COLLOQUIUM MATHEMATICUM

VOL. L 1986 FASC. 2

A POLYNOMIAL CHARACTERIZATION OF AFFINE SPACES OVER GF(3)

BY

J. DUDEK (WROCŁAW)

1. Introduction. We adopt here the definitions and notation from Grätzer [10] and Marczewski [14]. In particular we denote by $p_n(\mathfrak{A})$ the number of all essentially n-ary polynomials of an algebra $\mathfrak{A}$.

An identity $f = g$ is said to be *regular* [15] if the sets of variables occurring in both sides are equal.

If E is a set of identities, then by E^* we shall denote the variety of all algebras satisfying all identities of E.

The identity $f = g$ is called *nontrivial for the class* E^* if the class $(E \cup \{f = g\})^*$ is properly contained in E^* and is different from the class $\{x = y\}^*$.

Let $f = f(x_1, \ldots, x_n)$ be a function on a set A. We say that f *admits a permutation* $\sigma \in S_n$ *of its variables* if $f = f^\sigma$, where for a permutation $\sigma \in S_n$ we shall write $f^\sigma(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n})$. By $G(f)$ we denote the group of all admissible permutations of f. The group $G(f)$ is called the *admissible group of the function* f (see [13]).

Let f be an n-ary polynomial. Then a permutation $\sigma \in S_n$ is said to be *trivial for* f (with respect to a set of identities E) if the identity $f = f^\sigma$ is an identity in E^*.

For a given groupoid $(G, \cdot)$ we write $x_1 \ldots x_n$ instead of

$$(\ldots((x_1 x_2) \ldots) x_{n-1}) x_n$$

and xy^n will stand for the expression $(\ldots(xy) \ldots y)y$ where x occurs once and y occurs n times ($n \geqslant 1$). The variety of all idempotent and commutative groupoids $(G, \cdot)$ will be denoted by $V(\cdot)$ and by $M(\cdot)$ we denote the subvariety of $V(\cdot)$ of all medial groupoids. Recall that a groupoid $(G, \cdot)$ is *medial* if it satisfies the medial law $(xy)(uv) = (xu)(yv)$. For a given $n \geqslant 1$, $V_n(\cdot)$ denotes the subvariety of $V(\cdot)$ of all groupoids $(G, \cdot)$ satisfying $xy^n = x$. We put $M_n(\cdot) = M(\cdot) \cap V_n(\cdot)$.

Let $(G, +)$ be an abelian group of an odd exponent m. Denote by $G(m)$ the groupoid $\left(G, \frac{m+1}{2}(x+y)\right)$. If p is prime, then $G(p)$ is called an *affine*

groupoid. Using the main result of [16] we infer that $G(p)$ is equivalent to an affine space over the Galois field GF(p), i.e., $G(p) = (G, I(G, +))$, where $I(\mathfrak{A})$ denotes the full idempotent reduct of an algebra $\mathfrak{A}$.

Using the formula from [1] (or from [11]) we get for the groupoid $G = G(3)$ the following equality:

$$(*) \qquad p_n(G) = \frac{2^n - (-1)^n}{3} \quad \text{for all } n.$$

Thus $p_4(G) = 5$ and every groupoid G with (*) is, of course, an idempotent groupoid.

In this paper we prove the following

THEOREM. *Let* $(G, \cdot)$ *be an idempotent groupoid* (card $G > 1$). *Then* $(G, \cdot)$ *is an affine space over* GF(3) *if and only if* $p_4(G, \cdot) = 5$.

Previously G. Grätzer and R. Padmanabhan [12] proved the same assertion under the assumption that (*) holds for $n = 2$, 3 and 4.

2. Now we state without proof a result concerning binary algebras, used in this paper.

THEOREM ([2], th. 2.1, see also [4]). *Let* $\mathfrak{A}$ *be an algebra containing two essentially binary idempotent polynomials* $+$ *and* $\cdot$, *where* $+$ *is commutative and* $\cdot$ *is noncommutative. Then*

$$p_n(\mathfrak{A}) \geqslant 2^n - 1 \quad \textit{for all } n.$$

3. Proof of the theorem. The proof splits into two cases: $(G, \cdot)$ is noncommutative and $(G, \cdot)$ is commutative.

