PACIFIC JOURNAL OF MATHEMATICS
Vol. 118, No. 2, 1985

COMPOSITION ALGEBRAS OF POLYNOMIALS

J. L. BRENNER

Dedicated to the memory of Ernst G. Straus

Briefly, a composition algebra A involves two operations: addition and composition (substitution of polynomials). Let C be an arbitrary commutative ring, and $C[x, y, \ldots]$ the ring of polynomials in the indeterminates $x, y, \ldots$ with coefficients from C. Addition of polynomials is commutative; composition is associative, and is distributive (on one side) over addition. (Notice that if the number of indeterminates is greater than 1, the operation of composition is not a binary operation.) We find the ideal structure of A in some special cases. In particular, the ideals of A are all principal (generated by a single element) if C is a principal ideal ring (e.g. Z) and the number of variables is 1: $A = (C[x], +, \circ)$, provided further that for all $c \in C$, $2|c + c^2$. [An example is the algebraic integers in $Q(\sqrt{-7})$.]

We start in a general context. An ideal J in A is the kernel of a homomorphism. Thus J enjoys these three properties:

1.01. J is a module over C: If $c_1, c_2 \in C$, $t_1, t_2 \in J$, then $c_1t_1 + c_2t_2 \in J$.

1.02. If $t \in J$ and $n_1, n_2, \ldots \in A$, then $t(x, y, \ldots) \circ [n_1, n_2, \ldots] \equiv t(n_1, n_2, \ldots)$ lies in J.

1.03. If $t_2, t_3, \ldots \in J$ and if $n_1, n_2, \ldots \in A$, then $n_1(x, y, \ldots) \circ [n_2 + t_2, n_3 + t_3, \ldots] - (n_1(x, y, \ldots) \circ [n_2, n_3, \ldots])$ lies in J.

Since n_1 is a sum of monomials, it follows from 1.01 that 1.03 can be replaced by the simpler requirement

1.04. $$\textstyle\prod_{i=2}^{k}(n_i + t_i)^{\alpha_i} - \prod_{i=2}^{k} n_i^{\alpha_i} \quad \text{lies in } J.$$

1.05. DEFINITION. An ideal $J = \langle a \rangle$ in A is *principal* if J is the smallest ideal containing a. A is a *principal ideal composition algebra* (in short, A is principal) if every ideal is principal.

Even if C is a principal ideal ring (say $C = \mathbf{Z}$) it can be seen that A is not necessarily principal, so the property of being principal is not inherited. Recall the same situation in ordinary ring theory: $\mathbf{Z}[x, y]$ is not a principal ideal ring.

When the number of indeterminates is 1, the situation is more tractable.

2. Ideals in the composition algebra $A = (\mathbf{Z}[x], +, \circ)$. In this section, all ideals in A are described, in case the number of variables is 1, and in case $C = \mathbf{Z}$. "Described" means that the additive basis for J is given, J being taken as a module over C. It turns out that A is principal in this case. At bottom, the proof depends on a result in **[1]**. The present paper, by its dedication, recalls the contribution of E. G. Straus as referee of **[1]**.

Note that if the number of variables is 1, A is a near ring. The characterization of an ideal J in A specializes as follows.

2.01. If $t_1, t_2 \in J$ then $t_1 + t_2 \in J$.

2.02. If $t_1 \in J$ and $n \in A$, then $t_1 \circ n \in J$.

2.03. If $\alpha \geq 1$, $t \in J$, $n \in A$, then

$$(n + t)^{\alpha} - n^{\alpha} \text{ lies in } J.$$

2.04. LEMMA. *If t lies in the ideal J, $\alpha \geq 1$, then t^{α} lies in J.*

Proof. Take $n = 0$ in 2.03.

2.05. COROLLARY $(n + t)^{\alpha} - n^{\alpha} - t^{\alpha}$ *lies in J.*

2.06. LEMMA. *If n_1 is any polynomial, and if t lies in the ideal J, then $n_1(t) - n_1(0)$ lies in J.*

Proof. If $n_1(x) = \Sigma_0^k a_{\alpha} x^{\alpha}$, then $n_1(t) - n_1(0) = \Sigma_1^k a_{\alpha} t^{\alpha}$. Use 2.04.

