The completing step is to prove that $\langle A; f \rangle$ is equivalent to $\langle A; m \rangle$. For this aim, it suffices to show that $f$ is a polynomial of $\langle A; m \rangle$. Assume first that $f$ is binary. The binary polynomials $q_0, \ldots, q_{p-1}$ of $A$, defined by $q_0 = e_1^2$ (i.e., the second binary projection) and $q_k = m(e_0^2, q_{k-1}, e_1^2)$ for $k > 0$, are, by definition, polynomials of $\langle A; m \rangle$, too. Moreover, they are pairwise different, since, by $(\delta)$, for any $a, b \in A$ and $k = 0, \ldots, p-1$ the equality $q_k(a, b) = -ka + (k+1)b$ holds. But $A$ has exactly $p$ binary polynomials, whence $f = q_i$ follows for some $i$ $(0 \le i < p)$. Thus, $f$ is a polynomial of $\langle A; m \rangle$. Finally, let $f$ be $n$-ary with $2 < n \le 4$. Then $(\gamma_n)$ shows that $f$ is generated by $m$ and some binary polynomials of $A$. Just we saw, however, that binary polynomials of $A$ are generated by $m$. Hence, $f$ is a polynomial of $\langle A; m \rangle$, q.e.d.

Remarks. 1. Our theorem is not a generalization of the Grätzer—Padmanabhan theorem, because the last one contains no assumption on the power of subalgebras in $A$. In fact, groupoids satisfying $(3,1)$—$(3,4)$ cannot have two-element subgroupoids, as the identity (15) in [5] shows. In other words, $(3,1)$—$(3,4)$ together imply $(3^*)$ for any groupoid $A$. It is an open problem whether $(p^*)$ follows from $(p, 1)$—$(p, 4)$ for some (possibly for all) primes $p > 3$.

2. The method we used allows some minor generalizations of our theorem. Thus, we can take any algebra $\langle A; F \rangle$ instead of $\langle A; f \rangle$ where the arities of operations from $F$ do not exceed 4. Moreover, if we require $(p, k)$ for $k = 0, \ldots, n$ then it suffices to assume that all operations from $F$ are at most $n$-ary. Hence it follows that an arbitrary algebra $A$ satisfying $(p^*)$ and $(p, k)$ for every non-negative integer $k$, is equivalent to an affine space over $GF(p)$.

### References

[1] G. Grätzer, *Universal Algebra*, Van Nostrand (1968).
[2] S. Mac Lane—G. Birkhoff, *Algebra* Macmillan (1967).
[3] B. Csákány, *Varieties of affine modules*, Acta Sci. Math., **37** (1975), 3—10.
[4] G. Grätzer, *Composition of functions*, Proc. Conf. on Universal Algebra, pp. 1—106, Queen's Univ. (Kingston, Ont., 1970).
[5] G. Grätzer—R. Padmanabhan, *On idempotent, commutative and nonassociative groupoids* Proc. Amer. Math. Soc., **28** (1971), 75—80.
[6] J. Płonka, *On the arity of idempotent reducts of groups*, Coll. Math., **21** (1970), 35—37.
[7] K. Urbanik, *On algebraic operations in idempotent algebras*, Coll. Math., **13** (1965), 129—157.

# On affine spaces over prime fields

By B. CSÁKÁNY in Szeged

The aim of this note to prove a result for affine spaces over arbitrary prime fields like the Grätzer—Padmanabhan characterization theorem of affine spaces over $GF(3)$. Our terminology and notation are the standard ones (see [1]) excepting that the identical mapping of any set will be considered as an essentially unary operation which permits to give a more concise form for the succeeding propositions. Under this agreement, $p_1(A)$ — the number of essentially unary polynomials — equals 1 for any idempotent algebra.

Following Płonka [6], for any group $\mathbf{G} = \langle G; + \rangle$ the algebra $\langle G; I \rangle$, where $I$ denotes the set of all idempotent polynomials of $\mathbf{G}$, is called the idempotent reduct of $\mathbf{G}$. Concerning this notion we shall need the fact that idempotent reducts of abelian groups of exponent $p$ are exactly the affine spaces over $GF(p)$; furthermore, the free affine space over $GF(p)$ with an $n$-element free generating set is the same as the idempotent reduct of $\mathbf{Z}_p^{n-1}$, where $\mathbf{Z}_p$ is the group of order $p$.

The characterization theorem we mentioned above (i.e., the join of Theorems 2 and 3 in [5]) may be formulated as follows:

A groupoid $A$ is equivalent to an affine space over $GF(3)$ if and only if

$$(3, k) \qquad p_k(A) = \frac{1}{3}\left(2^k - (-1)^k\right)$$

holds for $k = 1, 2, 3, 4$. In this case $(3, k)$ remains valid for all non-negative integers $k$.

