Acta Sci. Math., 41 (1979), 119—125

Affine algebras in congruence modular varieties

CHRISTIAN HERRMANN

Algebras which are polynomially equivalent to a module have been characterized by CSÁKÁNY [3], [4] in terms of the associated system of congruence classes. Recently, SMITH [10] and GUMM [7] characterized such algebras within congruence permutable classes following the lines of "Remak's Principle", cf. [2, p. 167]. In this note their results will be extended to congruence modular classes.

Definition. A (general) algebra A is called *abelian* if in the congruence lattice of $A\times A$ there exists a common complement of the kernels of the two projections.

Theorem. *Every abelian algebra in a congruence modular variety is polynomially equivalent to a module over a suitable ring. The abelian algebras form a subvariety.*

Here the polynomial equivalence of two algebras with the same base set means that the sets of their algebraic functions coincide.

Corollary A. *Let $\mathscr{A}$ and $\mathscr{B}$ be subvarieties of a congruence modular variety, $\mathscr{A}$ abelian and $\mathscr{B}$ congruence distributive. Then every algebra in the join of $\mathscr{A}$ and $\mathscr{B}$ is a direct product of an algebra in $\mathscr{A}$ and an algebra in $\mathscr{B}$.*

Now, the finite base theorems of BAKER [1] and MCKENZIE [9] join into one.

Corollary B. *There exists a finite equational base for every congruence modular variety which is generated by finitely many finite algebras each of which is either abelian or generates a congruence distributive subvariety.*

The idea of the proof can be easily stated: For an abelian group A the difference is a homomorphism of A^2 onto A which has the diagonal $D=\{(x, x)\,|\,x\in A\}$ as its kernel. Thus, the group structure can be recovered from the natural homomorphism $A^2\to A^2/D$ via the identification $x\mapsto(x, 0)+D$ of A and A^2/D. In general,

Received August 1, 1977.

it is still true that an abelian algebra has a congruence $\varkappa$ which has D as a class — cf. HAGEMANN and HERRMANN [8] — and we may define the difference by the natural homomorphism $A^2 \to A^2/\varkappa$. Assume for a moment that 0 is an idempotent element of A. Then $x \mapsto [(x, 0)]\varkappa$ is an embedding of A into $A^2/\varkappa$ but not necessarily onto. Therefore, a limit construction is used to embed A into an algebra B which is closed under the group operations. Using DAY's [5] terms for congruence modularity one sees that A is a subgroup, too.

1. The centring congruence. The proofs rely on results of HAGEMANN and HERRMANN [8]. Thus, a general assumption to be made is that the algebras are *strictly modular* which means that every "diagonal" subdirect product $B \subseteq A^n$ — with n finite, $(x, \ldots, x) \in B$ for all x in A — is congruence modular. We write xy for pairs, $xyzu$ for quadruples, $[a]\alpha$ for the congruence class of a modulo α. Let η_0, η_1 denote the kernels of the two projections of A^2 onto A.

Proposition 1. *A strictly modular algebra A is abelian if and only if there is a congruence $\varkappa$ on A^2 such that*

(C) $\eta_0 \cap \varkappa = \eta_1 \cap \varkappa = 0$

(RR) $xx\varkappa uu$ *for all x and u in A.*

If A is abelian then $\varkappa = \zeta(A)$ is uniquely determined and it holds

(RS) $xy\varkappa uv$ *implies* $yx\varkappa vu$

(RT) $xy\varkappa uv$ *and* $yz\varkappa vw$ *imply* $xz\varkappa uw$

(SW) $xy\varkappa uv$ *if and only if* $xu\varkappa yv$.

Proof. Everything but (SW) is shown in [8], Thm. 1.4 and Prop. 1.6. Now, define λ by $xy\lambda uv$ if and only if $xu\varkappa yv$. Due to (RR), (RS) and (RT) λ is a congruence on A^2. Since $\varkappa$ is reflexive it satisfies (RR). Finally, assume $xy\lambda xv$, i.e. $xx\varkappa yv$. By (RR) we have $yy\varkappa xx$, hence $yy\varkappa yv$ and $y = v$ by (C). This proves $\eta_0 \cap \lambda = 0$ and, by symmetry, $\eta_1 \cap \lambda = 0$. By the uniqueness of $\varkappa$ it follows $\varkappa = \lambda$ which means (SW).