The next series of lemmas is directed to finding the smallest ideal $J(1)$ that contains 1.

2.07. LEMMA. *$J(1)$ contains $2x^{\nu}$ for $\nu = 1, 2, \ldots$.*

Proof. Use 2.05 with $n = x^{\nu}$, $t = 1$, $\alpha = 2$: $(x^{\nu} + 1)^2 - (x^{\nu})^2 - 1 = 2x^{\nu}$.

2.08. LEMMA. *$J(1)$ contains $x^2 + x$.*

Proof. Use 2.05 with $\alpha = 3$, $t = 1$, $n = x$, together with 2.07.

2.09. LEMMA. *Modulo $J(1)$, $x^\nu \equiv x^{2\nu} \equiv x^{4\nu} \equiv \cdots \equiv x^{2^s\nu}$, $s = 1, 2, \ldots$; $\nu = 1, 2, \ldots$.*

Proof. $(x + x^2) \circ x^\nu = x^\nu + x^{2\nu}$.

2.10. COROLLARY. *$J(1)$ contains $x + x^4$, $x + x^8$, $x^2 + x^8$, $x^{20} + x^5$, $x^3 + x^6$, $x^{19} + x^{38}$.*

2.11. LEMMA. *$J(1)$ contains $x^5 + x$, $x^{35} + x^7$, $x^{25} + x^5$, $x^{25} + x$.*

Proof. $(x + x^2)^3 \equiv x^3 + x^4 + x^5 + x^6 \equiv x + x^5$.

2.12. LEMMA. *$J(1)$ contains $x + x^{17}$.*

Proof. $(x + x^4)^5 - (x + x^4) \circ x^5 \equiv x^8 + x^{17}$.

2.13. LEMMA. *$J(1)$ contains $x + x^{19}$.*

Proof. $(x^4 + x^{17})^3 - (x^4 + x^{17}) \circ x^3 \equiv x^{25} + x^{38}$. Use 2.11.

2.14. LEMMA. *$J(1)$ contains $x^7 + x^{19}$.*

Proof. $(x + x^{17})^3 - (x + x^{17}) \circ x^3 \equiv x^{19} + x^{35}$.

2.15. LEMMA. *$J(1)$ contains $x + x^7$.*

Proof. Combine 2.13, 2.14.

2.16. THEOREM. *For $\nu = 1, 2, \ldots$, $J(1)$ contains $x^{3\nu+1} + x$, $x^{3\nu-1} + x$.*

Proof by induction. For $\nu = 1, 2$ Theorem 2.16 is already proved. Suppose $\mu \geq 3$. Then

$$\left(x^4 + x^{3\mu-4}\right)^3 - \left(x^4 + x^{3\mu-4}\right) \circ x^3 \equiv x^{3\mu+4} + x^{6\mu-4}.$$

By induction hypothesis, $x + x^{3\mu-2}$ lies in $J(1)$, so also does $(x + x^{3\mu-2}) \circ x^2 = x^2 + x^{6\mu-4}$. Hence $x^{3\mu+4} + x^2$ lies in $J(1)$. Similarly,

$$\left(x^2 + x^{3\mu-2}\right)^3 - \left(x^2 + x^{3\mu-2}\right) \circ x^3 \equiv x^{3\mu+2} + x^{6\mu-2} \quad \text{lies in } J(1);$$

and

$$x^{3\mu+2} + x^{6\mu-2} - (x + x^{3\mu-1}) \circ x^2 \equiv x^{3\mu+2} + x^2.$$

The inductive step from $x^{3\mu\pm1} + x$ to $x^{3\mu+6\pm1} + x^2$ has been completed.□

2.17. THEOREM. *$J(1)$ contains $x^{3\nu} + x^3$ for $\nu = 1, 2 \ldots$.*

Proof. $x^3 + x^6 = (x + x^2) \circ x^3$; $x^3 + x^9 \equiv (x + x^4)^3 - (x + x^2) \circ x^6$. If 3ν is a power of 3, then $x^{3\nu} + x^9 = (x^\nu + x^3) \circ x^3$. This gives an inductive proof, since $x^{3\nu} + x^3 \equiv x^{3\nu} + x^9 + (x^9 + x^3)$.

