DEMONSTRATIO MATHEMATICA
Vol. XXII No 1 1989

Czesław Sitarczyk

IDEMPOTENT POLYNOMIALS OVER RINGS

0. Let $\mathfrak{A} = (A,F)$ be an algebra. A polynomial $f(x_1,\ldots,x_n)$ over $\mathfrak{A}$ is said to be idempotent if $f(x,\ldots,x) = x$ for all $x \in A$. By the idempotent reduct $\mathfrak{J}(\mathfrak{A})$ we mean the algebra $(A,\mathfrak{Jl}(F))$ where $\mathfrak{Jl}(F)$ is the set of all idempotent polynomials over $\mathfrak{A}$.

In this paper we first prove the following: there are two idempotent ternary ring polynomials such that each idempotent polynomial over a commutative ring is a composition of them (see Theorem 1). This result is an answer for the first problem stated in [2] by J. Dudek and J. Płonka, in the case of commutative rings. Moreover, in general this cannot be done by means of binary polynomials. We give also a partial answer for the second problem of [2] (see Theorem 2).

Problems of this kind were studied by many authors, e.g. D. Webb [8], J. Słupecki [6], W. Sierpiński [5], R. Quackenbush [4], A. Szendrei [7].

1. By a ring $P = (P,+,-,\cdot)$ we shall always mean a commutative (associative) ring. The following statement is obvious: every n-ary polynomial $g(x_1,\ldots,x_n)$ over P can be written (not uniquely) in the form

(1) $$g(x_1,\ldots,x_n) = g_1(x_1,\ldots,x_n) + g_2(x_1,\ldots,x_n)$$

where

$$g_1(x_1,\ldots,x_n) = \sum_{1\leq i\leq n} d_i x_i$$

and

$$g_2(x_1,\dots,x_n) = \sum_{1\leq i_1,i_2\leq n} d_{i_1i_2}x_{i_1}x_{i_2} + \dots$$

$$+ \sum_{1\leq i_1,\dots,i_k\leq n} d_{i_1\dots i_k}x_{i_1}\dots x_{i_k}$$

where $d_i, d_{i_1}, \dots, d_{i_1 \dots i_k}$ are integers, for $i, i_1, \dots, i_k \in \{1,\dots,n\}$. Let us add that by dx we mean $dx = \underbrace{x + \dots + x}_{d\text{-times}}$, for $d > 0$, $dx = \underbrace{(-x) + \dots + (-x)}_{|d|\text{-times}}$, for $d < 0$, $0x = 0$, where 0 is the zero element of P.

We denote by m_r the number of uninomials of degree r occuring in a fixed from (1) of $g(x_1,\dots,x_n)$ with the sign plus.

If

$$\sum_{1\leq i\leq n} d_i = 1 \tag{2}$$

then the number of uninomials of degree 1 of the polynomial $g_1(x_1,\dots,x_n) = \sum_{1\leq i\leq n} d_ix_i$ with the sign plus is greater by 1, then the number of uninomials of degree 1 with the sign minus. Hence

$$g_1(x_1,\dots,x_n) = x_i + \sum_{m_1-1} (x_j - x_s), \quad \text{for some } 1\leq i\leq n \tag{3}$$

and $\sum_{m_1-1} (x_j - x_s)$ denote the sum of m_1-1 components of the form $(x_j - x_s)$, where $j, s \in \{1,\dots,n\}$.

If

$$\sum_{1\leq i_1,i_2\leq n} d_{i_1i_2} = 0, \dots, \sum_{1\leq i_1,\dots,i_k\leq n} d_{i_1\dots i_k} = 0, \tag{4}$$

then the number of uninomials of degree r with the sign plus is equal to the number of uninomials of the degree r with the sign minus (for $r = 2,\dots,k$). Thus

(5) $$g_2(x_1,\dots,x_n) =$$

$$= \sum_{m_2}(x_{i_1}x_{i_2}-x_{j_1}x_{j_2}) + \dots + \sum_{m_k}(x_{t_1}\dots x_{t_k}-x_{s_1}\dots x_{s_k}).$$

Let

$$g(x_1,\dots,x_n) = g_1(x_1,\dots,x_n) + g_2(x_1,\dots,x_n)$$

be a fixed representation of g, where g_1 and g_2 are of the form (3), (5) respectively. So $g(x_1,\dots,x_n)$ is idempotent. And conversely:

Lemma 1. Every idempotent polynomial $g(x_1,\dots,x_n)$ ($n \geq 1$) over an arbitrary ring $P = (P,+,-,\cdot)$ can be expressed in the form

$$g(x_1,\dots,x_n) = g_1(x_1,\dots,x_n) + g_2(x_1,\dots,x_n)$$

where g_1 is of the form (3) and $g_2(x_1,\dots,x_n)$ is of the form (5).