Lemma 2. *Let A be strictly modular and abelian, $\varkappa = \zeta(A)$. Then $A^2/\varkappa$ is strictly modular and abelian, too, and with $\lambda = \zeta(A^2/\varkappa)$ it holds for all a, b, c, e in A*

$$([ae]\varkappa, [be]\varkappa)\lambda([ab]\varkappa, [ee]\varkappa) \tag{1}$$

$$([ae]\varkappa, [bc]\varkappa)\lambda([ce]\varkappa, [ba]\varkappa). \tag{2}$$

Proof. Consider A^4 and let $\Theta_0, \Theta_1, \Theta_2, \Theta_3$ be the kernels of the projections. For each $i < j$ there is a "copy" $\varkappa_{ij}$ of $\varkappa$ on A^4 given by

$$x_0 x_1 x_2 x_3 \varkappa_{ij} y_0 y_1 y_2 y_3 \quad \text{if and only if} \quad x_i x_j \varkappa y_i y_j.$$

Because of $\varkappa_{01} \supseteq \Theta_0 \cap \Theta_1$ and $\varkappa_{23} \supseteq \Theta_2 \cap \Theta_3$ both permute and have join 1. Therefore, the map φ with $\varphi(x_0 x_1 x_2 x_3) = ([x_0 x_1]\varkappa, [x_2 x_3]\varkappa)$ is a homomorphism of

A^4 onto C^2 where $C=A^2/\varkappa$. Its kernel is $\varepsilon=\varkappa_{01}\cap\varkappa_{23}$. We claim that the image of $\mu=\varepsilon+\varkappa_{12}\cap\varkappa_{03}$ is the congruence $\zeta(C)$ on C^2. We have to show

$$\varkappa_{01}\cap\mu=\varkappa_{23}\cap\mu=\varepsilon \quad \text{and} \quad xxxx\mu uuuu \quad \text{for all } x \text{ and } u \text{ in } A.$$

The second is obvious. By modularity we get $\varkappa_{01}\cap\mu=\varepsilon+\varkappa_{01}\cap\varkappa_{12}\cap\varkappa_{03}$. Now, consider $x_0x_1x_2x_3\varkappa_{01}\cap\varkappa_{12}\cap\varkappa_{03}y_0y_1y_2y_3$. By (RS) we have $x_2x_1\varkappa y_2y_1$ and $x_1x_0\varkappa y_1y_0$, hence $x_2x_0\varkappa y_2y_0$ by (RT). With $x_0x_3\varkappa y_0y_3$ and a second application of (RT) it follows $x_2x_3\varkappa y_2y_3$. This shows $x_0x_1x_2x_3\varkappa_{23}y_0y_1y_2y_3$, i.e. $\varkappa_{01}\cap\varkappa_{12}\cap\cap\varkappa_{03}\subseteq\varkappa_{23}$ and $\varkappa_{01}\cap\mu=\varepsilon$. $\varkappa_{23}\cap\mu=\varepsilon$ follows by symmetry.

By Proposition 1 the image of μ has properties (RT) and (SW), i.e.

(3) $\quad xyuv\mu abcd$ and $uvst\mu cdef$ imply $xyst\mu abef$, and

(4) $\quad xyuv\mu abcd$ if and only if $xyab\mu uvcd$.

On the other hand, all the arguments about μ remain valid if we interchange $\varkappa_{01}$ and $\varkappa_{23}$ with $\varkappa_{12}$ and $\varkappa_{03}$. In particular, property (SW) reads then

(5) $\quad xyuv\mu abcd$ if and only if $byuc\mu axvd$.

