Algebra Universalis, 7 (1977) 357–360 Birkhäuser Verlag, Basel

On composition of polynomials

P. Erdös and S. Fajtlowicz

We shall use the following notation: If A is an algebra then $A^{(n)}$ will denote the set of all n-ary polynomial operations of A, and $A^{(\omega)}$ will denote the set of all polynomial operations of A: by an algebra over a field F we shall mean here a member of the variety generated by $F=(F;+,\cdot,(a)_{a\in F})$, (we shall identify here an algebra with its universe).

The following concept of order of enlargeability ε was introduced by E. Marczewski in [4]:

$$\varepsilon(A)=\min\left\{n:\underset{B}{\forall}([A^{(n)}=B^{(n)}]\Rightarrow[A^{(\omega)}\supseteq B^{(\omega)}])\right\}$$

where the minimum of an empty set is assumed to be ∞, (Marczewski first called $\varepsilon(A)$ the degree of extendability of A, but later he changed his terminology to the above).

The order of enlargeability was studied extensively by Urbanik in [5] and [6]. Let $\gamma(A)$ be the minimal number of generators of a finitely generated algebraic structure A. As usual if every element of A is an algebraic constant we put $\gamma(A)=0$, but if A is not finitely generated we put $\gamma(A)=\infty$. For any subalgebra B of A let $\gamma(B,A)=\min\alpha(C)$ where C is any subalgebra of A containing B. Further, we put $\gamma_0(A)=\sup\gamma(B,A)$, where the supremum is taken over all finitely generated subalgebras B of A. This concept was introduced by Urbanik [5], who showed that in a number of instances it is true that $\gamma_0(A)=\varepsilon(A)$. We shall show that this identity holds for algebras A over uncountable fields F, unless $A=F$. (If the cardinality of F is $\aleph_0$, then $\varepsilon(F)=1$ but $\gamma_0(F)=0$.) For fields of cardinality different than $\aleph_0$ we have a stronger result, namely that if $f:F^n\to F$ is an operation such that for every $i\le n$ and $(a_1,\ldots,a_{n-1})\in F^{n-1}$, $f(a_1,\ldots,a_{i-1},x,a_i,\ldots,a_{n-1})$ is a polynomial, then f is a polynomial. J. Jones [3] has recently published a problem corresponding to a special case of this theorem: F is the field of real numbers, $n=2$.

Presented by J. Mycielski. Received May 25, 1976. Accepted for publication in final form October 13, 1976.

The idea of the proof of Theorem 2, below comes from Wolfgang Schmidt, who proved that for the ring of integers we have that $\varepsilon = 1$. We are publishing the theorem with his kind permission.

In the proof of Theorem 1 integers are identified with the set of their predecessors. For the definition of bicentrality see [1] or [2].

THEOREM 1. *Let F be a field of cardinality $\neq \aleph_0$ and let $f: F^n \to F$, $n \geq 2$. If for every $(a_1, \ldots, a_{n-1}) \in F^{n-1}$ and $i \leq n$, we have that $f(a_1, \ldots, a_{i-1}, x, a_i, \ldots, a_{n-1}) \in F^{(1)}$, then $f \in F^{(n)}$.*

Proof. If F is finite then the theorem is obvious because every operation on F can be represented as a polynomial with coefficients from F. For infinite fields we shall prove the theorem by induction on n. For $n = 1$ the theorem is obvious. So suppose the theorem is true for n, and let $f: F^{n+1} \to F$, $n \geq 1$. By the inductive assumption it follows that for every $a \in F$, the operation $f(x_0, x_1, \ldots, x_{n-1}, a) \in F^{(n)}$. Thus for every $a \in F$ there exists an integer k_a and functions $f_\beta: F \to F$, $\beta = 0, 1, \ldots, k_a^n - 1$, such that

$$f(x_0, \ldots, x_{n-1}, a) = \sum_{\beta \in k_a^n} f_\beta(a) x_0^{\beta(0)} x_1^{\beta(1)} \cdots x_{n-1}^{\beta(n-1)}. \tag{$*$}$$

