PACIFIC JOURNAL OF MATHEMATICS
Vol. 52, No. 2, 1974

MAXIMAL IDEALS IN THE NEAR RING OF POLYNOMIALS MODULO 2

J. L. BRENNER

A near ring (or semiring) is a structure with addition and composition. Under addition, the structure is a commutative group. Composition is associative and distributive on one side: $(p+q)\circ r = p\circ r + q\circ r$. An example is the set of polynomials with coefficients from the ring of integers [or indeed from any ring]; composition is ordinary composition of polynomials. Another example is the set of endomorphisms of an abelian group.

An ideal in a near ring is, as usual the *kernel of a homomorphism*. (This definition first appeared in G. Birkhoff's 1934 paper, "On the combination of subalgebras," in Proceedings of the Cambridge Philosophical Society.) For $N = \boldsymbol{Z}_2[x, \circ]$, the near ring of polynomials with coefficients from the field $\boldsymbol{Z}_2$ of two elements, the ideal structure is more intricate than it is for $\boldsymbol{Z}_p[x, \circ]$ $(p > 2)$. In this article, all maximal ideals in N are found. Unexpectedly, there are just two of them. There are several other proper ideals. A device due to the referee shows how to construct many of them. Application of his idea is given in the following article.

2. Introduction and summary. The definition of "ideal" shows that, if I is an ideal, then

2.1. I is additively closed:

$$\{t_1 \in I, t_2 \in I\} \Longrightarrow \{t_1 + t_2 \in I\}\ .$$

2.2. N admits I, in short $I\circ N \subset N$. Explicitly,

$$\{t \in I, n \in N\} \Longrightarrow \{t\circ n \in I\}\ .$$

2.3. Composition contracts on the right, i.e.,

$$\{t \in I, n_1, n_2 \in N\} \Longrightarrow \{n_1\circ(n_2 + t) - n_1\circ n_2 \in I\}\ .$$

THEOREM 2.4. *Conversely, a subset I is an ideal if it satisfies* 1, 2, 3. (This is a known fact.)

The identity for "$\circ$" is the polynomial x.

Among the results of this article are the following. The set of all polynomials p in N such that $p(0) = p(1)$ is a maximal ideal V, but there is another one T (Theorem 3.3). Both maximal ideals are *principal*, i.e., generated by a single element, together with repeated applications of 2.1–2.3. The smallest (the principal) ideal J containing 1 is determined (Theorem 3.9).

3. **The maximal ideals.** The near ring $N = Z_2[x, \circ]$ has just two maximal ideals, T and V. T is the additive closure of

$$\{1, x + x^2, x^3, x + x^4, x + x^5, x^6, x + x^7, x + x^8, x^9, \cdots\},$$

and V is the additive closure of $\{1, x + x^a \ (a > 1)\}$.

THEOREM 3.1. *V is a maximal ideal.*

Proof. V is an ideal, since V contains every polynomial $p(x)$ such that $p(0) = p(1)$. With this characterization, V was discovered by D. Doi Watkins, as a student. If an ideal K contains V properly, then K contains x^b, hence x; hence N.

LEMMA 3.2. *Every maximal ideal contains* 1.

Proof. Either a maximal ideal is V, or else it contains a polynomial $p(x)$ such that $p(0) \neq p(1)$. Apply 2.2.

THEOREM 3.3. *The set T is a maximal ideal.*

This theorem is conveniently proved by characterizing T as in 3.5. It is interesting first to note Lemma 3.4 which shows that, if T is an ideal, T is a maximal ideal.

LEMMA 3.4. *Let $p(x)$ be any polynomial not in T. Then $p(x) = x + q(x)$, $q(x) \in T$.*

Proof. Use induction. By successive subtraction of $x^{3a\pm1} + x$ or of x^{3a}, $p(x)$ can be reduced to x.

The following characterization of T is due to the referee.

LEMMA 3.5. *Let θ be an imaginary over Z_2, such that $\theta^2 + \theta + 1 = 0$. Then $\theta^3 + 1 = 0$, and T consists of all polynomials $p(x)$ in $Z_2[x]$ such that $p(\theta)^2 + p(\theta) = 0$.*

Proof. If $p(x) = x^{3a\pm1} + x$, then $p(\theta) = 0, 1$. If $p(x) = x^{3a}$, then $p(\theta) = 1$. The lemma follows, since T is nothing but the additive closure of the polynomials $x^{3a\pm1} + x$, x^{3a}, 1.

