COMMUTATOR THEORY WITHOUT JOIN-DISTRIBUTIVITY

PAOLO LIPPARINI

ABSTRACT. We develop Commutator Theory for congruences of general algebraic systems (henceforth called algebras) assuming only the existence of a ternary term d such that $d(a, b, b)[\alpha, \alpha]a[\alpha, \alpha]d(b, b, a)$, whenever α is a congruence and $a\alpha b$.

Our results apply in particular to congruence modular and n-permutable varieties, to most locally finite varieties, and to inverse semigroups.

We obtain results concerning permutability of congruences, abelian and solvable congruences, connections between congruence identities and commutator identities. We show that many lattices cannot be embedded in the congruence lattice of algebras satisfying our hypothesis. For other lattices, some intervals are forced to be abelian, and others are forced to be nonabelian.

We give simplified proofs of some results about the commutator in modular varieties, and generalize some of them to single algebras having a modular congruence lattice.

It is easy to show that if a group G has three normal subgroups, any two of which intersect in the trivial subgroup and generate the whole G, then G must be abelian.

Put in another way, if

$$G$$

$$\{1\}$$
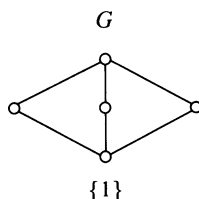
$$M_3$$

is a sublattice of the lattice of normal subgroups of G, then G is abelian.

Normal subgroups of a group correspond to congruences (compatible equivalence relations): the above example is probably the simplest one showing how deeply the structure of a general algebra is affected by the shape of its congruence lattice.

For algebras belonging either to a modular variety [Jo] or to a locally finite variety [HMK] many surprising results of this kind have been obtained; how-

ever, very little is known in the general case [FLT, DF]; moreover, the deep reasons of this influence are very far from being completely understood.

Of course, in the above example, the reason is distributivity of the commutator; the situation for rings is entirely similar: the ideal product in a commutative ring satisfies the same formal properties as the commutator of normal subgroups.

That this is not just an odd coincidence was first discovered by J. D. H. Smith who, in [Sm], succeeded in defining a commutator operation (as useful as group commutator and ideal product) for congruences of algebras in permutable varieties; Smith's theory was soon generalized to modular varieties by J. Hagemann and C. Herrmann [HH]; subsequently many people provided strengthenings and simplifications (see [FMK, Gu]).

This notion of commutator not only makes it possible to define and study abelian, nilpotent and solvable algebras in general, but has been applied successfully to the solution of many older problems, and has been used both to simplify earlier proofs and to extend results which were originally proved only for congruence distributive varieties.

The commutator could be defined in many ways, which are equivalent only under the assumption of congruence modularity. The question has naturally arisen whether one or the other of these notions of commutator could be used to extend the theory to a larger class of varieties.

However, some results by H.-P. Gumm imply that if, within a variety $\underline{V}$, some commutator operation is distributive over joins, and there is a ternary term d (call it a *difference term*) such that $d(a, b, b) = a$ and $d(a, a, b)[\alpha, \alpha]b$ hold whenever $a\alpha b$, then $\underline{V}$ must be modular, no matter how the commutator is defined (we shall provide a simplified proof, holding even for single algebras, in Theorem 3.2).

Hence—so it seems—many researchers became pessimistic about the possibility of generalizing commutator theory. However, very recently, a particular commutator operation (the one defined using a generalization of the term condition) played an essential role in D. Hobby and R. McKenzie's deep study of locally finite varieties [HMK]. With a more limited scope, this commutator has been used also in [Lp] in order to show that n-permutable varieties satisfy nontrivial lattice identities.

Thus, we decided to study such a commutator in a general setting (see [DG, KMK] for different approaches). By the quoted result of H. P. Gumm, to move beyond modular varieties we have to renounce either distributivity or the existence of a difference term. We choose the first way. As a starting point for this paper, we show that many results from the modular commutator theory carry over using only this hypothesis. Indeed, rather surprisingly, in most cases just the existence of a *weak difference term* (see Definition 2.1) will do.