Because the cardinality of F is bigger than $\aleph_0$ there are an integer k and an infinite subset $F_0 \subseteq F$ such that for every $a \in F_0$, we have $k_a < k$. Let M be a $k^n \times k^n$ matrix such that for every $\alpha, \beta \in k^n$ the (α, β)-entry of M is the monomial $x_{0,\alpha}^{\beta(0)}, x_{1,\alpha}^{\beta(1)} \cdots x_{n-1,\alpha}^{\beta(n-1)}$. Let

$$\Delta = \Delta(x_{0,0}, \ldots, x_{n-1,0}, x_{0,1}, \ldots, x_{n-1,1}, \ldots, x_{0,k^n-1}, \ldots, x_{n-1,k^n-1})$$

be the determinant of the matrix M. Since Δ is a linear combination of monomials with coefficients ± 1 with no two of these monomials equal, Δ is a nonzero polynomial and thus there are elements $a_{i,\alpha} \in F$, $i \in n$, $\alpha \in k^n$ such that

$$\Delta(a_{0,0}, \ldots, a_{n-1,0}, a_{0,1}, \ldots, a_{n-1,1}, \ldots, a_{0,k^n-1}, \ldots, a_{n-1,k^n-1}) \neq 0.$$

Let us consider the system of k^n linear equations in the unknowns x_β

$$f(a_{0,\alpha}, a_{1,\alpha}, \ldots, a_{n-1,\alpha}) = \sum_{\beta \in k^n} x_\beta a_{0,\alpha}^{\beta(0)} a_{1,\alpha}^{\beta(1)}, \ldots, a_{n-1,\alpha}^{\beta(n-1)} \tag{$**$}$$

where $\alpha \in k^n$. By the choice of $a_{i,\alpha}$ the determinant of the right side is different from 0 and thus by Cramer's rule the system $(**)$ has a unique solution, which is a linear combination of $f(a_{0,\alpha}, \ldots, a_{n-1,\alpha}, a)$. Because for every $a_0, a_1, \ldots, a_{n-1} \in F^n$, $f(a_0, \ldots, a_{n-1}, x)$ is a polynomial, for every $\beta \in k^n$ there is a polynomial π_β such that the solution of (**) is $\pi_\beta(a)$. Again, because (**) has a unique solution, therefore in view of (*), for every $a \in F_0$, we have $\pi_\beta(a) = f_\beta(a)$, $\beta \in k^n$. Let

$$\psi(x_0, \ldots, x_{n-1}, x_n) = f(x_0, \ldots, x_{n-1}, x_n) - \sum_{\beta \in k^n} \pi_\beta(x_n) x_0^{\beta(0)}, \ldots, x_{n-1}^{\beta(n-1)}.$$

Let $(a_0, \ldots, a_{n-1}) \in F^n$. Then $\chi(x) = \psi(a_0, \ldots, a_{n-1}, x)$ is a polynomial. But now from (*) it follows that for every $a \in F_0$, $\chi(a) = 0$. Since F_0 is infinite $\chi = 0$ and so $\psi = 0$. Thus

$$f = \sum_{\beta \in k^n} \pi_\beta(x_n) x_0^{\beta(0)} x_1^{\beta(1)}, \ldots, x_n^{\beta(n)} \quad \text{i.e., } f \text{ is a polynomial.}$$

