

A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity

By

JOACHIM HAGEMANN and CHRISTIAN HERRMANN

For any group A the lattice $L(A)$ of normal subgroups of A can be endowed with the operation $[,]$ of taking the mutual commutator. Similarly for a ring A we can define $[I, J]$ as the ideal generated by $IJ + JI$ to establish an operation on the ideal lattice $L(A)$. As the example of simple groups (rings) shows, $[,]$ cannot be defined in terms of $L(A)$ alone. The purpose of the present note is to define $[,]$ in terms of the lattices $L(B)$ and the canonical lattice embeddings $\hat{p}: L(A) \rightarrow L(B)$ where p is a homomorphism of B onto A . Actually, it will suffice to consider those B which are congruences of A (whence subalgebras of $A \times A$) and p which are natural projections.

In our presentation we follow Smith [15] who introduced commutators $[,]$ of congruences for algebras in congruence permutable varieties using algebraic properties of congruences. In the extreme case that $\beta = \gamma$ is the greatest and $[\beta, \gamma]$ the smallest congruence this algebraic condition means that there is a congruence of $A \times A$ having the diagonal $\{(x, x) | x \in A\}$ as a class. Our lattice theoretic condition then specialises to: In the congruence lattice of $A \times A$ there is a common complement to the kernels of the two natural projections. Thus, in this case our result is known as "Remark's Principle" for groups, loops, rings. The analysis of the general case relies heavily on a way of conceiving congruence lattices of congruences which is due to Freese and Jónsson [4].

The lattice theoretic characterisation allows several applications: First, we show (in § 2) that the commutator operation distributes over joins. Then we characterise (in § 3) prime and semiprime congruences. Particular interest is paid (in § 4) to algebras A such that $[\beta, \beta] = \beta$ for all congruences β . Such an algebra is called neutral since in every subdirect product $C \subseteq A \times B$ the kernel of the projection onto A is a neutral element in the congruence lattice of C : every congruence of C is the restriction of the product $\alpha \times \beta$ of suitable congruences α of A and β of B .

The prerequisites of the paper are elementary universal algebra (see e.g. [3], [14]) and basic results about modular lattices (see e.g. [12; I, II]).

§ 1. Centrality. Throughout this paper we are going to work in an equationally defined class of algebraic systems each of which has a modular lattice of congruences. Seemingly weaker, one may suppose that every algebra A considered is *strictly*

modular which means that for any diagonal subalgebra $B \subseteq A^n$ (i.e. $(x, \dots, x) \in B$ for all $x \in A$) the congruence lattice of B is modular. We denote the meet and join in a congruence lattice by \cap and $+$ resp. and by 0 and 1 its smallest and greatest element. Recall that by the Isomorphism Theorem for a given homomorphism p of an algebra B onto an algebra A there is a lattice isomorphism \hat{p} of the congruence lattice $L(A)$ of A onto the interval $1/\ker(p)$ of $L(B)$ mapping a congruence onto its inverse image under $p \times p$. The inverse isomorphism \hat{p} maps a congruence onto its image under $p \times p$.

We are going to rephrase Smith's definition [15] of centrality in a slightly more general form which will coincide with the original one in the congruence permutable case. Let α, β, γ be congruences of an algebra A such that $\alpha \subseteq \beta \cap \gamma$. We may consider $\beta \subseteq A \times A$ as a subdirect square of A with projections p_0 and p_1 onto A . Let us say that γ *centralises* β *modulo* α *by means of* κ if and only if κ is a congruence of the algebra β such that the following hold (writing xy for a pair $(x, y) \in A \times A$):

- (C0) $\kappa \subseteq \hat{p}_0 \gamma \cap \hat{p}_1 \gamma$,
- (C1) $\kappa \cap \hat{p}_0 \alpha = \kappa \cap \hat{p}_1 \alpha = \hat{p}_0 \alpha \cap \hat{p}_1 \alpha$,
- (RR) $x\gamma u$ implies $xx\kappa uu$,
- (RS) $xy\kappa uv$ implies $yx\kappa vu$,
- (RT) $xy\kappa uv$ and $yz\kappa vw$ imply $xz\kappa uw$.

Observe that from (C0) and (RR) it follows $\kappa + \hat{p}_i 0 = \hat{p}_i \gamma$ ($i = 0, 1$). Thus, if A has permuting congruences then γ centralises β (modulo $\alpha = 0$ by means of a suitable κ) if and only if it does so in the sense of Smith [15]. In particular, if A is a group (ring) this means that the corresponding normal subgroups (ideals) C and B centralise (annihilate) each other — see Smith [15; 2.1].

Proposition 1.1. *If γ centralises β modulo α by means of κ then there is a sublattice of $L(\beta)$ containing the elements and satisfying the relations indicated in Fig. 1.*

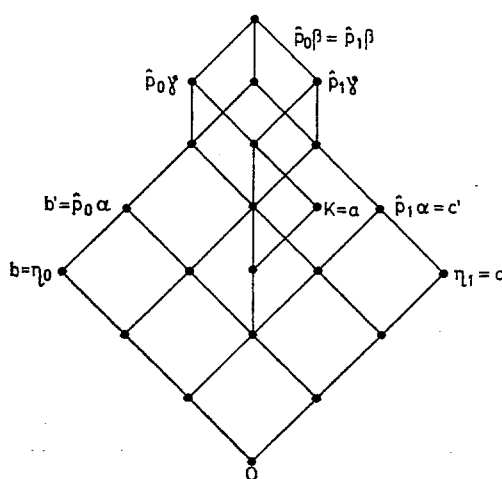


Fig. 1

Observation 1.2. *The lattice given in Fig. 1 is the modular lattice freely generated by a, b, c subject to $a \geq bc$ (the meet of b and c). This can be easily derived from the description of the free modular lattice with 3 generators. To apply this to the proof of the proposition we need the following observations due to Freese and Jónsson [4]. For later use we state them slightly more generally.*

