Reprint from

algebra universalis

Vol. 9, fasc. 1, 1979 pages 8–34

Algebras in permutable varieties: Geometrical properties of affine algebras

H. Peter Gumm

BIRKHÄUSER VERLAG BASEL

Algebra Universalis, **9** (1979) 8–34 Birkhäuser Verlag, Basel

Algebras in permutable varieties: Geometrical properties of affine algebras

H. Peter Gumm

Introduction

If $\mathbf{V}$ is a congruence permutable variety then every finite simple algebra $\mathbf{A} \in \mathbf{V}$ is either functionally complete or $\mathbf{A} \times \mathbf{A}$ has a skew congruence, see Werner [22]. In this case the skew congruence together with the projection congruences generate a 0-1-sublattice of $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ which is isomorphic to the lattice $\mathcal{M}_3$.

We use a geometric approach to study this situation, which is inspired by the methods introduced in Wille [24]. Although the geometric structure we obtain is very elementary it turns out that the geometric approach is very suggestive and easy to handle to give us interesting algebraic results.

In particular we can coordinatize the geometry by an abelian group so that the algebra $\mathbf{A}$ becomes functionally or even polynomially equivalent to a module over a ring $\mathbf{R}$.

The interplay between geometry and algebra is developed in Chapters 1 through 5 and the central result, Theorem 4.7 is then applied in Chapters 6 and 7 to prove theorems classifying various algebras in permutable varieties and to give unified proofs to a list of known results.

There are also obvious applications to the theory of functionally complete algebras which have not been included here.

Moreover it is clear from the proofs that in most of the theorems the assumption that the algebras in question generate a permutable variety can be weakened to the requirement that certain congruences admit a Mal'cev-function as defined in 3.1.

§0. Preliminaries

We use standard universal algebra terminology and refer the reader to G. Grätzer [10] for any undefined notion of universal algebra. As a reference to

Presented by G. Grätzer. Received December 15, 1976. Accepted for publication in final form August 24, 1977.

more special algebraic structures appearing in this article we recommend Denes, Keedwell [8] for the notion and basic properties of loops, quasigroups and nets and Birkhoff [2] for lattices, rings and modules.

If $\mathbf{A}=(A, F)$ is a universal algebra, A the base set and F the family of fundamental operations then the operations which can be built up by composition from the operations of F together with the n-ary projections, $n>0$, will be called the *polynomials* of $\mathbf{A}$. $\mathbf{A}^+$ will be the algebra with the same base set as $\mathbf{A}$ and with every element of A added as a 0-ary fundamental operation. The *algebraic functions* of $\mathbf{A}$ are then exactly the polynomials of $\mathbf{A}^+$. Equality of polynomials in the case of polynomials of single algebras will then be equality of maps.

We do not make a distinction between *polynomials* and *polynomial* symbols (see [10]). For a single algebra the maps induced by a polynomial of a variety are exactly the polynomials as described previously. We think there will be no danger of confusion as far as this article is concerned. Two algebras will be called *polynomially equivalent* if they have (up to isomorphy) the same base set and the same set of polynomials. Two varieties are *polynomially equivalent* if their free algebras $F(\omega)$ on the countable generation set $\omega=\{x_1, x_2, \dots\}$ are polynomially equivalent.

A binary relation Θ is *compatible* with an n-ary operation $f: A^n \to A$ if for all $(x_1, y_1), \dots, (x_n, y_n)\in\Theta$ we have that $(f(x_1, \dots, x_n), f(y_1, \dots, y_n))\in\Theta$. We also say "$f$ is compatible with Θ" or "Θ admits f."

Congruences are equivalence relations on A which are compatible with all fundamental operations (equivalently polynomials or algebraic functions) of $\mathbf{A}$. For $(x, y)\in\Theta$ we frequently write $x\Theta y$ or "x is congruent to y modulo Θ."

$\circ$ denotes relational product of congruences. The set of all congruences on an algebra $\mathbf{A}$ forms a lattice $\mathfrak{C}(\mathbf{A})$ with set-inclusion as ordering. The biggest element of this lattice is denoted ι, the smallest ω. These two congruences are frequently called the *trivial congruences*. If $\mathbf{A}_1\times\cdots\times\mathbf{A}_n$ is the direct product of the family of algebras $(\mathbf{A}_i)_{i\in I}$ then the kernels of the canonical projections

$$\mathbf{A}_1\times\cdots\times\mathbf{A}_n\to\mathbf{A}_{k_1}\times\cdots\times\mathbf{A}_{k_r}$$

where $(k_1, \dots, k_r)$ is a subfamily of $(1, \dots, n)$, will be called *factor congruences*.

§1. Permutable varieties and functionally complete algebras

Let Θ and Ψ be congruences on the universal algebra $\mathbf{A}=(A, F)$. The smallest equivalence relation containing Θ and Ψ is itself a congruence relation, denoted

by $\Theta \vee \Psi$. A fortiori $\Theta \vee \Psi$ is the smallest congruence relation containing Θ and Ψ. This congruence can be described in the following way:

$\forall x, y \in A$ $(x, y) \in \Theta \vee \Psi$ iff $\exists n \in N$, $x_0, \ldots, x_n \in A$ s.th. $x = x_0$, $y = x_n$, $\forall i < n$ $x_i \Theta x_{i+1}$ if i even, and $x_i \Psi x_{i+1}$ if i odd.

Or, equivalently, if we define:

$$(\Theta \circ \Psi)^1 := \Theta \circ \Psi, \qquad (\Theta \circ \Psi)^n := (\Theta \circ \Psi)^{n-1} \circ \Theta \circ \Psi,$$

we have:

$$\Theta \vee \Psi = \bigcup \{(\Theta \circ \Psi)^n \mid n \in N\}.$$

DEFINITION 1.1. Let Θ and Ψ be equivalence relations. Θ and Ψ *permute* if $\Theta \circ \Psi = \Psi \circ \Theta$. Let $\mathbf{A} = (A, F)$ be a universal algebra. $\mathbf{A}$ *has permutable congruences* if for any two congruences Θ and Ψ on $\mathbf{A}$ Θ and Ψ permute. If every algebra in a variety $\mathbf{V}$ has permutable congruences then $\mathbf{V}$ will be called a *permutable variety.*

Examples: Groups, Rings, Modules, Boolean algebras have permutable congruences.

The following lemma is well known:

LEMMA 1.2. (i) *Let Θ and Ψ be equivalence relations. Θ and Ψ permute if and only if $\Theta \vee \Psi = \Theta \circ \Psi$.*

(ii) *Let the algebra $\mathbf{A}$ have permutable congruences. Then $\mathfrak{C}(\mathbf{A})$, the lattice of all congruences on $\mathbf{A}$ satisfies the modular law.*

Proof. (i) follows trivially from the foregoing description of $\Theta \vee \Psi$. (ii) can be found in Schmidt [21], II.§9, Satz 2.

One of the main tools for the study of permutable varieties is supplied by the following theorem of A. I. Mal'cev [15].

THEOREM 1.3 (Mal'cev). *Let $\mathbf{V}$ be a variety of universal algebras. $\mathbf{V}$ is a permutable variety if and only if there exists a ternary polynomial p in the language of $\mathbf{V}$ such that the equations*

$$p(x, y, y) = x, \qquad p(x, x, y) = y \tag{$*$}$$

hold in every algebra $\mathbf{A} \in \mathbf{V}$.

The proof of the only-if-direction of this theorem would require many definitions we otherwise do not need in the following so we only show the if-direction.

Let $\mathbf{V}$ be a variety having a ternary polynomial p, satisfying the equations $(*)$ in every algebra of $\mathbf{V}$. Let Θ and Ψ be congruences on an algebra $\mathbf{A}=(A, F)\in\mathbf{V}$. We have to show: $\Theta\circ\Psi=\Psi\circ\Theta$. For $(x, z)\in\Theta\circ\Psi$ we have by definition of $\Theta\ \Psi$ an element $y\in A$ such that $(x, y)\in\Theta$ and $(y, z)\in\Psi$. Since the polynomial p is compatible with Θ and Ψ we have: $x=p(x, y, y)\Psi p(x, y, z)\Theta p(x, x, z)=z$. Thus $(x, z)\in\Psi\ \Theta$ whence $\Theta\circ\Psi\leq\Psi\ \Theta$. Equality now follows by symmetry.

Note that we have not fully made use of the fact that p is a polynomial, we only needed that p is compatible with all the congruences on $\mathbf{A}$ and that p satisfies the equations $(*)$. This is the form in which we will use the above theorem in the sequel, so let us state as a corollary:

COROLLARY 1.4. *Let Θ and Ψ be equivalence relations on a set S. Let p be a ternary operation on S satisfying the equations $(*)$ and let p be compatible with Θ and Ψ. Then Θ and Ψ permute.*

Theorem 1.3 now tells us immediately that the foregoing examples of varieties are permutable varieties. We only have to find a ternary polynomial satisfying $(*)$. For groups take $p(x, y, z):=xy^{-1}z$, for rings and modules: $p(x, y, z):=x-y+z$ and for Boolean algebras: $p(x, y, z):=x'y'z+xy'z'+xyz$.

Of course we may find many more polynomials in Boolean algebras satisfying the equations $(*)$. The reason for this is that the 2-element Boolean algebra $\mathbf{2}$ is *primal* which means that every function $f:\mathbf{2}^n\to\mathbf{2}$ can be expressed by a polynomial. Algebras with a similar "sufficiently rich" structure have been investigated by several authors. Those algebras will be called 'functionally complete.'

DEFINITION 1.5. A finite algebra $\mathbf{A}=(A, F)$ is *functionally complete* if for every $n\in N$ every map $f:A^n\to A$ is an algebraic function.

