Pacific Journal of Mathematics

# POLYNOMIAL NEAR-FIELDS?

YONG SIAN SO

Vol. 96, No. 1 November 1981

PACIFIC JOURNAL OF MATHEMATICS
Vol. 96, No. 1, 1981

# POLYNOMIAL NEAR-FIELDS?

YONG-SIAN SO

**It is well known that all finite fields can be obtained as homomorphic images of polynomial rings. Hence it is natural to raise the question, which near-fields arise as homomorphic images of polynomial near-rings.**

**It is the purpose of this paper to give the surprising answer: one gets no proper near-fields at all—in dramatic contrast to ring and field theory. Another surprising result is the fact that all near-fields contained in the near-rings of polynomials are actually fields.**

Homomorphic images are essentially factor structures. So we take a commutative ring $R$ with identity, from the near-ring $R[x]$ of all polynomials over $R$ (or the near-ring $R_0[x]$ of all polynomials without constant term over $R$) and look for ideals $I$ such that $R[x]/I$ becomes a near field. With this notation (and containing the one of [1] and [2]) we get our main result:

THEOREM 1. *If $R[x]/I$ (or $R_0[x]/I$) is a near-field then it is isomorphic to $R/M$ (where $M$ is a maximal ideal of $R$) and hence a field.*

The proof requires a series of lemmas as well as a number of results on near-fields.

Our first reduction is the one of $R[x]$ to $R_0[x]$.

LEMMA 1. *If $I$ is an ideal of (the near-ring) $R[x]$ such that $R[x]/I$ is a near-field, then there exists an ideal $J$ of $R_0[x]$ with $R[x]/I \cong R_0[x]/J$.*

*Proof.* $R_0[x] \subseteqq I$ implies $x \in I$, hence $R[x] \subseteqq I$, a contradiction. So we have $R_0[x] \nsubseteq I$ and—since $I$ must be maximal in order to get a near-field—$R_0[x] + I = R[x]$. By a version of the isomorphic theorem (which is valid in our case) we get

$$R[x]/I = (R_0[x] + I)/I \cong R_0[x]/(I \cap R_0[x])$$

and $J := R_0[x] \cap I$ will do the job.

REMARK 1. The converse of Lemma 1 does not hold: Take $J := \{a_2x^2 + a_3x^3 + \cdots + a_nx^n / n \in \boldsymbol{N},\ n \geqq 2,\ a_i \in \boldsymbol{R}\}$. Then $\boldsymbol{R}_0[x]/J \cong \boldsymbol{R}$ is a (near) field, but the near-ring $\boldsymbol{R}[x]$ is simple ([2] or [3], 7.89), so there is no $I \trianglelefteq \boldsymbol{R}[x]$ with $\boldsymbol{R}[x]/I \cong \boldsymbol{R}$.

We can therefore reduce our search to get suitable ideals of $R_0[x]$ which yield near-field factors.

LEMMA 2. *Let* $I \trianglelefteq R_0[x] =: N$. *Then* $R_0[x]/I$ *is a near-field* iff $I$ *is a maximal N-subgroup of N.*

*Proof.* $\Rightarrow$: Suppose that $N/I$ is a near-field. Then $N/I$ is $N/I$-simple by ([3], 8.3). Consider the canonical epimorphism $h: N \to N/I$ with kernel $I$. If $M$ is some $N$-subgroup strictly between $I$ and $N$ then $h(M)$ turns out to be a proper $N/I$-subgroup of $N/I$, which is a contradiction. Hence $I$ is a maximal $N$-subgroup of $N$.

$\Leftarrow$: Let $I$ be a maximal $N$-subgroup of $N$ and take $h$ as above. If $M$ is a proper $N/I$-subgroup of $N/I$ then $h^{-1}(M)$ is an $N$-subgroup of $N$ strictly between $I$ and $N$, which cannot happen. Hence $N/I$ is $N/I$-simple and again by ([3], 8.3) a near-field.

Due to the works of Clay-Doi [2], Brenner [1] and Straus [5] we know quite a bit about maximal ideals of $R[x]$. These informations can be used to find all ideals $I$ of $R_0[x]$ which are maximal $R_0[x]$-subgroups of $R_0[x]$ and which we call "strictly maximal" ones (from now on).

First we need some

NOTATIONS.

(i) $((x^2)) := \{a_2x^2 + \cdots + a_nx^n / n \in \mathbf{N},\ n \geqq 2,\ a_i \in R\}$.

(ii) If $I \trianglelefteq R_0[x]$ then $I_1 := \{a \in R/\text{some } ax + a_2x^2 + \cdots + a_nx^n \in I\}$ $I' := \{a \in R/ax \in I\}$.

(iii) If $M \triangleleft R$ then $Mx := \{mx/m \in M\}$.

LEMMA 3. (i) $((x^2))$ *is an ideal of* $R_0[x]$ *with* $R_0[x]/((x^2)) \cong R$.

(ii) $I_1$ *and* $I'$ *are ideals of* $R$ *with* $I' \subseteqq I_1$.

*Proof.* Straightforward.