Observation 1.3. *Let S be a diagonal subalgebra of $A \times A$ with canonical projections $p_i = p_{iS}$ ($i = 0, 1$) onto A . Let $\eta_i = \hat{p}_i 0$ be the kernel of p_i and β the congruence of A which is generated by S . Then it holds*

- (1) $\hat{p}_0 \lambda = \hat{p}_1 \lambda$ for all $\lambda \supseteq \beta$ in $L(A)$.
- (2) $\eta_i + (\hat{p}_0 \lambda \cap \hat{p}_1 \lambda) = \hat{p}_i \lambda$ for $i = 0, 1$ and all λ in $L(A)$.
- (3) $\eta_0 + \eta_1 = \hat{p}_0 \beta = \hat{p}_1 \beta, \quad \eta_0 \cap \eta_1 = 0$.

Namely, observe that $x_0 x_1 \hat{p}_i \lambda u_0 u_1$ if and only if $x_i \lambda u_i$ and $x_0 x_1 \eta_i u_0 u_1$ if and only if $x_i = u_i$. Thus, for $\lambda \supseteq \beta$ and xy and uv in $S \subseteq \beta$ $x \lambda u$ implies $y \lambda v$ which proves (1). For arbitrary λ from $xy \hat{p}_0 \lambda uv$ one concludes $x \lambda u$ and $xy \eta_0 x \hat{p}_0 \lambda \cap \hat{p}_1 \lambda u u \eta_0 uv$ verifying (2). $\eta_0 + \eta_1 \subseteq \hat{p}_0 \beta$ follows, trivially, since $xy \eta_i uv$ implies that x, y, u , and v are in the same β -class. Conversely, let be xy and uv in S such that $x \beta u$. Then there are x_1, \dots, x_n with $x S x_1 S^{-1} x_2 \dots S x_n S^{-1} u$ and it follows

$$xy \eta_0 x x_1 \eta_1 x_2 x_1 \eta_0 x_2 x_3 \dots \eta_1 u x_n \eta_0 uv.$$

This proves (3).

Proof of 1.1. The given relations are $\eta_i \leq \hat{p}_i \alpha \leq \hat{p}_i \beta \cap \hat{p}_i \gamma$, (C0), (C1), $\kappa + \eta_i = \hat{p}_i \gamma$, (2), and (3). Thus, it suffices to show that $b' = \hat{p}_0 \alpha$ and $c' = \hat{p}_1 \alpha$ are in the sublattice generated by $a = \kappa$, $b = \eta_0$, and $c = \eta_1$. From the relations $ac' = b'c'$ and $b \leq b' \leq b + c$ it follows $cb' = cc'b' = cac' = ac$ and, by modularity,

$$b' = b'(b + c) = b + cb' = b + ac.$$

By symmetry, $c' = c + ab$.

Conversely, if there is a κ such that the relations of Fig. 1 are satisfied then γ centralises β modulo α (by means of a suitable κ'). As it turns out only 3 of the relations in Fig. 1 are needed. This is the content of the following

Theorem 1.4. *For congruences α, β, γ of an algebra A such that $\alpha \subseteq \beta \cap \gamma$ the following are equivalent:*

- (i) γ centralises β modulo α .
- (ii) In the quotient algebra A/α , γ/α centralises β/α (modulo 0).
- (iii) There are an algebra B , a homomorphism p of B onto A , and congruences σ and τ of B such that

$$\sigma + \hat{p}\alpha \supseteq \hat{p}\beta, \quad \tau + \hat{p}\alpha \supseteq \hat{p}\gamma, \quad \text{and} \quad \sigma \cap \tau \subseteq \hat{p}\alpha.$$

The order relations satisfied in (iii) are indicated in Fig. 2.

The map $g = (p_{0S_0} \times p_{0S_1})|T$ is a homomorphism of T onto $R = S_0 \circ S_1^{-1} \subseteq A \times A$ mapping (xz, yz) onto xy . The kernel of g is contained in ε . Hence, the induced lattice isomorphism \tilde{g} maps the interval $1/\varepsilon$ of $L(T)$ isomorphically into $L(R)$.

Observe that $\check{g}\varepsilon_j = \hat{p}_{jR}\alpha$ as well as $\check{g}\varepsilon = \hat{p}_{0R}\alpha \cap \hat{p}_{1R}\alpha$ and $\check{g}(\xi + \varepsilon) = \kappa_0 * \kappa_1$. Therefore, $(\kappa_0 * \kappa_1) \cap \hat{p}_{iR}\alpha = \hat{p}_{0R}\alpha \cap \hat{p}_{1R}\alpha$ for $i = 0, 1$.

If $S_0 = S_1$ and $\kappa_0 = \kappa_1$ then the validity of (RR) for γ and $\kappa_0 * \kappa_1$ is a consequence of $\kappa_0 + \hat{p}_{0S_0}\alpha = \hat{p}_{0S_0}\gamma$. Namely, if $x\gamma u$ then there are x_i, z_i such that the first line in the definition of $\kappa_0 * \kappa_1$ is satisfied with $z = x$ and $w = u$ and one just takes the second line to be the same. If (RR) holds for κ_0 then $xy\kappa_0uv$ implies $y\gamma v$ and $yy\kappa_0vv$ whence $xy\kappa_0 * \kappa_1uv$ by definition with $m = 1, z = y$, and $w = v$. Thus, $\kappa_0 \subseteq \kappa_0 * \kappa_1$ and (RR) follows for $\kappa_0 * \kappa_1$, trivially. This shows, for both cases, that $(\kappa_0 * \kappa_1) + \hat{p}_{iR}\alpha = \hat{p}_{iR}\gamma$.