I proved that T is an ideal originally in Spring 1969. (That proof did not involve imaginaries.) But Lemma 3.5 permits a shorter proof.

LEMMA 3.6. *If* $[x^2 + x] \circ p(\theta)$, $[x^2 + x] \circ q(\theta) = 0$, *then*

$$[x^2 + x] \circ (p(\theta) + q(\theta)) = 0 .$$

LEMMA 3.7. *If* $g(x)$ *is any polynomial in* $Z_2[x]$, *then for every* $p(x)$ *in* T, $[p(x)^2 + p(x)] \circ g(\theta) = 0$.

Proof. If $g(\theta) = 0, 1, \theta$ this is clear. The only other possibility is $g(\theta) = 1 + \theta$; but $1 + \theta$ is the imaginary conjugate to θ: $(1 + \theta)^2 + (1 + \theta) + 1 = 0$.

LEMMA 3.8. *If* $f(x)$, $g(x)$ *are any polynomials in* $Z_2[x]$, *then for every* $p(x)$ *in* T, $h(\theta) = f \circ (g(\theta) + p(\theta)) + f \circ g(\theta)$ *has the value* 0 *or* 1, *so that* $h(\theta)^2 + h(\theta) = 0$.

Proof. If $p(\theta) = 0$, this is clear. If $p(\theta) = 1$, then $h(\theta) = f(g(\theta) + 1) + f(g(\theta))$. There are only four possibilities: $g(\theta) = 0, 1, \theta, 1 + \theta$. In the last two cases, $h(\theta) = f(\theta) + f(\theta + 1)$; thus $h(\theta) = 0$ or 1 in all cases.

The proof of Theorem 3.3 is complete.

THEOREM 3.9. *Let* J *be the intersection of* T, V. *As an additive group,* J *has index* 4 *in the additive group* N. J *is the smallest ideal in* N *containing* 1.

Proof. The fact that, as an additive group, the index $N: J$ is 4 is clear: J contains a binomial $x^b + x$ or $x^b + x^3$ for every degree $b > 3$. The cosets of N mod J are thus represented by $1, x, x^3, x + x^3$. Since J is the intersection of two ideals, J must be an ideal. The main difficulty is to show that, if an ideal contains 1, it must contain J. This is a consequence of the following series of lemmata.

LEMMA 3.10. *If an ideal contains* 1, *it must contain* $x + x^2$.

Proof. $(1 + x)^3 - x^3 = 1 + x + x^2$; see 2.3.

LEMMA 3.11. *If an ideal contains* $x + x^2$, *it contains* $x^a + x^{2a}$.

Proof. Use 2.2 with $n = x^a$.

LEMMA 3.12. *If an ideal contains* t, *it contains* t^a.

Proof. Use 2.3 with $n_1 = x^a$, $n_2 = 0$.

LEMMA 3.13. *If an ideal contains $x + x^2$, it contains $x + x^5$, $x^5 + x^{25}$, $x^7 + x^{35}$.*

Proof. $x + x^5 = (x + x^2)^3 - (x + x^2) - (x^2 + x^4) + (x^3 + x^6)$; $x^5 + x^{25} = (x + x^5) \circ x^5$; $x^7 + x^{35} = (x + x^5) \circ x^7$.

LEMMA 3.14. *If an ideal I contains $x + x^2$, it contains $x + x^7$.*

Proof. There are several steps in the proof.

First, I contains $x + x^4$. Next I contains $x^4 + x^{17} = (x + x^4)^5 - (x^5 + x^{20}) - (x^4 + x^8)$. Then I contains $x + x^{19} = (x^4 + x^{17})^3 - (x^{12} + x^{51}) - (x^5 + x^{25}) - (x + x^5)$. Finally, I contains both $x + x^{17} = (x + x^2) + (x^2 + x^4) + (x^4 + x^{17})$, and $x^3 + x^{51}$; and hence I contains $x^7 + x^{19} = (x + x^{17})^3 - (x^3 + x^{51}) - (x^7 + x^{35})$.