The commutator proves particularly useful in studying the influence that congruence lattices have on their algebras; this is the main theme of the present paper. The example quoted at the beginning is illuminating in this respect; we still can prove, without distributivity, that M_3 as a sublattice of Con **A** forces **A** to be abelian! Many results of this kind are obtained in §5, for example, the smallest nonmodular lattice N_5 has effects opposite to those of M_3; moreover, projective quotients are either both abelian or both nonabelian.

The hypothesis of the existence of a weak difference term is not very restric-

tive; the whole of §2 is devoted to examples. Besides modular varieties (and hence groups, rings, quasigroups, lattices) they include n-permutable varieties, neutral varieties (those satisfying $[\alpha, \alpha] = \alpha$ identically), and a large class of semigroups. Locally finite varieties have been thoroughly studied in [HMK] using *tame congruence theory*. The existence of a weak difference term in a locally finite variety is equivalent to many conditions [HMK, Theorem 9.6], among those is the omission of type 1.

In this way, our results may be seen as a common generalization of the modular commutator theory and of some parts of tame congruence theory. They are completely new for n-permutable varieties; there are lots of things to be discovered about the commutator in n-permutable varieties. [Lp] seems to be just a beginning.

Some of our results on the relationships between commutator identities and congruence identities suggest that commutator theory may play an important role in the study of *congruence varieties* (see [Jo]). Indeed, the commutator had been implicitly used already in the 70's in [FLT] in order to show that certain lattices cannot be represented as congruence lattices of algebras with few operations (see also [Ta]).

A marginal but very remarkable fact is that within distributive varieties the commutator is trivial; nevertheless, it can be used to provide some results [FMK, Chapter VIII and Corollary 10.3]. The situation is similar for neutral varieties [Lp, remarks after Theorem 3, HMK, Exercise 6.23(12)].

Finally, it is interesting to note that most of our results hold for single algebras having a weak difference term, disregarding whether or not such a term exists within a whole variety. Anyway, in most cases, the existence of a weak difference term is proved by using a Mal'cev condition, holding for a variety to which the algebra belongs. In this way, in some sense, our theory seems to isolate those consequences of Mal'cev conditions which are actually used for single algebras. Once the Mal'cev condition is used to obtain a weak difference term, we need it no more.

We are indebted to Professor K. A. Kearnes for many suggestions which have been used in the revision of this paper.

The paper is divided as follows: in §1 we introduce the commutator, and prove some lemmata about it. The lemmata are simple, but they will prove powerful in connection with the existence of a weak difference term. Most of §1 is folklore; probably the only new result is that, surprisingly, the modularity of $\mathrm{Con}\,\mathbf{A}$ has some strong consequences on the commutator, no matter what $\underline{V}(\mathbf{A})$ is.

In §2 we present examples of varieties with a difference term or a weak difference term. In §3 and §4 we use weak difference terms in order to compute the join of two congruences, to obtain congruence identities and commutator identities, as well as permutability results. Using a result by A. Day and R. Freese on Polin's variety we show (Theorem 4.4) that, for varieties, every lattice identity implying commutator distributivity implies congruence modularity.

The difference between §3 and §4 is that the former contains abstract results, in the sense that the concrete definition of the commutator is not used. We need only the difference term and some formal properties of the commutator; while in the latter we make heavy use of the definition of $[\alpha, \beta]$, and use the lemmata of §1. Most of the results in §3 and §4 seem to be new even in the

particular case of locally finite varieties omitting type 1.

In §5 we show how deeply the structure of an algebra is affected by its congruence lattice; in particular, we find that many lattices cannot be sublattices of the congruence lattices of algebras with a weak difference term. Also, we show that projective quotients are either both abelian or both nonabelian; moreover, many definitions of abelian-like properties turn out to be (unexpectedly, cf. [Ta, p. 23]) equivalent. Finally, we indicate how our abstract treatment of §3 can be used to extend our results to an even broader class of algebras.

A large part of the results proved in this paper have been announced in [Lp].

We now recall the basic notions of universal algebra (otherwise called general theory of algebraic systems), and establish the notations which shall be used in this paper (generally they coincide with [FMK]). A more systematic introduction to universal algebra is given, e.g., in the first chapters of [BS] or [MKNT]; for a less technical presentation of the subject and of its aims the reader can look at [MK] and at the introduction of [Sm].