To finish step A let be γ, β, S, κ central modulo α . Define, inductively, $S_0 = S, \kappa_0 = \kappa, S_{n+1} = S_n \circ S_n^{-1}$, and $\kappa_{n+1} = \kappa_n * \kappa_n$. Then, by the claim, (RR) holds for κ_1 and we get a sequence $\gamma, \beta, S_n, \kappa_n$ ($n \geq 1$) of quadruples central modulo α satisfying (RR), (RS), and $\kappa_n \subseteq \kappa_{n+1}$. Clearly, $\beta = \bigcup S_n$. Let be $\lambda = \bigcup \kappa_n$. Then $\gamma, \beta, \beta, \lambda$ is a central quadruple modulo α , too. Moreover, $\beta \circ \beta = \beta$ and $\lambda * \lambda = \lambda$ whence (RT) is obvious.

Step B. Let p be a homomorphism of B onto $A, \alpha \subseteq \beta \cap \gamma$ congruences of A . Then γ centralises β modulo α if and only if $\hat{p}\gamma$ centralises $\hat{p}\beta$ modulo $\hat{p}\alpha$.

In view of step A we have to associate with a quadruple γ, β, S, κ central modulo α a quadruple $\hat{p}\gamma, \hat{p}\beta, T, \lambda$ central modulo $\hat{p}\alpha$ and vice versa. For the first, let be $T \subseteq B \times B$ the inverse image of S under $p \times p, q = (p \times p)|T$, and $\lambda = \check{q}\kappa$. Conversely, let be $q = (p \times p)|T, S = q(T)$, and observe that

$$\lambda \supseteq \hat{p}_{0T}\hat{p}\alpha \cap \hat{p}_{1T}\hat{p}\alpha \supseteq \ker q.$$

Thus, everything works out if one chooses $\kappa = \check{q}\lambda$.

Step C. If there are congruences φ and χ on A such that $\alpha \cap \varphi = \alpha \cap \chi = \varphi \cap \chi$ then $\alpha + \chi$ centralises $\alpha + \varphi$ modulo α .

Namely, consider $\varphi \subseteq A \times A$ as an algebra with projections $p_{0\varphi}$ and $p_{1\varphi}$. In particular, we have congruences $\varepsilon = \hat{p}_{0\varphi}\alpha \cap \hat{p}_{1\varphi}\alpha$ and $\xi = \hat{p}_{0\varphi}\chi \cap \hat{p}_{1\varphi}\chi$ on φ . It follows $\xi \cap \hat{p}_{0\varphi}\alpha \subseteq \hat{p}_{0\varphi}\chi \cap \hat{p}_{0\varphi}\alpha = \hat{p}_{0\varphi}(\chi \cap \alpha) \subseteq \hat{p}_{0\varphi}\varphi = \hat{p}_{1\varphi}\varphi$, hence

$$\xi \cap \hat{p}_{0\varphi}\alpha \subseteq \hat{p}_{1\varphi}\chi \cap \hat{p}_{1\varphi}\varphi = \hat{p}_{1\varphi}(\chi \cap \varphi) \subseteq \hat{p}_{1\varphi}\alpha \quad \text{and} \quad \xi \cap \hat{p}_{0\varphi}\alpha \subseteq \varepsilon.$$

Symmetrically, one has $\xi \cap \hat{p}_{1\varphi}\alpha \subseteq \varepsilon$ and by modularity one concludes

$$(4) \quad (\xi + \varepsilon) \cap \hat{p}_{i\varphi}\alpha = \varepsilon + (\xi \cap \hat{p}_{i\varphi}\alpha) = \varepsilon \quad \text{for } i = 0, 1.$$

Now, let p denote the canonical homomorphism of A onto A/α and let T be the image of φ under the map $p \times p$. Then T is a reflexive and symmetric subalgebra of $A/\alpha \times A/\alpha$ and its transitive closure is the congruence $\check{p}(\alpha + \varphi)$ of A/α . Observe that ε is just the kernel of $g = (p \times p)|\varphi$. Thus, g is an isomorphism of $1/\varepsilon$ onto $L(T)$. Since $pp_{i\varphi} = p_{iT}g$, trivially, it follows $\check{g}\hat{p}_{i\varphi}\lambda = \hat{p}_{iT}\check{p}\lambda$ for all $\lambda \supseteq \alpha$. In particular, $\check{g}\hat{p}_{i\varphi}\alpha = \eta_{iT}$ and $\check{g}\hat{p}_{i\varphi}(\alpha + \chi) = \hat{p}_{iT}\check{p}(\alpha + \chi)$ for $i = 0, 1$. By (4) one concludes $\check{g}(\xi + \varepsilon) \cap \eta_{iT} = \check{g}((\xi + \varepsilon) \cap \hat{p}_{i\varphi}\alpha) \subseteq \check{g}\varepsilon = 0$ and by (2)

$$\begin{aligned} \check{g}(\xi + \varepsilon) + \eta_{iT} &= \check{g}((\hat{p}_{0\varphi}\chi \cap \hat{p}_{1\varphi}\chi) + \hat{p}_{i\varphi}\alpha) = \check{g}(\hat{p}_{i\varphi}\chi + \hat{p}_{i\varphi}\alpha) = \\ &= \check{g}\hat{p}_{i\varphi}(\alpha + \chi) = \hat{p}_{iT}\check{p}(\alpha + \chi). \end{aligned}$$

Thus, $p(\alpha + \chi)$, $\tilde{p}(\alpha + \varphi)$, T , $g(\xi + \varepsilon)$ is a central quadruple (modulo 0) on A/α . By A and B the claim follows.

