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

REMARK ON THE PRECEDING PAPER, IDEALS IN NEAR RINGS OF POLYNOMIALS OVER A FIELD

E. G. STRAUS

In this note we extend the characterization of ideals in near rings $N = F[x, \circ]$ of polynomials over a field F under addition and composition, the most interesting and exceptional cases of whice are given in the preceding paper by J. L. Brenner.

The results can be summarized in the following theorems.

THEOREM 1. *If F is infinite then N contains no nontrivial ideals.*

THEOREM 2. *If F is finite and* char $F > 2$ *then every ideal of N is also an ideal of the ring $F[x]$.*

THEOREM 3. *Those ideals of N which are also ideals of $F[x]$ consist of multiples of polynomials $p(x)$ of the form*

$$(1) \qquad p(x) = \text{l.c.m.}\ [(x^{q^{n_i}} - x)^{m_i} \mid 1 \leqq n_1 < \cdots < n_k;\ m_i \geqq 0]$$

where $q = |F|$.

THEOREM 4. *If F is finite of characteristic 2 then $N = F[x, \circ]$ contains ideals which are not ideals of $F[x]$.*

If $|F| > 2$ then every ideal, I, of N is a module over $F[x^2]$ and contains an ideal J of $F[x]$ which is generated by the squares of the elements of I. The ideal J contains the ordinary product of every two elements of I.

Proof of Theorem 1. Let $I \neq \{0\}$ be an ideal of N and let $p(x) \in I$, $p \neq 0$. Since F is infinite there exists an element $a \in F$ so that $p(a) \neq 0$. Thus $p(a) \in I$ and hence $F \subset I$.

If char $F \neq 2$ then by Criterion 2.03 of the preceding paper we have $2x = (x+1)^2 - x^2 - 1 \in I$ and hence $x \in I$ so that $I = N$.

If char $F = 2$ then we have

$$x^2 + x = (x+1)^3 + x^3 + 1 \in I$$
$$ax^2 + a^2x = (x+a)^3 + x^3 + a^3 \in I \qquad a \in F,\ a \neq 0, 1\ .$$

Thus

$$a(x^2 + x) + ax^2 + a^2x = (a + a^2)x \in I$$

and hence $x \in I$ so that again $I = N$.

Proof of Theorem 2. Let I be an ideal of N. Then for every $f \in N$ and $p \in I$ we have

$$fp = \frac{1}{2}((f + p)^2 - f^2 - p^2) \in I .$$

Thus I is closed under multiplication by $F[x]$ and is therefore an ideal of $F[x]$.

Proof of Theorem 3. We first show that every ring ideal $pf[x]$ with p of the form (1) satisfies the criteria of § 2 of the preceding paper. Closure under addition is obvious. Criterion 2.02 follows from the fact that for $f(x) = a_0 + a_1 x + \cdots a_k x^k$ we have

$$(x^{q^n} - x) \circ f(x) = \sum_{i=1}^{k} a_i (x^{iq^n} - x^i)$$

where the right side is obviously divisible by $x^{q^n} - x$. Criterion 2.03 is again obviously satisfied since $f(g + ph) - f(g)$ is divisible by p for all $f, g, h \in F[x]$.

Conversely, if $I = pF[x]$ is an ideal of N then we must have

$$p(x) \mid p(f(x)) \text{ for all } f \in N ,$$

if θ is a zero of multiplicity m of p then it must therefore be a zero of multiplicity $\geqq m$ of $p(f(x))$. In other words, $p(x)$ must have a zero of order $\geqq m$ at every element of $F(\theta)$ thus $p(x)$ is divisible by $(x^{|F(\theta)|} - x)^m$. Starting with a zero, θ, of highest degree over F we thus get successively the expression for p given in (1).

Proof of Theorem 4. We observe that for each $n \geqq 1$ the set of polynomials

$$I = (x^{q^n} + x)^2 F[x^2] + (x^{q^n} + x)^4 F[x] , \tag{2}$$

where $q = |F|$, is an ideal of N but is clearly not an ideal of $F[x]$; since it contains $p(x) = (x^{q^n} + x)^2$ but does not contain $xp(x)$. To prove that I is an ideal we observe that it is obviously closed under addition. Also for each $f, g, h, k \in N$ we have

$$f(g + ph(x^2) + p^2 k(x)) - f(g) \equiv ph(x^2) f'(g(x)) \pmod{p^2} .$$

Now $f'(g(x))$ is a polynomial in g^2 and hence contained in $F[x^2]$. Thus $f(g + i) - f(g) \in I$ for all $i \in I$.

Finally, in order to show that $i(f(x)) \in I$ for all $f \in N$, $i \in I$ it suffices to show that for all $g \in N$

$$p(f)g(f^2) \equiv ph(x^2) \qquad (\bmod\ p^2)$$

for a suitable $h \in N$. Since $p(f_1 + f_2) = p(f_1) + p(f_2)$ it suffices to prove this fact for $f(x) = x^k$. If $k = 2l$ is even then $p(x^k) = p^2(x^l) \equiv O(\bmod\ p^2)$. If $k = 2l + 1$ is odd then

$$p(x^k) = x^{2kq^n} + x^{2k} = (x^{2q^n} + x^2 + x^2)^k + x^{2k} \equiv x^{2k-2}p(x) \qquad (\bmod\ p^2)\ .$$

If $|F| > 2$ we can see that the construction in (2) is rather typical. Pick $a \in F$ with $a^2 + a \neq 0$ then for every $i \in I, f \in N$ we have

$$(a^2 + a)fi^2 = a((f + i)^3 + f^3 + i^3) + ((f + ai)^3 + f^3 + a^3i^3) \in I$$

and thus $fi^2 \in I$. In other words the squares of the elements of I generate an ideal of $F[x]$ contained in I and therefore itself an ideal J of N of the form $p^2F[x]$ where p is a polynomial of the form (1).

Since the square of every element of I is divisible by p^2 it follows that all elements of I are divisible by p. Finally we have for every $i \in I$, $f \in N$

$$(a^2 + a)f^2i = a^2((f + i)^3 + f^3 + i^3) + ((f + ai)^3 + f^3 + a^3i^3) \in I$$

and thus $f^2i \in I$, so that I is a module over $F[x^2]$. Every module over $F[x^2]$ can be expressed in the form $f(x^2)F[x^2] + g(x)F[x^2]$ where the first part gives the ideal of all polynomials in x^2 contained in the module and the second part the coset involving terms of odd degree with g chosen so that its highest term of odd degree has minimal degree. Once we have determined the polynomial p of form (1) then I has the form

$$I = p(x)[f(x^2)F[x^2] + g(x)F[x^2]] + p^2(x)F[x]\ . \tag{3}$$

Here f, g are determined (mod p) so that there are only finitely many possible choices leading to ideals of N. We forego the somewhat complicated detailed description of this determination. It is clear, however, from (3) that there can be nontrivial ideals of N containing 1 only when $|F| = 2$.

Received November 2, 1972.

UNIVERSITY OF CALIFORNIA, LOS ANGELES