THEOREM 2. *If F is a countable field then $\varepsilon(F) = \infty$.*

Proof. To prove the theorem we have to show that for every $n > 1$ there is an operation $f: F^n \to F$ which is not a polynomial such that for every n-tuple of polynomials $\psi_1, \psi_2, \ldots, \psi_n$ whose variables come from fixed $(n-1)$ element set of variable $f(\psi_1, \psi_2, \ldots, \psi_n)$ is a polynomial. Let $\varphi_1 = (\psi_1^1, \ldots, \psi_n^1)$, $\varphi_2 = (\psi_1^2, \ldots, \psi_n^2) \cdots$ be a sequence of all n-tuples of polynomials of $n-1$ variables. Since for every positive integer k the polynomials $\psi_1^k, \psi_2^k, \ldots, \psi_n^k$ are algebraically dependent, there is a nontrivial polynomial σ_k such that $\sigma_k(\psi_1^k, \psi_2^k, \ldots, \psi_n^k) = 0$. Let $\pi_k = \sigma_1, \sigma_2 \cdots \sigma_k$ and let $X_k = \{x \in F^n : \pi_k(x) = 0\}$. Thus for $l \leq k$ we have that $\operatorname{Im} \varphi_l \subseteq X_k$. Moreover, each of the sets X_k is a subset of X_{k+1} and $\bigcup_{k=1}^{\infty} X_k = F^n$. Without loss of generality we can assume that $X_k \neq X_{k+1}$. Because each element of F^n belongs to all but finitely many sets X_k, for every sequence ε_i of zeros and ones the formula $f(x) = \sum_{i=1}^{\infty} \varepsilon_i \pi_i(x)$ defines an operation on F. Because $\operatorname{Im} \varphi_k \subseteq X_k$ we have that for every k $f(\psi_1^k, \ldots, \psi_n^k) = \sum_{i=1}^{k-1} \varepsilon_i \pi_i(\psi_1^k, \ldots, \psi_n^k)$ is a polynomial. However different sequences ε_i yield different operations f and so some of them are not polynomials. Thus Theorem 2 is proved.

THEOREM 3. *If $A \neq F$ is an algebra over a field of cardinality $\neq \aleph_0$ then $\varepsilon(A) = \gamma_0(A)$.*

Proof. If $A \neq F$ then $\varepsilon(F) \leq \gamma_0(A)$, because by Theorem 1 $\varepsilon(F)$ equals 0 or 1. Because every two polynomial operations which are equal on F are equal on A, by Urbanik's Theorem 4.1 of [5], we have that $\varepsilon(A) \leq \gamma_0(A)$.

Suppose now that $k < \gamma_0(A)$. Let f_m be an operation such that

$f_m(x_1, \ldots, x_m) = 0$ if and only if the set $\{x_1, x_2, \ldots, x_m\}$ is contained in a subalgebra generated by k elements. Because $k < \gamma_0(A)$ there is an integer s such that f_s is not identically equal to zero and hence f_s is not a polynomial. Nevertheless, for every $\pi_1, \ldots, \pi_s \in A^{(k)}$ we have that $f_s(\pi_1, \ldots, \pi_s) \in A^{(k)}$ because it is identically equal to 0. Thus $\gamma(A) \leq \varepsilon(A)$ i.e. Theorem 3 is proved.

COROLLARY. *Polynomial rings over fields of cardinality* $\neq \aleph_0$ *are bicentral.*

Proof. Let F be an uncountable field and let R be a polynomial ring over F. Then R is a free algebra in the variety of algebras generated by F. If the number of variables of R is infinite then the corollary follows from Theorem 1 of [2]. If the number of variables is finite and equals n then by Theorem 3 $\varepsilon(R) = n$, and thus R is bicentral by Theorem 2 of [2].

Using Theorem 2 one may show that polynomial rings in finitely many variables over countable fields are not bicentral.

REFERENCES

[1] P. M. COHN, *Universal Algebra*, Harper & Row, 1965.
[2] S. FAJTLOWICZ, *Algebras of homomorphisms*, Rendiconti di Mathematica (6) 3 (1970), 523–527.
[3] J. JONES, *Problems for solution*, Canadian Mathematical Bulletin, Vol. 17 (5) 1975, p. 767.
[4] E. MARCZEWSKI, *Independence in abstract algebras. Results and problems*, Colloquium Mathematicum *14* (1966), 169–188.
[5] K. URBANIK, *On some numerical constants associated with abstract algebras*, Fundamenta Mathematicae, LIX (1966), 263–287.
[6] K. URBANIK, *On some numerical constants associated with abstract algebras, II*, Fundamenta Mathematicae, LXII (1968), 191–210.

University of Houston
Houston, Texas
U.S.A.