

Varieties in which congruences and subalgebras are amicable

By B. CSÁKÁNY in Szeged

In earlier articles [6], [8] we proved: If in each algebra of the variety \mathcal{A} any subalgebra is a block of a unique congruence, and

$$\left\{ \begin{array}{l} \text{every congruence has a unique block which is a subalgebra} \\ \text{all block of any congruence are subalgebras} \end{array} \right\}$$

then \mathcal{A} is equivalent to the variety of all

$$\left\{ \begin{array}{l} \text{unital right modules} \\ \text{affine modules} \end{array} \right\}$$

over some ring with unit element.

These results suggest that it may be fruitful to investigate those varieties in which there exists a similar but more general connection between congruences and subalgebras. Such a connection can be introduced in the following way.

Let M be a non-void set, \mathfrak{S} a set of its subsets and Σ a set of equivalences of M . We say that \mathfrak{S} and Σ are *amicable*, if every $S \in \mathfrak{S}$ is a block of some $\sigma \in \Sigma$ and every $\sigma \in \Sigma$ has a block which belongs to \mathfrak{S} . Uniqueness of the corresponding equivalences and blocks is not required. If, especially, \mathbf{M} is an algebra, \mathfrak{S} the set of its subalgebras and Σ the set of congruences of \mathbf{M} , then in the above case we say shortly that in \mathbf{M} the congruences and subalgebras are amicable. Finally, if the same is fulfilled in each algebra of a variety \mathcal{A} , we say that in \mathcal{A} congruences and subalgebras are amicable.

Following KUROŠ ([2], § 14; see also [11]), we call a variety \mathcal{A} Abelian, if in all algebras of \mathcal{A} any two operations commute. Our result consists of a full description of equationally complete Abelian varieties with the property in the title.

Theorem. *A variety \mathcal{A} is an equationally complete Abelian variety in which congruences and subalgebras are amicable if and only if \mathcal{A} is equivalent to one of the following varieties:*

- (a) *varieties of vector spaces over fields,*
- (b) *the variety of pointed sets,*
- (c) *varieties of affine spaces over fields (see [3], Ch. XII, and [8]),*
- (d) *the variety of sets.*

Corollary. *An Abelian variety is categorically free (i.e., exhausted by its free algebras) if and only if it is an equationally complete variety in which congruences and subalgebras are amicable.*

As a preparation of the proof, we formulate several lemmas.

Lemma 1. *In any Abelian algebra the set of all idempotent elements¹⁾ forms a subalgebra.*

Indeed, let f and g be n -ary, resp. m -ary polynomials on the Abelian algebra A ; further, let a_1, \dots, a_n be idempotent elements of A . Since f and g commute, we have $g(f(a_1, \dots, a_n), \dots, f(a_1, \dots, a_n)) = f(g(a_1, \dots, a_1), \dots, g(a_n, \dots, a_n)) = f(a_1, \dots, a_n)$, i.e., $f(a_1, \dots, a_n)$ is also idempotent.

Lemma 2. *In any algebra a subset closed with respect to endomorphisms generates a fully invariant congruence.*

Let A be an arbitrary algebra, M a subset of A , and denote by the sign \sim the congruence of A generated by M (i.e., the smallest congruence of A under which all elements of M are congruent). Then, for $a, b \in A$, $a \sim b$ means that there exist elements $a = a_0, a_1, \dots, a_k = b$ such that for suitable translations (i.e., unary algebraic functions) τ_1, \dots, τ_k of A and elements $m_{10}, \dots, m_{k0}, m_{11}, \dots, m_{k1} \in M$ the equations $m_{ij}\tau_i = a_{i-1+j}$ ($i=1, \dots, k; j=0, 1$) hold. For any $x \in A$ and for $i=1, \dots, k$ let the image of x under τ_i defined by $t_i(x, c_{i1}, \dots, c_{ii})$, where t_i is a polynomial of A and $c_{i1}, \dots, c_{ii} \in A$. Suppose that M is closed with respect to endomorphisms of A . For any such endomorphism φ denote by τ_i^φ the translation $x \rightarrow t_i(x, c_{i1}\varphi, \dots, c_{ii}\varphi)$. Then for $a\varphi = a_0\varphi, a_1\varphi, \dots, a_k\varphi = b\varphi$, for $\tau_1^\varphi, \dots, \tau_k^\varphi$, and for the elements $m_{ij}\varphi \in M$ we have $(m_{ij}\varphi)\tau_i^\varphi = t_i(m_{ij}\varphi, c_{i1}\varphi, \dots) = (t_i(m_{ij}, c_{i1}, \dots))\varphi = a_{i-1+j}\varphi$, whence $a\varphi = b\varphi$, which was needed.