Suppose 3ν is not a power of 3, say $3\nu = \mu\rho$ with μ a power of 3 ($\mu \geq 3$) and ρ prime to 3, $\rho > 1$. Then $x^{\mu\rho} + x^3 \equiv x^{\mu\rho} + x^\mu = (x^\rho + x) \circ x^\mu$. □

2.18. THEOREM. *The module $J(1)$ with basis*

$$\langle 1, 2x^\nu, x^{3\nu+1} + x, x^{3\nu-1} + x, x^{3\nu} + x^3 | \nu = 1, 2, \ldots \rangle$$

is an ideal in $(\mathbf{Z}[x], +, \circ)$.

Proof. Under the natural mapping $\mathbf{Z}[x] \to \mathbf{Z}_2[x]$, the module $J(1)$ is mapped into the ideal J of [1]. Thus $J(1)$ is the full inverse image of an ideal, so $J(1)$ is an ideal. (A second proof is given in §4.)

2.19. REMARK. 2.18 can be used to derive certain properties of binomial and multinomial coefficients.

2.20. REMARK. It turns out that $J(1)$ is multiplicatively closed.

2.21. THEOREM. *Each of the modules*

$$V(1) = \langle 1, 2x^\nu, x^\nu + x | \nu = 1, 2, \ldots \rangle,$$

$$T(1) = \langle 1, 2x^\nu, x^{3\nu+1} + x, x^{3\nu-1} + x, x^{3\nu} | \nu = 1, 2, \ldots \rangle$$

is an ideal.

See [**1**].

The proofs of 2.22–2.25 are left to the reader.

2.22. THEOREM. *If c is any integer, $cJ(1)$, $cT(1)$, $cV(1)$ are ideals. $cJ(1) = J(c)$ is the smallest ideal that contains c. If c, d are constants, $c|d$, then $J(d) \subset J(c)$, $dV(1) = V(d) \subset V(c)$, $dT(1) = T(d) \subset T(c)$ (just as, in ring theory, $(d) \subset (c)$).*

2.23. THEOREM. $c\mathbf{Z}[x]$, $T(c)$, $V(c)$, $J(c)$ *are the only ideals in* $(\mathbf{Z}[x], +, \circ)$, *with inclusion relations given in* 2.22, *and in the diagram*

$$\begin{tikzcd} & c\mathbf{Z}[x] \arrow[dl, dash] \arrow[dr, dash] & \\ T(c) \arrow[dr, dash] & & V(c) \arrow[dl, dash] \\ & J(c) & \end{tikzcd}$$

2.24. THEOREM. *Every ideal J in A is closed under multiplication, that is, if $t_1, t_2 \in J$ then $t_1t_2 \in J$.*

2.25. THEOREM. $(\mathbf{Z}[x], +, \circ)$ *is a principal-ideal composition algebra, that is, a principal ideal near ring.*

3. Ideals in the composition algebra $A_m = (\mathbf{Z}_m[x], +, \circ)$ when m is odd. If m is an odd prime, the ideals in A_m were given in [**2**]. If m is odd and composite, the results are similar but not identical. The proof of Lemma 3.01 appears in [**2**].

3.01. LEMMA. *Every (near-ring) ideal in A_m is a ring ideal in the polynomial ring $\mathbf{Z}_m[x]$.*

Proof. Let J be an ideal in A_m, $f \in J$. It has to be proved that if $g \in A_m$, then $fg \in J$. First, $(f+g)^2 - g^2 - f^2 = 2fg \in J$, because of 2.03, 2.04. Next, 2 is invertible, and by 2.06, $(\frac{1}{2}x)\circ(2fg) - \frac{1}{2}0 \equiv fg$ lies in J. □

If the ideal J contains a nonzero constant c, §2 describes J. If the ideal J contains a polynomial that is not 0 at every place in $\mathbf{Z}_m$, then J contains a nonzero constant, by 2.02. Hence the only interesting ideals in A_m consist of polynomials that take only the value 0; because of 3.01, each such ideal has a single "basis." Note that the (single polynomial) basis is the generator of a module with coefficients from $\mathbf{Z}_m[x]$ (not from $\mathbf{Z}_m$ as in §2).

