Sonderabdruck aus
ARCHIV DER MATHEMATIK
Vol. 36, 1981 BIRKHÄUSER VERLAG, BASEL UND STUTTGART Fasc. 6

Congruence modularity is permutability composed with distributivity

By

H. Peter Gumm

0. The main result of this paper is a Mal'cev type characterization of congruence modular varieties, using ternary polynomials only.

The polynomials we produce are especially nice, since they are just Jónsson's polynomials for congruence distributivity and Mal'cev's polynomial for permutability glued together.

Moreover, the fact that modularity can be described by ternary terms at all is somewhat surprising as there are nonmodular varieties all of whose 3-generated algebras are congruence modular.

A. Day [1] was the first one to give a Mal'cev type characterization for congruence modularity. His results will be used in this paper, however, we do not compose our polynomials from Day's quaternary polynomials.

Since it fits in nicely, we also present some new results about permutability of congruences in a modular variety, which generalize those given in Gumm [2], Herrmann [5] and Gumm, Herrmann [4].

These results were obtained while the author was a guest of the Math. Departments of Lakehead University and of McMaster University. This is the opportunity to thank A. Day and G. Bruns for making this stay pleasant and fruitful.

1. To produce our polynomials we make use of the concept of the commutator $[\alpha, \beta]$ of two congruences α and β. This concept was developed for modular varieties by Hagemann and Herrmann in [6], (c.f. Gumm [3]). Actually, apart from Lemma 1, we will only need the following facts: $[\ ,\ ]$ is a binary operation on every congruence lattice of an algebra in a modular variety, satisfying:

1. $[\ ,\ ]$ is monotonic in both arguments.
2. $[\alpha, \beta] \leqq \alpha \wedge \beta$ for any two congruences α, β.
3. $[\alpha, \beta \vee \gamma] = [\alpha, \beta] \vee [\alpha, \gamma]$.

For the special case $[\alpha, \alpha] = 0$ the following result is in Ch. Herrmann [5]. For a proof again, we recommend [3] or Taylor [9].

Research supported in part by NSERC operating grant A-8190.

1.1. Lemma. *In a modular variety there exists a ternary polynomial p such that*

$$p(x, y, y) = x \quad \text{is an equation true in } \mathscr{V}$$

and

$$p(x, x, y)\,[\alpha, \alpha]\,y \quad \text{for all} \quad (x, y) \in \alpha,$$

where α is a congruence on $\mathscr{A} \in \mathscr{V}$.

The following quite obvious corollary has been overlooked for some time. After I first noticed, it, I learned that W. Taylor [9] had found it independently.

1.2. Corollary. *Let θ and ψ be congruences on an algebra $\mathscr{A}$ in a modular variety $\mathscr{V}$. Then*

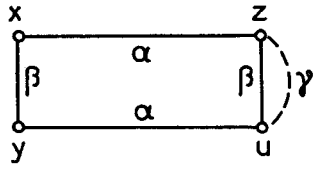
$$\theta \circ \psi \subseteqq [\theta, \theta] \circ \psi \circ \theta \quad \text{and}$$
$$\theta \circ \psi \subseteqq \psi \circ \theta \circ [\psi, \psi].$$

Proof. $x\,\theta\,y\,\psi\,z$ implies

$$x\,[\theta, \theta]\,p(y, y, x)\,\psi\,p(z, y, x)\,\theta\,p(z, y, y) = z \quad \text{and}$$
$$x = p(x, y, y)\,\psi\,p(x, y, z)\,\theta\,p(y, y, z)\,[\psi, \psi]\,z.$$

We also recall from [2] the

1.3. Shifting Lemma. *Let $\mathscr{A}$ have a modular congruence lattice, α, β, γ congruences on $\mathscr{A}$ with $\alpha \wedge \beta \leqq \gamma$ and x, y, z, u elements of $\mathscr{A}$. Then*



implies $x\,\gamma\,y$.

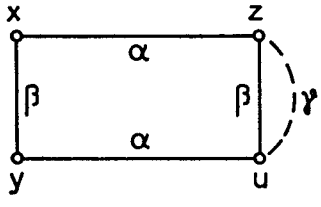
This is a special instance of applying the modular law, namely notice that

$$(x, y) \in \beta \wedge (\alpha \vee (\beta \wedge \gamma)) = (\alpha \wedge \beta) \vee (\beta \wedge \gamma) \leqq \gamma$$

by modularity.