The following fact is familiar:

Lemma 3. *A free algebra in an equationally complete variety has no other fully invariant congruences than the trivial ones.*

Lastly, we recall a useful result of KLUKOVITS [12]:

Lemma 4. *A variety \mathcal{A} (of type τ) is Hamiltonian (i.e., in any algebra of \mathcal{A} every subalgebra is a block of some congruence) if and only if for any n -ary polynomial symbol f (of type τ) there exists a ternary polynomial symbol h_f (of type τ) such that in \mathcal{A} the identity*

$$(1) \quad f(x_1, \dots, x_n) = h_f(x_0, x_1, f(x_0, x_2, \dots, x_n))$$

holds.

¹⁾ We call an element of an algebra A *idempotent* if it forms a one-element subalgebra of A . A class of algebras is *idempotent* if its every algebra consists of idempotent elements only.

Proof of the theorem. Sufficiency is obvious. To prove the necessity, let us consider an equationally complete Abelian variety \mathcal{A} in which congruences and subalgebras are amicable. The last condition means exactly that \mathcal{A} is Hamiltonian and any algebra in \mathcal{A} has at least one idempotent element. We shall distinguish two cases.

I. \mathcal{A} is not idempotent.

Let F_ω be the \mathcal{A} -free algebra with countable free generating set. The idempotent elements of F_ω form a proper subset M in F_ω . By Lemma 1, M is a subalgebra in F_ω . Obviously, M is closed under endomorphisms of F_ω . Since \mathcal{A} is Hamiltonian, M is a block of the congruence generated by itself in F_ω . Hence this congruence has at least two blocks. On the other hand, this congruence is fully invariant by Lemma 2, and, using Lemma 3, we get that our congruence is just the equality. It follows that F_ω has a unique idempotent element 0. Then there exist an essentially nullary polynomial whose value is 0 in F_ω ; denote it also by 0. Now we shall distinguish two subcases.

a) For some $n > 1$, \mathcal{A} has an essentially n -ary polynomial.

Suppose that n is the minimal among such natural numbers; we show that $n=2$. Denote by F_n the \mathcal{A} -free algebra freely generated by the set $\{x_1, \dots, x_n\}$ and let f be an essentially n -ary polynomial. Since n is minimal, $f(0, \varepsilon_n^2, \dots, \varepsilon_n^n)$ — where ε_n^i denotes the i -th n -ary projection — is essentially not more than unary and so for some i ($2 \leq i \leq n$) $f(0, x_2, \dots, x_n) \in [x_i]$ holds, i.e., for a suitable unary f_i we have $f(0, x_2, \dots, x_n) = f_i(x_i)$. Applying Lemma 4, we get

$$f(x_1, \dots, x_n) = h_f(0, x_1, f(0, x_2, \dots, x_n)) = h_f(0, x_1, f_i(x_i)) \in [x_1, x_i],$$

whence f is essentially binary. In what follows we write f multiplicatively.

Let F_2 be the \mathcal{A} -free algebra with free generators x and y . Define on F_2 an equivalence \sim as follows: for $a, b \in F_2$, let $a \sim b$ if $a \cdot 0 = b \cdot 0$. This relation is a fully invariant congruence on F_2 . Indeed, for any m -ary operation g and $a_1, \dots, a_m, b_1, \dots, b_m \in F_2$ from $a_i \sim b_i$ ($i=1, \dots, m$) it follows (using that f and g commute):

$$(2) \quad \begin{aligned} g(a_1, \dots, a_m) \cdot 0 &= g(a_1, \dots, a_m) \cdot g(0, \dots, 0) = \\ &= g(a_1 \cdot 0, \dots, a_m \cdot 0) = g(b_1 \cdot 0, \dots, b_m \cdot 0) = g(b_1, \dots, b_m) \cdot 0, \end{aligned}$$

whence $g(a_1, \dots, a_m) \sim g(b_1, \dots, b_m)$. Further, if $a, b \in F_2$ and σ is any endomorphism of F_2 , then $a \sim b$ implies

$$(3) \quad a\sigma \cdot 0 = a\sigma \cdot 0\sigma = (a \cdot 0)\sigma = (b \cdot 0)\sigma = b\sigma \cdot 0,$$

i.e., $a\sigma \sim b\sigma$.