Proof. Let

$$g(x_1,\dots,x_n) = g_1(x_1,\dots,x_n) + g_2(x_1,\dots,x_n)$$

be an idempotent polynomial over P (see (1)). It is enough to show that $g(x_1,\dots,x_n) = h_1(x_1,\dots,x_n) + h_2(x_1,\dots,x_n)$ where $h_1(x_1,\dots,x_n)$ satisfies (2) and $h_2(x_1,\dots,x_n)$ satisfies (4). Substituting x_1 for all variables in $g(x_1,\dots,x_n)$ we get

$$\Big(\sum_{1\leq i\leq n} d_i\Big)x_1 + \Big(\sum_{1\leq i_1,i_2\leq n} d_{i_1i_2}\Big)x_1^2 + \dots$$

$$+ \Big(\sum_{1\leq i_1,\dots,i_k\leq n} d_{i_1\dots i_k}\Big)x_1^k = x_1.$$

So

$$\Big(1 - \sum_{1\le i\le n} d_i\Big)x_1 - \Big(\sum_{1\le i_1,i_2\le n} d_{i_1 i_2}\Big)x_1^2 - \ldots$$

$$- \Big(\sum_{1\le i_1,\ldots,i_k\le n} d_{i_1\ldots i_k}\Big)x_1^k = 0$$

holds in P. Hence

$$g(x_1,\ldots,x_n) = g(x_1,\ldots,x_n) + 0 =$$

$$= g(x_1,\ldots,x_n) + \Big(1 - \sum_{1\le i\le n} d_i\Big)x_1 - \ldots - \Big(\sum_{1\le i_1,\ldots,i_k\le n} d_{i_1\ldots i_k}\Big)x_1^k =$$

$$= \Big(1 - \sum_{1\le i\le n} d_i\Big)x_1 + \sum_{1\le i\le n} d_i x_i + \sum_{1\le i_1,i_2\le n} d_{i_1 i_2} x_{i_1} x_{i_2} -$$

$$- \Big(\sum_{1\le i_1,i_2\le n} d_{i_1 i_2}\Big)x_1^2 + \ldots + \sum_{1\le i_1,\ldots,i_k\le n} d_{i_1\ldots i_k} x_{i_1}\ldots x_{i_k} -$$

$$- \Big(\sum_{1\le i_1,\ldots,i_k\le n} d_{i_1\ldots i_k}\Big)x_1^k = h_1(x_1,\ldots,x_n) + h_2(x_1,\ldots,x_n)$$

where

$$h_1(x_1,\ldots,x_n) = \Big(1 - \sum_{1\le i\le n} d_i\Big)x_1 + \sum_{1\le i\le n} d_i x_i$$

and

$$h_2(x_1,\ldots,x_n) = \sum_{1\le i_1,i_2\le n} d_{i_1 i_2} x_{i_1} x_{i_2} - \Big(\sum_{1\le i_1,i_2\le n} d_{i_1 i_2}\Big)x_1^2 + \ldots +$$

$$\sum_{1\le i_1,\ldots,i_k\le n} d_{i_1\ldots i_k} x_{i_1}\ldots x_{i_k} - \Big(\sum_{1\le i_1,\ldots,i_k\le n} d_{i_1\ldots i_k}\Big)x_1^k$$

and h_1 satisfies (2) and h_2 satisfies (4). This completes the proof of the lemma.

In the sequel the following idempotent polynomials will play an important role

$$f_o(x_1,x_2,x_3) = x_1 + x_2x_3 - x_1^2$$

$$f_1(x_1,x_2,x_3) = x_1 + x_2 - x_3$$

and

$$f_n(x_1,\ldots,x_{2n+1}) = x_1 + x_2\ldots x_{n+1} - x_{n+2}\ldots x_{2n+1}$$

for $n \geqslant 2$. Note that

$$f_1(x_1,f_o(x_1,x_2,x_3),f_o(x_1,x_4,x_5)) = x_1 + x_2x_3 - x_4x_5 =$$
$$= f_2(x_1,x_2,x_3,x_4,x_5).$$

In general we have

L e m m a 2. For each $n \geqslant 2$, the polynomial f_n is a composition of f_o and f_1.

P r o o f . Observe that the following formulas are true

(i) $$f_n(x_1,\ldots,x_{2n+1}) =$$

$$= f_{k+1}(f_{k+1}(x_1,f_k(x_1,x_2,\ldots,x_{k+1},x_{2k+2},\ldots,x_{3k+1}),$$
$$x_{k+2},\ldots,x_{2k+1},f_k(x_1,x_{3k+2},\ldots,x_{4k+1},x_{k+2},\ldots,x_{2k+1}),$$
$$x_{2k+2},\ldots,x_{3k+1}),x_1,x_{2k+2},\ldots,x_{3k+1},x_1,x_{k+2},\ldots,x_{2k+1}),$$

for $n = 2k$, $k \geqslant 1$.

