Ideal theory in the semiring Z^+

By PAUL J. ALLEN and LOUIS DALE (Alabama)

It is well known that the ring of integers Z is a principal ideal ring and that Z is Noetherian. It is equally well known that the semiring (the definitions and results appearing in ALLEN [1] and [2] will be used throughout this paper) of non-negative integers Z^+ is not a principal ideal semiring. It is generally assumed without question that Z^+ is Noetherian; however, a proof has not been presented in the semiring literature, and prior to this paper, the ideals in Z^+ have not been classified. It will be shown that there is only one basic type of ideal in Z^+ and that all ideals in Z^+ are related to this basic type in a natural way. Consequently, it will be an easy matter to classify ideals in Z^+ and present a proof that Z^+ is a Noetherian semiring. From these results, the discovery is made that Z^+ is an "almost principal" ideal semiring

When $n \in Z^+$, the notation T_n will be used to denote $\{t \in Z^+ \mid t \geqq n\} \cup \{0\}$. The following are elementary facts concerning T_n.

Theorem 1. *If $n \in Z^+$, then T_n is an ideal in Z^+ such that*

1. $T_0 = T_1 = Z^+$,
2. *If* $1 \leqq n < m$, *then* $T_m \subset T_n$ *and* $T_m \neq T_n$,
3. $T_n \cup T_m = T_k$, *where* $k = \min \{n, m\}$,
4. $T_n \cap T_m = T_q$, *where* $q = \max \{n, m\}$, *and*
5. $\cap \{T_i \mid i \in Z^+\} = \{0\}$.

PROOF. Let $a \in T_n$ and $b \in T_n$. Since $a \geqq n$ and $b \geqq n$, it follows that $a + b \geqq 2n \geqq n$. Moreover, if $k \in Z^+$, where $k \neq 0$, then $ka \geqq kn \geqq n$. Therefore, $a + b \in T_n$ and $ka \in T_n$ and *it* is clear that T_n is an ideal in Z^+. The proofs of properties (1) through (5) are straightforward and will be omitted.

When $a \in Z^+$ and $b \in Z^+$, the notation $S(a, b)$ will be used to denote the set $\{t \in Z^+ \mid a \leqq t \leqq b\}$.

Theorem 2. *If $n > 1$, then $S(n, 2n)$ is a finite basis for T_n.*

PROOF. Let $p \in T_n$. If $p \in S(n, 2n)$ or $p = cn$ for some $c \in Z^+$, then p is generated by $S(n, 2n)$. Let $p > 2n$ and $p \neq cn$ for any $c \in Z^+$. There exists a $k \geqq 2$ such that $kn < p < (k+1)n$. However, this guarantees the existence of an $s < n$ such that $kn + s = p$, and it follows that $n + s \in S(n, 2n)$. Therefore, $p = kn + s = (k-1)n + n + s$, where $n \in S(n, 2n)$ and $(n+s) \in S(n, 2n)$, and it follows that $S(n, 2n)$ is a basis for T_n.

Theorem 3. *Z^+ satisfies the ascending chain condition on T_n-ideals.*

PROOF. Let $\{T_{n_\alpha}\}$ be an ascending chain of T_n-ideals in Z^+. It follows from Theorem 1 that $\{n_\alpha\}$ is a nonincreasing sequence of positive integers. Since any nonincreasing sequence of positive integers is finite there exists $\mu \in Z^+$ such that $n_i = n_\mu$ for each $i \geqq \mu$. Therefore $T_{n_i} = T_{n_\mu}$ for each $i \geqq \mu$ and Z^+ satisfies the ascending chain condition on T_n-ideals.

The following lemmas will be essential in the characterization of all ideals in Z^+. They also give some methods by which one can determine if an ideal in Z^+ contains a T_n-ideal.

Lemma 4. *Let I be an ideal in Z^+. If $a \in I$, $m \in Z^+$, where $m \neq 0$,* and *$S(ma, (m+1)a) \subset I$, then there exists an $n \in Z^+$ such that $T_n \subset I$.*

PROOF. Suppose $p \in Z^+$, $p > (m+1)a$ and $p \neq ca$ for $c \in Z^+$. Since there exists $k \geqq m+1$ such that $ka < p < (k+1)a$, one has $ka + s = p$ for some $s < a$. Clearly $s < a$ implies that $ma + s \in S(ma, (m+1)a) \subset I$. Therefore, $p = ka + s = (k-m)a + ma + s \in I$. Consequently, $T_{ma} \subset I$ and the lemma follows.