We first examine the case $m = p^r$, p an odd prime, $r \geq 1$. If the ideal J contains a (nonzero) constant c, then J contains $c\mathbf{Z}_m[x]$. Otherwise, every polynomial in J is 0 at every place in $\mathbf{Z}_m$. Every such polynomial is a multiple of a distinguished one, $f_{p,r}(x)$, of lowest degree:

$$f_{p,r}(x) = x^r\left(x^{\phi(p^r)} - 1\right).$$

This assertion follows from the fact that if two polynomials vanish at a place, so also does their gcd. We have to consider the ring ideals $(n_1(x)f_{p,r}(x))$.

3.02. LEMMA. *If $n_1(x)$ is an arbitrary polynomial in $\mathbf{Z}_m[x]$, then the ring ideal $(n_1(x)f_{p,r}(x))$ is an ideal in the composition algebra A_m.*

Proof. The properties to check are 2.01, 2.02, 2.03. 2.01 is obviously satisfied. As for 2.02, note that

$$\begin{aligned}\left(n_1(x)f_{p,r}(x)\right)\circ n(x) &= n_1(n(x))f_{p,r}(n(x))\\ &= n_1(n(x))n(x)^r\left(n(x)^{\phi(p^r)}-1\right).\end{aligned}$$

It can be checked that the last factor is a multiple of $x^{\phi(p^r)} - 1$, so that 2.02 is satisfied. This leaves 2.03. Here, the binomial theorem shows that

$$\left(n(x)+n_1(x)f_{p,r}(x)\right)^{\alpha} - n(x)^{\alpha}$$

is a multiple of $n_1(x)f_{p,r}(x)$, and Lemma 3.02 is verified. □

If m is odd but not a prime power, criteria 2.01–2.03 must be adjusted. 2.01 must be changed to read

3.021. If $c_1, c_2 \in \mathbf{Z}_m$ and $t_1, t_2 \in J$, then $c_1t_1 + c_2t_2 \in J$. The conditions 3.021, 2.02, 2.03 characterize ideals in A_m.

If m is odd, there are ideals in A_m that contain nonzero constants. Such an ideal can be a homomorphic image of $J(c)$, or can be the union of such images (since $\mathbf{Z}_m$ is not necessarily a principal ideal ring).

The interesting ideals in A_m are a little more complicated to describe when m is divisible by several primes. The difficulty lies just in finding the polynomials of lowest degree that are zero at every place in $\mathbf{Z}_m$. Suppose

$$m = p_1^{\alpha(1)} \cdots p_k^{\alpha(k)}.$$

Then a polynomial f of lowest degree that is zero at every place in $\mathbf{Z}_m$ is

$$f_m(x) = \mathrm{LCM}\left[f_{p_1,\alpha(1)}(x),\ldots,f_{p_k,\alpha(k)}(x)\right].$$

The rest of the theory is unaltered.

If m is even, it is not true that every ideal in the composition algebra A_m is a ring ideal in $\mathbf{Z}_m[x]$. See **[2]**, where the case $m = 2$ (among others) is fully discussed.

3.03. *Problem*. Describe the ideals in A_m if m is even.

4. Ideals in the composition algebra $A = (C[x], +, \circ)$ if C is a principal ideal ring. Even if C is a principal ideal ring, the ideals in $A = (C[x], +, \circ)$ can be hard to describe. The task is much simplified in the presence of the additional condition 4.01.

4.01. *Condition.* If $c \in C$, then $c + c^2$ is a multiple of 2.

Note that this condition is trivially satisfied if 2 is invertible; but there are many rings in which 4.01 is satisfied, but 2 is not invertible. For instance, let C be the ring of algebraic integers in $Q(\sqrt{m})$, m squarefree. If m is odd, the ring C is the set

$$\left\{ \tfrac{1}{2}(a + b\sqrt{m}) | a, b \text{ of the same parity} \right\}.$$

The condition $2 | c + c^2$ requires that m satisfy the further condition $m \equiv 1 \bmod 4$.