Moreover, recall that $\varkappa$ is reflexive and satisfies (RR). Thus, since $\mu\supseteq\varkappa_{01}\cap\varkappa_{23}$ and $\mu\supseteq\varkappa_{12}\cap\varkappa_{03}$, we have

(6) $xxuv\mu aauv$, (7) $xyuu\mu xycc$, (8) $xyux\mu ayua$, (9) $xyyv\mu xbbv$.

Now, we are ready to prove (1): $aaba\mu babb$ holds by (8) and $baaa\mu bbba$ by (9) whence $aaaa\mu baba$ by (3). $eeaa\mu aaaa$ holds by (6) and it follows $eeaa\mu baba$ by the transitivity of μ. An application of (5) yields $aeab\mu beaa$. Since $beaa\mu beee$ by (7) one concludes $aeab\mu beee$ by the transitivity of μ. Thus, $aebe\mu abee$ by (4). To prove (2) substitute in $aaaa\mu baba$ b by c to get $aaaa\mu caca$. By (6) it holds $eeaa\mu aaaa$ and by (7) $eebb\mu eeaa$ whence $eebb\mu caca$ by the transitivity of μ. Thus, $aebc\mu ceba$ by (5).

2. Embedding into a "linear" algebra. Call an algebra A *linear* — with respect to an abelian group structure $(A, +, -, 0)$ on A — if 0 is an idempotent element of A and if "$-$" (and "$+$") are homomorphisms of A^2 into A. Linear algebras are just reducts of modules: If A is linear let R be the set of all unary functions on A which are induced by terms in the language of A with 0 added as a constant. With pointwise addition and with composition R becomes a unitary ring. Its operation on A makes A a faithful unitary R-module A_R. Given any fundamental operation f of A one has

$$f(x_1 \dots x_n)=f(x_1 0 \dots 0)+\dots+f(0 \dots 0x_n),$$

i.e. f is described by a term in the language of A_R — cf. Smith [10]. For a class

$\mathscr{C}$ of algebras let $\mathbf{D}\mathscr{C}$, $\mathbf{H}\mathscr{C}$, $\mathbf{S}\mathscr{C}$, $\mathbf{P}_s^f\mathscr{C}$ denote the class of all direct unions, homomorphic images, subalgebras, and finite subdirect products of algebras in $\mathscr{C}$ resp.

Lemma 3. *Let A be a strictly modular abelian algebra having an idempotent element* 0. *Then A can be embedded into an algebra B in $\mathbf{DHP}_s^f A$ which is linear with respect to an abelian group* $(B, +, -, 0)$.

Proof. In view of Lemma 2 we may define a series of strictly modular abelian algebras:

$$A_0 = A, \quad A_{n+1} = A_n^2/\zeta(A_n).$$

Let π_n be the canonical homomorphism of A_n^2 onto A_{n+1}. Clearly, for every n, $0_{n+1}=$ $=[xx]\zeta(A_n)$ is an idempotent element of A_{n+1}. Thus, with $0_0=0$ and $\varepsilon_n x=$ $=[x0]\zeta(A_n)$ one gets due to (C) for every n an embedding $\varepsilon_n\colon A_n\to A_{n+1}$ such that $\varepsilon_n 0_n=0_{n+1}$. Let A_∞ be the direct union over the system (A_n, ε_n) and identify A_n with its image in A_∞. Applying Lemma 2(1) to A_n we see that for each n $\varepsilon_{n+1}\circ\pi_n=\pi_{n+1}\circ(\varepsilon_n\times\varepsilon_n)$. Therefore, $a-b=\pi_n(a, b)$ if a and b are in A_n, defines a map of A_∞^2 into A_∞. By definition it is compatible with the fundamental operations of A_∞ and it holds $a-0=a$, $a-a=0$. Moreover, by Lemma 2(2) it follows $a-(b-c)=c-(b-a)$. Thus, with $a+b=a-(0-b)$ one gets an abelian group structure on A_∞ which makes it linear.