DEFINITION 1.6. Let S be a set. The *discriminator* on S is the ternary operation $d:S^3\to S$ with

$$d(x, y, z):=\begin{cases}z, & \text{if } x=y\\ x, & \text{if } x\neq y\end{cases}$$

For an algebra $\mathbf{A}=(A, F)$ define a new algebra $\mathbf{A}^+:=(A, F\cup\bar{A})$ which has the same underlying set as $\mathbf{A}$ and the same fundamental operations but additionally

has a nullary operation with value a for every element $a \in A$. We quote a theorem which is due to Pixley [18] and Werner [23]:

THEOREM 1.7. *For a finite algebra* $\mathbf{A}$ *the following conditions are equivalent:*
(i) $\mathbf{A}$ *is functionally complete.*
(ii) *The discriminator on* A *is an algebraic function of* $\mathbf{A}$.
(iii) $\mathbf{A}$ *is simple and* $\mathbf{A}^+$ *generates a permutable and congruence distributive variety.*

If we actually want to find all functionally complete algebras in familiar varieties such as groups, rings or modules another theorem is more useful. We first state a lemma which is an immediate consequence of Corollary 1 in [2], Chapter VII, §4:

LEMMA 1.8. *Let* $\mathbf{A}$ *be an algebra in a permutable variety. If* $\mathbf{A}$ *is a subdirect product of finitely many simple algebras* $\mathbf{A}_1, \ldots, \mathbf{A}_n$ *then* $\mathbf{A}$ *is already isomorphic to a direct product of some of those factors.*

Using this lemma, Quackenbush and Werner proved in [22]:

THEOREM 1.9. *Let* $\mathbf{A}$ *be a finite simple algebra in a permutable variety. If* $\mathbf{A} \times \mathbf{A}$ *has only factor congruences then* $\mathbf{A}$ *is functionally complete.*

For the proof we refer to [22]. A shorter proof than is actually given there can be obtained by combining Theorem 1 of [22] with a lattice theoretical result of Burris [3], Theorem 1.2.

Now suppose $\mathbf{A}$ is a finite simple algebra in a permutable variety and $\mathbf{A}$ is not functionally complete. Then by the above theorem $\mathbf{A} \times \mathbf{A}$ has a congruence Θ which is not a factor congruence. Since $\mathbf{A}$ is simple and since $(\mathbf{A} \times \mathbf{A})/\pi_1 \simeq (\mathbf{A} \times \mathbf{A})/\pi_2 \simeq \mathbf{A}$, the intervals $[\pi_1, \iota]$ and $[\pi_2, \iota]$ in $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ are prime intervals. Since $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ is modular we conclude that the sublattice generated by π_1, π_2 and Θ in $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ is isomorphic to the lattice $\mathcal{M}_3$ given in Fig. 1.
Since the biggest (resp. smallest) element of the lattice $\mathcal{M}_3$ coincides with the biggest (resp. smallest) element of $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ we say that $\mathcal{M}_3$ is a 0-1-*sublattice* of

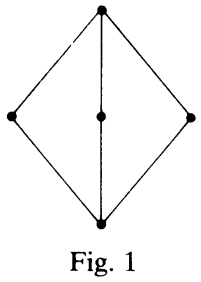

Fig. 1

$\mathfrak{C}(\mathbf{A}\times\mathbf{A})$. Thus $\mathbf{A}\times\mathbf{A}$ has three congruences α_1, α_2, α_3 satisfying:

$$\alpha_i \circ \alpha_j = \iota \quad \text{and} \quad \alpha_i \wedge \alpha_j = \omega, \quad \text{for} \quad 1 \leq i < j \leq 3.$$

This situation will be studied more closely in the following chapter.

§2. Geometric 3-nets and S-3-systems

Let S be a set with more than 3 elements; Θ_1, Θ_2, Θ_3 equivalence relations on S such that

$$\Theta_i \circ \Theta_j = \iota, \quad \text{for} \quad i \neq j. \tag{1}$$

$$\Theta_i \wedge \Theta_j = \omega, \quad \text{for} \quad i \neq j. \tag{2}$$

Then the quadruple $\mathbf{S} := (S, \Theta_1, \Theta_2, \Theta_3)$ *will be called an* S*-3-System.*

It will be useful and more illustrative to introduce a geometrical interpretation as "*Äquivalenzklassengeometrie*" as introduced in Werner [23].

Call the elements of S *points* and the equivalence classes of Θ_1, Θ_2, Θ_3 *lines.* Two lines will be called *parallel* if they are classes of the same equivalence relation. An incidence relation is defined naturally by the membership relation $\in$. We will say "a lies on l" for $a \in l$, where a is a point and l is a line.

LEMMA 2.1. *The Äquivalenzklassengeometrie of an* S*-3-system has the following properties:*

($S1$) *There are* 3 *parallel-classes of lines.*

($S2$) *Each point lies on exactly one line of each parallel-class.*

($S3$) *If* l_1 *and* l_2 *are two non-parallel lines then there is exactly one point which lies both on* l_1 *and on* l_2.

Proof. ($S1$) and ($S2$) are immediately clear. For ($S3$) let l_1 and l_2 be lines of different parallel-classes. Without loss of generality l_1 (resp. l_2) is a parallel class of Θ_1 (resp. Θ_2). Let x and y be arbitrary with $x \in l_1$ and $y \in l_2$. Then by definition $l_1 = [x]\Theta_1$ $(= \{s \in S \mid x\Theta_1 s\})$ and $l_2 = [y]\Theta_2$. Since $\Theta_1 \circ \Theta_2 = \iota$ there is an element $z \in S$ with $x\Theta_1 z \Theta_2 y$, i.e. $z \in l_1$ and $z \in l_2$. Now suppose there is another point u lying on l_1 and on l_2. Then we have $u\Theta_1 z$ and $u\Theta_2 z$, thus $u\Theta_1 \wedge \Theta_2 z$. Since by (2) $\Theta_1 \wedge \Theta_2 = \omega$ we must have $u = z$.

A geometrical structure with the above properties is called a *geometric* 3*-net* in combinatorics. More precisely, a geometric 3-net is a triple $\mathbf{N} := (N, L, \Pi)$ where N is a set with more than 3 elements, $L \subseteq P(N)$ and Π is an equivalence

relation on L such that $(S1)$, $(S2)$ and $(S3)$ are fulfilled with N as the set of points, L the set of lines and Π the relation of parallelism. $\in$ is understood to be the incidence relation.

LEMMA 2.2. *Every geometrical 3-net is the Äquivalenzklassengeometrie of an S-3-system.*

The proof is obvious.

The importance of nets in combinatorics arises from the fact that they give rise to latin squares and thus to quasigroups. More precisely a net defines a class of quasigroups all of which are isotopic and among which there is always a loop, i.e. a quasigroup with a unit element. A quasigroup in turn defines a geometrical 3-net in a very natural way. We are mainly interested in the loop arising from a net, thus by lemmas 2.1 and 2.2 also from an S-3-system, so we will demonstrate this interchanging process in the sequel. For nets this construction can be found in books on combinatorics, we only mention Denes-Keedwell [8].

First let $\mathbf{Q}$ be a quasigroup. Let M_Q be its multiplication table. M_Q can be considered as a $|Q|\times|Q|$-matrix, $M_Q=(a_{ik})$. (We allow $|Q|$ to be infinite.) Let us define now: $S:=Q\times Q$ and define Θ_1, Θ_2 and Θ_3 by

$$\begin{aligned}
&(x, y)\Theta_1(x', y') \quad \text{iff} \quad x = x' \\
&(x, y)\Theta_2(x', y') \quad \text{iff} \quad y = y' \qquad (\dagger) \\
&(x, y)\Theta_3(x', y') \quad \text{iff} \quad x \cdot y = x' \cdot y',
\end{aligned}$$

where $\cdot$ denotes multiplication in the quasigroup $\mathbf{Q}$. Then $\mathbf{S}:=(S, \Theta_1, \Theta_2, \Theta_3)$ is an S-3-system. The corresponding geometrical 3-net is then easily exhibited.

An example will demonstrate what we do:

•	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	4	5	1	2
4	4	5	2	3	1
5	5	3	1	2	4

Fig. 2.1

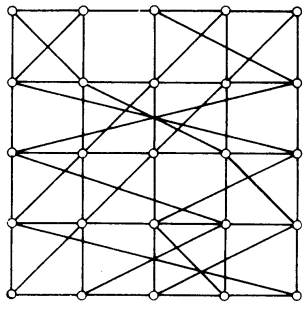

Fig. 2.2

For the inverse process start with an S-3-system $\mathbf{S}=(S, \Theta_1, \Theta_2, \Theta_3)$. The conditions $\Theta_i \circ \Theta_j = \iota$ and $\Theta_i \wedge \Theta_j = \omega$ for $i \neq j$ implies that S is isomorphic as a set to $S_{/\Theta_i} \times S_{/\Theta_j}$ for $i \neq j$. The isomorphisms

$$S_{/\Theta_1} \times S_{/\Theta_2} \simeq S_{/\Theta_2} \times S_{/\Theta_3} \simeq S_{/\Theta_3} \times S_{/\Theta_1}$$

tell us that $S_{/\Theta_1} \simeq S_{/\Theta_2} \simeq S_{/\Theta_3}$. In other words there is a set Q and bijections f_1, f_2, f_3 such that $f_i : S_{/\Theta_i} \to Q$ and a bijection $g : S \to Q \times Q$ given by

$$g(s) = (f_1([s]\Theta_1), f_2([s]\Theta_2)).$$

Now pick an arbitrary element $e \in S$ and an arbitrary element $1 \in Q$. We may suppose we have chosen f_1 and f_2 so that $f_1([e]\Theta_1) = f_2([e]\Theta_2) = 1$ and $g^{-1}(1, x)$ $\Theta_3 g^{-1}(x, 1)$. Define a multiplication $\cdot$ on Q by setting:

(i) $x \cdot 1 = x$

(ii) $x \cdot y = z$ if and only if $g^{-1}(x, y)\Theta_3 g^{-1}(z, 1)$.