In the lemmas and theorems of this section, 4.01 is assumed to hold. We try to characterize the smallest ideal $J(c)$ that contains c.

4.02. LEMMA. *If an ideal J in A contains f, and if $c \in C$, then J contains cf.*

Proof. $(cx) \circ f - (cx) \circ 0 = cf$. See 3.01.

4.03. LEMMA. *If the ideal $J(c)$ in A contains the constant c, then $J(c)$ contains $2cx^\nu$, $\nu = 1, 2, \ldots$.*

Proof. $(x^\nu + c)^2 - x^{2\nu} - c^2 = 2cx^\nu$.

4.04. LEMMA. *$J(c)$ contains $cx^2 + c^2x$.*

Proof. $(x + c)^3 - x^3 - c^3 \equiv cx^2 + c^2x$.

4.05. COROLLARY. *$J(c)$ contains $c(x^2 + x)$.*

Proof. $c(x^2 + x) \equiv cx^2 + c^2x + (c + c^2)x$.

4.06. REMARK. $J(c)$ contains $(c^\mu + c^\nu)x^\sigma$, $\mu \geq \nu \geq 1$, $\sigma \geq 1$.

4.07. THEOREM. *$J(c)$ contains $cJ(1)$.*

The proof is parallel to the proof of the corresponding result in §2.

It is not obvious that $J(1)$ is an ideal in the present context; this has to be proved. A direct argument follows, based on several lemmas.

4.08. LEMMA. *$J(1)$ is multiplicatively closed. Moreover,*

$$x^3 \circ \left\langle x^{3\nu+1} + x, x^{3\nu-1} + x, x^{3\nu} + x^3 \right\rangle \subset J(1).$$

4.09. REMARK. None of $V(1)$, $T(1)$, $J(1)$ is an ordinary ring ideal.

4.10. LEMMA. *If $n(x)$ is any polynomial, then each of $x^{3\nu+1}+x$, $x^{3\nu-1}+x$, $x^{3\nu}+x^3$ admits multiplication by $(n(x))^3$.*

Proof. Take $n(x)=\sum_0^k a_i x^i$. Then $(n(x))^2 \equiv \sum_0^k a_i^2 x^{2i} \bmod 2$, that is, the two sides of the congruence differ by twice some polynomial. Hence

$$(n(x))^3 \equiv \left(\sum_0^k a_i x^{2i}\right)\left(\sum_0^k a_j x^j\right) \quad \bmod 2,$$

since by hypothesis, $2|a_i + a_i^2$. The product can be computed. Some of the terms are $a_i^2 x^{3i}$ $(0 \le i \le k)$; see second assertion of Lemma 4.08. The remaining terms in the product occur in pairs: $a_i a_j (x^{2i+j} + x^{2j+i})$. The two exponents are either both prime to 3 or both divisible by 3, since their sum is $(2i+j)+(2j+i)=3(i+j)$. The lemma is proved. □

4.11. LEMMA. *If n is an arbitrary polynomial, then $(x^2+x)\circ n(x) = (n(x))^2 + n(x)$ lies in $J(1)$ and its constant term is divisible by 2.*

Proof. Take $n(x)=\sum_0^k a_i x^i$. Then

$$(n(x))^2 + n(x) \equiv \sum_0^k \left(a_i x^{2i} + a_i^2 x^i\right) \equiv \sum_0^k a_i (x^{2i} + x^i). \qquad \square$$

4.12. LEMMA. *$(x^4+x^2)\circ n(x)$ lies in $J(1)$.*

Proof. $(x^4+x^2)\circ n(x) = (x^2+x)\circ x^2 \circ n(x)$.

4.13. LEMMA. *$(x^5+x^4)\circ n(x)$ lies in $J(1)$.*

Proof. $(n(x))^5 + (n(x))^4 = (n(x))^3[(n(x))^2 + n(x)]$. According to 4.11, the [ ] lies in $J(1)$ and has zero constant term. Apply 4.10.