(ii) $$f_n(x_1,\ldots,x_{2n+1}) =$$

$$= f_{k+1}(f_{k+1}(x_1,f_{k+1}(x_1,x_2,\ldots,x_{k+2},x_{2k+3},\ldots,x_{3k+3}),$$
$$x_{k+3},\ldots,x_{2k+2},f_{k+1}(x_1,x_{3k+3},\ldots,x_{4k+3},x_{k+3},\ldots,x_{2k+2},x_{3k+3}),$$
$$x_{2k+3},\ldots,x_{3k+2}),x_1,x_{2k+3},\ldots,x_{3k+2},x_1,x_{k+3},\ldots,x_{2k+2})$$

for $n = 2k+1$, $k \geqslant 1$.

We give only the proof for (i)

$$f_{k+1}(f_{k+1}(x_1,f_k(x_1,x_2,\dots,x_{k+1},x_{2k+2},\dots,x_{3k+1}),x_{k+2},\dots,x_{2k+1},$$
$$f_k(x_1,x_{3k+2},\dots,x_{4k+1},x_{k+2},\dots,x_{2k+1}),x_{2k+2},\dots,x_{3k+1}),$$
$$x_1,x_{2k+2},\dots,x_{3k+1},x_1,x_{k+2},\dots,x_{2k+1}) =$$
$$= x_1+(x_1+x_2\dots x_{k+1}-x_{2k+2}\dots x_{3k+1})x_{k+2}\dots x_{2k+1} -$$
$$-(x_1+x_{3k+2}\dots x_{4k+1}-x_{k+2}\dots x_{2k+1})x_{2k+2}\dots x_{3k+1}+x_1x_{2k+2}\dots x_{3k+1}-$$
$$-x_1x_{k+2}\dots x_{2k+1} = x_1+x_1x_{k+2}\dots x_{2k+1}+x_2\dots x_{k+1}x_{k+2}\dots x_{2k+1} -$$
$$-x_{k+2}\dots x_{2k+1}x_{2k+2}\dots x_{3k+1}-x_1x_{2k+2}\dots x_{3k+1} -$$
$$-x_{2k+2}\dots x_{3k+1}x_{3k+2}\dots x_{4k+1}+x_{k+2}\dots x_{2k+1}x_{2k+2}\dots x_{3k+1}+$$
$$+x_1x_{2k+2}\dots x_{3k+1}-x_1x_{k+2}\dots x_{2k+1} = x_1+x_2\dots x_{2k+1}-x_{2k+2}\dots x_{4k+1}=$$
$$= x_1+x_2\dots x_{n+1}-x_{n+2}\dots x_{2n+1} = f_n(x_1,\dots,x_{2n+1}).$$

Using these formulas we see that any f_n is a composition of f_o and f_1.

T h e o r e m 1. In an arbitrary ring $P=(P,+,-,\cdot)$ every idempotent polynomial $g(x_1,\dots,x_n)$ $(n\geq 1)$ over P is a composition of f_o and f_1.

P r o o f . The proof proceeds on induction with respect to k (see formula (1)).

Let

$$(6)\qquad g(x_1,\dots,x_n) = g_1(x_1,\dots,x_n) + g_2(x_1,\dots,x_n)$$

where g_1 and g_2 are of the form (3), (5), respectively. If $k = 1$, then $g(x_1,\dots,x_n) = g_1(x_1,\dots,x_n)$. Then by (5)

$$g(x_1,\dots,x_n) = g_1(x_1,\dots,x_n) = x + \sum_{m_1-1}(x_j-x_r) =$$

$$= x_i+(x_j-x_r)+\sum_{m_1-2}(x_s-x_t) = f_1(x_i,x_j,x_r)+(x_s-x_t)+\sum_{m_1-3}(x_p-x_q) =$$

$$= f_1(f_1(x_i,x_j,x_r),x_s,x_t)+\sum_{m_1-3}(x_p-x_q).$$

This shows that $g(x_1,\dots,x_n)$ is a composition of f_1.