Now it can be readily checked that $(Q, \cdot)$ is a quasigroup satisfying $x \cdot 1 = 1 \cdot x = x$, thus $\mathbf{Q} := (Q, \cdot, 1)$ is a loop. Since the map g is an isomorphism we will in the sequel identify $Q \times Q$ and S, so we say that the "multiplication table of $(Q, \cdot, 1)$ is defined on S." By this identification we have then:

$$(x, y)\Theta_1(x', y') \quad \text{iff} \quad x = x',$$
$$(x, y)\Theta_2(x', y') \quad \text{iff} \quad y = y',$$
$$(x, y)\Theta_3(x', y') \quad \text{iff} \quad x \cdot y = x' \cdot y',$$

for all $x, y, x', y' \in Q$.

This guarantees us (compare with condition (†) of the last page) that the S-3-system we obtain by $\mathbf{Q}$ from the previous construction is the same as the S-3-system we started out with to construct our loop.

Again we demonstrate this with an example:

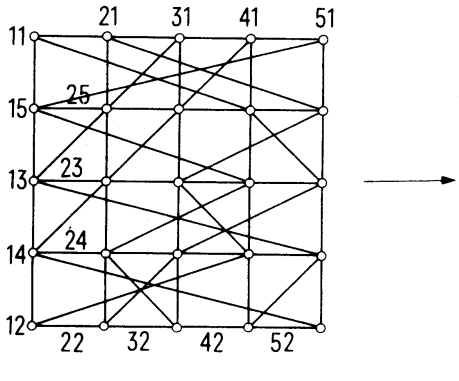

Fig. 2.3

·	1	2	3	4	5
1	1	2	3	4	5
5	5	3	4	1	2
3	3	4	2	5	1
4	4	5	1	2	3
2	2	1	5	3	4

Fig. 2.4

In Fig. 2.3 the labels of the points of the net shall denote their image under g, and Q has been chosen as $\{1, 2, 3, 4, 5\}$.

Let us write down as a result of this chapter:

LEMMA 2.3. *Let* $\mathbf{S}=(S, \Theta_1, \Theta_2, \Theta_3)$ *be an* S*-3-system. Let* e *by an arbitrary element of* S*. Then there exists a loop* $\mathbf{L}=(L \cdot, 1)$ *and a bijection* $g: L\times L\to S$ *such that* $e=g(1, 1)$ *and for arbitrary* $x, y, x', y'\in L$ *we have*

$$(x, y)\Theta_1(x', y') \quad \textit{iff} \quad x=x'$$
$$(x, y)\Theta_2(x', y') \quad \textit{iff} \quad y=y'$$
$$(x, y)\Theta_3(x', y') \quad \text{iff} \quad x\cdot y=x'\cdot y',$$

if we are identifying $L\times L$ *with* S *via the bijection* g.

Note at this point that Θ_3 need not be a congruence on $\mathbf{L}\times\mathbf{L}$.

§3. Compatible functions on S-3-systems

The remarks at the end of §1 together with Theorem 1.9 suggest us to study S-3-systems in the case where S is the underlying set of an algebra $\mathbf{A}$ in a permutable variety and Θ_1, Θ_2 and Θ_3 are congruence relations on $\mathbf{A}$. According to Theorem 1.3 $\mathbf{A}$ has a polynomial p satisfying the equations

$$p(x, x, y)=y,\ p(x, y, y)=x \qquad (*)$$

If Θ_1, Θ_2, Θ_3 are congruences on $\mathbf{A}$ the polynomial p has to be compatible with Θ_1, Θ_2, Θ_3.

DEFINITION 3.1. A ternary operation p satisfying the equations $(*)$ will be called a *Mal'cev-function.*

One key observation for the sequel is given by:

THEOREM 3.2. *Let* $\mathbf{S}=(S, \Theta_1, \Theta_2, \Theta_3)$ *be an* S*-3-system. Let* $p: S^3\to S$ *be a Mal'cev-function compatible with* Θ_1, Θ_2 *and* Θ_3*. Then* p *is uniquely determined.*

Proof. We will prove this theorem in 3 steps. Let us use the description of the net associated with the given S-3-system as introduced in Lemma 2.1. If $x=y$ or $y=z$ then $p(x, y, z)$ is uniquely determined by the equations $(*)$. So we may suppose for now that $x\neq y$ and $y\neq z$.

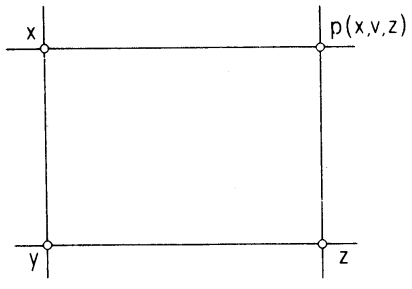

Fig. 3.1

Step 1: x and y lie on a line l_1, y and z lie on a line l_2 and $l_1 \neq l_2$. Then for some $i \neq k$ we have $l_1 = [y]\Theta_i$ and $l_2 = [y]\Theta_k$. Therefore $x\Theta_i y$ and $z\Theta_k y$ hence by compatibility:

$$p(x, y, z)\Theta_i p(x, x, z) = z$$
$$p(x, y, z)\Theta_k p(x, y, y) = x$$

Thus $p(x, y, z)$ lies on the Θ_i-line through z and on the Θ_k-line through x. By condition $(S3)$ in §2 there is exactly one point with this locus.

Step 2: x, y and z lie on a Θ_k-line l. Say $k = 1$. Take a Θ_2 line through y and a Θ_3-line through x. They have exactly one point in common, say x'. Applying the result of step 1, we know that $p(x', y, z)$ is uniquely determined as the "fourth parallelogram-point" for x', y, z. Since y and z are congruent to x modulo Θ_1 and since p is idempotent by $(*)$, we have $x = p(x, x, x)\Theta_1 p(x, y, z)$. Therefore $p(x, y, z) \in [x]\Theta_1 = l$. Since $x\Theta_3 x'$ we get that $p(x, y, z)$ lies on a Θ_3-line through $p(x', y, z)$ and on the Θ_1-line l. Thus by $(S3)$ and the fact that $p(x', y, z)$ is uniquely determined we know that $p(x, y, z)$ is uniquely determined.

Step 3: x, y and z are arbitrary. Let l_1 be a Θ_1-line and l_2 a Θ_2-line. The Θ_2-lines through x, y and z meet l_1 in the points x', y', and z'. The Θ_1-lines through x, y, and z meet l_2 in the points x'', y'', and z''. $p(x', y', z')$ and $p(x'', y'', z'')$ are uniquely determined by step 2 and the equations $(*)$. Since

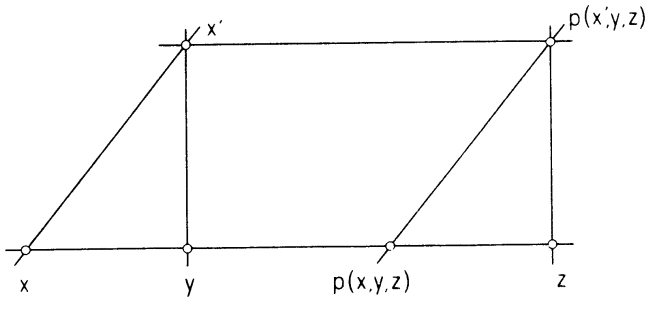

Fig. 3.2

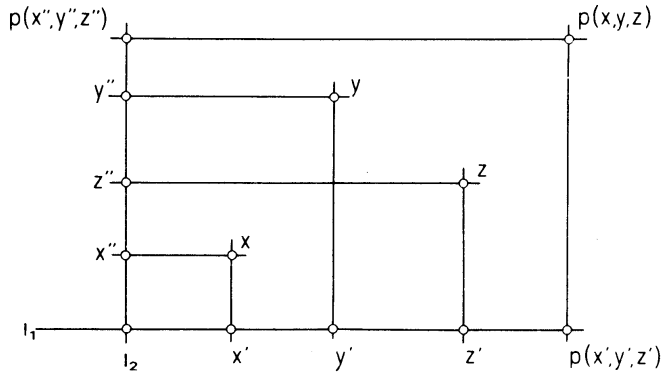

Fig. 3.3

$x\Theta_2 x'$, $y\Theta_2 y'$, and $z\Theta_2 z'$ as well as $x\Theta_1 x''$, $y\Theta_1 y''$, and $z\Theta_1 z''$ we have:

$$p(x, y, z)\Theta_2 p(x', y', z') \text{ and } p(x, y, z)\Theta_1 p(x'', y'', z'')$$

thus $p(x, y, z)$ lies on the Θ_1-line through $p(x'', y'', z'')$ and on the Θ_2-line through $p(x', y', z')$. $p(x, y, z)$ is uniquely determined since $p(x', y', z')$ and $p(x'', y'', z'')$ are and since $(S3)$ holds.
Notice that in step 3 we could have started taking, for example, l_1 and l_2 being Θ_3 and Θ_2 lines respectively. The result, since it is unique, must be the same.