LEMMA 4. *Let $I$ be a strictly maximal ideal of* $R_0[x]$ *and* $h: R \to R/I'$ *the canonical epimorphism. We define $h'$ as follows*: $h': R_0[x] \to (R/I')_0[x]$

$$a_nx^n + \cdots + a_1x \longmapsto h(a_n)x^n + \cdots + h(a_1)x\ .$$

*Then* $J := h'(I)$ *is a strictly maximal ideal in* $(R/I')_0[x] = h'(R_0[x])$ *and $J'$ is the zero ideal in* $R/I'$.

*Proof.* By ([4], 4.6), $h'$ is a near-ring epimorphism and we get

$R_0[x]/I \cong h'(R_0[x])/h'(I) = (R/_{I'})_0[x]/J$. So $J$ must be strictly maximal in $(R/I')_0[x]$, by arguments as in Lemma 2. Observe that $(I')_0[x] \subseteq I$.

Now suppose that $r' \in R/I'$ is in $J'$. Then $r'x \in J = h'(I)$ and there is some $i \in I$ with $h'(i) = r'x$. Let $i = a_1x + \cdots + a_nx^n$. Then $h'(i) = h(a_1)x + \cdots + h(a_n)x^n = r'x$, whence $-rx + a_1x + \cdots + a_nx^n \in \operatorname{Ker} h' = (I')_0[x] \subseteq I$ for some $r \in R$ with $h(r) = r'$. Hence $rx$ must be in $I$, so $r \in I'$ and consequently $r'$ is the zero element of $R/I'$. This shows that $J'$ is the zero ideal of $R/I'$.

By using the second isomorphism theorem, we therefore can confine our attention to strictly maximal ideals $I$ with $I' = \{0\}$. But then the worst cases are behind of us:

LEMMA 5. *Let $I$ be a strictly maximal ideal in $R_0[x]$ with $I' = \{0\}$. Then $R$ is an integral domain.*

*Proof.* Let $a, b \in R$, $a \neq 0$, $b \neq 0$ and $ab = 0$. Then $ax \circ bx = abx = 0 \in I$. If both $ax \notin I$, $bx \notin I$ then $(ax + I) \circ (bx + I) = abx + I = I$; a contradiction to the fact that a near-field has no divisors of zero. So we get $ax \in I$ or $bx \in I$, whence $a \in I'$ or $b \in I'$, a contradiction. $R$ is therefore an integral domain.

By ([3], 8.9), the characteristic of a near-field is either 0, a prime $\neq 2$ or $= 2$. We treat these 3 cases separately, and start with:

LEMMA 6. *Let $I$ be a strictly maximal ideal of $R_0[x]$ with $I' = \{0\}$ and* $\operatorname{Char} R_0[x]/I = 0$. *Then there exists a maximal ideal $M$ of $R$ with $R_0[x]/I = R/M$.*

*Proof.* By Lemma 5, $R$ is an integral domain. It is easy to see that in our case $\operatorname{Char} R = \operatorname{Char} R_0[x] = \operatorname{Char} R_0[x]/I = 0$, hence $R$ is infinite.

*Case* 1. $((x^2)) \subseteq I$. Since $I_1$ cannot be $= R$ (otherwise $I = R_0[x]$), $I_1$ is contained in a maximal ideal $M$ of $R$. $I = ((x^2)) + I_1x \subseteq ((x^2)) + Mx$ which is a proper ideal of $R_0[x]$. But $I$ is a strictly maximal ideal, hence $I = ((x^2)) + Mx$ and $R_0[x]/I \cong (\{ax/a \in R/M\}, +, 0) \cong (R/M, +, \cdot)$.

*Case* 2. $((x^2)) \nsubseteq I$. Since $I$ is a strictly maximal ideal we get $I + ((x^2)) = R_0[x]$. Then $I_1 = R$ and we can select a polynomial $i = b_nx^n + \cdots + b_1x \in I$ with $b_1 \neq 0$ and $n$ minimal for being a polynomial in $I$ with nonzero coefficient of $x$. If $r \in R$ then $i \circ (rx) - rx \circ i \in I - I = I$. But $i \circ (rx) - rx \circ i = b_{n-1}(r^n - r^{n-1})x^{n-1} + \cdots + b_2(r^n - r^2)x^2 +$

$b_1(r^n - r)x$. Since $R$ is an integral domain, hence embeddable into a field, the set of all $s \in R$ with $s^n = s$ has cardinality $\leqq n$. Since $R$ is infinite, we can take $r \in R$ so that $r^n \neq r$. Then $i \circ (rx) - rx \circ i$ is a polynomial in $I$ with nonzero coefficient of $x$ and a degree $\leqq n - 1$ which is a contradiction. So Case 2 cannot occur.

Hence we have proved our Theorem 1 in the case when $\operatorname{Char} R_0[x]/I = 0$. Now we consider the case of characteristic $p \neq 2$.