On the basis of Lemma 3, \sim is trivial. Suppose that it is the complete relation; then 0 is a right zero element with respect to f . Let f^* denote the polynomial $\varepsilon_2^2 \cdot \varepsilon_2^1$.

Using Lemma 4, we get

$$xy = f^*(y, x) = h_{f^*}(0, y, f^*(0, x)) = h_{f^*}(0, y, x \cdot 0) = h_{f^*}(0, y, 0),$$

a contradiction since f is essentially binary. Hence it follows that \sim is the equality relation on F_2 . This means that the mapping $\varphi_1: F_2 \rightarrow F_2$ defined by $a\varphi_1 = a \cdot 0$ is 1-1. Moreover, φ_1 maps F_2 onto itself. Indeed, as (2) and (3) show, the image of F_2 under φ_1 is a fully invariant subalgebra in F_2 , whence, by Lemma 2 and 3, this image is either $\{0\}$ or F_2 . The first case infer that \mathcal{A} is trivial. Thus, $F_2\varphi_1 = F_2$; i.e., $\varphi_1: F_2 \rightarrow F_2$ is a bijection. We can get in an analogous way that the mapping $\varphi_2: F_2 \rightarrow F_2$ defined by $a\varphi_2 = 0 \cdot a$ is also a bijection.

Let $f^{-1}(x, y)$ be the unique element of F_2 for which $f^{-1}(x, y)\varphi_1 = x$ holds. Then $f^{-1}(x, y) \cdot 0 = x$ is an identity in \mathcal{A} , whence $f^{-1}(x, 0) \cdot 0 = x$ follows. We get similarly a binary polynomial ^{-1}f satisfying $0 \cdot ^{-1}f(0, x) = x$. Now we take the polynomial $f^{-1}(\varepsilon_2^1, 0) \cdot ^{-1}f(0, \varepsilon_2^2)$; it will be called addition and denoted additively. We see that 0 is the unit element with respect to addition.

Next we prove that in \mathcal{A} the direct and the \mathcal{A} -free products of two algebras coincide. As it was proved in [5] (Theorem 1), this fact jointly with the existence of 0 in \mathcal{A} implies that \mathcal{A} is equivalent to the variety of all unital right semimodules over some associative semiring R with unit element. Let $A, B \in \mathcal{A}$; then $A \times B$ is generated by the union of its subalgebras $(A, 0) = \{(a, 0) \mid a \in A\}$ and $(0, B) = \{(0, b) \mid b \in B\}$; furthermore, $(A, 0) \cong A$ and $(0, B) \cong B$. Consider an arbitrary algebra $C \in \mathcal{A}$ and homomorphisms $\psi: (A, 0) \rightarrow C$, $\chi: (0, B) \rightarrow C$. We have to prove that ψ and χ admit a common homomorphic extension $\eta: A \times B \rightarrow C$. Define η by means $(a, b)\eta = (a, 0)\psi + (0, b)\chi$. Obviously, η is an extension of ψ and χ . On the other hand, for any m -ary polynomial g and elements $a_1, \dots, a_m \in A$, $b_1, \dots, b_m \in B$ we have

$$\begin{aligned} g((a_1, b_1), \dots, (a_m, b_m))\eta &= (g(a_1, \dots, a_m), g(b_1, \dots, b_m))\eta = (g(a_1, \dots, a_m), 0)\psi + \\ &+ (0, g(b_1, \dots, b_m))\chi = g((a_1, 0), \dots, (a_m, 0))\psi + g((0, b_1), \dots, (0, b_m))\chi = \\ &= g((a_1, 0)\psi, \dots, (a_m, 0)\psi) + g((0, b_1)\chi + \dots + (0, b_m)\chi) = \\ &= g((a_1, 0)\psi + (0, b_1)\chi, \dots, (a_m, 0)\psi + (0, b_m)\chi) = g((a_1, b_1)\eta, \dots, (a_m, b_m)\eta), \end{aligned}$$

i.e., η is a homomorphism.