Lemma 5. *Let I be an ideal in Z^+. If there exists an $a \in I$ such that $a+1 \in I$, then there exists an n such that $T_n \subset I$.*

PROOF. If I is a T_n-ideal, the lemma is obvious. Suppose I is not a T_n-ideal and a is the least element in I such that $a+1 \in I$. Since I is an ideal, a series of simple calculations show that the following elements belong to I:

$$\begin{array}{l} a,\ a+1 \\ 2a, 2a+1, 2a+2 \\ 3a, 3a+1, 3a+2, 3a+3 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ aa, aa+1, aa+2, aa+3, \ldots, aa+a = a(a+1). \end{array}$$

The last row of elements is $S(a^2, (a+1)a)$ and in view of Lemma 4, there exists an $n \in Z^+$ such that $T_n \subset I$.

Lemma 6. *Let $a \in Z^+$ and $b \in Z^+$ where $a \neq 0$ and $b \neq 0$. If d is the greatest common divisor of a and b, then there exists $s \in Z^+$ and $t \in Z^+$ such that $sa = tb + d$* or *$tb = sa + d$.*

PROOF. From elementary number theory, it is well known that $d = s'a + t'b$ for some integers s' and t'. Since $0 \leqq d \leqq a$, $0 \leqq d \leqq b$ and both a and b are positive, it follows that $s' \leqq 0$ and $t' \geqq 0$, or $s' \geqq 0$ and $t' \leqq 0$. If perchance $s' \leqq 0$ and $t' \geqq 0$, then $tb = sa + d$ where $0 \leqq t' = t$ and $0 \leqq -s' = s$. On the other hand, if $s' \geqq 0$ and $t' \leqq 0$, then $sa = tb + d$ where $0 \leqq s' = s$ and $0 \leqq -t' = t$, and the conclusions follows.

The above lemma is necessary for the following:

Lemma 7. *Let I be an ideal in Z^+, $a \in I$ and $b \in I$. If a and b are relatively prime, then there exists an n such that $T_n \subset I$.*

PROOF. Since 1 is the greatest common divisor of a and b, the above lemma guarantees the existence of $s\in Z^+$ and $t\in Z^+$ such that $sa=tb+1$ or $tb=sa+1$. Since I is an ideal it is clear that $sa\in I$ and $tb\in I$. Consequently, $sa+1\in I$ or $tb+1\in I$ and the lemma follows from Lemma 5.

It is easy to see that for $m\neq n$, T_m and T_n differ by at most a finite number of elements. Since $Z^+=T_1$, it follows that Z^+ differs from a T_n-ideal by at most a finite number of elements. Consequently, if I is an ideal in Z^+ containing a T_n-ideal, then $T_n\subset I\subset Z^+$ and it follows that Z^+ and I differ by at most a finite number of elements. It will be shown that an ideal I in Z^+ not containing a T_n-ideal differs from the multiples of some positive integer $d>1$ by at most a finite number of elements. Consequently, if I is an ideal in Z^+ not containing a T_n-ideal, then there exist $m\in Z^+$ and $d\in Z^+$, where $d>1$, such that $dT_m\subset I\subset (d)$.

In view of the above remarks, the ideals in Z^+ are classified according to the following definition.

Definition 8. An ideal I in Z^+ will be called a *T-ideal* if $T_k\subset I$ for some $k\in Z^+$. All other ideals in Z^+ will be called *M-ideals*.

It is clear that Z^+ is a T-ideal and $\{0\}$ is an M-ideal. The following theorem gives a characterization of T-ideals in Z^+ and will be used to show that Z^+ is Noetherian.

Theorem 9. *An ideal I in Z^+ is a T-ideal if and only if I has a finite basis and $I=K\cup T_k$ where T_k is the maximal T_n-ideal contained in I and $K=\{t\in I\,|\,0<t<k\}$.*

PROOF. Suppose I is a T-ideal and $T_n\subset I$. Let $S=\{n\in Z^+\,|\,T_n\subset I\}$. It is clear that S is a non-empty subset of Z^+ and by the Well-Ordering Principle, S contains a least element, say k. By Theorem 1, $T_n\subset T_k$ for each $n\in S$ and it is clear that T_k is the maximal T_n-ideal contained in I. Letting $K=\{t\in I\,|\,0<t<k\}$ one has $I=K\cup T_k$. According to Theorem 2, $S(k, 2k)$ is a finite basis for T_k. Since K is a finite set, $S(k, 2k)\cup K$ is a finite basis for I. The converse of the theorem is obvious.