LEMMA 7. *Let $I$ be a strictly maximal ideal of $R_0[x]$ with $\operatorname{Char} R_0[x]/I \neq 2$. Then there exists a maximal ideal $M$ of $R$ with $I = Mx + ((x^2))$, hence $R_0[x]/I \cong R/M$.*

*Proof.* First we show: $x^2 \in I$. Since $x \notin I$, $-x \notin I$. If $x^2 \notin I$ we have: $(x^2 + I) \circ (-x + I) = -((x^2 + I) \circ (x + I)) = -(x^2 + I) = -x^2 + I$ by ([3], 8.10(b)). But $(x^2 + I) \circ (-x + I) = x^2 \circ (-x) + I = x^2 + I$. So we have $2x^2 \in I$. Since $(p, 2) = 1$ there are $a, b \in Z$ with $1 = a \cdot p + b \cdot 2$. $x^2 = (a \cdot p + b \cdot 2)x^2 = apx^2 + 2bx^2 \in I$ because $px^2 \in I$ as a result of $\operatorname{Char} R_0[x]/I = p$. This is contradiction, hence $x^2 \in I$. Then we have $x^{2n} = x^2 \circ x^n \in I$ for all $n \in N$.

Now we show: $x^n \in I$ for all $n \in N$ and $n \geqq 2$. Let $n \geqq 2$. Then $x^2 \circ (x^n + x^{n-1}) = x^{2n} + 2x^{2n-1} + x^{2n-2} \in I$, and we get $2x^{2n-1} \in I$ because $x^{2n} \in I$ for $n \geqq 1$. As above, we have $x^{2n-1} \in I$. Hence we have: $x^n \in I$ for $n \geqq 2$. And as a result of this we have $((x^2)) \subseteqq I$ and, similarly to the proof of Lemma 6, we have $I = Mx + ((x^2))$ where $M$ is a maximal ideal of $R$. Therefore $R_0[x]/I \cong R/M$.

So it remains the case that $\operatorname{Char} R_0[x]/I = 2$, which—as usual—causes the most trouble.

LEMMA 8. *Let $I$ be a strictly maximal ideal in $R_0[x]$ with $\operatorname{Char} R_0[x]/I = 2$. Then $(2R)_0[x] \subseteqq I$.*

*Proof.* Since $x + I \in R_0[x]/I$ we have $2x + I = I$. Hence $2x \in I$. But for all $f \in R_0[x]$ $2x \circ f = 2f \in I$, hence $(2R)_0[x] \subseteqq I$.

LEMMA 9. *Let $I$ be a strictly maximal ideal in $R_0[x]$ with $\operatorname{Char} R_0[x]/I = 2$. Also, let $h\colon R \to R/2R$ be the canonical epimorphism and $h'\colon R_0[x] \to (R/2R)_0[x]\colon a_nx^n + \cdots + a_1x \to h(a_n)x^n + \cdots + h(a_1)x$. Then $R_0[x]/I \cong (R/2R)_0[x]/h'(I)$.*

The proof is similar to the one of Lemma 4 and therefore omitted.

In view of this result, we only have to look at the case: $\operatorname{Char} R = \operatorname{Char} R_0[x]/I = 2$, $R$ an integral domain and $I' = \{0\}$.

We now treat the infinite case:

LEMMA 10. *Let $I$ be a strictly maximal ideal in $R_0[x]$ with* $\operatorname{Char} R = \operatorname{Char} R_0[x]/I = 2$, *$R$ an infinite integral domain and $I' = \{0\}$. Then there exists a maximal ideal $M$ of $R$ with $I = ((x^2)) + Mx$, hence $R_0[x]/I = R/M$.*

*Proof.* Suppose there is no maximal ideal $M$ of $R$ with $I = ((x^2)) + Mx$. Then we get $I_1 = R$, otherwise $I_1$ would be in a maximal ideal $M_1$ of $R$ and $I \subseteqq ((x^2)) + M_1x$.

Let $U := \{a_nx^n + \cdots + a_1x \in I / n \in N,\ a_1 \neq 0\}$. Clearly $U \neq \{0\}$, since $I_1 = R$. Let $m$ be the minimum of the degrees of nonzero polynomials in $U$. Since $I' = \{0\}$, $m$ is $\geqq 2$. Let $e \in R\backslash\{0, 1\} \neq \emptyset$. Let $b_mx^m + \cdots + b_1x \in U \subseteqq I$. $(b_mx^m + \cdots + b_1x) \circ (ex) + e^mx \circ (b_mx^m + \cdots + b_1x) = b_{m-1}(e^m + e^{m-1})x^{m-1} + \cdots + b_1(e^m + e)x \in I$. Since $m$ is minimal, $b_1(e^m + e) = 0$. We get $e^m + e = 0$, $e^{m-1} + 1 = 0$, because $R$ is an integral domain. But $1^{m-1} + 1 = 0$, so we get for all $e \in R\backslash\{0\}$ $e^{m-1} + 1 = 0$.

So $m - 2 \geqq 1$; consequently $e^{m-1} = e \cdot e^{m-2} = 1$ and hence $e^{m-2}$ is the inverse of $e$ in $R$. $R$ is then a field with $e^{m-1} = 1$ for all $e \in R\backslash\{0\}$, hence with infinitely many roots of unity, a contradiction.

So there is a maximal ideal $M$ of $R$ with $I = ((x^2)) + Mx$.

In particular, if $R$ is a field, we get $I = ((x^2))$.