A. Day shows implicitly in [1] that a (quasi) variety is congruence modular if and only if $\beta \wedge (\alpha \circ (\beta \wedge \delta) \circ \alpha) \subseteqq (\alpha \wedge \beta) \vee (\beta \wedge \delta)$ for some congruences α, β and δ in the free algebra on four generators.

But if $(x, y) \in \beta \wedge (\alpha \circ (\beta \wedge \delta) \circ \alpha)$ then there exist z and u with



with $\gamma := (\alpha \wedge \beta) \vee (\beta \wedge \delta)$.

Applying the Shifting Lemma gives us $(x, y) \in \gamma$, hence for a (quasi) variety the Shifting Lemma is equivalent to modularity.

We have all tools at hand now to prove our main theorem:

1.4. Theorem. *Let $\mathscr{V}$ be a (Quasi-)variety of universal algebras. Then the following are equivalent:*

(i) *$\mathscr{V}$ is congruence modular.*

(ii) *For congruences $\alpha, \beta, \gamma \in \mathrm{Con}(\mathscr{A})$ with $\mathscr{A} \in \mathscr{V}$ we have*

$$\alpha \leqq \beta \vee \gamma \Rightarrow \alpha \circ \beta \subseteq [(\alpha \wedge \beta) \vee (\alpha \wedge \gamma)] \circ \beta \circ \alpha .$$

(iii) *There exists a natural number n and ternary polynomials $q_0, \ldots, q_n, p$, such that the following identities are true in $\mathscr{V}$:*

1. $q_0(x, y, z) = x$
2. $q_i(x, y, x) = x$ *for* $0 \leqq i \leqq n$
3. $q_i(x, y, y) = q_{i+1}(x, y, y)$ *for i even*
4. $q_i(x, x, y) = q_{i+1}(x, x, y)$ *for i odd*

} *(Distributive part),*

5. $q_n(x, y, y) = p(x, y, y)$
6. $p(x, x, y) = y$

} *(Permutable part).*

Comment. It may be interesting to notice that p could be trivial (i.e. a projection). In that case p would be the third projection and $q_n(x, y, y)$ would be equal to y. We may suppose i is even, since otherwise we have $q_{n-1}(x, y, y) = y$ as well. Thus define $q_{n+1}(x, y, z) = z$.

Now the equations we are left with are precisely B. Jónsson's equations showing the $\mathscr{V}$ is congruence-distributive [7].

On the other hand, if all the q_i's are projections, this would imply $q_i(x, y, z) = x$ for every i. Hence, what we are left with are the equations

$$x = p(x, y, y) \quad \text{and} \quad p(x, x, y) = y ,$$

which are precisely *A.* I. Mal'cev's equations for permutability of congruences [8].

Proof of 1.4. For (i) $\rightarrow$ (ii) we use Corollary 2 and the properties of the commutator yielding

$$[\alpha, \alpha] \leqq [\alpha, \beta \vee \gamma] = [\alpha, \beta] \vee [\alpha, \gamma] \leqq (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) .$$

Thus $\alpha \circ \beta \leqq ((\alpha \wedge \beta) \vee (\alpha \wedge \gamma)) \circ \beta \circ \alpha$.

(ii) $\rightarrow$ (iii): Let $F_{\mathscr{V}}(3)$ be the free algebra in $\mathscr{V}$ generated by $X = \{x, y, z\}$. Consider the congruences $\theta_{(x,y)}$, $\theta_{(y,z)}$ and $\theta_{(x,z)}$ which are generated by the nontrivial partitions of X.

Clearly $\theta_{(y,z)} \vee \theta_{(x,z)} \geqq \theta_{(x,y)}$. Hence (ii) tells us:

$$\theta_{(x,y)} \circ \theta_{(y,z)} \leqq ((\theta_{(x,y)} \wedge \theta_{(y,z)}) \vee (\theta_{(x,y)} \wedge \theta_{(x,z)})) \circ \theta_{(y,z)} \circ \theta_{(x,y)} .$$

(x, z) is in the left hand side, hence in the right hand side, which implies that there exist elements $t_0, \ldots, t_n, r$ in $F_{\mathscr{V}}(3)$ such that

(0) $x = t_0$.

(2′) $t_i \theta_{(x,y)} \wedge \theta_{(y,z)} t_{i+1}$ for i even.

(3′) $t_i \theta_{(x,y)} \wedge \theta_{(x,z)} t_{i+1}$ for i odd.

(4) $t_n \theta_{(y,z)} r$ and

(5) $r \theta_{(x,y)} z$.

We rewrite (2') and (3') by

(1) $t_i \theta_{(x,y)} x$ for all i.