Thus, \mathcal{A} is equivalent to the variety of all unital right semimodules over a semiring R . Then the Hamiltonian property of \mathcal{A} guarantees that R is an associative ring, and, as semimodules over rings are modules, \mathcal{A} is equivalent to the variety of unital right modules over the ring R (see [12], Theorem 7). Now, the Abelian property and the equational completeness of \mathcal{A} together imply, that R is a field and \mathcal{A} is equivalent to the variety of all vector spaces over R (see [6], § 2).

b) For $n > 1$, \mathcal{A} has no essentially n -ary polynomials.

Let F_2 be again the \mathcal{A} -free algebra freely generated by x and y . Define on F_2 an equivalence \sim as follows: for $a, b \in F_2$, let $a \sim b$ if $[a] \cap \{x, y\} = [b] \cap \{x, y\}$. We shall prove that \sim is a fully invariant congruence on F_2 .

Since all operations in \mathcal{A} are essentially no more than unary, the set of translations of F_2 is the same as that of its (polynomial) operations. The last ones commute pairwise, whence it follows that all translations of F_2 are endomorphisms. Thus, it is enough to prove that \sim is invariant under endomorphisms.

Let $C_x = \{a \mid a \in F_2, [a] \cap \{x, y\} = \{x\}\}$. Define C_y similarly; and let $C_0 = \{a \mid a \in F_2, [a] \cap \{x, y\} = \emptyset\}$. Then all the blocks of \sim are C_x, C_y, C_0 and none of them may be void. Indeed, if $[a] \cap \{x, y\} = \{x, y\}$, then let, e.g., $a = t(x)$, where t is a polynomial. For suitable polynomial r we have $r(a) = y$, whence $r(t(x)) = y$, showing that \mathcal{A} is trivial, a contradiction. On the other hand, $x \in C_x, y \in C_y$ and $0 \in C_0$. Remark that $C_x \subseteq [x]$ and $C_y \subseteq [y]$.

In the following, l, k, q, r, s, t, u denote (unary) polynomials. Consider an arbitrary endomorphism φ of F_2 . First we show that φ maps C_0 into itself. Let $l(x) \in C_0$ and suppose $l(x)\varphi \in C_x$. Then for a suitable k we have $k(l(x)\varphi) = x$, whence $k(l(x\varphi)) = x$. If $x\varphi = q(x)$, then, by the Abelian property, $k(q(l(x))) = k(l(q(x))) = x$ holds showing that $l(x) \in C_x$, a contradiction; and if $x\varphi = q(y)$, then $k(l(q(y))) = x$ and \mathcal{A} is trivial, in contrast to the assumption. Supposing that $l(x)\varphi \in C_y$ we get a contradiction analogously.

Let now $l(x) \in C_x$ and suppose $l(x)\varphi \in C_x$. Consider an arbitrary element $r(x)$ from C_x ; we must prove that $r(x)\varphi \in C_x$. For suitable s, t we have $s(l(x\varphi)) = x$ and $t(r(x)) = x$. Hence $s(l(t(r(x)\varphi))) = s(l(t(r(x\varphi)))) = t(r(s(l(x\varphi)))) = x$, and thus $r(x)\varphi \in C_x$. Suppose that $l(x)\varphi \in C_y$ and $u(l(x)\varphi) = y$. Let r and t be as above; then $u(l(t(r(x)\varphi))) = t(r(u(l(x)\varphi))) = t(r(y)) = y$, whence $r(x)\varphi \in C_y$. These considerations show also that $l(x)\varphi \in C_0$ implies $r(x)\varphi \in C_0$.

We got that \sim is a fully invariant congruence in F_2 with three blocks. By virtue of Lemma 3, \sim is the equality, and so $F_2 = \{x, y, 0\}$, i.e., \mathcal{A} has no other operations than 0. Hence \mathcal{A} is the variety of pointed sets.