We still have to look at the case: $\operatorname{Char} R = 2$, $R$ a finite integral domain, $I' = \{0\}$. But a finite integral domain is a field. So for our $R$ we have either $R = \boldsymbol{Z}_2$ or $R = GF(2^n)$ with $n \geqq 2$.

First some preparations:

LEMMA 11. *Let $F$ be a field with* $\operatorname{Char} F = 2$, $|F| > 2$. *Let $I$ be a strictly maximal ideal in $F_0[x]$. If $x^m \in I$ then $x^{m+i} \in I$ for $m + i \geqq 4$ where $i \in N$.*

*Proof.* $x^{2m+1} + x^{m+2} = (x^m + x)^3 + x^3 + x^{3m} \in I$. Since $|F| > 2$, it is possible to choose $a$ with $a \neq 0$, $a \neq 1$. From $(x^m + ax)^3 + (ax)^3 \in I$ we get $ax^{2m+1} + a^2x^{m+2} \in I$. But $ax \circ (x^{2m+1} + x^{m+2}) = ax^{2m+1} + ax^{m+2} \in I$. By adding of these two polynomials we get $(a^2 + a)x^{m+2} \in I$. Since $a^2 + a \neq 0$, we have $x^{m+2} \in I$. So we have: $x^m, x^{m+2}, x^{m+4}, x^{m+6}, \cdots \in I$.

But $x^{2m} = x^m \circ x^2 \in I$, we also have $x^{2m+2} \in I$. $x^{2m+2} = (x^{m+1}) \circ x^2 \in I$, so we have either $x^2 \in I$ or $x^{m+1} \in I$ since $F_0[x]/I$ is a near-field and has no zero-divisor.

If $x^{m+1} \in I$ we get: $x^{m+i} \in I$ for all $i \in N$.

If $x^2 \in I$ then $x^4 + x^5 = (x^2 + x)^3 + x^3 + x^6 \in I$. Hence then $x^5 \in I$.

So we have: $x^2, x^4, x^6, \cdots \in I$, $x^5, x^7, x^9, \cdots \in I$.

Hence $x^{m+i} \in I$ for $m + i \geqq 4$, where $i \in N$.

LEMMA 12. *Let $I \neq F_0[x]$ be an ideal of $F_0[x]$, when $F$ is a field of characteristic 2. If there is an $n \geqq 2$, so that $x^m \in I$ for all $m \geqq n$, then $I \subseteqq ((x^2))$.*

*Proof.* Suppose $I \nsubseteq ((x^2))$. Then there is some $f \in I \backslash ((x^2))$. Without loss of generality, we can assume $f = x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$.

$$f \circ x^{n-1} = x^{n-1} + a^2(x^{n-1})^2 + \cdots + a_{n-1}(x^{n-1})^{n-1} \in I$$
$$x^{n-1} = f \circ x^{n-1} + a_2(x^{n-1})^2 + \cdots + a_{n-1}(x^{n-1})^{n-1} \in I$$

since the degrees of second, third, $\cdots$ terms are $\geqq n$. Therefore we can reduce $n$ and we get: $x^{n-2}, x^{n-3}, \cdots, x^2 \in I$. But then $x = f + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in I$, a contradiction. Hence $I \subseteqq ((x^2))$.

LEMMA 13. *Let $I$ be a maximal ideal in $F_0[x]$, when $F$ is a field of characteristic 2 and $|F| > 2$. If there is some $n \in N$ with $n \geqq 2$, so that $x^m \in I$ for all $m \geqq n$, then $I = ((x^2))$.*

*Proof.* Use Lemma 12.

LEMMA 14. *Let $I$ be a strictly maximal ideal in $F_0[x]$, when $F$ is a field of characteristic 2 and $|F| > 2$. If there is an $n \in N$ with $n \geqq 2$, $x^n \in I$, then $I = ((x^2))$.*

*Proof.* According to Lemma 11 we have: $x^m \in I$ for all $m \geqq \max(n, 4)$. Lemma 13 will do the rest of the job.

LEMMA 15. *Let $F$ be a field of characteristic 2 and $I$ a strictly maximal ideal of $F_0[x]$. Then there is an odd number $t$ with $x^t + \cdots + a_1x \in I$.*

*Proof.* Since $I \neq \{0\}$, there is a $k \in N$ with $x^{2k} + \cdots + b_1x \in I$, otherwise our assertion is already proved.

$(x^{2k} + \cdots + b_1x + x)^3 + x^3 = (x^{2k} + \cdots + b_1x)^3 + (x^{2k} + \cdots + b_1x)^2x + (x^{2k} + \cdots + b_1x)x^2 \in I$. We get $x^{4k+1} + \cdots + x^{2k+2} + \cdots \in I$. For $n \geqq 1$, $4k + 1$ is greater than $2k + 2$ and so there is a polynomial of degree $4k + 1$ (an odd number) in $I$.

LEMMA 16. *Let $F$ be a finite field of characteristic 2 and $I$ a strictly maximal ideal of $F_0[x]$. Then the near-field $F_0[x]/I$ is finite.*

*Proof.* We know from Lemma 15 that there is an odd number

$t$ with $x^t + \cdots + a_1x \in I$.