COROLLARY 3.3. *Let* $\mathbf{S}=(S, \Theta_1, \Theta_2, \Theta_3)$ *be an* S*-3-system. Let* p *be a Mal'cev-function on* S *which is compatible with* Θ_1, Θ_2, *and* Θ_3. *Then for all* x, y, $z \in S$ *we have:*

$$p(x, y, z) = p(z, y, x).$$

Proof. Define $\hat{p}$: $S^3 \to S$ by $\hat{p}(x, y, z) := p(z, y, x)$. Then $\hat{p}$ is a compatible Mal'cev-function on S since p was. By theorem 3.2 p is unique, so we must have: $\hat{p} = p$.

LEMMA 3.4. *Let* $\mathbf{S}=(S, \theta_1, \theta_2, \theta_3)$ *be an* S*-3-system and* p *a compatible Mal'cev-function on* S. *Then the loop* $\mathbf{L}$ *associated with* $\mathbf{S}$ *satisfies:*

$$\text{(R)} \qquad \forall x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4\ (x_1 \cdot y_1 = x_2 \cdot y_2 \ \&\ x_1 \cdot y_3 = x_2 \cdot y_4 \ \&\ x_3 \cdot y_1 = x_4 \cdot y_2 \Rightarrow x_3 \cdot y_3 = x_4 \cdot y_4).$$

Proof. Recall that by construction of the loop and by Lemma 2.3 we have: $x \cdot y = x' \cdot y'$ *iff* $(x, y)\Theta_3(x', y')$.

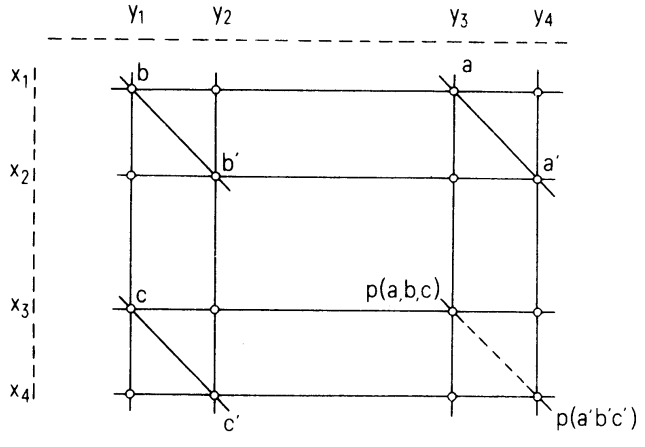

Fig. 3.4

Thus the hypothesis of the statement (R) says: $(x_1, y_1)\Theta_3(x_2, y_2)$, $(x_1, y_3)\Theta_3(x_2, y_4)$ and $(x_3, y_1)\Theta_3(x_4, y_2)$. This implies: $(x_3, y_3) = p((x_1, y_3), (x_1, y_1), (x_3, y_1))\Theta_3 p((x_2, y_4), (x_2, y_2), (x_4, y_2)) = (x_4, y_4)$. Hence $x_3 \cdot y_3 = x_4 \cdot y_4$. Note that p can be computed componentwise since p is compatible with Θ_1 and Θ_2.

The proof is illustrated by the following figure, noting that by step 1 of the proof of Theorem 3.2 p is an operation assigning the fourth parallelogram-point to x, y, z if x, y and y, z lies on two different lines.
The next lemma is well known, compare [8]:

LEMMA 3.5. *A loop* $\mathbf{L}$ *satisfying the condition* (R) *of Lemma* 3.4 *is associative, i.e. a group.*

Proof. For arbitrary $x, y, z \in L$ set $x_1 := y_2 := 1$, $x_2 := y$, $x_3 := x$, $x_4 := x \cdot y$, $y_1 := y$, $y_3 := y \cdot z$, $y_4 := z$.

LEMMA 3.6. *Let the S-3-system* $\mathbf{S}$ *admit the Mal'cev-function p. Let* $\mathbf{L} = (L, \cdot, 1)$ *be the associated loop (which, by the above lemma is a group). Then for arbitrary elements* $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbf{L} \times \mathbf{L}$ *we have:*

$$p((x_1, y_1), (x_2, y_2), (x_3, y_3)) = (x_1 \cdot x_2^{-1} \cdot x_3, y_1 \cdot y_2^{-1} \cdot y_3).$$

Proof. By step 3 in the proof of Theorem 3.2 we have for $x := (x_1, y_1)$, $y := (x_2, y_2)$, $z := (x_3, y_3)$ and $l_1 := [(x_1, y_1)]\Theta_1$ and $l_2 := [(x_1, y_1)]\Theta_2$:

$$x' = (x_1, y_1),\ y' = (x_1, y_2),\ z' = (x_1, y_3)$$

and

$$x'' = (x_1, y_1),\ y'' = (x_2, y_1),\ z'' = (x_3, y_1)$$

thus

$$\begin{aligned} p(x', y', z') &= p((x_1, y_1), (x_1, y_2), (x_1, y_3)) \\ &= (p(x_1, x_1, x_1), p(y_1, y_2, y_3)) \\ &= (x_1, p(y_1, y_2, y_3)) \\ &:= (x_1, \bar{p}) \end{aligned}$$

and similarly

$$p(x'', y'', z'') = (p(x_1, x_2, x_3), y_1) := (\bar{\bar{p}}, y_1).$$

For the computation of $p(x', y', z')$ we use step 2 in the proof of 3.2:

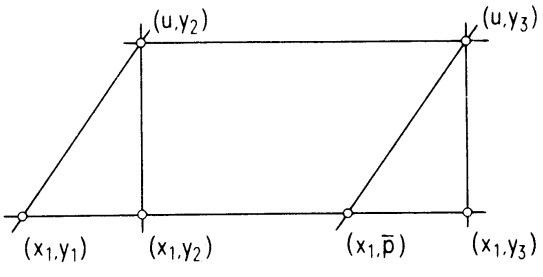

Fig. 3.5

From the above picture we immediately get the equations $x_1 \cdot y_1 = u \cdot y_2$ since $(x_1, y_1)\theta_3(u, y_2)$ and $x_1 \cdot \bar{p} = u \cdot y_3$ since $(x_1, \bar{p})\theta_3(u, y_3)$, which has as solution $\bar{p} = y_1 \cdot y_2^{-1} \cdot y_3$ and similarly $\bar{\bar{p}} = x_1 \cdot x_2^{-1} \cdot x_3$ thus $p(x', y', z') = (x_1, y_1 \cdot y_2^{-1} \cdot y_3)$ and $p(x'', y'', z'') = (x_1 \cdot x_2^{-1} \cdot x_3, y_1)$ then step 3 yields $p((x_1, y_1), (x_2, y_2), (x_3, y_3)) = (x_1 \cdot x_2^{-1} \cdot x_3, y_1 \cdot y_2^{-1} \cdot y_3)$.

COROLLARY 3.7. *Under the conditions as above,* **L** *is an abelian group.*

Proof. Lemma 3.6 and Corollary 3.3.

Since **L** is an abelian group we will from now on write + for multiplication and 0 for the neutral element. So let us formulate the result of the last chapter:

THEOREM 3.8. *Let* **S** *be an S-3-system and p a compatible Mal'cev-function on S. Then the associated loop is an abelian group* **G**. *p is uniquely determined and*

$$p(x, y, z) = x - y + z \quad \text{in} \quad \mathbf{G} \times \mathbf{G}.$$

§4. Algebras and affine functions

Suppose now, we have a Mal'cev-function on an S-3-system **S** which is compatible with Θ_1, Θ_2, Θ_3. We will from now on always assume that the

underlying set S of $\mathbf{S}$ is $G \times G$ where $\mathbf{G}$ is the abelian group associated with $\mathbf{S}$ by 2.3 and 3.8.

Let $f: S^n \to S$ be an n-ary operation on S which is compatible with Θ_1, Θ_2, Θ_3. Then f is a map $f: (G \times G)^n \to G \times G$. Since f is compatible with Θ_1 and Θ_2, f can be written as a direct product $f_1 \times f_2$ of maps $f_1, f_2: G^n \to G$, i.e.

$$(P): f((x_1, y_1), \ldots, (x_n, y_n)) = (f_1(x_1, \ldots, x_n), f_2(y_1, \ldots, y_n)).$$

Since f is compatible with Θ_3 and by the description of Θ_3 in Lemma 2.3 we have for $x := (x_1, \ldots, x_n)$, $y := (y_1, \ldots, y_n)$, $x' := (x'_1, \ldots, x'_n)$, $y' := (y'_1, \ldots, y'_n) \in G^n$:

LEMMA 4.1. (i) $x + y = x' + y'$ *implies* $f_1(x) + f_2(y) = f_1(x') + f_2(y')$.
(ii) $f_1(x) + f_2(0) = f_1(0) + f_2(x)$
(iii) $f_1(x) + f_2(y) = f_1(x + y) + f_2(0)$.

Proof. $x + y = x' + y'$ says: For all $1 \leq k \leq n$ $x_k + y_k = x'_k + y'_k$. Thus by Lemma 2.3 $(x_k, y_k)\Theta_3(x'_k, y'_k)$ and $f((x_1, y_1), \ldots, (x_n, y_n))\Theta_3 f((x'_1, y'_1), \ldots, (x'_n, y'_n))$ hence

$$(f_1(x_1, \ldots, x_n), f_2(y_1, \ldots, y_n))\Theta_3(f_1(x'_1, \ldots, x'_n), f_2(y'_1, \ldots, y'_n))$$

so by Lemma 2.3 $f_1(x) + f_2(y) = f_1(x') + f_2(y')$. (ii) follows trivially from (i).

For (iii) set $x' := x + y$ and $y' := 0$ $(= (0, \ldots, 0))$ and apply (i).