Theorem 10. *If $n\in Z^+$ and $d\in Z^+$, then dT_n is an ideal in Z^+ such that*

1. *$dT_1=(d)$ and $dT_n=T_n$ if and only if $d=1$,*
2. *$dT_n=\{0\}$ if and only if $d=0$,*
3. *If $m<k$, then $dT_k\subset dT_m$,*
4. *$dT_m\cup dT_k=dT_p$, where $p=\min\{m, k\}$,*
5. *$dT_m\cap dT_k=dT_q$, where $q=\max\{m, k\}$, and*
6. *$\bigcap\{dT_n\,|\,n\in Z^+\}=\{0\}$.*

PROOF. Suppose $x\in dT_n$ and $y\in dT_n$. Then there exist $k\geqq n$ and $q\geqq n$ such that $x=kd$ and $y=qd$. Clearly, $k+q\geqq n$ and $x+y=kd+qd=(k+q)d\in dT_n$. If $c\in Z^+$ where $c\neq 0$, then $ck\geqq n$ and $cx=c(kd)=(ck)d\in T_nd$. Therefore, dT_n is an ideal in Z^+. The proofs of (1) through (6) are straightforward and are omitted.

It will be shown that for any ideal I in Z^+ there exist $n\in Z^+$ and $d\in Z^+$ such that dT_n is contained in I. Consequently, the dT_n-ideal is the basic type of ideal in Z^+ and the study of ideals in Z^+ is reduced to the problem of finding a maximal dT_n-ideal for each ideal in Z^+. It has already been observed in the previous theorem that $dT_n=T_n$ if $d=1$ and $dT_n=\{0\}$ if $d=0$. Consequently, it only remains to study the case for $d>1$. For this purpose, in the remainder of this paper it will be assumed that $d>1$ unless otherwise stated.

The following three lemmas are analogues of well known properties of ideals in Z.

Lemma 11. *If $p\in Z^+$, $q\in Z^+$ and p divides q, then $qT_n\subset pT_n$.*

PROOF. Suppose $a\in qT_n$. There exists $k\geqq n$ such that $a=kq$. Since p divides q, there exists $t\geqq 1$ such that $q=tp$. Consequently, $a=kq=k(tp)=(kt)p\in pT_n$, since $kt\geqq n$, and it follows that $qT_n\subset pT_n$.

Lemma 12. *If $dT_c\subset bT_a$ then b divides d.*

PROOF. Suppose $dT_c\subset bT_a$. Since $cd\in bT_a$, there exists $p\geqq a$ such that $cd=pb$ and b divides cd. By definition of dT_c, $(c+1)d\in bT_a$ and there exists $q\geqq a$ such that $(c+1)d=qb$. Consequently, b divides $(c+1)d=cd+d$ and in view of the fact that b divides cd, one has b divides d.

Lemma 13. *If $bT_a\cap dT_c\neq\{0\}$, then there exist $p\in Z^+$ and $q\in Z^+$ such that $qT_p\subset bT_a\cap dT_c$.*

PROOF. Suppose $x\in bT_a\cap dT_c$. It is clear that $xT_1\subset bT_a$ and that $xT_1\subset dT_c$, and the proof is complete.

The following two lemmas are essential to show that Z^+ is Noetherian on dT_n-ideals.

Lemma 14. *Any ascending sequence $\{bT_{a_j}\}$ is finite.*

PROOF. Suppose $\{bT_{a_j}\}$ is an ascending sequence of ideals in Z^+. By Theorem 10, $\{a_j\}$ is a decreasing sequence of positive integers and is therefore finite; i.e., there exists $\alpha\in Z^+$ such that $a_\alpha=a_n$ for each $n\geqq\alpha$. Therefore, $bT_{a_\alpha}=bT_{a_n}$ for each $n\geqq\alpha$.

Lemma 15. *Any ascending sequence $\{b_iT_a\}$ is finite.*

PROOF. Let $\{b_iT_a\}$ be an ascending sequence of ideals in Z^+. In view of Lemma 12, b_i divides b for $i\in\{2, 3, 4, \dots\}$. Since b is finite and not zero there can only be a finite number of distinct b_i's. Hence, there is an $\alpha\in Z^+$ such that $b_\alpha=b_n$ for each $n\geqq\alpha$ and it follows that $b_\alpha T_a=b_nT_a$ for each $n\geqq\alpha$.