We show: For all $n \geqq 6t$ there is some $x^n + \cdots + b_1x \in I$.

For all $l \geqq 1$, $(x^t + \cdots + a_1x + x^{t+l})^3 + (x^{t+l})^3 \in I$. Hence $(x^{t+l})^2(x^t + \cdots + a_1x) + (x^{t+l})(x^t + \cdots + b_1x)^2 \in I$, whence $x^{3t+2l} + \cdots + x^{3t+l} + \cdots \in I$. Since $(x^t + \cdots + a_1x)^3 = x^{3t} + \cdots \in I$, there are polynomials of following degrees in $I$: $3t$, $3t+2$, $3t+4$, $\cdots$. Since $3t$ is odd, we have: For all odd numbers $k \geqq 3t$, there is some normed polynomial of degree $k$ in $I$.

$$(x^t + \cdots + a_1x)^6 = x^{6t} + \cdots \in I\,.$$
$$(x^t + \cdots + a_1x)^2 = x^{2t} + \cdots + e_1x \in I\,.$$
$$(x^{2t+l} + x^{2t} + \cdots + e_1x)^3 + (x^{2t+l})^3 \in I\,.$$

Hence $(x^{2t+l})^2(x^{2t} + \cdots) + (x^{2t+l})(x^{2t} + \cdots)^2 \in I$, whence $x^{6t+2l} + \cdots + x^{6t+l} + \cdots \in I$. Therefore there are also polynomials of following degrees in $I$: $6t$, $6t+2$, $6t+4$, $\cdots$.

We get: For all $k \geqq 6t$ there exists some polynomial $x^k + \cdots + b_1x \in I$. Hence $|F_0[x]/I| \leqq |F|^{6t}$, which is finite.

LEMMA 17. *Let $F$ be $GF(2^n)$, $n \geqq 2$ and $I$ a strictly maximal ideal of $F_0[x]$. Then $I = ((x^2))$.*

*Proof.* Lemma 16 tells us that $K := F_0[x]/I$ is a finite near-field. By 8.34 of [3], all finite near-fields (except 7 exceptional cases of orders $5^2$, $11^2$, $7^2$, $23^2$, $11^2$, $29^2$, $59^2$) are Dikson near-fields. Our $K$ cannot be exceptional, so it is a Dickson near-field. In this case, we know from 3.3 of [6] that the center $C(K) := \{f \in K/f \circ g = g \circ f$ for all $g \in K\}$ is closed with respect to addition.

Since, by the well-known rules how to calculate in $GF(2^n)$, $x + I$ and $x^{2^n} + I$ belong to $C(K)$, so does their sum $x + x^{2^n} + I$. So we get $(x^{2^n} + x + I) \circ (x^{2^n-1} + I) = (x^{2^n-1} + I) \circ (x^{2^n} + x + I)$. $(x^{2^n-1})^{2^n} + x^{2^n-1} + I = (x^{2^n} + x)^{2^n-1} + I = (x^{2^n})^{2^n-1} + (x^{2^n})^{2^n-2} + \cdots + x^{2^n}x^{2^n-2} + x^{2^n-1} + I = x^{(2^n-1)2^n} + \sum_{k=1}^{2^n-2} x^{2^nk+(2^n-1-k)} + x^{2^n-1} + I$. Hence $\sum_{k=1}^{2^n-2} x^{2^nk+(2^n-1-k)} \in I$. But $2^nk + (2^n - 1 - k) = (2^n - 1)k + (2^n - 1) = (2^n - 1)(k + 1)$, so $\sum_{k=1}^{2^n-2} x^{(2^n-1)(k+1)} = \sum_{k=1}^{2^n-2} (x^{2^n-1})^{k+1} = (\sum_{k=1}^{2^n-2} x^{k+1}) \circ x^{2^n-1} \in I$. Since $K$ is a near-field, either $\sum_{k=1}^{2^n-2} x^{k+1} \in I$ or $x^{2^n-1} \in I$. If $x^{2^n-1} \in I$, we are through, for we get $I = ((x^2))$ by Lemma 14. So we may assume that $\sum_{k=1}^{2^n-2} x^{k+1} = x^{2^n-1} + \cdots + x^2 \in I$.

The multiplicative group of $GF(2^n)$ is cyclic. Therefore there is some $c \in GF(2^n)$ of order $2^n - 1$. We know: $c \neq 0$, $c \neq 1$. $c^{2^n-1} = 1$ and for all $l < 2^n - 1$ $c^l \neq 1$ and for all $l, j \leqq 2^n - 1$, $l \neq j$: $c^l + c^j \neq 0$. Since $c^{2^n-1}x^{2^n-1} + \cdots + cx^2 = (x^{2^n-1} + \cdots + x^2) \circ (cx) \in I$, $c^{2^n-1}x^{2^n-1} + \cdots + c^{2^n-1}x^2 = c^{2^n-1}x \circ (x^{2^n-1} + \cdots + x^2) \in I$, we get $(c^{2^n-1} + c^{2^n-2})x^{2^n-2} + \cdots$