DEFINITION 4.2. An operation $f: A^n \to A$ is *affine with respect to* an abelian group $\mathbf{G}$ if there is a bijective map $i: A \to G$ such that for all $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in A$ we have:

$$i \circ f(x) + i \circ f(y) = i \circ f \circ i^{-1}(i(x) + i(y)) + i \circ f \circ i^{-1}(0)$$

We can always assume that i is the identity map, so we write:

$$f(x) + f(y) = f(x + y) + f(0). \tag{A}$$

An algebra $\mathbf{A}$ *is affine with respect to* an abelian group $\mathbf{G}$ if every fundamental operation is affine with respect to $\mathbf{G}$ (where i is the identity map).

It is immediate that affine functions also satisfy:

$$f(x) - f(y) = f(x - y) - f(0) \tag{A'}$$

LEMMA 4.3. *Let* $\mathbf{S}$ *be an* S*-3-system with a compatible Mal'cev-function. Then every map which is compatible with* Θ_1, Θ_2 *and* Θ_3 *is affine.*

Proof. Suppose $f: S^n \to S$ is compatible. Let $\mathbf{G}$ be the abelian group associated with $\mathbf{S}$. For $x := (x_1, \ldots, x_n)$, $y := (y_1, \ldots, y_n) \in S^n$ we can write:

$$x = (x', x'') = ((x_1', x_1''), \ldots, (x_n', x_n''))$$

and

$$y = (y', y'') = ((y_1', y_1''), \ldots, (y_n', y_n''))$$

both elements of $(G \times G)^n$ and by (P) we find f_1, f_2 with $f_1, f_2: G^n \to G$ so that by Lemma 4.1 we can compute:

$$\begin{aligned} f(x)+f(y) &= (f_1(x'), f_2(x''))+(f_1(y'), f_2(y'')) \\ &= (f_1(x')+f_1(y'), f_2(x'')+f_2(y'')) \\ &= (f_1(x')+f_1(0)+f_2(y')-f_2(0), f_2(x'')+f_2(0)+f_1(y'')-f_1(0)) \\ &= (f_1(x'+y')+f_1(0), f_2(x''+y'')+f_2(0)) \\ &= (f_1(x'+y'), f_2(x''+y''))+(f_1(0), f_2(0)) \\ &= f(x+y)+f(0). \end{aligned}$$

DEFINITION 4.4. Let f and g be n-ary (resp. k-ary) operations on the set A. f and g *commute* if

$$f(g(x_{11}, \ldots, x_{1k}), \ldots, g(x_{n1}, \ldots, x_{nk})) = g(f(x_{11}, \ldots, x_{n1}), \ldots, f(x_{1k}, \ldots, x_{nk})).$$

LEMMA 4.5. *Under the same hypothesis as in Lemma* 4.3 *every compatible operation commutes with the Mal'cev-function.*

Proof. For simplicity we give the proof only for unary compatible operations. For $x, y, z \in S$ we know that $p(x, y, z) = x - y + z$ in the abelian group $\mathbf{G} \times \mathbf{G}$.

$$\begin{aligned} f(p(x, y, z)) &= f(x-y+z) \\ &= f(x-y)+f(z)-f(0) && \text{by } (A) \\ &= f(x)-f(y)+f(0)+f(z)-f(0) && \text{by } (A') \\ &= f(x)-f(y)+f(z) \\ &= p(f(x), f(y), f(z)). \end{aligned}$$

Now we are able to formulate our main results:

THEOREM 4.6. *Let* $\mathbf{A} = (A, F)$ *be an algebra in a permutable variety* $\mathbf{V}$. *Let* p *be the Mal'cev-polynomial for permutability. Then the following conditions are*

equivalent:

(i) $\mathcal{M}_3$ *is a* 0-1-*sublattice of* $\mathfrak{C}(A)$

(ii) *There is an abelian group* $\mathbf{G}$ *such that* $\mathbf{G}\times\mathbf{G}$ *can be defined on* A *with an arbitrary choice of* $(0,0)\in A$ *and with* $p(x, y, z) = x - y + z$. *Moreover every algebraic function on* $\mathbf{A}$ *is affine w.r. to* $\mathbf{G}\times\mathbf{G}$ *and of the form* $f_1 \times f_2$ *with* $f_1, f_2 : G^n \to G$.

THEOREM 4.7. *Let* $\mathbf{A}$ *be an algebra in a permutable variety. Let* p *be the Mal'cev-polynomial. Let* Θ_{π_1} *and* Θ_{π_2} *be the kernels of the canonical projections* π_1, $\pi_2 : A \times A \to A$. *Then the following conditions are equivalent:*

(i) *There is a congruence* Θ *on* $\mathbf{A}\times\mathbf{A}$ *such that* Θ *is a complement of* Θ_{π_1} *and of* Θ_{π_2} *in* $\mathfrak{C}(\mathbf{A}\times\mathbf{A})$.

(ii) $\mathbf{A}$ *is affine w.r. to an abelian group* $\mathbf{G}$.

(iii) *Every fundamental operation of* $\mathbf{A}$ *commutes with* p.

(iv) $D := \{(x, x) \mid x \in A\}$ *is a class of a congruence on* $\mathbf{A}\times\mathbf{A}$.

(v) $\forall x, y, z \in A$ $(p(x, y, z) = z \Leftrightarrow x = y)$ *and* D *is a class of a congruence on* $\mathbf{A}\times\mathbf{A}$.

Proof of Theorem 4.6. (i)→(ii): Since $\mathcal{M}_3$ as a 0-1-sublattice of $\mathfrak{C}(\mathbf{A})$ defines an S-3-system, (i)→(ii) is done in the last two chapters and in Lemmas 4.1 and 4.3.

(ii)→(i): Since every algebraic function, thus also every algebraic operation is of the form $f_1 \times f_2$, the kernels Θ_{π_1} and Θ_{π_2} of the projection maps $\pi_1, \pi_2 : G \times G \to G$ are congruences on $\mathbf{A}$, so $\mathbf{A}$ is isomorphic to a direct product.

Define a congruence Θ_D on $\mathbf{A}$ by

$$((x, y), (x', y')) \in \Theta_D \quad \textit{iff} \quad x - y = x' - y'.$$

Since all algebraic functions of $\mathbf{A}$ are affine, Θ_D is immediately seen to be a congruence, even a congruence of the abelian group $\mathbf{G}\times\mathbf{G}$ and it is immediately checked that Θ_D together with Θ_{π_1} and Θ_{π_2} form a 0-1-$\mathcal{M}_3$ in the congruence lattice $\mathfrak{C}(\mathbf{G}\times\mathbf{G})$ thus also in $\mathfrak{C}(\mathbf{A})$.

Proof of Theorem 4.7. (i)→(ii): (i) states that Θ, Θ_{π_1} and Θ_{π_2} generate a 0-1-$\mathcal{M}_3$ in $\mathfrak{C}(\mathbf{A}\times\mathbf{A})$. By the last Theorem and by construction of $\mathbf{G}\times\mathbf{G}$, Θ_{π_1} and Θ_{π_2} are congruences on $\mathbf{G}\times\mathbf{G}$ with $(\mathbf{G}\times\mathbf{G})_{/\Theta_{\pi_i}} \simeq \mathbf{G}$, so $\mathbf{A}$ is affine w.r. to $\mathbf{G}$.

(ii)→(iii) is Lemma 4.5

(ii)→(iv): D is a class of Θ_D as defined in the proof of Theorem 4.6

(iv)→(v): Let Ψ_D be the congruence having D as a congruence class. Suppose $p(x, y, z) = z$.

Then in $\mathbf{A}\times\mathbf{A}$ we have:

$$(z, z) = p((x, z), (y, z), (z, z))\Psi_D p((x, z), (y, z), (y, y)) = (x, y)$$

Since D is a congruence class, we conclude that $(x, y)\in D$ from where it follows that $x = y$.

(v)$\rightarrow$(i): For $\Theta := \Psi_D$ we have for arbitrary elements (x, y), $(x', y')\in A\times A$:

$$(x, y) = p((x, x), (y, x), (y, y))\Theta_{\pi_2} p((x', x), (y', x), (y, y))$$

and

$$p((x', x), (y', x), (y, y))\Psi_D p((x', x), (y', x), (y', y')) = (x', y')$$

yielding: $\Theta_{\pi_2}\circ\Psi_D = \iota$. Correspondingly we obtain $\Theta_{\pi_1}\circ\Psi_D = \iota$. Suppose $(x, y)\Theta_{\pi_1}\wedge\Psi_D(x', y')$. Then $x = x'$ whence $(x, y)\Psi_D(x, y')$ so

$$(x, p(y, y', x)) = p((x, y), (x, y'), (x, x))\Psi_D(x, x)$$

so by definition of Ψ_D $p(y, y', x) = x$ and therefore $y = y'$. Hence $\Theta_{\pi_1}\wedge\Psi_D = \omega$ and similarly $\Theta_{\pi_2}\wedge\Psi_D = \omega$.

It remains to prove the implication (iii)$\rightarrow$(i), we will do this with the following lemma:

LEMMA 4.8. *Let* $\mathbf{A}$ *be an arbitrary algebra and let p be any Mal'cev-function defined on A. Define a binary relation* Δ *on* $A\times A$ *by*

$$\begin{aligned}(x, y)\Delta(x', y') \quad \textit{iff} \quad & x = p(x', y', y)\\ \text{and} \quad & y = p(y', x', x)\\ \text{and} \quad & x' = p(x, y, y')\\ \text{and} \quad & y' = p(y, x, x').\end{aligned}$$

Then

(i) *if the equation* (Ξ):

$$p(p(x, y, z), u, v) = p(x, y, p(z, u, v))$$

holds for all elements $x, y, z, u, v\in A$ *then* Δ *is an equivalence relation,*

(ii) *if every fundamental operation of* $\mathbf{A}$ *commutes with p then* Δ *is a compatible relation*

(iii) *if p commutes with itself,* (Ξ) *holds.*

Proof. (i): Clearly Δ is reflexive and symmetric. If $(x, y)\Delta(x', y')$ and $(x', y')\Delta(x'', y'')$ we have

$$\begin{aligned} x &= p(x', y', y) \\ &= p(p(x'', y'', y'), y', y) \\ &= p(x'', y'', p(y', y', y)) \quad \text{by} \quad (\Xi) \\ &= p(x'', y'', y) \end{aligned}$$

Similarly we get the other three equations establishing $(x, y)\Delta(x'', y'')$ and thus transitivity.