3. Using the Day terms. For all of the following suppose that we work within a fixed congruence modular variety $\mathscr{V}$. Then, due to Day [5] there are a number n and 4-variable terms $m_0, \ldots, m_n$ in the language of $\mathscr{V}$ such that the following identities hold in $\mathscr{V}$:

(m1) $m_0(xyzu) = x$ and $m_n(xyzu) = y$,

(m2) $m_i(xxzz) = x$ for all $i = 0, \ldots, n$,

(m3) $m_i(xyzz) = m_{i+1}(xyzz)$ for i even,

(m4) $m_i(xyxy) = m_{i+1}(xyxy)$ for i odd.

We define by induction $p_0(xzu)=x$,

$$p_{i+1}(xzu) = \begin{cases} m_{i+1}(p_i(xzu), p_i(xzu), u, z) & \text{for } i \text{ even}, \\ m_{i+1}(p_i(xzu), p_i(xzu), z, u) & \text{for } i \text{ odd}. \end{cases}$$

Obviously, in $\mathscr{V}$ it holds $p_i(xzz)=x$ for all i. Put $p(xzu)=p_{n-1}(xzu)$. Then $p(xzz)=x$ holds in $\mathscr{V}$.

Call an algebra A *affine* if it is polynomially equivalent to a linear algebra A^∇ or, in other words, if there is an abelian group structure $(A, +, -, 0)$ on A

such that for every fundamental operation f of A there is an f^{∇} linear with respect to $(A, +, -, 0)$ such that

$$f(x_1 \dots x_n) = f^{\nabla}(x_1 \dots x_n) + f(0 \dots 0).$$

Lemma 4. *In an affine algebra $A \in \mathscr{V}$ it holds $p(xzu) = x - z + u$.*

Proof. Since A is polynomially equivalent to an R-module A_R for each $i = 0, \dots, n$ there are $\alpha_i, \beta_i, \gamma_i, \delta_i$ in R and c_i in A such that

$$m_i(xyzu) = \alpha_i x + \beta_i y + \gamma_i z + \delta_i u + c_i$$

holds in A. $(m2)$ yields $0 = m_i(0000) = c_i$, $x = m_i(xx00) = (\alpha_i + \beta_i)x$, and $0 = m_i(00zz) = (\gamma_i + \delta_i)z$. Since A_R is faithful it follows $\alpha_i + \beta_i = 1$ and $\gamma_i + \delta_i = 0$. In particular, we get

$$m_i(xxvw) = x - \delta_i v + \delta_i w \quad \text{for} \quad i = 0, \dots, n.$$

By induction one concludes

$$p_k(xzu) = x - \sum_{i=1}^{k} (-1)^i \delta_i z + \sum_{i=1}^{k} (-1)^i \delta_i u. \tag{10}$$

On the other hand, $(m1)$ yields $0 = m_0(0y00) = \beta_0 y$ and $0 = m_0(000u) = \delta_0 u$, as well as $0 = m_n(000u) = \delta_n u$ and $y = m_n(0y00) = \beta_n y$ whence $\beta_0 = \delta_0 = \delta_n = 0$ and $\beta_n = 1$. Finally, $(m3)$ and $(m4)$ imply $\beta_i y = m_i(0y00) = m_{i+1}(0y00) = \beta_{i+1} y$ for i odd and $(\beta_i + \delta_i)y = m_i(0y0y) = m_{i+1}(0y0y) = (\beta_{i+1} + \delta_{i+1})y$ for i even. Thus, it holds $\beta_{i+1} = \beta_i$ for i odd and $\beta_{i+1} = \beta_i + \delta_i - \delta_{i+1}$ for i even. By induction one gets $\beta_k = \beta_{k+1} = \sum_{i=1}^{k} (-1)^i \delta_i$ for k odd. In particular, with $m = n - 1$ if n even and $m = n$ if n odd we have $1 = \beta_n = \sum_{i=1}^{m} (-1)^i \delta_i$. Then with (10) it follows $p(xzu) = x - z + u$.