3.1. Noncommutative case. Some lemmas are needed.

LEMMA 1. *Let* $\mathfrak{A}$ *be an idempotent algebra containing an essentially binary noncommutative polynomial, say,* xy. *Suppose that there exists a 4-ary polynomial* $f = f(x_1, x_2, x_3, x_4)$ *admitting a cycle of all its variables. Then* $p_4(\mathfrak{A}) \geqslant 2^n - 1$ *for all* n.

Proof. Let f be a 4-ary polynomial. If $f = f^\sigma$ for a cycle σ of order 4, then $(13)(24) \in G(f)$, i.e., $f(x_1, x_2, x_3, x_4) = f(x_3, x_4, x_1, x_2)$ and hence by putting $x_1 = x_2 = x$ and $x_3 = x_4 = y$ and denoting $x + y = f(x, x, y, y)$ we get $x + y = y + x$. Thus the polynomial $x + y$ is idempotent, commutative and essentially binary (since xy is essentially binary). Therefore $\mathfrak{A}$ satisfies the assumption of the quoted theorem, and we get $p_n(\mathfrak{A}) \geqslant 2^n - 1$ for all n.

LEMMA 2. *Let* $\mathfrak{A}$ *be an idempotent algebra having an essentially binary noncommutative polynomial and let* $p_4(\mathfrak{A}) < 15$. *Then for every 4-ary polynomial* $f = f(x_1, x_2, x_3, x_4)$ *over* $\mathfrak{A}$ *the polynomials* $f(x_1, x_2, x_3, x_4)$, $f(x_2, x_3, x_4, x_1)$, $f(x_3, x_4, x_1, x_2)$ *and* $f(x_4, x_1, x_2, x_3)$ *are different.*

Proof. It follows from Lemma 1 and the quoted theorem (in the case if, e.g., $f(x_1, x_2, x_3, x_4) = f(x_3, x_4, x_1, x_2)$).

LEMMA 3. *There is no idempotent noncommutative groupoid* $(G, \cdot)$ *for which* $p_4(G, \cdot) = 5$.

Proof. Assume to the contrary that such a groupoid $(G, \cdot)$ exists. Then, of course, $(G, \cdot)$ is not a diagonal semigroup (see [17]) since for such semigroups we have $p_4 = 0$. Using Lemma 3 of [3] we infer that at least one of the polynomials $x_1 x_2 x_3 x_4$ and $x_1(x_2(x_3 x_4))$ is essentially 4-ary, say, the first one. Then using Lemma 2 we infer that the polynomials:

$$(**) \qquad x_1 x_2 x_3 x_4, \quad x_2 x_3 x_4 x_1, \quad x_3 x_4 x_1 x_2 \quad \text{and} \quad x_4 x_1 x_2 x_3$$

are different and essentially 4-ary. By the assumption $p_4(G, \cdot) = 5$ there exists one more essentially 4-ary polynomial $g = g(x_1, x_2, x_3, x_4)$ such that g is different from the polynomials (**) and all polynomials $g(x_1, x_2, x_3, x_4)$, $g(x_2, x_3, x_4, x_1)$, $g(x_3, x_4, x_1, x_2)$, $g(x_4, x_1, x_2, x_3)$ are essentially 4-ary and different by Lemma 2. It is easy to see that none of g's is equal to the polynomials from (**) because if $g^\sigma = f^\tau$ where σ, τ belong to the cyclic group C_4 generated by (1, 2, 3, 4), then $g = f^{\tau\sigma^{-1}}$ and $\tau\sigma^{-1} \in C_4$. Thus $p_4(G, \cdot) \geqslant 8$, a contradiction. The proof of the lemma is completed.

3.2. Commutative case.

LEMMA 4. *Let* $(G, \cdot) \in V(\cdot)$. *Then the polynomial* $s_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4$ *is essentially 4-ary iff* $\operatorname{card} G \geqslant 2$.