LEMMA 3.15. *The ideal I containing $x + x^2$ must contain $x + x^a$ for every a prime to 3.*

Proof. It has already been shown that I contains $x + x^a$ for $a = 2, 4, 5, 7, 8, 10$. The process of forming successively $(x + x^a)^3$ (which are in I for these values of a) can be used to construct an inductive proof. For example,

$$\begin{aligned}
&(x + x^5)^3 - (x^3 + x^{15}) - (x + x^7) = x + x^{11}\ ;\\
&(x^4 + x^5)^3 - (x^{12} + x^{15}) - (x^2 + x^{14}) = x^2 + x^{13} \equiv x + x^{13}\ ,\\
&(x^2 + x^7)^3 \equiv x + x^{16}\\
&(x + x^8)^3 \equiv x + x^{17}\ .
\end{aligned}$$

In each of the last three formulas, the first parenthesis has the form $x^b + x^{9-b}$. Using $(x^b + x^{12-b})^3$ for $b = 5, 4, 2, 1$, one finds that $x + x^{19}$, $x + x^{20}$, $x + x^{22}$, $x + x^{23}$ are in I. In that part of the argument, the only thing needed is the assertion of the lemma for $a = 11, 13, 14, 16, 17$. The inductive proof may be completed by successive applications of this idea.

LEMMA 3.16. *The ideal I containing $x + x^2$ contains also $x^3 + x^{3a}$ for every a.*

Proof. I contains $x^3 + x^9 = (x^2 + x^5)^3 - (x^6 + x^{15}) - (x^3 + x^{12})$. The proof may be completed by induction. Suppose $b = cd$, where c is a power of 3 and d is prime to 3.

By Lemma 3.15, $x + x^d$ is in I, so $x^c + x^{cd} = (x + x^d) \circ x^c$ is in I

also. If $c > 9$, then $(x^3 + x^9) \circ x^{c/9} = x^{c/3} + x^c$ is in I. By induction, then, $x^3 + x^{27}$, and in general $x^3 + x^c$, is in I. But $x^3 + x^{cd} = (x^c + x^{cd}) + (x^3 + x^c)$.

This completes the proof of Theorem 3.9.

THEOREM 3.17. *The only maximal ideals in N are T, V.*

Proof. This follows from Theorems 3.2, 3.9.

THEOREM 3.18. *Both ideals T, V are principal.*

Proof. The generators are respectively x^3, $x^3 + x + 1$.

Each of T, V can be used to define other ideals.

4. Other ideals in $Z_2[x, \circ]$.

THEOREM 4.1. *Let K be an ideal in N. The set of polynomials $p(x)$ in K such that $p(1) = p(0)$ is an ideal in N.*

Proof. Use 2.1–2.3.

LEMMA 4.2. *The intersection of ideals in N is an ideal in N.*

4.1–4.2 yield the following.

THEOREM 4.4. *The principal ideal I generated by $x + x^2$ is the additive closure of*

$$\{x + x^a \ (a \text{ prime to } 3);\ x^3 + x^{3b}\}\ .$$

Proof. Apply Theorem 4.1 to J.

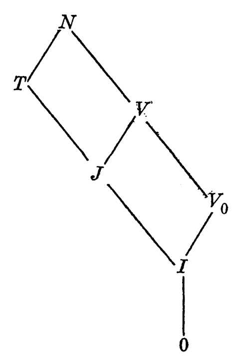

FIG. 1. Inclusion relations for some ideals in $Z_2[x, \circ]$.

The subset of V consisting of polynomials with no constant term is also an ideal, V_0. See Fig. 1.

5. **Conclusion.** The succeeding paper shows that there are other ideals in N. I am looking forward to the opportunity of reading it.

In $\boldsymbol{Z}_p[x, \circ]$ $(p > 2)$ the ideal structure seems not to be intricate. For example, the only ideal containing 1 is the entire near ring.

Acknowledgment. Thanks are due to the referee for a prompt and careful reading of the manuscript.

Received October 2, 1972 and in revised form November 4, 1972. Research partially supported by NSF Grant GP-32527.

College of Notre Dame, Belmont, Ca.

Present address: 10 Phillips Road
Palo Alto, Ca 94303