Summarising, step **A** and **B** together prove (i) \Leftrightarrow (ii). Finally, in the proof of (iii) \Rightarrow (i) step **B** allows us to consider the case where $B = A$ and p is the identity map on A , only. Let $\alpha, \beta, \gamma, \sigma, \tau$ be congruences on A such that $\sigma \cap \tau \subseteq \alpha \subseteq \beta \cap \gamma$, $\beta \subseteq \alpha + \sigma$, and $\gamma \subseteq \alpha + \tau$. Put $\sigma' = \beta \cap \sigma$, $\gamma' = \gamma \cap \tau$. Then $\sigma' \cap \tau' \subseteq \alpha$ and, by modularity, $\alpha + \sigma' = \beta$ and $\alpha + \tau' = \gamma$. Now, define $\varphi = \sigma' + (\alpha \cap \tau')$ and $\chi = \tau' + (\alpha \cap \sigma')$. By modularity we get $\alpha \cap \varphi = \alpha \cap \chi = \varphi \cap \chi$. Clearly,

$$\alpha + \varphi = \beta \quad \text{and} \quad \alpha + \chi = \gamma.$$

Thus, by step **C** γ centralises β modulo α .

Proposition 1.6. *For congruences $\alpha \subseteq \beta \cap \gamma$ of an algebra A there is at most one congruence κ of β satisfying (C0), (C1), and (RR). Any such satisfies (RS) and (RT), too.*

Proof. Let κ_0 and κ_1 be such. By Claim 1.5 $\gamma, \beta, \beta, \kappa_0 * \kappa_1$ is central modulo α and $\kappa_i \subseteq \kappa_0 * \kappa_1$. In particular, we have

$$\begin{aligned} \hat{p}_0 \alpha \cap \kappa_i &= \hat{p}_0 \alpha \cap \hat{p}_1 \alpha = \hat{p}_0 \alpha \cap (\kappa_0 * \kappa_1) \quad \text{and} \quad \hat{p}_0 \alpha + \kappa_i = \hat{p}_0 \gamma = \\ &= \hat{p}_0 \alpha + (\kappa_0 * \kappa_1). \end{aligned}$$

By modularity it follows $\kappa_i = \kappa_0 * \kappa_1$. Then, (RS) and (RT) are obvious.

§ 2. Commutators. For every two congruences γ and β of an algebra A there is a smallest congruence α of A such that γ centralises β modulo α . This α shall be called the *commutator* $[\gamma, \beta]$ of γ and β .

Namely, for families α_i and κ_i such that γ centralises β modulo α_i by means of κ_i one has that γ centralises β modulo $\bigcap \alpha_i$ by means of $\bigcap \kappa_i$.

Corollary 2.1. *If β, γ, δ are congruences of A such that $\delta \subseteq \beta \cap \gamma$ then γ centralises β modulo δ if and only if $\delta \supseteq [\gamma, \beta]$.*

Proof. Let be $\alpha = [\gamma, \beta] \subseteq \delta \subseteq \beta \cap \gamma$ and κ such that γ centralises β modulo α by means of κ . Then by 1.1 the relations of Fig. 1 are valid and one has

$$\hat{p}_0 \alpha \subseteq \hat{p}_0 \delta \subseteq \hat{p}_0 \beta \cap \hat{p}_0 \gamma.$$

Define $\sigma = \hat{p}_1 \alpha + \kappa \cap \hat{p}_0 \delta$ and $\tau = \kappa + \hat{p}_0 \delta \cap \hat{p}_1 \alpha$. Then $\sigma + \hat{p}_0 \delta = \hat{p}_0 \beta$ and $\tau + \hat{p}_0 \delta = \hat{p}_0 \gamma$ are trivial. By modularity one gets

$$\begin{aligned} \sigma \cap \tau &= \kappa \cap (\hat{p}_1 \alpha + \kappa \cap \hat{p}_0 \delta) + \hat{p}_0 \delta \cap \hat{p}_1 \alpha = \\ &= \kappa \cap \hat{p}_1 \alpha + \kappa \cap \hat{p}_0 \delta + \hat{p}_0 \delta \cap \hat{p}_1 \alpha \subseteq \hat{p}_0 \delta. \end{aligned}$$

Thus, (iii) in Thm. 1.4 is satisfied with $B = \beta$ and $p = p_0$. Consequently, γ centralises β modulo δ . The converse is trivial.

Theorem 2.2. *For congruences β, γ, β_i ($i \in I$) of an algebra A one has*

$$[\gamma, \beta] = [\beta, \gamma] \subseteq \beta \cap \gamma \quad \text{and} \quad [\gamma, \sum \beta_i] = \sum [\gamma, \beta_i].$$

In other words, using the terminology of Steinfeld [16] and Keimel [9] the congruence lattice $L(A)$ of a strictly modular algebra together with the commutator operation $[,]$ forms a completely m -distributive negatively ordered algebraic cm -lattice.

Proof. The first claim is obvious in view of Thm. 1.4. The second is proved in three steps.

Step A. If γ centralises β modulo α and $\delta \subseteq \gamma$ then δ centralises β modulo $\alpha \cap \delta$.

Step B. If γ centralises β modulo α and $\alpha \subseteq \alpha'$ then $\gamma + \alpha'$ centralises $\beta + \alpha'$ modulo α' .

Step C. If for all $i \in I$ γ centralises β_i modulo α then γ centralises $\sum \beta_i$ modulo α .