Corollary 5. *If α is a congruence of $A \in \mathscr{V}$ such that A/α is affine then α permutes with every congruence of A.*

Proof. Let β be a congruence of A and suppose $x\alpha y\beta z$. Then $p(xyz)\beta x$ since $p(xyy) = x$ holds in $\mathscr{V}$ and $p(xyz)\alpha z$ by Lemma 4. Thus, $z\alpha p(xyz)\beta x$.

4. Proof of the Theorem. First, suppose that the abelian algebra $A \in \mathscr{V}$ has an idempotent element 0. Construct the linear algebra $A_\infty \supseteqq A$ according to Lemma 3. By Lemma 4 there is a term $p(xyz)$ in the language of $\mathscr{V}$ such that $p(xyy) = x = p(yyx)$ holds in A_∞. In particular, all subalgebras of A_∞ are congruence permutable and each of the embeddings ε_n is onto: $\eta_1 \circ \varkappa = 1$ implies that for every xy there is uv such that $00\eta_1 uv\varkappa xy$ which means $u0\varkappa xy$. Thus, in fact $A_\infty = A$ and A is linear itself. Since $x - y + z = p(xyz)$ is represented by a term in the language of A we get every term of A_R after joining 0 as a constant. In general, choose an arbitrary element 0 of A and consider the map $\varepsilon\colon A \to A^2/\varkappa$ with $x = [x0]\varkappa$. $A^2/\varkappa$

has the idempotent element $[xx]\varkappa$ hence it is linear by the above. ε is still one-to-one by (C) and in view of Lemma 2 (1) it satisfies

$$f(x_1, \ldots, x_n) = \varepsilon f(x_1, \ldots, x_n) - \varepsilon f(0, \ldots, 0). \tag{11}$$

for every fundamental operation f of A. Hence, it holds

$$p(\varepsilon x, \varepsilon y, \varepsilon z) = \varepsilon p(x, y, z) - \varepsilon p(0, 0, 0) = \varepsilon p(x, y, z) - \varepsilon 0 = \varepsilon p(x, y, z), \tag{12}$$

since p is a term and $\varepsilon 0 = [00]\varkappa$ is the neutral element of the linear algebra $A^2/\varkappa$. Therefore, $\varepsilon(A)$ is closed under the operation $p(xyz) = x - y + z$ and an abelian group with zero $0 = \varepsilon 0$, $x + z = p(x0z)$, and $x - y = p(xy0)$. If we transfer the group operations via ε^{-1} to A then (11) states that A is affine. Moreover, by (12) we have $p(xyz) = x - y + z$ on A. Indeed, A and A^2 are congruence permutable and ε is an onto map, too. Moreover, the full module structure of A_R can be recovered from A after adding the constant 0.

That the abelian algebras in a congruence modular variety form a subvariety is obvious by Proposition 1. As a defining set of identities one can use $p(xyy) = p(yyx) = x$ and the identities expressing the compatibility of p and the fundamental operations of $\mathscr{V}$; cf. GUMM [7].

5. Proof of Corollary A. First, observe that $\mathscr{A}$ and $\mathscr{B}$ have only the trivial algebra in common. Every algebra in the join of $\mathscr{A}$ and $\mathscr{B}$ is a homomorphic image C/Θ of a subdirect product $C \subseteq A \times B$ with $A \in \mathscr{A}$ and $B \in \mathscr{B}$. Let α and β denote the kernels of the projections of C onto A and B, respectively. Since $C/\alpha + \beta$ is in both $\mathscr{A}$ and $\mathscr{B}$ it must hold $\alpha + \beta = 1$. Then, by Corollary 5, C is the direct product of A and B.

Since B generates a congruence distributive variety, β is a neutral element of the congruence lattice of C (see [8, Thm. 4.1]) which implies $\Theta = \Theta + \alpha \cap \beta = (\Theta + \alpha) \cap \cap (\Theta + \beta)$. Thus, C/Θ is itself a subdirect product of an algebra in $\mathscr{A}$ and one in $\mathscr{B}$ and, by the above argument, even a direct product.