Theorem 16. *Z^+ satisfies the ascending chain condition on dT_n-ideals.*

PROOF. Let $\{b_iT_{a_i}\}$ be an ascending chain of ideals in Z^+. By Lemma 15, there exists $\alpha\in Z^+$ such that $b_\alpha=b_i$ if $i\geqq\alpha$. By Lemma 14, there exists $\beta\in Z^+$ such that $a_\beta=a_j$ if $j\geqq\beta$. If $k=\max\{\alpha, \beta\}$, then $b_kT_{a_k}=b_pT_{a_p}$ for $p\geqq k$.

When $x\in Z^+$, $y\in Z^+$ and $d\in Z^+$ where $d>1$, denote by $S_d(x, y)$ the set $\{k\in Z^+ | x\leqq k\leqq y$ and $k=md$ for some $m\in\{Z^+\}\}$.

Lemma 17. *$S_d(nd, 2nd)$ is a finite basis for dT_n.*

PROOF. Let $p=qd\in dT_n$. If $p\in S_d(nd, 2nd)$ or $p=a(nd)$ for some $a\in Z^+$, then p is generated by $S_d(nd, 2nd)$. Suppose $p\notin S_d(nd, 2nd)$ and $p\neq a(nd)$ for $a\in Z^+$. Since $p>2nd$ and there exists $k>2$ such that $knd<p<(k+1)nd$, it follows that there exists an $s=td<nd$ such that $knd+s=p$. However, $s<nd$ implies that $nd+s=nd+dt= =nd+td=(n+t)d\in S_d(nd, 2nd)$. Therefore, $p=knd+s=(k-1)nd+nd+s$ and $S_d(nd, 2nd)$ is a finite basis for dT_n.

Lemma 18. *Let I be an ideal in Z^+, $a \in I$ and d divide a, where $d > 1$. If there exists $m \in Z^+$ such that $S_d(ma, (m+1)a) \subset I$, then there exists $n \in Z^+$ such that $dT_n \subset I$.*

Proof. If d divides a, then there exists $b \in Z^+$ such that $a = bd$ and it follows that $S_d(ma, (m+1)a) = S_d((mb)d, (md+b)d)$. Clearly, if $p = qd$, where $mb \leqq q \leqq (m+1)b$, then $p \in S_d(ma, (m+1)a) \subset I$. Suppose $p = qd$, where $q > (m+1)b$. It is clear that $p > (m+1)a$ and there exists $k \geqq 1$ such that $k(ma) \leqq p \leqq (k+1)ma$. Consequently, there exists $s \in Z^+$ such that $s < ma$ and $k(ma) + s = p$. However, $k(ma) + s = (kmb)d + s = p = qd$ and if follows that $s = cd$ for some $c \in Z^+$. Moreover, $ma + s < (m+1)a$ and it is easy to see that $ma + s = m(bd) + cd = (mb+c)d \in S_d(ma, (m+1)a) \subset I$. Therefore, $ma + s \in I$ and $(k-1)ma \in I$ together imply that $p = qd = k(ma) + s = (k-1)ma + (ma+s) \in I$. This shows that for each $q \geqq mb$, $qd \in I$ and consequently, letting $n = mb$ it is clear that $dT_n \subset I$.

Theorem 19. *Let I be an ideal in Z^+, $a \in I$. and $b \in I$. If a and b are relatively prime, then there exists $n \in Z^+$ such that $dT_n \subset I$, where d is the greatest common divisor of a and b.*

Proof. Since d is the greatest common divisor of a and b, $b = pd$ for some $p \in Z^+$ and by Lemma 6, there exist positive integers s and t such that $sa = tb + d$ or $tb = sa + d$. Since I is an ideal, it is clear that $sa \in I$ and $tb \in I$. Consequently, if $sa = tb + d$, a series of simple calculations show that the following elements belong to I:

$$\begin{array}{l} bt,\ bt+d, \\ 2bt,\ 2bt+d,\ 2bt+2d, \\ 3bt,\ 3bt+d,\ 3bt+2d,\ 3bt+3d \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ ptb,\ ptb+d,\ ptb+2d,\ ptb+3d,\ \dots,\ ptb+pd. \end{array}$$

Substituting $b = pd$ in the last row one obtains

$$p^2td,\ (p^2t+1)d,\ (p^2t+2)d,\ \dots,\ (p^2t+p)d.$$

Since $ptb + pd = pt + b = (ptb+1)b$, the last row is $S_d(ptb, (pt+1)b)$ and Lemma 18 implies the existence of an $n \in Z^+$ such that $dT_n \subset I$. On the other hand, if $tb = sa + d$ a similar argument yields the same result.