Assume that the statement holds for each $k \leqslant h$. Let (6) hold and $k = h+1$. Then

$$g(x_1,\dots,x_n) = w(x_1,\dots,x_n)+\sum_{m_{h+1}}(x_{i_1}\dots x_{i_{h+1}}-x_{j_1}\dots x_{j_{h+1}})$$

where

$$w(x_1,\dots,x_n) = x_i+\sum_{m_1-1}(x_j-x_r)+\sum_{m_2}(x_{i_1}x_{i_2}-x_{j_1}x_{j_2})+$$

$$+\sum_{m_h}(x_{i_1}\dots x_{i_h}-x_{j_1}\dots x_{j_h}).$$

Then

$$g(x_1,\dots,x_n) = w(x_1,\dots,x_n)+(x_{i_1}\dots x_{i_{h+1}}-x_{j_1}\dots x_{j_h})+$$

$$+\sum_{m_{h+1}-1}(x_{r_1}\dots x_{r_{h+1}}-x_{s_1}\dots x_{s_h}) =$$

$$= f_{h+1}(w(x_1,\dots,x_n),x_{i_1},\dots,x_{i_{h+1}},x_{j_1},\dots,x_{j_{h+1}})+$$

$$+\sum_{m_{h+1}-1}(x_{r_1}\dots x_{r_{h+1}}-x_{s_1}\dots x_{s_{h+1}}).$$

Repeating this step $(m_{h+1}-1)$ times we conclude that $g(x_1,\dots,x_n)$ is a composition of w and f_{h+1}. Applying now lemma 2 and the inductional assumption we get our assertion.

R e m a r k . Theorem 1 says that in an arbitrary ring every idempotent polynomial can be constructed from idempotent terhary polynomials. The following example shows that in general this cannot be done by means of binary polynomials.

E x a m p l e . Let $\mathcal{B} = (B,+,\cdot)$ be a non-degenerated Boolean ring (i.e. satisfies $x^2 = x$). So we have only two essentially binary polynomials (i.e. depending on each variable) in $\mathcal{B}$, namely $x \vee y = x + y + xy$, $x \wedge y = xy$. Then the algebra $(B,\vee,\wedge)$ is a distributive lattice. The polynomial $h(x,y,z) = x + y + z$ is idempotent in $\mathcal{B}$. It satisfies the identities

$$(7) \qquad h(x,x,y) = h(x,y,x) = h(y,x,x) = y.$$

However $h(x,y,z)$ is not a composition of $\vee$ and $\wedge$. In fact in every non-degenerated lattice we have only nine essentially ternary polynomials (see [1]), and none of them satisfies (7).

T h e o r e m 2. The idempotent reduct, of every ring $P = (P,+,-,\cdot)$ is polynomially equivalent to an algebra (P,p) of type (4).

Recall that two algebras (A,F_i) $(i=1,2)$ are called polynomially equivalent if the sets $A(F_1)$ and $A(F_2)$ of their polynomials are equal.

P r o o f . Put $p(x_1,x_2,x_3,x_4) = x_1 + x_2 - x_3 + x_2x_4 - x_2x_3$. Since p is idempotent so by Theorem 2 it is a composition of f_0 and f_1.

Hence it suffices to show that each f_0 and f_1 is a composition of p. In fact, we have

$$p(x_1,x_2,x_3,x_3) = f_1(x_1,x_2,x_3)$$

$$p(x_1,x_2,x_3,f_1(x_1,x_3,x_2)) = x_1+x_2-x_3+x_1x_2-x_2^2 = q_1(x_1,x_2,x_3).$$

Further

$$q_1(x_1,x_2,x_1) = x_2 + x_1x_2 - x_2^2 = q_2(x_1,x_2)$$

and

$$f_1(x_1,q_2(x_3,x_2),q_2(x_2,x_3)) = x_1+x_2-x_3-x_2^2+x_3^2 = q_3(x_1,x_2,x_3)$$

which consequently gives

$$f_1(x_1,q_1(x_3,x_2,x_1),q_3(x_3,x_2,x_1)) = x_1+x_2x_3-x_1^2 = f_0(x_1,x_2,x_3).$$

This completes the proof of the theorem.

REFERENCES

[1] G. Birkhoff: Lattice theory, rev. ed. New York: American Mathematical Society, 1948.

[2] J. Dudek, J. Płonka: On the monoarity of algebras, Proceedings of the Klagenfurt Conference 1982.

[3] J. Płonka: On the arity of idempotent reducts of groups, Colloq. Math. 21 (1970), 35-37.

[4] R. Quackenbush: On the composition of idempotent functions, Algebra Universalis [1971a], 7-12.

[5] W. Sierpiński: Sur les fonctions de plusieurs variables, Fund. Math. 33 (1945), 169-173.

[6] J. Słupecki: The full three-valued propositional calculus (1936), Translated in McCall (1967) 335-337.

[7] A. Szendrei: On the arity of affine modules, Colloq. Math. 38 (1977), 1-4.

[8] D. Webb: Definition of Post's generalized negative and maximum in terms of one binary operation, Amer. J. Math. 58 (1936), 173-194.

INSTITUTE OF MATHEMATICS, PEDAGOGICAL UNIVERSITY,
45-052 OPOLE, POLAND
Received April 13, 1987.