Some knowledge of modular commutator theory (as exposed in [FMK, Gu]) is welcome, but probably not indispensable for reading this paper. Also tame congruence theory [HMK] is sometimes used or referred to in examples.

Algebras, denoted $\mathbf{A}, \mathbf{B}, \ldots$ are just sets $(A, B, \ldots)$ furnished with some operations; a class of algebras of the same type is a *variety* just in case it is closed under taking direct products, substructures and homomorphic images (a celebrated theorem by G. Birkhoff states that variety is the same as a class of algebras satisfying a given set of equations). A *term* (or derived operation) of an algebra $\mathbf{A}$ corresponds to what in group theory is called a "word"; it is just an operation obtained by composition from the basic operations of $\mathbf{A}$ (and the projections).

A *congruence* α on an algebra $\mathbf{A}$ is a compatible (admissible) equivalence relation on A, that is, the kernel of some homomorphism. $\mathrm{Con}\,\mathbf{A}$, the set of all congruences of the algebra $\mathbf{A}$, is naturally equipped with a *lattice* structure, with *meet*, denoted by $\cdot$ or juxtaposition, and *join* denoted by $+$ ($\mathrm{Con}\,\mathbf{A}$ is indeed a *complete* lattice: we shall use $\wedge$ and $\vee$ for infinite meets and joins). The largest and smallest elements of $\mathrm{Con}\,\mathbf{A}$ are denoted by $1_\mathbf{A}$ and $0_\mathbf{A}$; we shall omit the subscript $\mathbf{A}$, when there is no danger of confusion. A *block* of a congruence α is just an equivalence class of α; $a\alpha b$ means that a and b stay in the same α-block, that is, $(a, b) \in \alpha$ or, in other words, a and b are equivalent modulo α. When there is no danger of confusion, $\bar{a}, \bar{b}, \ldots$ denote n-tuples of elements of some algebra; in this case, $\bar{a}\alpha\bar{b}$ will mean that $a_1\alpha b_1$, $a_2\alpha b_2, \ldots$.

Given two congruences α and β on the algebra $\mathbf{A}$, we can form the relational product $\alpha \circ \beta = \{(a, c) | a\alpha b\beta c, \text{ for some } b \in A\}$, which is a compatible relation on $\mathbf{A}$, but not necessarily a congruence. If $n \geq 2$, two congruences α and β are said to *n-permute* if and only if $\beta \circ \alpha \circ \beta \circ \alpha \cdots = \alpha \circ \beta \circ \alpha \circ \beta \ldots$ (n factors on each side); so that, in particular, $\alpha + \beta = \alpha \circ \beta \circ \alpha \circ \beta \ldots$ (n factors). *Permute* is the same as 2-permute. A variety $\underline{V}$ is (congruence) *n-permutable* if and only if every pair of congruences of every algebra in $\underline{V}$ n-permute.

The distributive and modular laws for lattices are the respective equations $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $\alpha(\beta + \alpha\gamma) = \alpha\beta + \alpha\gamma$. A variety $\underline{V}$ is called *distributive* (or *modular*) iff for every $\mathbf{A} \in \underline{V}$, $\mathrm{Con}\,\mathbf{A}$ satisfies the distributive (or

modular) law; notice that the modular law is just the obvious generalization of the Dedekind law, holding for normal subgroups of a group.

If $\alpha \leq \beta$ are elements of a lattice L, we let $I(\alpha, \beta)$ be the *interval* $\{\gamma \in L | \alpha \leq \gamma \leq \beta\}$, which is naturally a sublattice of L. When $L = \text{Con}\,\mathbf{A}$, for some algebra $\mathbf{A}$, we shall call $I(\alpha, \beta)$ a *quotient* interval; in fact, $I(\alpha, 1_{\mathbf{A}}) \cong \text{Con}(\mathbf{A}/\alpha)$. Two intervals $I(\alpha, \beta)$ and $I(\alpha', \beta')$ are said to be (1 *step*) *projective* (or *transposed*) if and only if $\beta = \alpha + \beta'$ and $\alpha' = \alpha\beta'$ (or conversely). We shall show that, under our fairly general hypotheses, projective quotients are rather similar; much stronger results can be obtained within modular varieties. A classical result states that in a modular lattice any two transposed intervals are isomorphic, and [FMK, Remark 4.6] shows that commutators are also preserved.
□ denotes the end of a proof.