(2) $t_i \theta_{(y,z)} t_{i+1}$ for i even

(3) $t_i \theta_{(x,z)} t_{i+1}$ for i odd.

By the usual arguments then the t_i and r do correspond to ternary polynomials $\bar{q}_i$ and p such that (in accordance with (0), ..., (5)) the following equations are satisfied in $\mathscr{V}$:

(0) $x = \bar{q}_0(x, y, z)$.

(1) $\bar{q}_i(x, x, y) = x$ for all $0 \leqq i \leqq n$.

(2) $\bar{q}_i(x, y, y) = \bar{q}_{i+1}(x, y, y)$ for i even.

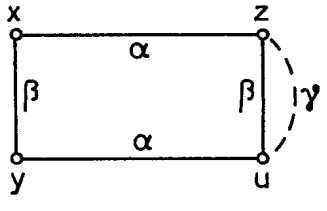
(3) $\bar{q}_i(x, y, x) = q_{i+1}(x, y, x)$ for i odd.

(4) $\bar{q}_n(x, y, y) = p(x, y, y)$.

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

By simply redefining $q_i(x, y, z) := \bar{q}_i(x, z, y)$ we get the desired polynomials.

For (iii) $\rightarrow$ (i) we prove the Shifting Lemma, i.e. we start with congruences α, β, γ with $\alpha \wedge \beta \leqq \gamma$ and elements x, y, z, u such that



We might as well assume $\alpha \wedge \beta = 0$, otherwise we would have to replace equality signs by $\equiv (\mathrm{mod}\ \alpha \wedge \beta)$.

Consider the following points (elements):

$$\tilde{p} := p(z, u, y), \quad \bar{q}_i := q_i(x, u, y), \quad \hat{q}_i := q_i(x, z, y) \quad \text{and}$$
$$\tilde{q}_n := q_n(z, y, u).$$

We obtain the following relations:

I $x \beta \bar{q}_i$ for all i,

II $x \beta \hat{q}_i$ for all i by using equation 2.

Equation 6 yields:

III $y(\beta \wedge \gamma) \tilde{p}$.

Thus the $\bar{q}_i$, $\hat{q}_i$ and $\tilde{p}$ lie on the β-line connecting x and y, in particular they are mutually β-congruent. Equations 3 and 4 now yield:

IV $\bar{q}_i \alpha \bar{q}_{i+1}$ for i even and

V $\hat{q}_i \alpha \hat{q}_{i+1}$ for i odd.

Hence with I and II and our convention that $\alpha \wedge \beta = 0$ we have:

VI $\bar{q}_i = \bar{q}_{i+1}$ for i even and

VII $\hat{q}_i = \hat{q}_{i+1}$ for i odd.

But notice that by definition we have

VIII $\bar{q}_i \gamma \hat{q}_i$ for every i.

This, together with VI and VII gives us:

$$x = \bar{q}_0 = \bar{q}_1 \gamma \hat{q}_1 = \hat{q}_2 \gamma \bar{q}_2 = \bar{q}_3 \gamma \hat{q}_3 \dots \bar{q}_n, \quad \text{i.e.}$$

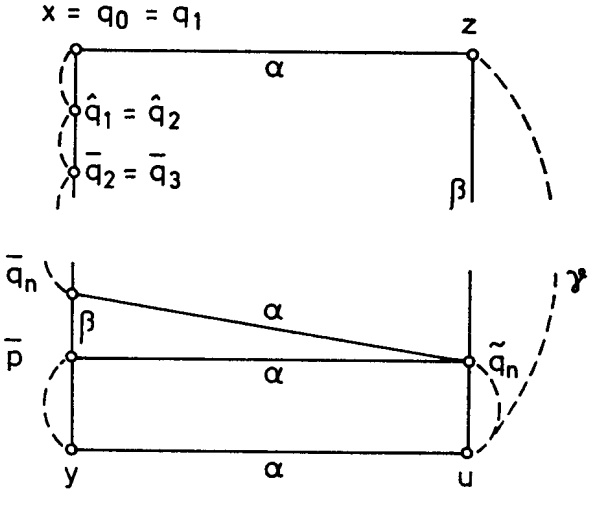
IX $x \gamma \bar{q}_n$. (No matter whether n is odd or even!)

Hence in view of III, all we have to do is to show that $\bar{q}_n = \bar{p}$. For this reason notice that

$$\bar{q}_n = q_n(x, u, y) \alpha q_n(z, y, u) = \tilde{q}_n \quad \text{and}$$
$$\bar{p} = p(z u y) \alpha p(z, y, y) = q_n(z, y, y) \alpha q_n(z, y, u) = \tilde{q}_n.$$

Hence $\bar{q}_n \alpha \bar{p}$ and $\bar{q}_n \beta \bar{p}$ by I and III. Thus $\bar{q}_n = \bar{p}$ and we are finished.