4.14. COROLLARY. *$(x^5+x)\circ n(x)$ lies in $J(1)$.*

Proof. $x^5+x=(x^5+x^4)+(x^4+x^2)+(x^2+x)$. Apply 4.11, 4.12, 4.13.

The last four lemmas can be generalized.

4.15. LEMMA. *if m is composite and not divisible by 3, then $(x^m+x)\circ n(x)$ lies in $J(1)$.*

Proof. Set $m = uv$, $1 < u \leq v < m$. Then

$$\begin{aligned}(x^m + x) \circ n(x) &\equiv (x^{uv} + x^u + x^u + x) \circ n(x)\\ &= (x^{uv} + x^u) \circ n(x) + (x^u + x) \circ n(x)\\ &= (x^v + x) \circ x^u \circ n(x) + (x^u + x) \circ n(x).\end{aligned}$$

The terms lie separately in $J(1)$ by an obvious induction hypothesis, based on 4.16.

4.16. LEMMA. *$(x^{3\nu+1} + x) \circ n(x)$, $(x^{3\nu+2} + x) \circ n(x)$ lie in $J(1)$.*

Proof.

$$(x^{3\nu+1} + x^4) \circ n(x) = (n(x))^3\left((n(x))^{3\nu-2} + n(x)\right);$$

$$(x^{3\nu+2} + x^4) \circ n(x) = (n(x))^3\left(n(x)^{3\nu-1} + n(x)\right).$$

Apply a suitable induction hypothesis, together with 4.10. □

4.17. LEMMA. *$(x^6 + x^3) \circ n(x)$ lies in $J(1)$.*

Proof. $(x^6 + x^3) \circ n(x) = (x^2 + x) \circ x^3 \circ n(x)$.. Apply 4.11.

4.18. LEMMA. *$(x^9 + x^6) \circ n(x)$ lies in $J(1)$.*

Proof. $(x^9 + x^6) \circ n(x) = (n(x))^3[n(x)^6 + n(x)^3]$. Apply 4.17, 4.10.

4.19. LEMMA. *If $\nu > 3$, $(x^{3\nu} + x^6) \circ n(x)$ lies in $J(1)$.*

Proof.

$$(x^{3\nu} + x^6) \circ n(x) = (n(x))^3\left[(n(x))^{3(\nu-1)} + (n(x))^3\right].$$

Apply 4.10 together with a suitable induction hypothesis.

Lemmas 4.11–4.19 show that $J(1)$ satisfies conditions 2.01–2.02. Now we turn to condition 2.03.

4.20. LEMMA. *The cosets of $J(1)$ in A are represented by $1, x, x^3, 1 + x, 1 + x^3, x + x^3, 1 + x + x^3$.*

4.21. LEMMA. *For $\alpha = 1, 2, 3$, if $n(x)$ is any polynomial and if $t \in J(1)$, then $(n + t)^\alpha - n^\alpha - t^\alpha$ is in $J(1)$.*

Proof. For $\alpha = 1, 2$ this is obvious. For $\alpha = 3$, note that mod 2, $(n+t)^3 \equiv n^3 + n^2t + nt^2 + t^3$, so that $(n+t)^3 - n^3 - t^3 \equiv n^2t + nt^2$. Since $(n_1 + n_2)^2 \equiv n_1^2 + n_2^2 \bmod 2$, and since $(t_1 + t_2)^2 = t_1^2 + t_2^2 \bmod 2$, the form $n^2t + nt^2$ is additive:

$$\begin{aligned}
&(n_1 + n_2)^2(t_1 + t_2) + (n_1 + n_2)(t_1 + t_2)^2 \\
&\quad \equiv n_1^2t_1 + n_1t_1^2 + n_2^2t_2 + n_2t_2^2 + n_1^2t_2 + n_2^2t_1 + n_1 + n_1t_2^2 + n_2t_1^2 \\
&\quad \equiv \left(n_1^2t_1 + n_1t_1^2\right) + \left(n_2^2t_2 + n_2t_2^2\right) + \left(n_1^2t_2 + n_1t_2^2\right) + \left(n_2^2t_1 + n_2t_1^2\right).
\end{aligned}$$