For (ii): Let f be a k-ary fundamental operation on $\mathbf{A}$ and suppose $(x_i, y_i)\Delta(x_i', y_i')$ for $1 \leq i \leq k$.

$$\begin{aligned} f(x_1, \ldots, x_k) &= f(p(x_1', y_1', y_1), \ldots, p(x_n', y_n', y_n)) \\ &= p(f(x_1', \ldots, x_n'), f(y_1', \ldots, y_n'), f(y_1, \ldots, y_n)) \end{aligned}$$

and three more equations give us:

$$f((x_1, y_1), \ldots, (x_n, y_n))\Delta f((x_1', y_1'), \ldots, (x_n', y_n')).$$

For (iii): Let p commute with p. Then by the equations $(*)$ of p (see 1.3) we get

$$\begin{aligned} p(x, y, p(z, u, v)) &= p(p(x, u, u), p(y, u, u), p(z, u, v)) \\ &= p(p(x, y, z), p(u, u, u), p(u, u, v)) \\ &= p(p(x, y, z), u, v) \end{aligned}$$

Now for the proof of (iii)$\rightarrow$(i) in Theorem 4.7 note that since p is a polynomial and every fundamental operation, (thus every polynomial) commutes with p we have a fortiori that p commutes with itself, so the above lemma yields the congruence Δ on $\mathbf{A} \times \mathbf{A}$. It is easy to check (much like in (v)$\rightarrow$(i)) that Δ forms a 0-1-$\mathcal{M}_3$ in $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ together with the projection congruences.

Let now $\mathbf{A}$ be affine w.r. to an abelian group $\mathbf{G}$. Let p be a Mal'cev-polynomial on $\mathbf{A}$. Since

$$\begin{aligned} p(x, y, z) &= p(x, 0, 0) + p(0, y, 0) + p(0, 0, z) \\ &= x + z + p(0, y, y) + p(0, 0, -y) \\ &= x - y + z \end{aligned}$$

we have by Theorems 3.2 and 3.8 that $\mathbf{G}$ is actually isomorphic to the group constructed in 3.8. For arbitrary $n \in N$ let us define congruences Δ_n on $\mathbf{A}\times\mathbf{A}$ by

$$(x, y)\Delta_n(x', y') \quad \textit{iff} \quad n(x-x') = y-y'. \tag{Σ}$$

LEMMA 4.9. *Δ_n is a congruence on $\mathbf{A}\times\mathbf{A}$ for every $n \in N$. Every congruence on $\mathbf{A}$ (resp. on $\mathbf{A}\times\mathbf{A}$) is a congruence on $\mathbf{G}$ (resp. $\mathbf{G}\times\mathbf{G}$).*

Proof. For an arbitrary fundamental operation f on $\mathbf{A}$ and for $(x_i, y_i)\Delta_n(x_i', y_i')$ we have:

$$\begin{aligned} n(f(x_1, \ldots, x_k) - f(x_1', \ldots, x_k')) = \\ &= n(f(x_1 - x_1', \ldots, x_k - x_k') - f(0, \ldots, 0)) \\ &= n(f(x_1 - x_1', \ldots, x_k - x_k')) - n(f(0, \ldots, 0)) \\ &= f(n(x_1 - x_1'), \ldots, n(x_k - x_k')) - f(0, \ldots, 0) \\ &= f(y_1 - y_1', \ldots, y_k - y_k') - f(0, \ldots, 0) \\ &= f(y_1, \ldots, y_k) - f(y_1', \ldots, y_k'). \end{aligned}$$

Let Φ be a congruence on $\mathbf{A}$ (resp. $\mathbf{A}\times\mathbf{A}$) then Φ must be compatible with $p(x, y, z) = x - y + z$ and therefore a congruence of $\mathbf{G}$ (resp. $\mathbf{G}\times\mathbf{G}$).

§5. More about affine algebras

Affine algebras are in many respects similar to modules, but the only thing which is often inconvenient is that the zero-element of the underlying abelian group is not a subalgebra of the affine algebra. Therefore the following definition, which can be found in McKenzie [16], will prove useful:

DEFINITION 5.1. Let $\mathbf{A} = (A, F)$ be an affine algebra. For $f \in F$, k-ary, define $f^\nabla : A^k \to A$ by $f^\nabla(x_1, \ldots, x_k) := f(x_1, \ldots, x_k) - f(0, \ldots, 0)$ and $F^\nabla := \{f^\nabla \mid f \in F\}$. $\mathbf{A}^\nabla := (A, F^\nabla)$ is then called the *linearization* of $\mathbf{A}$.

Note that by this definition $\{0\}$ becomes a subalgebra of $\mathbf{A}^\nabla$ and moreover every constant of $\mathbf{A}^\nabla$ coincides with 0.

Throughout this chapter $\mathbf{A}$ will be an affine algebra in a permutable variety. Since for the Mal'cev-polynomial p we have $p(x, y, z) = x - y + z$ we conclude that $x - y$ and $x + y$ are algebraic functions on $\mathbf{A}$ and on $\mathbf{A}^\nabla$. Immediately we get:

LEMMA 5.2. *$\mathbf{A}$ and $\mathbf{A}^\nabla$ have exactly the same algebraic functions and exactly the same congruences.*

From $\mathbf{A}^\nabla$ we now define an algebra $\mathbf{A}_0^\nabla$ by adding a nullary operation with value 0, denoted by 0. If $\mathbf{A}$ already had some nullary operation then $\mathbf{A}^\nabla$ and $\mathbf{A}_0^\nabla$ are polynomially equivalent and will therefore be considered as equal for our purposes.

THEOREM 5.3. *$\mathbf{A}_0^\nabla$ is polynomially equivalent to a module over a unitary ring.*

Proof. Let p be an n-ary polynomial of $\mathbf{A}_0^\nabla$. Then

$$p(x_1, \ldots, x_n) = p(x_1, 0, \ldots, 0) + \cdots + p(0, \ldots, 0, x_n) \qquad (\Omega)$$

by condition (A) and Lemma 4.3 and because $p(0, \ldots, 0) = 0$ in $\mathbf{A}^\nabla$. Let R be the set of all unary polynomials of $\mathbf{A}_0^\nabla$. Addition and composition of functions endows R with a ring-structure, in fact R becomes a subring of the ring of endomorphisms of the underlying group G. The identity map $i: A_0 \to A_0$ makes $\mathbf{R} = (R, +, \circ, i)$ a unitary ring. Since every polynomial of $\mathbf{A}_0^\nabla$ keeps 0 fixed, we have that every polynomial of $\mathbf{A}_0^\nabla$ is a group homomorphism of $\mathbf{G}^n \to \mathbf{G}$. The above equation shows that every polynomial of $\mathbf{A}_0^\nabla$ is a polynomial of the module ${}_{\mathbf{R}}G$. On the other hand every polynomial of ${}_{\mathbf{R}}G$ is a polynomial of $\mathbf{A}_0^\nabla$ because $x + y = p(x, 0, y)$ is a polynomial of $\mathbf{A}_0^\nabla$ and because the polynomials of every algebra are closed under composition. This module which we can always obtain, starting out with any affine algebra $\mathbf{A}$, will be denoted by $M(\mathbf{A})$.

Observing that the algebraic functions of $\mathbf{A}$ and $\mathbf{A}_0^\nabla$ coincide we can get $M(\mathbf{A})$ in a more direct way:

COROLLARY 5.4. *The algebraic functions of $\mathbf{A}$ with 0 as only constant are the polynomials of a module over a unitary ring $\mathbf{R}$.*

Remark. It should be noted here that we consider two polynomials (resp. algebraic functions) of a *single* universal algebra as equal if they are equal as mappings. This means particularly that $M(\mathbf{A})$ operates faithfully on $\mathbf{A}$.

For a cardinal α let $\mathcal{M}_\alpha$ denote the modular lattice of length 2 with α atoms.

LEMMA 5.5. *Let $\mathbf{A}$ be a simple affine algebra in a permutable variety. Then the underlying group $\mathbf{G}$ is either torsion-free or an elementary abelian p-group.*

Proof. The congruence lattice of $\mathbf{A} \times \mathbf{A}$ is modular since $\mathbf{A}$ is contained in a permutable variety. Since $\mathbf{A}$ is simple, $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ has to be of length 2. Thus $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ is isomorphic to $\mathcal{M}_\alpha$ for some cardinal α. Suppose $\mathbf{G}$ is not torsion-free.

Then there exists a smallest number q such that for some $0 \neq a \in G$ we have $qa = 0$. q obviously is prime.

Claim. For all $x \in G$ we have $qx = 0$.

The congruence Δ_q as defined in Lemma 4.9 is nontrivial if A has more than one element. Moreover, since $(a, 0)\Delta_q(0, 0)$ we have that $\Delta_q \wedge \Theta_{\pi_2} \neq \omega$. Since $\mathfrak{C}(\mathbf{A} \times \mathbf{A}) \simeq \mathcal{M}_\alpha$ we see that $\Delta_q = \Theta_{\pi_2}$ from where it readily follows that $qx = 0$ for all $x \in G$.