Our result is the following.

**Theorem.** *Let $p$ be an arbitrary prime. An algebra $A = \langle A; f \rangle$, where $f$ is at most quaternary, is equivalent to an affine space over $GF(p)$ if and only if*

$$(p, k) \qquad p_k(A) = \frac{1}{p}\left((p-1)^k - (-1)^k\right)$$

*holds for $k = 1, 2, 3, 4$, and*

$(p^*)$ *there exists no subalgebra $B$ in $A$ with $1 < |B| < p$. In this case $(p, k)$ remains valid for all non-negative integers $k$.*

3 A

Proof. Let $\mathcal{V}$ be the variety generated by $\mathbf{A}$ and, for any natural $k$, denote by $\mathbf{F}_k$ the free algebra over $\mathcal{V}$ with the free generating set $\{x_0, \ldots, x_{k-1}\}$. Suppose that $\mathbf{A}$ is equivalent to an affine space over $GF(p)$. The variety of all affine spaces over $GF(p)$ is equationally complete; hence it is equivalent to $\mathcal{V}$. Thus, for every natural $k$, $\mathbf{F}_k$ is equivalent to the idempotent reduct of $\mathbf{Z}_p^{k-1}$, implying $|F_k| = p^{k-1}$. The formula

$$(\alpha) \qquad |F_k| = \sum_{i=0}^{k} \binom{k}{i} p_i(\mathbf{A})$$

(see [4], p. 38.) gives

$$p_k(\mathbf{A}) = \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} |F_i| = \frac{1}{p} \left( (p-1)^k - (-1)^k \right),$$

which was needed. Further, any subalgebra of $\mathbf{A}$ is also equivalent to an affine space over $GF(p)$, which clearly cannot have $q$ elements for $1 < q < p$.

To prove the sufficiency, first we remark that $(p, 1)$ and $(p, 3)$ jointly imply that $f$ is at least binary and $\mathbf{A}$ is idempotent. Now, if $p = 2$, using URBANIK's description of idempotent algebras ([7], Theorem 4) we get that $\mathbf{A}$ is equivalent to an affine space over $GF(2)$, moreover, $f$ is essentially ternary.

Suppose $p > 2$. By $(\alpha)$, $(p, 1)$ and $(p, 2)$ we have $|F_2| = p$. Let $\mathbf{B}$ a minimal subalgebra of $\mathbf{A}$ having at least two elements. By $(p^*)$, we have $|B| \geqq p$. Since $\mathbf{B}$ is generated by two elements, it is a homomorphic image of $\mathbf{F}_2$, whence $|B| = p$ and $\mathbf{B} \cong \mathbf{F}_2$. Thus, the proper subalgebras of $\mathbf{F}_2$ are exactly the one-element ones.

Next we show that $\mathbf{F}_2^2 (= \mathbf{F}_2 \times \mathbf{F}_2)$ is generated by the set $S = \{\langle x_1, x_0 \rangle, \langle x_0, x_0 \rangle, \langle x_0, x_1 \rangle\}$. Let $\langle g_1(x_0, x_1), g_2(x_0, x_1) \rangle$ be an arbitrary element of $F_2^2$. Consider an essentially binary polynomial $h$ of $\mathbf{F}_2$. Then

$$\langle x_0, h(x_0, x_1) \rangle (= h(\langle x_0, x_0 \rangle, \langle x_0, x_1 \rangle)) \in [S],$$

$$\langle h(x_1, x_0), h(x_0, x_1) \rangle (= h(\langle x_1, x_0 \rangle, \langle x_0, x_1 \rangle)) \in [S].$$

Now, $h(x_1, x_0) \neq x_0$; hence $[\langle h(x_1, x_0), h(x_0, x_1) \rangle, \langle x_0, h(x_0, x_1) \rangle] (\subseteq [S])$ contains $p$ elements, i.e., all elements of $F_2^2$ with second component $h(x_0, x_1)$, and thus $\langle f(x_0, x_1), h(x_0, x_1) \rangle \in [S]$. Analogously, $\langle g_1(x_0, x_1), x_0 \rangle \in [S]$, whence $\langle g_1(x_0, x_1), g_2(x_0, x_1) \rangle \in [S]$ follows.