Thus the lemma has to be checked only for the atoms. □

4.22. LEMMA. *For $\alpha \geq 4$, if $n(x)$ is any polynomial and if $t \in J(1)$, then $(n+t)^\alpha - n^\alpha - t^\alpha \in J(1)$.*

Proof. The inductive argument proceeds in steps of 3. Modulo 2, note that $(n+t)^3 \equiv n^3 + n^2t + nt^2 + t^3$. Thus, mod 2,

$$(4.23) \quad (n+t)^\alpha - n^\alpha - t^\alpha \equiv (n^3 + n^2t + nt^2 + t^3)(n^{\alpha-3} + t^{\alpha-3} + s), \quad s \in J(1).$$

This uses the inductive hypothesis that $(n+t)^{\alpha-3} - n^{\alpha-3} - t^{\alpha-3}$ is a polynomial s in $J(1)$. There are three cases: $\alpha = 0, 1, -1 \bmod 3$.

If $\alpha \equiv 0 \bmod 3$, then also $\alpha - 3 \equiv 0 \bmod 3$. Complete the proof by referring to 4.10, 4.21.

If $\alpha \equiv 1 \bmod 3$, we assume wolg that the constant term in t is 0. The terms in the expansion of (4.23) that are not taken care of by 4.10 are

$$(n^2t + nt^2)s + t^3s + (n^2t + nt^2)t^{\alpha-3} + n^{\alpha-4}(n^3t + n^2t^2 + nt^3).$$

Of these four terms, the first three are in $J(1)$ by 4.21, 4.08. It remains to prove that $n^3t + n^2t^2 + nt^3$ is in $J(1)$. As to n^3t, see 4.10. Write $n^2t^2 + nt^3 = (n^2t + nt^2)t$ to complete the proof.

If $\alpha \equiv -1 \bmod 3$, again assume wolg that the constant term in t is 0. The terms in the expansion of (4.23) that require argument are $n^{\alpha-5}(n^4t + n^3t^2 + n^2t^3)$. It has to be proved that $n^4t + n^2t^3$ is in $J(1)$. By 4.21, $n^4t \equiv n^2t^2 \bmod J(1)$, and both n^2t^2, n^2t^3 have zero constant term. So it has to be proved that $n^2(t^2 + t^3) \in J(1)$. This last assertion follows from Lemma 4.24, with the application cited afterwards.

4.24. LEMMA. *If $t(x)$ is in $J(1)$ [and if $t(0) = 0$] then $p(x) = t + t^2$ is a polynomial in x with $p(0) = 0$ and such that the number of terms with exponent $\equiv 0 \bmod 3$ is even; the number of terms with exponent $\equiv 1 \bmod 3$ is even; the number of terms with exponent $\equiv -1 \bmod 3$ is even.*

Proof. $t_1 + t_2 + (t_1 + t_2)^2 \equiv (t_1 + t_1^2) + (t_2 + t_2^2) \mod 2$. Also the assertion of the lemma is valid for each atom (each generator) in $J(1)$. $\square$

Application of the lemma. If $p(x)$ has the properties stated, then so also does $m(x)p(x)$, where $m(x)$ is any polynomial, provided $p(0) = 0$. Set $m(x) = n^2 t$. $\square$

4.25. THEOREM. *if C is a principal ideal ring such that for every $c \in C$, $c + c^2$ is a multiple of 2, then the only ideals in the (near ring or) composition algebra $(C[x], +, \circ)$ are $cC[x]$, $cT(1)$, $cV(1)$, $cJ(1)$, with $J(1)$, $V(1)$, $T(1)$ defined as in 2.18, 2.21. The set of inclusion relations is the obvious set, together with those in the diagram below.*

$$\begin{tikzcd}[column sep=small] & cC[x] \arrow[dl, dash] \arrow[dr, dash] & \\ cT(1) \arrow[dr, dash] & & cV(1) \arrow[dl, dash] \\ & cJ(1) & \end{tikzcd}$$

The near-ring (composition algebra) ideals are all principal in this case.