The following theorem is needed for the characterization of M-ideals in Z^+.

Theorem 20. *If I is an M-ideal in Z^+, then there exist $n \in Z^+$ and $d \in Z^+$ such that $dT_n \subset I$.*

Proof. If $a \in I$ and $b \in I$ where a and b are relatively prime, then Lemma 7 implies $T_k \subset I$ for some k, a contradiction to the fact that I is an M-ideal. Consequently, if $a \in I$ and $b \in I$, then their greatest common divisor, say d, is greater than 1, and the previous theorem gives the desired result.

The following theorem gives a structure and characterization of M-ideals in Z^+ and is necessary to show that Z^+ is Noetherian.

Theorem 21. An ideal I in Z^+ is an M-ideal if and only if I has a finite basis and $I=L\cup qT_p$, where $q>1$, qT_p is a maximal dT_n-ideal contained in I, and $L=\{t\in I\,|\,0<t<pq\}$.

PROOF. The above theorem guarantees the existence of n and $d>1$ such that $dT_n\subset I$, if I is an M-ideal. Let $S=\{d\in Z^+\,|\,d$ is the greatest common divisor of some $a\in I$ and $b\in I\}$ and q be the least element in S. Theorem 19 assures that $W=\{n\in Z^+\,|\,qT_n\subset I\}$ is a non-empty subset of Z^+. Consequently, if p is the least element of W, then it is clear that $qT_p\subset I$. Suppose there exists $bT_a\subset I$ such that $qT_p\subset bT_a$. It follows from Theorem 12 that b divides q and consequently $b\leqq q$. Since b is the greatest common divisor of ba and $b(a+1)$ one has $b\in S$ and it follows that $q\leqq b$. Consequently, $b=q$. By Theorem 10, $a\leqq p$ and since $a\in W$ it follows that $p\leqq a$. Consequently, $p=a$ and $qT_p=bT_a$. Therefore qT_p is a maximal ideal in I. If $c\in I$, $c>pq$ and k is the greatest common divisor of c and pq, then $c=ka$ for some $a\in Z^+$, $k\in S$ and it can be shown that q divides k. Thus there exists $r\in Z^+$ such that $k=rq$. Consequently, $pq<c=ka(rq)a=(ra)q$ and it follows that $ra>p$ and $c\in qT_p$. If $L=\{t\in I\,|\,0<t<pq\}$ then it is clear that $I=L\cup qT_p$. In view of Lemma 17, $S_q(pq, 2pq)$ is a finite basis for I. The converse of the theorem is obvious.

Since any ideal in Z^+ is either a T-ideal or an M-ideal Theorems 9 and 21 give a classification and structure for all ideals in Z^+. These results can now be used to obtain the following theorem.

Theorem 22. *Z^+ is a Noetherian semiring.*

PROOF. In view of Theorem 9 and Theorem 21, any ideal in Z^+ has a finite basis, and it follows that Z^+ is Noetherian (see Allen [1]).

Definition 23. An ideal I in a semiring R will be called *almost principal* if there exists a finite set $S\subset R$ such that $I\cup S=P$, where P is a principal ideal in R. The semiring R will be called an *almost principal ideal semiring* if every ideal in R is almost principal.

Theorem 24. *Z^+ is an almost principal ideal semiring.*

PROOF. Let I be an ideal in Z^+. If I is a T-ideal, then by Theorem 9, $I=K\cup T_n$. Let $S=\{t\in Z^+\,|\,t\notin I\}$. It is clear that S is a finite subset of Z^+ and $I\cup S=Z^+=(1)$ is a principal ideal. If I is an M-ideal, then by Theorem 21, $I=L\cup dT_n$. Let $S=\{td\,|\,t\in Z^+$ and $td\notin I\}$. It is clear that S is a finite subset of Z^+ and $I\cup S=(d)$ is a principal ideal. In either case I is an almost principal ideal and the result follows.

References

[1] P. J. ALLEN, Cohen's theorem for a class of Noetherian semirings, *Publ. Math. (Debrecen)* **17** (1970), 169—171.

[2] P. J. ALLEN, A fundamental theorem of homomorphisms for semirings, *Proc. Amer. Math. Soc.* **21** (1969), 412—416.

(Received October 16, 1973.)