Namely, in **A** assume that γ centralises β modulo α by means of κ and consider $\lambda = \kappa \cap \hat{p}_0 \delta \cap \hat{p}_1 \delta$. Then (RR) is true for λ with respect to δ and by (C1) one has $\lambda \cap \hat{p}_1 \alpha \subseteq \hat{p}_0 \alpha$. Hence, $\lambda \cap \hat{p}_1 \alpha \subseteq \hat{p}_0 \alpha \cap \hat{p}_0 \delta = \hat{p}_0(\alpha \cap \delta)$ and (iii) of 1.4 applies to show the claim. **B** is immediate by 1.4. To prove **C** let γ centralise β_i modulo α by means of κ_i . Claim 1.5 describes a binary operation on the set of all quadruples γ, β, S, κ which are central modulo α and satisfy (RR). Let Q be the subgroupoid generated by the $\gamma, \beta_i, \beta_i, \kappa_i$ ($i \in I$). The quadruples in Q are of the form

$$\gamma, \beta_{i_1} + \cdots + \beta_{i_n}, \beta_{i_1} \circ \cdots \circ \beta_{i_n}, \kappa_{i_1} \cdots \kappa_{i_n}$$

and Q is directed by inclusion in each of its components. Thus, taking the union in each component one gets a quadruple $\gamma, \sum \beta_i, \sum \beta_i, \kappa$ which is central modulo α .

Summarising, **A** and $[\gamma, \beta] = [\beta, \gamma]$ prove $[\gamma, \beta_i] \subseteq [\gamma, \sum \beta_j]$. On the other hand if γ centralises β_i modulo α_i , then by **B** $\gamma = \gamma + \sum \alpha_j$ centralises β_i modulo $\sum \alpha_j$. Hence, by **C** γ centralises $\sum \beta_i$ modulo $\sum \alpha_j$. This implies $[\gamma, \sum \beta_i] \subseteq \sum [\gamma, \beta_i]$ and, with the above, equality.

Proposition 2.3. If $R \subseteq \gamma$ generates the congruence γ then the congruence κ on β which is generated by $\{(xx, uu) \mid xRu\}$ satisfies (C0)–(RT) and one has

$$[\gamma, \beta] = \check{p}_0(\eta_0 + (\kappa \cap \eta_1)).$$

Proof. Freese and Jónsson [4] considered the automorphism ' of β with $(xy)' = yx$. Clearly, it induces an automorphism ' of $L(\beta)$ with $\eta'_0 = \eta_1$ and $\eta'_1 = \eta_0$. Moreover, it leaves κ invariant since it leaves invariant its generating set. Now, let be $\alpha = \check{p}_0(\eta_0 + (\kappa \cap \eta_1))$. Then

$$\hat{p}_0 \alpha = \eta_0 + (\kappa \cap \eta_1) \quad \text{and} \quad \hat{p}_1 \alpha = (\eta_0 + (\kappa \cap \eta_1))' = \eta_1 + (\kappa \cap \eta_0).$$

Applying Observation 1.2 to $a = \kappa$, $b = \eta_0$, and $c = \eta_1$ one can read off from Fig. 1 $\hat{p}_0 \alpha \cap \kappa = \hat{p}_1 \alpha \cap \kappa = \hat{p}_0 \alpha \cap \hat{p}_1 \alpha$. Since $\check{p}_0(\eta_0 + \kappa)$ contains R we have

$$\eta_0 + \kappa \supseteq \hat{p}_0 \gamma \quad \text{and} \quad \alpha \supseteq [\gamma, \beta]$$

by Theorem 1.4. On the other hand, let λ be the congruence such that γ centralises

β modulo $[\gamma, \beta]$ by means of λ . Then due to (RR) the generating set of κ is contained in λ and so is κ . Consequently, $[\gamma, \beta] = \hat{p}_0(\eta_0 + (\lambda \cap \eta_1)) \supseteq \alpha$ and $\alpha = [\gamma, \beta]$. Now, we have $\kappa \subseteq \lambda$, $\hat{p}_0\alpha \cap \lambda = \hat{p}_0\alpha \cap \hat{p}_1\alpha \subseteq \kappa$, and $\hat{p}_0\alpha + \kappa = \eta_0 + \kappa = \hat{p}_0\gamma \supseteq \lambda$, hence $\kappa = \lambda$ by modularity.

Corollary 2.4. $[\gamma, \beta] = 0$ if and only if there is a congruence κ on β such that every set $\{xx|x\gamma u\}$ is a class of κ .

Proof. If $[\gamma, \beta] = 0$ just take κ satisfying (RR) and $\eta_0 \cap \kappa = 0$. Conversely, if there is any congruence on β which has every $\{xx|x\gamma u\}$ as a class then so does the congruence κ defined in 2.3. This κ satisfies (C0)–(RT) with respect to γ and β . Therefore, with $xy\lambda uv \Leftrightarrow x\kappa yv$ we get a congruence on γ satisfying (C0) and (RR)–(RT) with respect to β and γ . By hypothesis, $\eta_0 \cap \lambda = \eta_1 \cap \lambda = 0$ whence $[\beta, \gamma] = 0$.

§ 3. Prime and semiprime congruences. A congruence α of an algebra A is called *prime* if for all congruences β and γ of A $[\beta, \gamma] \subseteq \alpha$ implies $\beta \subseteq \alpha$ or $\gamma \subseteq \alpha$. The congruence α is called *semiprime* if $[\beta, \beta] \subseteq \alpha$ implies $\beta \subseteq \alpha$ or, equivalently, if $[\beta, \gamma] \subseteq \alpha$ implies $\beta \cap \gamma \subseteq \alpha$. An algebra A is called *prime* (semiprime) if its identical congruence is prime (semiprime). Combining Thm. 2.2 with the results of Keimel [9] one sees that the following hold: The prime congruences are exactly the \cap -irreducible semiprime congruences. The meet of semiprime congruences is semiprime. Every semiprime congruence is the meet of suitable prime congruences.