4.26. COROLLARY. *Theorem 4.25 holds if C is the ring of algebraic integers in $Q(\sqrt{-\Delta})$, where $-\Delta$ is any one of -3, -7, -11, -19, -43, -67, -163.*

4.27. REMARK. If the hypotheses of 4.08 do not hold, then the smallest ideal $J(c)$ containing c contains also

$$\begin{aligned}\Big\langle c, 2cx^\nu, (c^3 + c^4)x^\nu, (c^2 + c^3)x^{2\nu}, c^3(x^{3\nu+1} + x),\\ c^3(x^{3\nu-1} + x), c^3(x^{3\nu} + x^3), c^2(x^{6\nu+3} + x^3),\\ c^2(x^{6\nu+5} + x^5), c^2(x^{6\nu+7} + x^7),\\ (c^2 + c^3)\,(x^{2\nu+3} + x^3) \big| \nu = 1, 2, \ldots \Big\rangle\end{aligned}$$

However, the module with these generators need not be an ideal. (The assertion in 4.27 has a lengthy proof.)

4.28. *Problem.* Characterize the ideal $J(c)$ in a simple manner.

4.29. *Problem.* If C is the ring of Gaussian integers, is $J(1)$ the module (over C)

$$\Big\langle 1, 2x^\nu, (1 + i)x^\nu, x^{3\nu+1} + x, x^{3\nu-1} + x, x^{3\nu} + x^3 \big| \nu = 1, 2, \ldots \Big\rangle?$$

What are the other ideals in $(C[x], +, \circ)$?

5. Properties of the binomial coefficients. The first two properties are easy.

5.01. LEMMA. *C_k^{2k} is even.*

5.02. LEMMA. *If two of the lower suffixes of a multinomial coefficient are equal and positive, the coefficient is even.*

More generally if there are r pairs of positive and equal suffixes, $C^n_{i,j,k,l\cdots}$ is divisible by 2^r. [$C^4_{1,1,1,1}$, $C^8_{2,2,2,2}$, $C^{12}_{1,1,5,5} = 2^4 3^3 \cdot 7 \cdot 11$ *are all divisible by* 4.]

The next lemmas all follow from 2.03. A direct proof of 5.03 is immediate; without using 2.03, the others seem less obvious.

5.03. LEMMA. *Among the $n + 1$ binomial coefficients C_k^n, an even number are odd.*

5.04. LEMMA. *Among those binomial coefficients $C^n_{3\nu}$ with ν an integer and with $0 < 3\nu < n$, an even number are odd.*

(5.04 is immediate if n is a multiple of 3; 5.04 is true without this restriction.) R. J. Evans showed me a direct proof of 5.04.

5.05. LEMMA. *Let S be the collection of those multinomial coefficients C^n_{ijklm} that are odd, and in which $0 < i < n$, subject to the further restriction $j + m \equiv k \bmod 3$. Then S has odd cardinality.*

5.06. LEMMA. *The cardinality of the set*

$$\left\{ C^n_{i_0,i_1,\ldots,i_r} \middle| 0 < i_0 < n,\ i_1 + 2i_2 + \cdots + ri_r \equiv 0 \bmod 3,\quad C^n_{i_0,i_1,\ldots,i_r} \text{ is odd} \right\}$$

is even.

5.07. THEOREM. *The assertion of the preceding number remains true if the congruence $\sum j \cdot i_j \equiv 0 \bmod 3$ is replaced by the congruence $\sum a(j) i_j \equiv 0 \bmod 3$, where $a(j)$ are arbitrary integers.*

This conclusion is obtained by noting that the polynomial $(1 + \sum_{j>0} x^{a(j)})^n - 1^n - (\sum x^{a(j)})^n$ must lie in $J(1)$.

Acknowledgment. Professor Denis Floyd made valuable critical suggestions.

References

[1] J. L. Brenner, *Maximal ideals in the near ring of polynomials module* 2, Pacific J. Math., **52** (1974), 595–600.

[2] E. G. Straus, *Remark on the preceding paper, ideals in near rings of polynomials over a field*, Pacific J. Math., **52** (1974), 601–603.

Received July 19, 1984

10 Phillips Rd.
Palo Alto, CA 94303