Let $\varphi \colon F_3 \to F_2^2$ that homomorphism for which $x_0 \varphi = \langle x_0, x_0 \rangle$, $x_1 \varphi = \langle x_1, x_0 \rangle$, $x_2 \varphi = \langle x_0, x_1 \rangle$ holds. Then $\varphi$ is onto. Hence there exists an essentially ternary polynomial $m$ of $\mathbf{F}_3$ satisfying $(m(x_0, x_1, x_2)) \varphi = \langle x_1, x_1 \rangle$. But

$$(m(x_0, x_1, x_2)) \varphi = \langle m(x_0, x_1, x_0), m(x_0, x_0, x_1) \rangle,$$

whence we get that the identity

$$(\beta) \qquad m(x_0, x_1, x_0) = m(x_0, x_0, x_1) = x_1$$

holds in $\mathcal{V}$. This implies

$$(\gamma_3) \qquad (m(x_0, f_1(x_0, x_1), f_2(x_0, x_2))) \varphi = \langle f_1(x_0, x_1), f_2(x_0, x_1) \rangle$$

for any binary polynomials $f_1, f_2$.

Observe that $|F_3| = p^2 = |F_2^2|$. Thus $\varphi$ is an isomorphism; i.e., $\mathbf{F}_3 \cong \mathbf{F}_2^2$. We show that $\mathbf{F}_4 \cong \mathbf{F}_2^3$ is valid too. Since $|F_4| = |F_2^3| (= p^3)$, it is enough to show that the homomorphism $\psi \colon F_4 \to F_2^3$ for which

$$x_0 \psi = \langle x_0, x_0, x_0 \rangle, \quad x_1 \psi = \langle x_1, x_0, x_0 \rangle, \quad x_2 \psi = \langle x_0, x_1, x_0 \rangle, \quad x_3 \psi = \langle x_0, x_0, x_1 \rangle$$

holds, is surjective. Applying $(\beta)$, we get

$$(\gamma_4) \qquad (m(x_0, m(x_0, f_1(x_0, x_1), f_2(x_0, x_2)), f_3(x_0, x_3))) \psi =$$
$$= \langle f_1(x_0, x_1), f_2(x_0, x_1), f_3(x_0, x_1) \rangle$$

for any binary polynomials $f_1, f_2, f_3$. Hence $\psi$ is onto, indeed.

Now, let $0$ be an arbitrary element of $A$. Introduce the binary algebraic function $+$ on $A$, called addition and defined by $a + b = m(0, a, b)$ for all $a, b \in A$. We claim that $\langle A; + \rangle$ is an abelian group of exponent $p$. Using $(\beta)$ as well as the isomorphisms $\varphi$ and $\psi$ it follows

$$m(x_0, x_1, m(x_0, x_2, x_3)) = \langle x_1, x_1, x_1 \rangle \psi^{-1} = m(x_0, m(x_0, x_1, x_2), x_3)$$

in $\mathbf{F}_4$ and

$$m(x_0, x_1, x_2) = \langle x_0, x_1, x_1 \rangle \varphi^{-1} = m(x_0, x_2, x_1)$$

in $\mathbf{F}_3$, implying associativity, resp. commutativity of the addition. From $(\beta)$ we get $a + 0 = 0 + a = a$ for any $a \in A$. Further,

$$m(x_0, x_1, m(x_2, x_0, x_0)) = \langle x_1, m(x_1, x_0, x_0) \rangle \varphi^{-1} = m(x_2, x_1, x_0)$$

holds in $\mathbf{F}_3$, whence for any $a \in A$ we have $a + m(a, 0, 0) = m(a, a, 0) = 0$; i.e., $m(a, 0, 0)$ is the additive inverse for $a$. Finally, let $a \in A$, $a \neq 0$. Then every element of the subgroup by $a$ in $\langle A; + \rangle$ is contained in the subalgebra $\mathbf{C}$ of $\mathbf{A}$ generated by $\{a, 0\}$. Since $\langle C; + \rangle$ is also a subgroup of $\langle A; + \rangle$ and $|C| = p$, the order of $a$ equals $p$ in $\langle A; + \rangle$, proving our claim.

For arbitrary $a, b, c \in A$,

$$(\delta) \qquad m(a, b, c) = -a + b + c$$

holds. Indeed, let $\theta \colon F_4 \to A$ the homomorphism for which $x_0 \theta = 0$, $x_1 \theta = a$, $x_2 \theta = b$, $x_3 \theta = c$. Then, using $(\gamma_4)$, we get

$$m(a, b, c) = (m(x_1, x_2, x_3)) \theta = \langle m(x_1, x_0, x_0), x_1, x_1 \rangle \psi^{-1} \theta =$$
$$= (m(x_0, m(x_0, m(x_1, x_0, x_0), x_2), x_3)) \theta = -a + b + c.$$

In view of $(\delta)$ and Lemma 1 in [6], $\langle A; m \rangle$ is equivalent to an affine space over $GF(p)$.

3*