$+ (c^{2^n-1} + c^2)x^2 \in I$. Also $(c^{2^n-1} + c^{2^n-2})c^{2^n-2}x^{2^n-2} + \cdots + (c^{2^n-1} + c^2)c^2x^2 = ((c^{2^n-1} + c^{2^n-2})x^{2^n-2} + \cdots + (c^{2^n-1} + c^2)x^2) \circ (cx) \in I$ and $(c^{2^n-1} + c^{2^n-2})c^{2^n-2}x^{2^n-2} + \cdots + (c^{2^n-1} + c^2)c^{2^n-2}x^2 = (c^{2^n-2}x) \circ ((c^{2^n-1} + c^{2^n-2})x^{2^n-2} + \cdots + (c^{2^n-1} + c^2)x^2) \in I$. Hence $(c^{2^n-1} + c^{2^n-3})(e^{2^n-2} + c^{2^n-3})x^{2^n-3} + \cdots + (c^{2^n-1} + c^2)(c^{2^n-2} + c^2)x^2 \in I$. If we continue this procedure, we finally arrive at $(c^{2^n-1} + c^2)(c^{2^n-2} + c^2) \cdots (c^3 + c^2)x^2 \in I$ where the coefficient of $x^2 \neq 0$. So $x^2 \in I$ and we get $I = ((x^2))$ again by Lemma 14.

Our last case is $R = \boldsymbol{Z}_2$. This case is rather complicated and so the way is longer. Brenner has shown in [1] that there are only two maximal ideals in $\boldsymbol{Z}_2[x]$. One of them is $T :=$ the subgroup generated by $\{1, x + x^2, x^3, x + x^4, x + x^5, x^6, x + x^7, x + x^8, x^9, \cdots\}$. The other one is $V$, the subgroup generated by $\{1, x + x^2, x + x^3, x + x^4, \cdots\}$. We define $T_0$, $V_0$ as follows: $T_0 := T \cap (\boldsymbol{Z}_2)_0[x]$ and $V_0 := V \cap (\boldsymbol{Z}_2)_0[x]$. $T_0$ and $V_0$ are easily shown to be ideals in $(\boldsymbol{Z}_2)_0[x]$. They are even strictly maximal ideals as will be demonstrated in the following. Together with $((x^2))$, there are just three strictly maximal ideals in $(\boldsymbol{Z}_2)_0[x]$.

LEMMA 18. *Let $I$ be a strictly maximal ideal in $(\boldsymbol{Z}_2)_0[x]$ with $x^2 \in I$, then $I = ((x^2))$.*

*Proof.* Since $x^2 \in I$, $x^{2k} = x^2 \circ x^k \in I$ for all $k \in \boldsymbol{N}$. Hence $(x^4 + x)^3 + x^3 \in I$, whence $x^9 \in I$. But $x^9 = x^3 \circ x^3$ so $x^3 \in I$ since $(\boldsymbol{Z}_2)_0[x]/I$ has no divisors of zero. Therefore $x^{6k} + x^{4k+3} + x^{2k+6} + x^9 = (x^{2k} + x^3)^3 \in I$, from which we get that $x^{4k+3} \in I$ for all $k \in \boldsymbol{N}$. Also, $(x^{2k} + x)^3 + x^3 \in I$ gives us $x^{4k+1} \in I$ for all $k \in \boldsymbol{N}$. All $x^4$ and $x^{4k+2} = x^2 \circ x^{2k+1}$ are also in $I$, so, putting altogether, $x^n \in I$ for $n \geqq 2$, which means $I = ((x^2))$.

LEMMA 19. *Let $I$ be a strictly maximal ideal in $(\boldsymbol{Z}_2)_0[x]$ with $x^2 \notin I$, $x^3 \in I$. Then $I = T_0$*

*Proof.* By Lemma 16 and the information in the proof of Lemma 17, we know $(\boldsymbol{Z}_2)_0[x]/I$ is a finite Dickson near-field of characteristic 2, so it has order $2^t$ (by 8.13 of [3]). Since $x^2 + I \neq 0 + I$, the order $k$ of $x^2 + I$ divides $2^t - 1$. So we have $x^{2k} + I = (x^2 + I) \circ (x^2 + I) \circ \cdots \circ (x^2 + I) = x + I$ and $k/2^t - 1$. Hence $k$ is odd, whence $3/2^k + 1$. Let $2^k + 1 =: 3j$. For all $s \in \boldsymbol{N}$, $s \geqq 3$, we get $x^3 \circ (x^s + x^{s-1}) \in I$ whence $x^{3s-1} + x^{3s-2} \in I$ and $x^3 \circ (x^s + x^{s-2}) \in I$ whence $x^{3s-2} + x^{3s-4} \in I$. Hence $x^{3s-1} \equiv x^{3s-2} \equiv x^{3s-3} \equiv x^{3s-5} \equiv \cdots \equiv x^5 \equiv x^4 \pmod{I}$. In particular, $x \equiv x^{2^k} = x^{3j-1} \equiv x^4$ and we get $x^n + x \in I$ for all $n \in \boldsymbol{N}$, $3 \nmid n$, $n \geqq 4$. Also, from $(x^2 + I) \circ (x^2 + I) = x^4 + I = x + I$ we get $x^2 + I = x + I$ by 8.10.a of [3]. Hence all the additive generators of $T_0$ are in $I$, whence $T_0 \subseteqq I$. But $T_0$ is a subgroup of $(\boldsymbol{Z}_2)_0[x]$ of order 2, hence $T_0 = I$.