6. Proof of Corollary B. Let $\mathscr{C}$ be congruence modular and generated by finite algebras $A_1, \ldots, A_n, B_1, \ldots, B_m$ where each A_i is abelian and each B_i generates a congruence distributive subvariety. Let $\mathscr{A}$ and $\mathscr{B}$ be the subvarieties generated by the $A_1, \ldots, A_n$ and the $B_1, \ldots, B_m$, respectively. Then $\mathscr{B} = \mathbf{DHP}_s^f\mathbf{S}\{B_1, \ldots, B_m\}$ is congruence distributive due to [8, Cor. 4.3] and has a finite equational base due to BAKER [1]. The variety $\mathscr{A}$ is polynomially equivalent (via finitely many constants) to the variety of all modules over a fixed ring R: take the free algebra on countably many generators in $\mathscr{A}$ and apply the Theorem. Since $\mathscr{A}$ is locally finite, R has to be finite. Thus, $\mathscr{A}$ has a finite equational base, too.

By Corollary A $\mathscr{A}$ and $\mathscr{B}$ are independent in the sense of GRÄTZER, LAKSER, and PŁONKA [6, Thm. 2]. In particular, one can define predicates for the congruences

which yield the direct product decomposition. Therefore, $\mathscr{C}=\mathscr{A}\vee\mathscr{B}$ is finitely axiomatizable, i.e. it has a finite equational base.

The author wishes to express his warmest thanks to the J. Bolyai Society and to B. Csákány and A. P. Huhn for inviting him to Szeged, the most appropriate place where to write this paper.

Added in March 78. Since several reformulations of our Theorem have been discovered meanwhile it seems necessary to add the following

Scholion. *For a strictly modular algebra A the following are equivalent:*
(1) *A is abelian.*
(2) *For the commutator introduced in* [8] *it holds* $[1_A, 1_A]=0_A$.
(3) *The diagonal D is a congruence class of $A\times A$.*

Implications (1)$\Rightarrow$(2), (2)$\Rightarrow$(1), and (2)$\Leftrightarrow$(3) are instances of Thm. 1.4, Observation 1.2, and Cor. 2.4 in [8] respectively. Moreover, using Cor. 1.2 it is easily seen that for projective quotients α/β and γ/δ $[\gamma,\gamma]\subseteq\delta$ implies $[\alpha,\alpha]\subseteq\beta$. Thus, by Thm. 1.4 A is abelian if there is B and $\alpha\in\mathrm{con}\,(B)$ such that $B/\beta\cong A$ and $1_B/B$ is projective to a quotient of a sublattice of $\mathrm{con}\,(B)$ which is isomorphic to the 5-element lattice M_3.

References

[1] K. Baker, Finite equational bases for finite algebras in a congruence distributive equational class, *Advances in Math.*, **24** (1977), 207—243.
[2] G. Birkhoff, *Lattice Theory*, 3rd ed., Amer. Math. Soc. (Providence, 1967).
[3] B. Csákány, Abelian properties of primitive classes of universal algebras, *Acta Sci. Math.*, **25** (1964), 202—208. (Russian).
[4] B. Csákány, Varieties of affine modules, *Acta Sci. Math.*, **37** (1975), 3—10.
[5] A. Day, A characterization of modularity for congruence lattices of algebras, *Canad. Math. Bull.*, **12** (1969), 167—173.
[6] G. Grätzer—H. Lakser—J. Płonka, Joins and direct products of equational classes, *Canad. Math. Bull.*, **12** (1969), 741—744.
[7] H. P. Gumm, Algebras in congruence permutable varieties: geometrical properties of affine algebras, *Algebra Universalis*, **9** (1979), 8—34.
[8] J. Hagemann—C. Herrmann, A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity, *Arch. Math. (Basel)*, to appear.
[9] R. McKenzie, Para primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties, *preprint*.
[10] J. D. H. Smith, *Mal'cev varieties*, Springer Lecture Notes 554 (Berlin, 1976).

DEPARTMENT OF MATHEMATICS
TECHNICAL UNIVERSITY OF DARMSTADT
HOCHSCHULSTRASSE 1
61 DARMSTADT, GFR