On the way to a lattice theoretic characterisation of prime and semiprime congruences observe that in both definitions we may restrict ourselves to consider congruences β and γ containing α , only. Thus, for a homomorphism p of B onto A the congruence α is prime (semiprime) if and only if $\hat{p}\alpha$ is so.

An element a of a modular lattice $(L, +, \cdot)$ is called *prime* if for all b, c in L $bc \leq a$ implies $b \leq a$ or $c \leq a$. It is called *semiprime* if for all b, c in L with $bc \leq a$ the sublattice generated by a, b , and c is distributive. Again, the prime elements are exactly the finitely meet irreducible semiprime elements — cf. 1.2.

Theorem 3.1. A congruence α of an algebra A is prime (semiprime) if and only if for every algebra B and homomorphism p of B onto A the congruence $\hat{p}\alpha$ is a prime (semiprime) element of the lattice $L(B)$. It suffices to consider the case where $B \supseteq \alpha$ is a congruence of A and p the first projection.

Corollary 3.2. An algebra A is prime if and only if every homomorphism of a finite subdirect product onto A factors through one of the projections.

Corollary 3.3. Let \mathcal{C} be a class of algebras generating a congruence modular variety \mathcal{V} and $A \in \mathcal{V}$ a prime algebra. Then A is a homomorphic image of a subalgebra of an ultraproduct of algebras in \mathcal{C} .

This is an immediate consequence of Lemma 3.1 in Jónsson [8] — cf. Gierz and Keimel [5; 4.3]. For a finite class \mathcal{C} of finite groups 3.3 is due to Kovács and Newman

[10]. Namely, a finite group is prime if and only if it is monolithic with non-abelian minimal normal subgroup.

Proof of Theorem 3.1. Since α is \cap -irreducible if and only if $\hat{p}\alpha$ is we have to consider the case of "semiprime", only. If α is not semiprime then there is a $\gamma \supset \alpha$ with $[\gamma, \gamma] \subseteq \alpha$. Due to Proposition 1.1 there is a κ such that the sublattice of $L(\gamma)$ which is generated by $\hat{p}_0\alpha, \kappa$, and $\hat{p}_1\alpha$ is not distributive. But, $\hat{p}_0\alpha \supseteq \kappa \cap \hat{p}_1\alpha$ whence $\hat{p}_0\alpha$ is not a semiprime element of $L(\gamma)$.

Conversely, assume that α is semiprime and p a homomorphism of B onto A . Consider φ and χ in $L(B)$ such that $\varphi \cap \chi \subseteq \hat{p}\alpha$. Define $\sigma = \varphi + (\chi \cap \hat{p}\alpha)$ and $\tau = \chi + (\varphi \cap \hat{p}\alpha)$. By modularity we have $\sigma \cap \hat{p}\alpha = \tau \cap \hat{p}\alpha = \sigma \cap \tau$. Clearly,

$$\sigma + \hat{p}\alpha = \varphi + \hat{p}\alpha \quad \text{and} \quad \tau + \hat{p}\alpha = \chi + \hat{p}\alpha.$$

By Theorem 1.4 it follows that $[\check{p}(\chi + \hat{p}\alpha), \check{p}(\varphi + \hat{p}\alpha)] \subseteq \alpha$, whence

$$\check{p}(\chi + \hat{p}\alpha) \cap \check{p}(\varphi + \hat{p}\alpha) \subseteq \alpha \quad \text{and} \quad (\chi + \hat{p}\alpha) \cap (\varphi + \hat{p}\alpha) = \hat{p}\alpha.$$

Thus, the sublattice generated by $\hat{p}\alpha$, φ , and χ is distributive.

§ 4. Neutral algebras. Every normal subgroup of a completely reducible group is completely reducible and a direct factor. Similar theorems are known for Lie algebras and for primal algebras and their generalisations (see e.g. R. McKenzie [11]). They may be subsumed under the following claim.

Claim. Let \mathcal{A} and \mathcal{B} be sets of simple algebras contained in a congruence permutable variety such that for every $A \in \mathcal{A}$ the algebra A^2 has exactly four (i.e. no skew) congruences. Then every homomorphic image of a finite subdirect product D of algebras in $\mathcal{A} \cup \mathcal{B}$ can be represented as a direct product of algebras in \mathcal{A} and an algebra in the variety generated by \mathcal{B} .

If one passes to congruence modular varieties subdirect products take the place of direct products. For the proof one just observes that the congruence lattice of D^2 is a finite dimensional dually atomistic modular lattice and that every coatom corresponding to an algebra in \mathcal{A} is a central element since it cannot be dually perspective to any other coatom — cf. [2; ch. IV].

Here, we intend to get away from the hypothesis of simplicity, i.e. from dually atomistic lattices. Generalising the notion of a central element one defines: An element a of a modular lattice L is called *neutral* if for all b and c in L the sublattice generated by a , b , and c is distributive. This means that the map $x \mapsto (xa, x + a)$ yields a representation of L as a subdirect product of the intervals $a/0$ and $1/a$.