§6. Applications to single algebras

The applications of Theorems 4.6, 4.7 and 5.4 will, for the purpose of this note be divided into two classes. First we will describe certain single algebras in permutable varieties, and in a later chapter we will characterize some hamiltonian varieties of universal algebras, simplifying and at the same time sharpening some known results.

The first application generalizes a result of Quackenbush and a theorem of McKenzie.

THEOREM 6.1. *Let* $\mathbf{A}$ *be a simple algebra in a permutable variety. If* $\mathfrak{C}(\mathbf{A} \times \mathbf{A})$ *is isomorphic to* $\mathcal{M}_\alpha$ *for some* $\alpha \geq 3$, *then* $\mathbf{A}$ *is affine w.r. to a torsion-free abelian group or w.r. to an elementary abelian p-group.*

Proof. Follows from 4.7 and 5.5.

COROLLARY 6.2. (Quackenbush [20]). *If* $\mathbf{A}$ *is a finite algebra in a permutable variety and if* $\mathfrak{C}(\mathbf{A} \times \mathbf{A}) \simeq \mathcal{M}_n$ *then*

(a) $n = p^k + 1$ *where p is a prime*

(b) *If* $p > 1$ *then* $|\mathbf{A}| = p^m$.

Proof. (b): $\mathfrak{C}(\mathbf{A} \times \mathbf{A}) \simeq \mathcal{M}_n$ obviously implies that $\mathbf{A}$ is simple. Since $|\mathbf{A}|$ is finite, applying Theorem 6.1 we know that $\mathbf{A}$ is affine with respect to an elementary abelian p-group. In particular, the cardinality of $\mathbf{A}$ must be a prime power, say p^m.

(a). 5.4 implies that $\mathfrak{C}(\mathbf{A}) \simeq \mathfrak{C}(M(\mathbf{A}))$ and $\mathfrak{C}(\mathbf{A} \times \mathbf{A}) \simeq \mathfrak{C}(M(\mathbf{A}) \times M(\mathbf{A}))$, hence $M(\mathbf{A})$ is a simple module and the nontrivial congruences of $\mathbf{A} \times \mathbf{A}$ are in a canonical correspondence with the one-generated subspaces of $M(\mathbf{A}) \times M(\mathbf{A})$. Those one-generated subspaces are therefore lines of a geometric net given by $\mathcal{M}_n$ and must be of the same cardinality as $\mathbf{A}$. By part (b) this is p^m and we are left with counting the one-generated subspaces of $M(\mathbf{A}) \times M(\mathbf{A})$ which immediately yields $p^m + 1$. Hence we even get $m = k$.

Note that using elementary theory of modules, we can prove that $\mathbf{R}$ is a ring of matrices over a field and obtain the same result in a different way, compare Behrens [1], II, §1.

COROLLARY 6.3. (McKenzie [16]). *Every finite simple algebra in a permutable variety is either functionally complete or affine with respect to an elementary abelian p-group.*

Proof. $\mathfrak{C}(\mathbf{A}\times\mathbf{A})$ is isomorphic to $\mathcal{M}_n$ for some $n\in N$. If n is equal to 2 then the result follows from 1.9, otherwise 6.1 applies.

There is also an infinite analogue to Corollary 6.3 which follows from 6.1. This was pointed out to me by A. F. Pixley.

We define an algebra $\mathbf{A}$ to be *locally functionally complete* if every partial function from $\mathbf{A}^n$ to A with a finite domain is equal to an algebraic function on this finite domain. See [19] for a precise definition and equivalent formulations.

THEOREM 6.4. *An infinite simple algebra in a permutable variety is either locally functionally complete or affine with respect to an abelian group which is either torsion free or an elementary abelian p-group.*

Proof. It remains only to prove that if $\mathfrak{C}(\mathbf{A}\times\mathbf{A})\simeq\mathcal{M}_2$ then $\mathbf{A}$ is locally functionally complete, i.e. $\mathbf{A}^+$ is locally primal [19]. Hence by Theorem 4.3 of [19] and by the characterization of *local varieties* by Hu [11] it only remains to show that the local variety $\mathbf{L}(\mathbf{A}):=\mathbf{DHSP}_f(\mathbf{A}^+)$ is arithmetical. Here $\mathbf{D}$, resp. $\mathbf{P}_f$, are the operators of taking direct limits, resp. products of finitely many factors. Since $\mathbf{A}^+$ has no subalgebras we get by Lemma 1.8 that $\mathbf{L}(\mathbf{A}^+)=\mathbf{DHP}_f(\mathbf{A}^+)$. Again by [3] or [22] we conclude that finite powers of $\mathbf{A}^+$ have no skew congruences hence $\mathbf{HP}_f(\mathbf{A}^+)$ is a class of arithmetical algebras. It is straightforward to see that direct limits of arithmetical algebras are arithmetical hence $\mathbf{L}(\mathbf{A}^+)$ is arithmetical.

Another field where the results of Chapter 4 can be applied is given by the para-primal algebras. According to Krauss we define:

DEFINITION 6.5. A finite algebra $\mathbf{A}$ is *para-primal* if every subalgebra is simple and the variety generated by $\mathbf{A}$ has permutable congruences.

Para-primal algebras are generalizations of quasi-primal algebras which have been widely investigated. For the definition of quasi-primal algebras see Pixley [19]. We will use a characterization of quasi-primal algebras due to Pixley as our definition:

DEFINITION 6.5. A finite algebra $\mathbf{A}$ is *quasi-primal* iff $\mathbf{A}$ is para-primal and the variety generated by $\mathbf{A}$ is congruence distributive.

Para-primal algebras have been investigated by Clark and Krauss in [4] and [5] and recently by McKenzie [17].

The following characterization theorem was also found independently by McKenzie [17]:

THEOREM 6.6. *A para-primal algebra* $\mathbf{A}=(A, F)$ *is quasi-primal if and only if no non-trivial subalgebra is affine.*

Proof. If some subalgebra $\mathbf{B}$ of $\mathbf{A}$ is affine then by Theorem 4.7 $\mathcal{M}_3$ is a sublattice of $\mathfrak{C}(\mathbf{B}\times\mathbf{B})$ thus the variety generated by $\mathbf{B}$ is not congruence distributive. For the other direction let $V(\mathbf{A})$ be the variety generated by $\mathbf{A}$ and let $F_{V(\mathbf{A})}(3)$ be the free algebra on 3 generators in $V(\mathbf{A})$. It follows from Jonsson [12] that $V(\mathbf{A})$ is congruence distributive if and only if the congruence lattice of $F_{V(\mathbf{A})}(3)$ is distributive.

Since $\mathbf{F}:=F_{V(\mathbf{A})}(3)$ can be embedded in a finite direct power of $\mathbf{A}$ we have that $\mathbf{F}$ is a subdirect product of finitely many subalgebras of $\mathbf{A}$. Since every subalgebra of $\mathbf{A}$ is simple we may apply Lemna 1.8 to see that $\mathbf{F}$ is a direct product of subalgebras of $\mathbf{A}$. If for any two subalgebras $\mathbf{B}$ and $\mathbf{C}$ of $\mathbf{A}$ their product $\mathbf{B}\times\mathbf{C}$ has only factor-congruences then by Burris [3] or Werner [22] $\mathfrak{C}(\mathbf{F})$ is distributive and hence $\mathbf{A}$ is quasiprimal. Since this cannot occur we conclude that $\mathcal{M}_3$ is a 0-1-sublattice of $\mathfrak{C}(\mathbf{B}\times\mathbf{C})$. Then Theorem 4.6 yields that $\mathbf{B}$ and $\mathbf{C}$ are affine.

For the case of loops we get a sharper result:

COROLLARY 6.7. *A para-primal loop* $\mathbf{L}=(L, \cdot, 1)$ *is quasi-primal if and only if no nontrivial subloop is an elementary abelian p-group.*

Proof. The proof is the same as that of Theorem 6.6, with some additional conclusions. If for the constructed subloops $\mathbf{B}$ and $\mathbf{C}$ we have $\mathcal{M}_3$ as a 0-1-sublattice of $\mathfrak{C}(\mathbf{B}\times\mathbf{C})$ then, since loops have one-element subalgebras we can use a theorem of Lovász [14] to conclude that $\mathbf{B}\simeq\mathbf{C}$. Then by 4.7 $\mathbf{B}\times\mathbf{B}$ is affine over $\mathbf{G}\times\mathbf{G}$ and the Mal'cev-polynomial p is nothing else than $x-y+z$ in $\mathbf{G}\times\mathbf{G}$. Moreover the zero-element $(0, 0)$ of $\mathbf{G}\times\mathbf{G}$ can be chosen arbitrarily so we choose $(0, 0):=(1, 1)$, where 1 is the unit of $\mathbf{L}$. Then we get:

$$(x/y)\cdot z = p(x, y, z) = x-y+z$$

and by our choice of $(0, 0)$:

$$x\cdot z = (x/1)z = x-0+z = x+z$$

Thus the multiplication of the loop coincides with the addition of our abelian group. It follows that **B** *is* an abelian group and moreover an elementary abelian p-group by Theorem 6.1 since **B** is simple.

§7. Applications to hamiltonian algebras and varieties

DEFINITION 7.1. An algebra is *hamiltonian* if every subalgebra is a class of a congruence.

The following generalizes a theorem of Evans [9]:

THEOREM 7.2. *A loop* **L** *is an abelian group if and only if* $\mathbf{L}\times\mathbf{L}$ *is hamiltonian.*

Proof. Certainly abelian groups are hamiltonian so one direction is clear.