LEMMA 20. *Let* $I$ *be a strictly maximal ideal of* $(\boldsymbol{Z}_2)_0[x]$ *with* $x^2 \notin I$, $x^3 \notin I$, $x^2 + x^3 \in I$. *Then* $I = V_0$.

*Proof.* Since $x^2 + x^3 \in I$, also $(x^2 + x^3) \circ (x^s + x) \in I$, whence $x^{2s+1} + x^{s+2} \in I$ and $(x^2 + x^3) \circ (x^s + x^2) \in I$, implying that $x^{2s+2} + x^{s+4} \in I$. From the first result we get $x^5 \equiv x^4$, $x^7 \equiv x^5$, $x^9 \equiv x^6 \pmod I$ and from the second we derive $x^8 \equiv x^7$, $x^{10} \equiv x^8$, $x^{12} \equiv x^9, \cdots \pmod I$, so (since also $(x^2 + x^3) \circ x^2 = x^4 + x^6 \in I$) we get $x^4 \equiv x^5 \equiv x^6 \equiv \cdots \pmod I$. Since $x^2 \notin I$, there is some $k \in \boldsymbol{N}$ with $x^{2^k} + x \in I$ (same reason as in the proof of Lemma 19). Hence $x \equiv x^{2^k} \equiv x^4 \pmod I$. Also $(x^{2^k} + x) \circ x^2 \in I$, whence $x^2 \equiv x^{2^{k+1}} \equiv x^4 \pmod I$. Since $x^2 + x^3 \in I$, we get $x^2 \equiv x^3 \pmod I$, and therefore $x \equiv x^2 \equiv x^3 \equiv x^4 \equiv \cdots \equiv x^n \equiv \cdots \pmod I$. Thus for all $n \in \boldsymbol{N}$ $x^n + x \in I$, hence $V_0 \subseteq I$. But $V_0$ is a subgroup of index 2 in $(\boldsymbol{Z}_2)_0[x]$, so $V_0 = I$.

LEMMA 21. *Let* $I$ *be a strictly maximal ideal of* $(\boldsymbol{Z}_2)_0[x]$. *Then* $I$ *is either* $= ((x^2))$ *or* $= T_0$ *or* $= V_0$.

*Proof.* Suppose $I \neq ((x^2))$, $I \neq T_0$, $I \neq V_0$. Applying Lemmas 18, 19 and 20 we have: $x^2 \notin I$, $x^3 \notin I$, $x^2 + x^3 \notin I$. As in the proof of Lemma 17, let $C(K)$ be the center of $K := (\boldsymbol{Z}_2)_0[x]/I$. Obviously $x + I \in C(K)$, $x^2 + I \in C(K)$, hence $x + I + x^2 + I = x + x^2 + I \in C(K)$. So $(x^2 + x + I) \circ (x^3 + I) = (x^3 + I) \circ (x^2 + x + I)$, hence $x^6 + x^3 + I = x^6 + x^5 + x^4 + x^3 \in I$ and $x^5 + x^4 \in I$. Also, $(x^5 + x^4) \circ (x^2 + x) = x^{10} + x^9 + x^6 + x^5 + x^8 + x^4 \in I$. Since $(x^5 + x^4) \circ x^2 = x^{10} + x^8 \in I$ and $x^5 + x^4 \in I$, we have $x^9 + x^6 \in I$. But $I = x^9 + x^6 + I = (x^3 + x^2 + I) \circ (x^3 + I)$, implying that either $x^3 + x^2 \in I$ or $x^3 \in I$, both being contradictions.

LEMMA 22. *Let* $I$ *be a strictly maximal ideal of* $(\boldsymbol{Z}_2)_0[x]$. *Then* $(\boldsymbol{Z}_2)_0[x]/I \cong \boldsymbol{Z}_2$.

*Proof.* Applying Lemma 21, we know $I$ is either $= ((x^2))$ or $= T_0$ or $= V_0$. But $[(\boldsymbol{Z}_2)_0[x]: ((x^2))] = [(\boldsymbol{Z}_2)_0[x]: T_0] = [(\boldsymbol{Z}_2)_0[x]: V_0] = 2$. So we have in all of these three cases: $(\boldsymbol{Z}_2)_0[x]/I \cong \boldsymbol{Z}_2$.

This completes the proof of Theorem 1.

As a byproduct, we have a complete knowledge of all strictly maximal ideals in polynomial near-rings:

COROLLARY. *Let* $I$ *be a strictly maximal ideal of* $R_0[x]$. *Then there exists a maximal ideal* $M$ *of* $R$ *with* $I = ((x^2)) + Mx$, *unless* $R = \boldsymbol{Z}_2$. *In this case,* $I$ *might as well be* $= T_0$ *or* $= V_0$.