II. \mathcal{A} is idempotent.

Let us consider for a moment the case in which, for some $n > 1$, \mathcal{A} has an essentially n -ary (polynomial) operation. Suppose that n is minimal; it can be shown that $n \leq 3$. For this aim it suffices to repeat the consideration we made at the beginning of section a) with the only deviation that we must write x_2 instead of 0.

Hence we shall distinguish three subcases.

α) \mathcal{A} has an essentially binary polynomial.

Let f be such a polynomial; we shall write it multiplicatively. Again F_2 denotes the \mathcal{A} -free algebra with free generators x and y . Introduce a relation \sim on F_2 : for $a, b \in F_2$, let $a \sim b$ if there exist elements $u, a_1, b_1 \in F_2$ such that $a = ua_1, b = ub_1$ hold. Obviously, \sim is reflexive and symmetric; we show that it is also transitive. It suffices

to prove that if $ab=cd$ ($a, b, c, d \in F_2$) then for any $p \in F_2$ the equation

$$(4) \quad ap = cz$$

has a solution for z in F_2 . From Lemma 4 we get

$$rs = h_f(s, r, ss) = h_f(s, r, s)$$

and

$$(rs)t = h_f(r, rs, rt) = h_f(rr, rs, rt) = h_f(r, r, r) \cdot h_f(r, s, t) = r \cdot h_f(r, s, t).$$

Using these equalities as well as idempotency and permutability of operations in \mathcal{A} one can compute ap as follows:

$$\begin{aligned} ap &= h_f(b, a, bp) = h_f(b, a, h_f(p, b, p)) = \\ &= h_f(h_f(b, b, b), h_f(a, a, a), h_f(p, b, p)) = \\ &= h_f(h_f(b, a, p), h_f(b, a, b), h_f(b, a, p)) = (ab) \cdot h_f(b, a, p) = \\ &= (cd) \cdot h_f(b, a, p) = c \cdot h_f(c, d, h_f(b, a, p)). \end{aligned}$$

Thus, $z = h_f(c, d, h_f(b, a, p))$ is a solution of (4). Hence \sim is an equivalence. Moreover, \sim is a fully invariant congruence on F_2 ; indeed, for any m -ary polynomial g and elements $a_i, b_i, u_i \in F_2$ ($i=1, \dots, m$) we have $g(u_1 a_1, \dots, u_m a_m) = g(u_1, \dots, u_m) \cdot g(a_1, \dots, a_m) \sim g(u_1, \dots, u_m) \cdot g(b_1, \dots, b_m) = g(u_1 b_1, \dots, u_m b_m)$, and for arbitrary endomorphism φ of F_2 from $a \sim b$ it follows $a\varphi = u\varphi \cdot a_1 \varphi \sim u\varphi \cdot b_1 \varphi = b\varphi$.

By Lemma 3, the congruence \sim is trivial, and, since f is essentially binary, \sim is the complete relation. Hence $x \sim y$ in F_2 . This means that, for a suitable binary polynomial l , in F_2 the equality $x \cdot l(x, y) = y$ holds. Furthermore, $l(x, xy) = l(xx, xy) = l(x, x) \cdot l(x, y) = x \cdot l(x, y) = y$ is also fulfilled. An analogous consideration shows that, for some binary polynomial r , the equalities $r(x, y) \cdot y = x$, $r(xy, y) = x$ hold.

Since these equalities may be considered as identities in \mathcal{A} , we see that the algebras in \mathcal{A} are quasigroups with respect to polynomials f, l, r as multiplication, left and right division, respectively. Hence \mathcal{A} is a regular variety [7]. Now Theorem 3 in [8] gives that \mathcal{A} is equivalent to the variety of affine spaces over some field.

β) \mathcal{A} has no essentially binary polynomials, but it has an essentially ternary polynomial.