Theorem 4.1. *For a (strictly modular) algebra A the following are equivalent:*

- (i) *Every congruence of A has distributive congruence lattice.*
- (ii) *Every congruence of A is semiprime.*
- (iii) *For every congruence α of A , algebra B , and homomorphism p of B onto A the congruence $\hat{p}\alpha$ is a neutral element of $L(B)$.*
- (iv) *For every homomorphic image B of A , algebra C , subdirect product $D \subseteq B \times C$, and congruence δ of D there are congruences β of B and γ of C such that $\delta = (\beta \times \gamma) \upharpoonright D$.*

We suggest to call such algebras *neutral*. Clearly, the following are equivalent to A being neutral: every completely meet irreducible congruence of A is prime; $[\beta, \gamma] = \beta \cap \gamma$ for all congruences β and γ of A ; $[\gamma, \gamma] = \gamma$ for all (principal) congruences of A . The congruence lattice of a neutral algebra is a Brouwerian lattice — cf. Keimel [9; § 2]. In particular, it is distributive.

Examples of neutral algebras are: simple nonabelian groups, semisimple classical Lie algebras, and von Neumann regular rings. Actually, for classical Lie algebras and for rings satisfying a polynomial identity these are the only possible examples — see [1].

In [6] it has been shown that for an algebra A in a congruence permutable variety is neutral if and only if it has the following “Interpolation Property”: Every partial congruence preserving operation on A can be locally represented by polynomials with constants in A .

Corollary 4.2. *Finite subdirect products, homomorphic images, and direct unions of neutral algebras are neutral.*

Corollary 4.3. *The join of two congruence distributive subvarieties of a congruence modular variety is congruence distributive.*

According to condition (i) every simple algebra A such that A^2 has exactly four congruences is neutral. Thus, the following appears as a generalisation of the above Claim.

Corollary 4.4. *Let \mathcal{A} be a finite set of finite neutral algebras and \mathcal{B} a variety, both contained in a congruence modular variety. Suppose that every homomorphic image of a subalgebra of an algebra in \mathcal{A} is contained in $\mathcal{A} \cup \mathcal{B}$. Then any algebra in the variety generated by $\mathcal{A} \cup \mathcal{B}$ is a subdirect product of algebras in \mathcal{A} and an algebra in \mathcal{B} . If it is finitely generated then one needs only finitely many factors from \mathcal{A} . For the proofs we need an elementary lattice theoretic result from [6].*

Lemma 4.5. *Let M be a modular lattice with 0 and 1. Let a and b be elements of M with $ab = 0$ and such that the intervals $1/a$ and $1/b$ are distributive and for all $x \leq a + b$ it holds $x = (a + x)(b + x)$. Then M is distributive.*

Corollary 4.6. *Let M be a modular lattice with 0 and 1 and a_1, \dots, a_n neutral elements such that $a_1 \cdot \dots \cdot a_n = 0$ and for all i $1/a_i$ is distributive. Then M is distributive.*

Proof of Theorem 4.1. Let A be neutral, $\alpha \in L(A)$, $p: B \twoheadrightarrow A$. For arbitrary φ and χ in B put $\delta = (\varphi \cap \chi) + \check{p}\alpha$. By hypothesis $\check{p}\delta$ is semiprime in A , hence the sublattice generated by δ , φ , and χ in $L(B)$ is distributive due to Theorem 3.1. Thus, the sublattice generated by $\check{p}\alpha$, φ , and χ is distributive, too, which means that $\check{p}\alpha$ is neutral in $L(B)$. This proves (ii) \Rightarrow (iii).

Clearly, every homomorphic image of a neutral algebra is neutral. In the context of (iv) let b and c be the projections of D onto B and C resp. and $\beta = \check{b}(\delta + \ker b)$, $\gamma = \check{c}(\delta + \ker c)$. Observe that (iv) means just $\delta = (\delta + \ker b) \cap (\delta + \ker c)$. But,

if (iii) holds this is true since $\ker b$ is a neutral element of $L(D)$. This proves (iii) \Rightarrow (iv).

Now, assume that (iv) holds. First, we show that $L(A)$ is distributive. If otherwise, there would be congruences $\beta_0, \gamma_0, \delta_0$ forming the atoms of a five element nondistributive sublattice of $L(A)$. Then with $B = A/\beta_0$, $C = A/\gamma_0$, and δ corresponding to δ_0 in the subdirect product $A/\beta_0 \cap \gamma_0$ we would get a contradiction. Thus, due to Lemma 4.5 every subdirect square $D \subseteq A \times A$ has distributive congruence lattice, proving (i). In view of Theorems 3.1 (i) implies (ii) trivially. By Corollary 4.6 every finite subdirect product B of neutral algebras has distributive congruence lattice and so does every subdirect square of B . According to condition (i) B is neutral. Since every congruence on a direct union is a direct union of congruences direct unions of neutral algebras are neutral. The second corollary follows immediately by the fact that every algebra in the join is a homomorphic image of a subdirect product of an algebra in the first and an algebra in the second variety.

Before we prove 4.4 we introduce some operators for classes of algebras. For a class \mathcal{C} of algebras we write $D\mathcal{C}$ for (the class of all) direct unions, $H\mathcal{C}$ for homomorphic images, $P\mathcal{C}$ ($P_f\mathcal{C}$) for (finite) direct products, $P_s\mathcal{C}$ ($P_{sf}\mathcal{C}$) for (finite) subdirect products, and $P_u\mathcal{C}$ for ultraproducts of algebras in \mathcal{C} . The class \mathcal{C} is called a *local variety* if it is closed under D , H , S , and P_f . A local variety is a variety if it is closed under P_u . For any class \mathcal{C} the class $DHSP_f\mathcal{C} = DHP_{sf}S\mathcal{C}$ is the local variety $\text{Loc } \mathcal{C}$ generated by \mathcal{C} (cf. T. K. Hu [7]). The variety generated by \mathcal{C} is $HSP\mathcal{C}$ and coincides with $\text{Loc } \mathcal{C}$ if \mathcal{C} consist of finitely many finite algebras.