In particular, for a field $R \neq \boldsymbol{Z}_2$, there is just one strictly maximal ideal, namely $((x^2))$.

G. Pilz suggested to investigate near-fields which are contained in $R[x]$. Since all near-fields with the exception of a trivial one ([3], 8.1—we exclude this one from our considerations) are zero-symmetric, we only need to search them in $R_0[x]$.

LEMMA 23. *Let $R$ be an integral domain and $F$ a near-field in $R_0[x]$. Then there is a subfield $K$ of $R$ such that $F = \{ax/a \in K\}$.*

*Proof.* Straightforward.

LEMMA 24. *Let $F$ be a near-field in $R_0[x]$, $0 \neq f = a_n x^n + \cdots + a_1 x \in F$. Then $a_2, a_3, \cdots, a_n \in \mathfrak{P}(R)$ (prim-radical of $R$) and $a_1$ is a unit in $R$.*

*Proof.* We use the following epimorphisms: $h: R \rightarrow R/M$ where $M$ is a prime ideal of $R$, $h': R_0[x] \rightarrow (R/M)_0[x]$:

$$a_n x^n + \cdots + a_1 x \longmapsto h(a_n)x^n + \cdots + h(a_1)x \ .$$

In $(R/M)_0[x]$ we can apply Lemmas 2, 3 and get: $h(a_2) = h(a_3) = \cdots = h(a_n) = 0$. So we have $a_2, \cdots, a_n \in \mathfrak{P}(R)$.

Since $f \neq 0$, $a_1$ cannot be $= 0$, otherwise $f$ has no inverse in $F$.

Suppose $a_1$ were not a unit, so $a_1$ is in a maximal ideal $M_1$ of $R$. Let $h: R \rightarrow R/M_1$ and $h': R_0[x] \rightarrow (R/M_1)_0[x]$ be as above and we get $h'(a_n x^n + \cdots + a_1 x) = h(a_1)x = 0$, a contradiction to the fact that $h'(F) = \{ax/a \in K\}$ for some subfield $K$ of $h(R)$.

THEOREM 2. *Let $F$ be a near-field contained in $R_0[x]$, $F_1 := \{a_1/\text{some } a_n x^n + \cdots + a_1 x \in F\}$. Then $F \cong F_1 x$.*

*Proof.* Define $h: F \rightarrow F_1 x$.

$$a_n x^n + \cdots + a_1 x \longmapsto a_1 x$$

$h$ is surjective. We show it is injective, too. Let $f_1, f_2 \in F$ with $f_1 = a_n x^n + \cdots + a_1 x$ and $f_2 = b_m x^m + \cdots + a_1 x$. Then $f_1 - f_2 = \cdots + (a_2 - b_2)x^2 + 0x \in F$. But then $f_1 - f_2 = 0$ by Lemma 24. Hence $f_1 = f_2$ and $h$ is $1 - 1$.

It is easy to show that $h$ *is* a near-ring homomorphism, so $h$ is a near-ring isomorphism.

EXAMPLES. Take $R := \boldsymbol{Z}_2[t]/(t^4 + t^2 + 1)$. Then $K_1 := \{0, x\}$, $K_2 := \{0, x, t^2x, (t^2 + 1)x\}$ and $K_3 := \{0, x, (t^2 + t + 1)x^2 + t^2x, (t^2 + t + 1)x^2 +$

$(t^2+1)x\}$ are examples of subnear-fields of $R_0[x]$. Note that $K_3$ contains non-liear polynomials.

*Application.* Let $P$ be a planar near-ring with identity which is either contained in some $R_0[x]$ or a factor of $R_0[x]$. Then $P$ is a field and isomorphic to a subfield or a factorfield of $R$. This holds because a planar near-ring with identity is accurately a near-field, as can be easily seen.

## REFERENCES

1. J. L. Brenner, *Maximal ideals in the near-ring of polynomials mod* 2, Pacific J. Math., **52** (1974), 595–600.
2. J. R. Clay and D. K. Doi, *Maximal ideals in the near-ring of polynomials over a field.* In Colloqu. Math. Soc. Janus Bolyai 6, Rings, Modules and Radicals (ed. by A. Kertesz), pp. 117–133. Amsterdam, North Holland, 1973.
3. G. Pilz, *Near-rings*, Amsterdam, North Holland, 1977.
4. Y. S. So, *Polynom Fast-ring*, Dissertation, Univ. Linz, 1978.
5. E. G. Straus, *Remarks on the paper "Ideals in near-rings of polynomials over a field"*, Pacific J. Math., **52** (1974), 601–603.
6. H. Wähling, *Bericht über Fastkörper*, Jahresbericht Dt. Math. Ver., **76** (1975), 41–103.

Received December 15, 1979. I would like to thank Günter Pilz for his unselfish help and encouragement and to "Österreichischen Forschungsfonds" for the financial assistance (Project number 3479).

INSTITUTE FÜR MATHEMATIK
JOHANNES-KEPLER UNIVERSITÄT
A-4045 LINZ-AUHOF, AUSTRIA.

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

# Pacific Journal of Mathematics

Vol. 96, No. 1 November, 1981