Proof. If s_4 depends on all its variables, then $\operatorname{card} G \geqslant 2$. The converse implication follows from the idempotency and the commutativity of xy and the fact that xy is essentially binary on G if and only if $\operatorname{card} G \geqslant 2$.

LEMMA 5. *If* $(G, \cdot) \in V(\cdot)$, $\operatorname{card} G \geqslant 2$ *and* s_4 *admits only trivial permutations of its variables, then* $p_4(G, \cdot) \geqslant 12$.

Proof. By Lemma 4 we infer that s_4 is essentially 4-ary. Now permuting variables in this polynomial we get 12 different and essentially 4-ary polynomials over $(G, \cdot)$ since the only trivial permutations for s_4 are the identity permutation and the transposition (1, 2).

LEMMA 6. *Let* $(G, \cdot) \in V(\cdot)$ *and assume that it is not a semilattice. Suppose that* s_4 *admits a nontrivial permutation of its variables. Then the groupoid* $(G, \cdot)$ *satisfies the following identity:*

$$(+) \qquad x_1 x_2 x_3 x_4 = x_4 x_2 x_3 x_1.$$

Proof. Since $(G, \cdot)$ is not a semilattice we infer that the polynomial $x_1 x_2 x_3$ does not admit any nontrivial permutation of its variables. Now applying Theorem 1 of [5] we get our assertion.

LEMMA 7. *Every affine groupoid* $G(p)$ *is medial.*

Proof. The medial law follows immediately from the definition of $G(p)$.

LEMMA 8. *If a groupoid* $(G, \cdot)$ *from* $V(\cdot)$ *satisfies the identity* $(+)$, *then* $(G, \cdot)$ *is medial.*

Proof. Using Theorem 3 of [5] we infer that the groupoid $(G, \cdot)$ is a Płonka sum of affine groupoids $G(3)$, i.e., groupoids from the variety $M_2(\cdot)$. Now, using Lemma 7 and Theorem 1 of [15], we infer that the groupoid $(G, \cdot)$ is medial since the medial law is regular.

LEMMA 9. *If* $(G, \cdot) \in M(\cdot)$ *and the polynomial* xy^2 *is commutative, then* $(G, \cdot)$ *is a semilattice. Moreover the assertion is also true if* $(G, \cdot) \in V(\cdot)$ *and it is distributive (i.e.* $z(xy) = (zx)(zy)$).

Proof. First of all observe that if $(G, \cdot) \in V(\cdot)$, then the medial law implies the distributive law. Let now $xy^2 = yx^2$. Then we have $xy^2 = (xy^2)(yx^2) = ((xy)y)((yx)x) = ((xy)y)((xy)x) = (xy)(yx) = (xy)(xy) = xy$. Using the identity $xy = xy^2$ and the distributive law we get $(xy)z = (xz)(yz) = (x(yz))(z(yz)) = (x(yz))((yz)z) = (x(yz))(yz) = x(yz)$. Hence $(xy)z = x(yz)$ and $(G, \cdot)$ is a semilattice.

LEMMA 10. *If* $(G, \cdot) \in M(\cdot)$, $\operatorname{card} G \geqslant 2$ *and the polynomial* xy^2 *is not essentially binary, then* $xy^2 = x$, *i.e.*, $(G, \cdot) \in M_2(\cdot)$.

Proof. Let $xy^2 = y$. Then we have $xy = yx = (xy^2)x = ((xy)y)x = ((xy)x)(yx) = ((yx)x)(yx) = x(yx) = x$, a contradiction. Therefore $xy^2 = x$ and hence $(G, \cdot) \in M_2(\cdot)$.

We should mention here that this lemma is generalized in [7] (see Theorem 1).

LEMMA 11. *If* $(G, \cdot) \in V(\cdot)$ *and* xy^2 *is essentially binary and noncommutative, then* $p_4(G, \cdot) \geqslant 15$.

