing elements. If ϕ is one to one and onto Z^+ , then it can be shown quite easily that E is a Noetherian semiring. This is done by showing first that ideals of the form dT_{a_i} satisfy the ascending chain condition and extending this to any ascending chain of ideals in E.

The structure of ideals in a Euclidean semiring gives us only a glimpse into the structure of the semiring itself. Since every Euclidean semiring is an ideal in itself it follows that the set of images of the basis for the semiring is bounded. This seems to be the only general conclusion that is apparent concerning the semiring. While we have developed a decomposition theorem for ideals in a Euclidean semiring, this in no way gives us a decomposition theorem for the semiring itself.

University of Alabama in Birmingham Birmingham, Alabama 35294

REFERENCES

- [1] Jacobson, Nathan, Lectures in Abstract Algebra, Volume 1. Princeton, New Jersey: D. Van Nostrand Co. Inc., 1951.
- [2] Miller, Kenneth S., Elements of Abstract Algebra, New York Harper Brothers, 1958.
- [3] Allen, P.J., Cohen's Theorem for a Class of Noetherian Semirings. Publ. Math. (Debrecen). 17(1970) 169-171.