Now, in the proof of 4.4 we have $SP(\mathcal{A} \cup \mathcal{B}) = P_s(\mathcal{A} \cup \mathcal{B})$ by hypothesis. Thus, if $C \in SP(\mathcal{A} \cup \mathcal{B})$ is finitely generated then C is a subdirect product

$$C \subseteq A_1 \times \cdots \times A_n \times B$$

with $A_i \in \mathcal{A}$ and $B \in \mathcal{B}$. Since the A_i are neutral any homomorphic image is again of that form. This proves $C \in P_s(\mathcal{A} \cup \mathcal{B})$ for every finitely generated $C \in HSP(\mathcal{A} \cup \mathcal{B})$. Now, every algebra in $HSP(\mathcal{A} \cup \mathcal{B})$ is a subalgebra of an ultraproduct of such, i.e. in $SP_u P_s(\mathcal{A} \cup \mathcal{B}) \subseteq SP_u SP(\mathcal{A} \cup \mathcal{B}) = SPP_u(\mathcal{A} \cup \mathcal{B}) = P_s(\mathcal{A} \cup \mathcal{B})$ since both \mathcal{A} and \mathcal{B} are closed under P_u .

Finally, let us make some remarks about classes of neutral algebras. By Corollary 4.2 for a class \mathcal{C} contained in a congruence modular local variety $\text{Loc } \mathcal{C}$ is congruence distributive and in fact consists of neutral algebras if all algebras in $S\mathcal{C}$ are neutral. In particular, the algebras A for which $\text{Loc } A$ is congruence distributive form a local subvariety.

Using condition (i) of Theorem 4.1 one concludes that an algebra A is neutral if and only if for the algebra A^* which arises from A by adding all its elements as constants the local variety $\text{Loc } A^*$ is congruence distributive. In particular, direct powers of finite neutral algebras are neutral.

For infinite algebras that may not be true. But, if A is a direct product of neutral algebras such that every congruence on A is induced via a family of congruences on the factors and a filter on the index set and if all homomorphic images of A

which are given by an ultrafilter are neutral then A is neutral. The first condition is always satisfied in a variety in which every congruence on a direct product $A \times B$ is a direct product of a congruence of A and one of B (e.g. for rings with 1).

Finally, if the class of neutral algebras in a congruence modular variety is closed under ultraproducts then it can be axiomatised by finitely many positive universal-existential sentences (whence it is closed under direct products, too). Namely, recall that Mal'cev [13] described the congruence generated by a given set of pairs in A via unary polynomial operations with constants in A . Using this for each m one easily constructs a sequence $\Phi_n(s, t, \vec{u}, \vec{v}, \vec{x}, \vec{y})$ of universal existential formulas with vectors of variables having length m such that for $R = \{(c_i, d_i) \mid 1 \leq i \leq n\}$ and $S = \{(e_i, f_i) \mid 1 \leq i \leq n\}$ one has $(a, b) \in [\gamma, \beta]$ — where β is generated by R and γ by S — if and only if there is an n such that $\Phi_n(a, b, \vec{c}, \vec{d}, \vec{e}, \vec{f})$. In particular, the principal congruence β generated by (a, b) is perfect ($[\beta, \beta] = \beta$) if and only if there is an n such that $\Phi_n(a, b, a, b, a, b)$.

References

- [1] E. P. ARMENDARIZ and J. W. FISCHER, Regular P.I.-rings. Proc. Amer. Math. Soc. **39**, 247—251 (1973).
- [2] G. BIRKHOFF, Lattice Theory. Providence R.I. 1967.
- [3] P. M. COHN, Universal algebra. New York 1965.
- [4] R. FREESE and B. JÓNSSON, Congruence modularity implies the Arguesian identity. Algebra Universalis **6**, 225—228 (1976).
- [5] G. GIERZ and K. KEIMEL, A lemma on primes appearing in algebra and analysis. Houston J. Math. **3**, 207—224 (1977).
- [6] J. HAGEMANN and C. HERRMANN, Arithmetical locally equational classes and representation of partial functions. To appear in Coll. Math. Soc. J. Bolyai, Universal Algebra Conf. Esztergom 1977.
- [7] T. K. HU, Locally equational classes of universal algebras. Chinese J. Math. **1**, 143—165 (1973).
- [8] B. JÓNSSON, Algebras whose congruence lattices are distributive. Math. Scand. **21**, 110—121 (1972).
- [9] K. KEIMEL, A unified theory of minimal prime ideals. Acta Math. Ac. Sci. Hung. **32**, 51—69 (1972).
- [10] L. G. KOVÁCS and M. F. NEWMAN, Minimal verbal subgroups. Proc. Cambridge Phil. Soc. **62**, 347—350 (1966).
- [11] R. MCKENZIE, Paraprimal varieties: a study of finite axiomatizability and definable principal congruences in locally finite varieties. To appear in Algebra Universalis.
- [12] F. MAEDA, Kontinuierliche Geometrien. Berlin 1958.
- [13] I. A. MAL'CEV, On a general theory of algebraic systems (russian). Mat. Sbornik **53**, 3—20 (1954).
- [14] I. A. MAL'CEV, Algebraic Systems. Berlin 1973.
- [15] J. D. H. SMITH, Mal'cev varieties. Berlin 1976.
- [16] O. STEINFELD, Primelemente und Primradikale in gewissen verbandsgeordneten algebraischen Strukturen. Acta Math. Ac. Sci. Hung. **19** 243—261 (1968).

Eingegangen am 10. 2. 1979

Anschrift der Autoren:

J. Hagemann and C. Herrmann, Fachbereich Mathematik AG1,
Technische Hochschule Darmstadt, Schloßgartenstr. 7 D-6100 Darmstadt