Proof. It follows from the quoted theorem, taking xy instead of $x+y$ and xy^2 instead of xy.

It is worth to add that in [9] we prove for such groupoids even more, namely, $p_n(G, \cdot) \geqslant 3^{n-1}$ for all $n \geqslant 1$.

LEMMA 12. *If* $(G, \cdot) \in V(\cdot)$ *and* $p_4(G, \cdot) = 5$, *then* $(G, \cdot)$ *is an affine space over* GF(3).

Proof. Since $p_4(G, \cdot) = 5$ we infer by Lemma 4 that the polynomial $s_4 = x_1 x_2 x_3 x_4$ is essentially 4-ary and by Lemma 5 the polynomial s_4 admits a nontrivial permutation of its variables. Using Lemmas 6 and 8 we infer that $(G, \cdot) \in M(\cdot)$. Again by the assumption $p_4(G, \cdot) = 5$ we infer that $(G, \cdot)$ is not a semilattice. Then the polynomial xy^2 is noncommutative by Lemma 9, and is not essentially binary by Lemma 11, therefore in view of Lemma 10, $(G, \cdot) \in M_2(\cdot)$. But every groupoid from $M_2(\cdot)$ is an affine space over GF(3) (see [12] or [6], [8]).

3.3. Proof of the theorem. If $(G, \cdot)$ is an affine space over GF(3),

then using (*) we have $p_4(G, \cdot) = 5$. Let now $(G, \cdot)$ be idempotent and $p_4(G, \cdot) = 5$. Using Lemma 3 we infer that $(G, \cdot)$ is commutative. Now the proof follows from Lemma 12. The proof of the theorem is completed.

REFERENCES

[1] B. Csákány, *On affine spaces over prime fields*, Acta Scientiarum Mathematicarum 37 (1975), p. 33–36.

[2] J. Dudek, *O pewnych własnościach grupoidów idempotentnych i niektórych innych algebr binarnych*, Ph. D. Thesis, University of Wrocław, Wrocław (1970).

[3] – *The number of algebraic operations in idempotent groupoids*, Colloquium Mathematicum 21 (1970), p. 169–177.

[4] – *Binary minimal algebras*, Acta Facultatis Rerum Naturalium Universitatis Comenianae Mathematica-Mimoriadne Číslo (1971), p. 21–22.

[5] – *A characterization of some idempotent abelian groupoids*, Colloquium Mathematicum 30 (1974), p. 219–223.

[6] – *Medial groupoids and Mersenne numbers*, Fundamenta Mathematicae 114 (1981), p. 109–112.

[7] – *On binary polynomials in idempotent commutative groupoids*, ibidem 120 (1984), p. 187–191.

[8] – *Varieties of idempotent commutative groupoids*, ibidem 120 (1984), p. 193–204.

[9] – *Polynomials in idempotent commutative groupoids*, submitted for Dissertationes Mathematicae.

[10] G. Grätzer, *Universal Algebra*, Springer-Verlag, 1979.

[11] – *Composition of function. Proceedings of Conference on Universal Algebra*, Queen's University, Kingston, Ontario, 1970, p. 1–106.

[12] G. Grätzer and R. Padmanabhan, *On idempotent, commutative and nonassociative groupoids*, Proceedings of the American Mathematical Society 28 (1971), p. 75–80.

[13] G. Grätzer and J. Płonka, *On the number of polynomials of an idempotent algebra I*, Pacific Journal of Mathematics 32 (1970), p. 697–709.

[14] E. Marczewski, *Independence in abstract algebras, results and problems*, Colloquium Mathematicum 14 (1966), p. 169–188.

[15] J. Płonka, *On a method of construction of abstract algebras*, Fundamenta Mathematicae 61 (1968), p. 183–189.

[16] – *On the arity of idempotent reducts of groups*, Colloquium Mathematicum 21 (1970), p. 35–37.

[17] – *Diagonal algebras*, Fundamenta Mathematicae 58 (1966), p. 309–321.

Reçu par la Rédaction le 7. 08. 1981