It may be instructive to see how the polynomials work by looking at the following picture: (Notice, that $\tilde{q}_n \gamma \wedge \beta u$ by Equation 2.)



2. Permutability formulas. We will show how to use the formulas

$$\theta \circ \psi \subseteqq [\theta, \theta] \circ \psi \circ \theta \quad \text{and} \quad \theta \circ \psi \subseteqq \psi \circ \theta \circ [\psi, \psi]$$

to give us the following results:

2.1. Theorem. *Let $\mathscr{A}$ be an algebra in a modular variety and θ and ψ congruences on $\mathscr{A}$. Then the following conditions are equivalent:*

(i) *θ permutes with ψ.*

(ii) *$\theta^{(n)}$ permutes with $\psi^{(m)}$ for all $n, m \in \mathbb{N}$.*

(iii) *$\theta^{(n)}$ permutes with $\psi^{(m)}$ for some $n, m \in \mathbb{N}$.*

Here we use the following Definition:

$$\theta^{(1)} := \theta,\ \theta^{(n+1)} := [\theta^{(n)}, \theta^{(n)}].$$

θ is called *solvable*, in case $\theta^{(n)} = 0$ for some $n \in \mathbb{N}$.

Note that we have as a corollary the result from [4] that solvable congruences permute with every congruence.

Proof of 2.1. Iterating the formula $\theta \circ \psi \subseteqq [\theta, \theta] \circ \psi \circ \theta$ and its symmetric form we obtain:

$$\theta \circ \psi \subseteqq \psi \circ \theta^{(n)} \circ \psi^{(m)} \circ \theta \quad \text{for any } n, m.$$

Namely, by symmetry we are done if we show the induction step from n to $n + 1$. Assuming the above formula we obtain

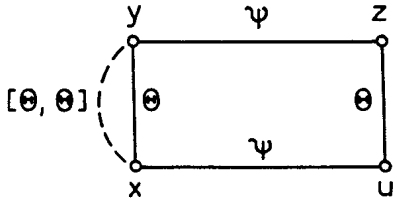
$$\begin{aligned}\theta \circ \psi &\subseteqq \psi \circ \theta^{(n)} \circ \psi^{(m)} \circ \theta \subseteqq \psi \circ [\theta^{(n)}, \theta^{(n)}] \circ \psi^{(m)} \circ \theta^{(n)} \circ \theta \\ &\subseteqq \psi \circ \theta^{(n+1)} \circ \psi^{(m)} \circ \theta.\end{aligned}$$

Now the above formula gives us (iii) $\rightarrow$ (i) since $\psi^{(m)} \subseteqq \psi$ and $\theta^{(n)} \subseteqq \theta$. It remains to prove (i) $\rightarrow$ (ii).

Again by induction we may assume we have already proven that $\theta^{(n-1)}$ permutes with $\psi^{(m)}$ we have to show $\theta^{(n)}$ permutes with $\psi^{(m)}$. Changing notation, we have to show that $[\theta, \theta]$ permutes with ψ in case θ permutes with ψ. Suppose $(x, z) \in [\theta, \theta] \circ \psi$, i.e. for some y we have

$$x [\theta, \theta] y \psi z.$$

In particular $(x, y) \in \theta$ hence $x \theta y \psi z$. Since θ and ψ permute we find a u with



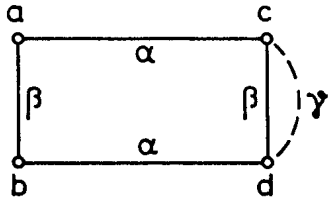
The shifting lemma gives us $(u, z) \in (\theta \wedge \psi) \vee [\theta, \theta]$.

Now $[\theta \wedge \psi, \theta \wedge \psi] \leqq [\theta, \theta]$ hence $(\theta \wedge \psi)^{(2)}$ permutes with $[\theta, \theta]$ which implies that $\theta \wedge \psi$ permutes with $[\theta, \theta]$ by the direction (iii) $\rightarrow$ (i).

Hence there exists an element w with $u \theta \wedge \psi w [\theta, \theta] z$, hence $x \psi w [\theta, \theta] z$ which was to be shown.