Let f be essentially ternary and consider the polynomial $t = h_f(\varepsilon_3^2, \varepsilon_3^2, \varepsilon_3^1)$. We show that in \mathcal{A} the identity $h_t(x, y, x) = h_t(x, x, y) = y$ holds (i.e., \mathcal{A} is a normal variety). Take the \mathcal{A} -free algebra F_3 with free generators x, y and z . By the assumption, $h_f(\varepsilon_3^1, \varepsilon_3^1, \varepsilon_3^2)$ is essentially at most unary, and by the idempotency, it is a projection. But $f(x, y, z) = h_f(x, x, f(x, y, z))$ shows that $h_f(\varepsilon_3^1, \varepsilon_3^1, \varepsilon_3^2) = \varepsilon_3^1$ is impossible. Hence $h_f(\varepsilon_3^1, \varepsilon_3^1, \varepsilon_3^2) = \varepsilon_3^2$, and $h_t(x, y, x) = h_t(x, y, t(x, x, x)) = t(y, x, x) = h_f(x, x, y) = y$.

On the other hand, t is also essentially ternary. Indeed, in the opposite case h_f were a projection, which is impossible because of (1). Repeating the consideration made for h_f before, we get $h_t(x, x, y) = y$.

Introducing now the binary algebraic operation $a+b = h_t(x_0, a, b)$ on the countably generated \mathcal{A} -free algebra $F_\omega (= \langle x_0, x_1, \dots \rangle)$, we can proceed similarly as in the proof of Theorem 1 in [8] to prove that \mathcal{A} is equivalent to the variety of affine modules over some ring R . Note that the main identity marked with (3) in [8] is an immediate consequence of the Abelian property of \mathcal{A} here. Moreover, \mathcal{A} is equivalent to the variety of affine spaces over the field R , because \mathcal{A} is equationally complete and Abelian (see Theorem 4 in [8]).

γ) For $n > 1$, \mathcal{A} has no essentially n -ary polynomials.

Then, evidently, \mathcal{A} is equivalent to the variety of sets. The proof is complete.

Corollary follows directly from GIVANT's characterization of categorically free varieties [10] and our theorem.

Remarks 1. As we have seen, in varieties of modules as well as of affine modules the congruences and subalgebras are amicable. This is the case also in varieties of modules over semigroups (see [1], p. 55) with unit and zero element. Groups, rings and lattices furnish no other varieties with the considered property (abelian groups and zero rings are equivalent to modules).

2. Section β) together with Remark 4 in [9] enables us to give another characterization for ALIEV's variety of S^* -algebras [4]. Namely, if an equationally complete Abelian variety \mathcal{S} , in which congruences and subalgebras are amicable, has no binary polynomials, but has an essentially at least ternary polynomial, then \mathcal{S} is equivalent to the variety of S^* -algebras.

References

- [1] P. M. COHN, *Universal Algebra*, Harper & Row (1956).
- [2] A. G. KUROV, *General Algebra* (Lecture Notes), Moscow State University (1970). (Russian)
- [3] S. MAC LANE, G. BIRKHOFF, *Algebra*, Macmillan (1967).
- [4] I. S. O. ALIEV, On the minimal variety of symmetric algebras, *Algebra i Logika*, 5: 6 (1966), 5—14. (Russian)
- [5] B. CSÁKÁNY, Primitive classes of algebras which are equivalent to classes of semi-modules and modules, *Acta Sci. Math.*, 24 (1963), 157—164. (Russian)
- [6] B. CSÁKÁNY, Abelian properties of primitive classes of universal algebras, *Acta Sci. Math.* 25 (1964), 202—208. (Russian)
- [7] B. CSÁKÁNY, Characterizations of regular varieties, *Acta Sci. Math.*, 31 (1970), 187—189.
- [8] B. CSÁKÁNY, Varieties of affine modules, *Acta Sci. Math.*, 37 (1975), 3—10.
- [9] B. CSÁKÁNY—L. MEGYESI, Varieties of idempotent medial quasigroups, *Acta Sci. Math.*, 37 (1975), 17—23.
- [10] S. R. GIVANT, A representation theorem for universal classes of algebras in which all members are free, *Notices AMS*, 19 (1972), A—767.
- [11] L. KLUKOVITS, On commutative universal algebras, *Acta Sci. Math.*, 34 (1973), 171—174.
- [12] L. KLUKOVITS, Hamiltonian varieties of universal algebras, *Acta Sci. Math.*, 37 (1975), 11—15.

(Received September 28, 1973)