For the other direction note that $D:=\{(x, x) \mid x \in L\}$ is a subalgebra of $\mathbf{L}\times\mathbf{L}$ and therefore has to be a congruence class. Theorem 4.7 applies and we get that **L** is affine w.r. to an abelian group **G** and as in the proof of 6.7 we may choose the zero of the group as the unit of the loop to get that $x \cdot y = x + y$, i.e. the multiplication of the loop **L** and the abelian group **G** coincide.

COROLLARY 7.3. (Evans [9]). *A variety of hamiltonian loop is a variety of abelian groups.*

Another field of applications leads to the characterization of varieties of modules and affine modules, due to Csákány and Klukovits.

DEFINITION 7.4. An *affine module* is the full idempotent reduct of a module.

THEOREM 7.5. (Csákány [6]). *Let* **V** *be a variety such that for every algebra* **A** *in* **V**:

(i) *Every subalgebra is a class of a unique congruence*

(ii) *Every congruence class is a subalgebra*

Then **V** *is polynomially equivalent to the variety of all affine modules over a fixed unitary ring* **R**.

THEOREM 7.6. (Csákány [7]). *Let V be a variety such that for every algebra* **A** *in* **V**:

(i) *Every subalgebra is a class of a unique congruence*

(ii) *Every congruence has a unique class which is a subalgebra*

Then $\mathbf{V}$ *is polynomially equivalent to the variety of all modules over a fixed unitary ring* $\mathbf{R}$.

THEOREM 7.7. (Csákány [6]). *Let* $\mathbf{V}$ *be a variety such that*

(i) $\mathbf{V}$ *has permutable congruences*

(ii) *Any two polynomials of* $\mathbf{V}$ *commute*

(iii) *There is a nullary operation* 0 *forming a one-element subalgebra in every* $\mathbf{A} \in \mathbf{V}$.

Then $\mathbf{V}$ *is polynomially equivalent to the variety of all modules over a fixed commutative unitary ring* $\mathbf{R}$.

Let us add another theorem:

THEOREM 7.8. *Let* $\mathbf{V}$ *be a variety such that*

(i) $\mathbf{V}$ *has permutable congruences*

(ii) *There is a nullary constant* 0 *forming a one-element subalgebra in every* $\mathbf{A} \in \mathbf{V}$

(iii) $\mathbf{V}$ *is hamiltonian*

Then $\mathbf{V}$ *is polynomially equivalent to the variety of all modules over a fixed unitary ring* $\mathbf{R}$.

Proofs. To obtain a common proof for all those four theorems let us first note that the conditions of 7.5 and of 7.6 both imply that $\mathbf{V}$ has permutable congruences. In the case of 7.5 we prove this as follows: Let Θ and Ψ be congruences on an algebra $\mathbf{A} \in \mathbf{V}$ and let x, y, z be elements of A with $x\Theta y\Psi z$. Then $B := [z]\Theta := \{a \in A \mid a\Theta z\}$ is a subalgebra of $\mathbf{A}$ by (ii), therefore $[B]\Psi := \bigcup_{b \in B} [b]\Psi$ is another subalgebra of $\mathbf{A}$ and by 7.5(i) is a class of a unique congruence α. Thus $[B]\Psi$ is a class of α and on the other hand $[B]\Psi$ is contained in $[z](\Theta \vee \Psi)$. It follows from the uniqueness (i) that $\alpha = \Theta \vee \Psi$. Since $x\Theta \vee \Psi z$ we conclude $x \in [B]\Psi$ but this implies that there exists an element $c \in A$ with $z\Theta c\Psi x$. Thus Θ and Ψ permute. In the case of 7.6 we refer to Csákány [6] for the proof that $\mathbf{V}$ has permutable congruences.

Let now $F(\omega)$ denote the free algebra in $\mathbf{V}$ with countably many generators. We will apply Theorem 4.7 to show that $F(\omega)$ is affine w.r. to an abelian group:

In Theorem 7.7 every polynomial commutes with the Mal'cev-polynomial for permutability, thus Theorem 4.7 (iii) applies.

In the other theorems the hamiltonian properties imply that D, the diagonal subalgebra of $F(\omega) \times F(\omega)$ is a congruence class, thus we can apply Theorem 4.7

(iv). Now consider $F(\omega)_0^\nabla$ where the 0 has been chosen as the one-element subalgebra which is easily seen to exist in 7.6 and obviously in 7.7 and 7.8. Thus in 7.6, 7.7 and 7.8 we have that $F(\omega)$ is polynomially equivalent to $F(\omega)_0^\nabla$ and thus to a module by Theorem 5.3. Since $F(\omega)$ determines the variety $\mathbf{V}$ uniquely the Theorems 7.6, 7.7, 7.8 follow. Note that in 7.7 because of (ii) the ring $\mathbf{R}$ is commutative.

For Theorem 7.5 we do not have a distinguished constant 0 but (ii) implies that every polynomial is idempotent, i.e. every element is a one-element subalgebra. Obviously $F(\omega) = F(\omega)^\nabla$ so as in 5.3 we get a ring $\mathbf{R}$ such that every polynomial of $F(\omega)$ is a module polynomial. On the other hand let $q(z_1, \ldots, z_n)$ be an idempotent module polynomial, i.e.

$$\sum_{i=1}^{n} a_i = 1 \qquad \text{in the ring } \mathbf{R}. \tag{σ}$$

We have to show that q is a polynomial of $F(\omega)$. Certainly q is an algebraic function of $F(\omega)$. Every algebraic function of a free algebra however is a polynomial of this free algebra with possibly some variables added. hence it remains to show that

$$q(x_{i_1}, \ldots, x_{i_n}) \in \mathbf{U} := \langle \{x_{i_1}, \ldots, x_{i_n}\} \rangle,$$

the subalgebra of $F(\omega)$ generated by $\{x_{i_1}, \ldots, x_{i_n}\}$, see [7]. Then we will have established that $q(x_{i_1}, \ldots, x_{i_n})$ itself is a polynomial, i.e. no variables have been added as constants. Let us take the congruence Θ_U which has U as a class. Θ_U exists by 7.5(i). Then by (σ) we get

$$x_{i_1} = a_1 x_{i_1} + \cdots + a_n x_{i_1} \Theta_U a_1 x_{i_1} + \cdots + a_n x_{i_n} = q(x_{i_1}, \ldots, x_{i_n})$$

In particular $q(x_{i_1}, \ldots, x_{i_n}) \in U$ hence $q(x_{i_1}, \ldots, x_{i_n})$ is a polynomial in $x_{i_1}, \ldots, x_{i_n}$.

REFERENCES

[1] E. A. Behrens, *Ringtheorie*, BI Wissenschaftsverlag, Bibliographisches Institut Mannheim, 1975.
[2] G. Birkhoff, *Lattice theory*, A.M.S. Colloquium Publ., Vol. XXV, Am. Math. Soc., Providence, R.I. 1967.
[3] S. Burris, *Separating sets in modular lattices with applications to congruence lattices*, preprint, 1974.
[4] D. Clark and P. Krauss, *Para primal algebras*, preprint, 1976.
[5] D. Clark and P. Kraus , *Varieties generated by paraprimal algebras*, preprint, 1976.

[6] B. CSÁKÁNY, *Abelian properties of primitive classes of universal algebras*, Acta Sci. Math., *24* (1963), 157–164. (Russian)
[7] B. CSÁKÁNY, *Varieties of affine modules*, Acta Sci. Math., *37* (1975), 3–10.
[8] J. DÉNES and A. D. KEEDWELL, *Latin squares and their applications*, Academic Press, New York and London 1974.
[9] T. EVANS, *Properties of algebras almost equivalent to identities*, Journal London Math. Soc. *35* (1962), 53–59.
[10] G. GRÄTZER, *Universal Algebra*, D. Van Nostrand Co. Inc., Princeton, N.J. 1968.
[11] T. K. HU, *Locally equational classes of universal algebras*, Preprint.
[12] B. JÓNSSON, *Algebras whose congruence lattices are distributive*, Math. Scand. *21* (1967), 110–121.
[13] L. KLUKOVITS, *Normal abelian varieties*, Preprint.
[14] L. LOVÁSZ, *Operations with structures*, Acta Math. Acad. Sci. Hung *18* (1967), 321–328.
[15] A. I. MAL'CEV, *On the general theory of algebraic systems*, Math. Sbornik *35* (77), (1954), 3–20. (Russian)
[16] R. MCKENZIE, *On minimal, locally finite varieties with permutable congruence relations*, Preprint (1976).
[17] R. MCKENZIE, *Paraprimal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties*, Preprint (1976).
[18] A. F. PIXLEY, *Completeness in arithmetical algebras*, Algebra Universalis *2* (1972), 177–192.
[19] A. F. PIXLEY, *The ternary discriminator function in universal algebra*, Math. Ann. *191* (1971) 167–180.
[20] R. W. QUACKENBUSH, *Finite simple algebras in congruence permutable varieties*, Proceed. Lattice theory conference Ulm 1975, Appendix.
[21] E. T. SCHMIDT, *Kongruenzrelationen algebraischer Strukturen*, Mathematische Forschungsberichte. VEB Deutscher Verlag der Wissenschaften. Berlin 1969.
[22] H. WERNER, *Congruences on products of algebras and functionally complete algebras*, Algebra Universalis *4* (1974), 99–105.
[23] H. WERNER, *Produkte von Kongruenzklassengeometrien universeller Algebren*. Math. Zeitschr. *121* (1971), 111–140.
[24] R. WILLE, *Kongruenzklassengeometrien*, Springer Lecture Notes Math. *113* (1973).

Technische Hochschule
Darmstadt
West Germany