As a corollary to the proof we get a stronger kind of Shifting Lemma, namely:

2.2. Shifting Theorem. *Let α, β, γ be congruences on an algebra $\mathscr{A}$ in a modular variety such that $(\alpha \wedge \beta)^{(n)}$ permutes with $\gamma^{(m)}$ for some $n, m \in \mathbb{N}$. Then*

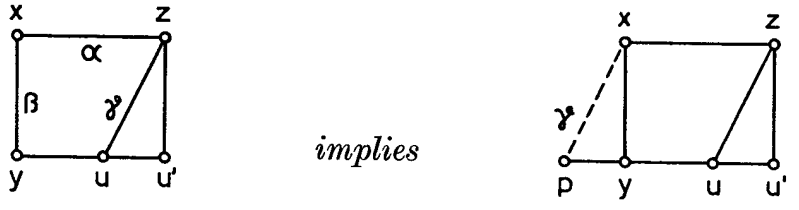


implies $(a, b) \in (\alpha \wedge \beta) \circ \gamma$.

Clearly 2.2 implies the original Shifting Lemma.

The following theorem strengthens Satz 3 of [2]:

2.3. Theorem. *In every modular variety there exists a ternary polynomial $p(x, y, z)$ such that $p(x, x, y) = y$ and for congruences α, β, γ with $\alpha \wedge \beta \leqq \gamma$ and elements x, y, z, u, u' we have*



with $p = p(u, u', y)$.

Proof. Define $\bar{q}_i$ and $\hat{q}_i$ precisely as in the proof of 1.4. Hence $x\gamma \vee (\alpha \wedge \beta)\bar{q}_n$. Finally you get:

$$p(u, u', y)\,\gamma\, p(z, u', y)\,(\alpha \wedge \beta)\,\bar{q}_n$$

and

$$p(u, u', y)\,\alpha\, y\,.$$

Hence $x\gamma \vee (\alpha \wedge \beta)p\alpha y$. Consequently we have $x\gamma p\alpha y$.

With the help of 2.3 we can generalize the permutability result of Korollar 5 of [2]:

2.4. Corollary. *Let α, β and γ be congruences on an algebra in a modular variety such that $\gamma \leqq \alpha \circ \beta = \beta \circ \alpha$ and $\gamma^{(n)}$ permutes with $(\alpha \wedge \beta)^{(m)}$ for some m, n. Then γ permutes with α (and with β).*

Remark. The special case where $\alpha \wedge \beta \leqq \gamma$ was first proven in [2]. Combining this with the result of [4], that solvable congruences permute with every other congruence, *A.* Wolf gave a short argument to show that the condition $\alpha \wedge \beta \leqq \gamma$ could be relaxed to $(\alpha \wedge \beta)^{(n)} \leqq \gamma$.

Corollary 2.4 in its present form subsumes all these versions as well as the result that solvable congruences permute with every congruence; just set $\beta = 1$, the universal congruence, and $m = 1$.

Remark. The formulas $\theta \vee \psi = (\theta^{(n)} \vee \psi^{(m)}) \circ \theta \circ \psi$ or $\theta \vee \psi = \theta \circ (\theta^{(n)} \vee \psi^{(m)}) \circ \psi$ are easy to prove and show how easily joins of congruences can sometimes be computed in modular varieties.

References

[1] A. Day, A characterization of modularity for congruence lattices of algebras. Canad. Math. Bull. **12**, 167–173 (1969).

[2] H. P. Gumm, Über die Lösungsmengen von Gleichungssystemen über allgemeinen Algebren. Math. Z. **162**, 51–62 (1978).

[3] H. P. Gumm, An easy way to the commutator in modular varieties. Arch. Math. **34**, 220–228 (1980).

[4] H. P. GUMM and CH. HERRMANN, Algebras in modular varieties, Baer refinements, cancellation and isotopy. Preprint 1978. Houston J. Math. **5**, 503—523 (1979).
[5] CH. HERRMANN, Affine algebras in congruence-modular varieties. Acta Sci. Math. (Szeged) **41**, 119—125 (1979).
[6] J. HAGEMANN and CH. HERRMANN, A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity. Arch. Math. **32**, 234—245 (1979).
[7] B. JÓNSSON, Algebras whose congruence lattices are distributive. Math. Scand. **21**, 110—121 (1967).
[8] A. I. MAL'CEV, On the general theory of algebraic systems (Russian). Mat. Sb. **35**, 3—20 (1954).
[9] W. TAYLOR, Some applications of the term condition. Preprint 1980.

Eingegangen am 6. 6. 1980

Anschrift des Autors:

H. Peter Gumm
Fachbereich Mathematik
Technische Hochschule
Schloßgartenstr. 7
6100 Darmstadt