1. COMMUTATORS AND CENTRALIZERS

In this section we shall introduce the commutator we use, and prove some simple lemmata about it. The results are weak in comparison with the ones obtained for algebras in modular varieties; but they hold for all algebras. It is rather surprising to discover that modularity of $\text{Con}\,\mathbf{A}$ has strong consequences, no matter what $\underline{V}(\mathbf{A})$ is (see Corollary 1.3(e) and Proposition 4.1).

1.1. Definitions. If $\mathbf{A}$ is an algebra, and $\alpha, \beta \in \text{Con}\,\mathbf{A}$, then $M(\alpha, \beta)$ is the set of all *matrices* of the form:

$$\begin{vmatrix} t(\overline{a}, \overline{b}) & t(\overline{a}, \overline{b}') \\ t(\overline{a}', \overline{b}) & t(\overline{a}', \overline{b}') \end{vmatrix}$$

where $\overline{a}, \overline{a}' \in A^n$, $\overline{b}, \overline{b}' \in A^m$, for some $n, m \geq 0$, t is any $m + n$-ary term operation of $\mathbf{A}$, and $\overline{a}\alpha\overline{a}'$, $\overline{b}\beta\overline{b}'$.

If $\alpha, \beta, \gamma \in \text{Con}\,\mathbf{A}$, we say that α *centralizes* β *modulo* γ, in symbols $C(\alpha, \beta; \gamma)$, if and only if, for every $a, b, c, d \in A$:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} \in M(\alpha, \beta) \quad \text{and} \quad a\gamma b \quad \text{imply} \quad c\gamma d.$$

The *commutator* $[\alpha, \beta]$ of α and β is the least congruence γ of $\mathbf{A}$ such that α centralizes β modulo γ (this definition is justified by Proposition 1.2(3) below).

A congruence α is *abelian* if and only if $[\alpha, \alpha] = 0$.
The *solvable series* $\alpha^{(n)}$ is defined recursively as follows:

$$\alpha^{(0)} = \alpha, \quad \text{and} \quad \alpha^{(n+1)} = [\alpha^{(n)}, \alpha^{(n)}].$$

A congruence α is *solvable* if and only if $\alpha^{(n)} = 0$, for some nonnegative integer n.

An algebra $\mathbf{A}$ is *abelian* (*solvable*) if and only if $1_{\mathbf{A}}$ is an abelian (solvable) congruence.

The condition $[1, 1] = 0$ is usually called the Term Condition, and has a long history (see [Qu]). R. Freese and R. McKenzie [FMK] denoted $[\alpha, \beta]$ by $C(\alpha, \beta)$, and seemed to be the first to give it the status of a commutator. See [FMK, Chapter I] for a clear exposition of why this definition generalizes both the usual commutator for groups, and the ideal product for commutative rings.

1.2. Proposition. *For every algebra* $\mathbf{A}$ *and* $\alpha, \alpha_i, \alpha', \beta, \beta', \gamma, \gamma_i \in \mathrm{Con}\,\mathbf{A}$:

(1) $C(\alpha, \beta; \gamma)$ *if and only if* $C(\alpha, \beta; \gamma\beta)$.

(2) *If* $C(\alpha, \beta; \gamma)$ *and* $\alpha' \le \alpha$, $\beta' \le \beta$ *then* $C(\alpha', \beta'; \gamma)$.

(3) *If* $C(\alpha, \beta; \gamma_i)$ *for every* $i \in I$, *then* $C(\alpha, \beta; \bigwedge_{i\in I}\gamma_i)$.

(4) *If* $C(\alpha_i, \beta; \gamma)$ *for every* $i \in I$, *then* $C(\bigvee_{i\in I}\alpha_i, \beta; \gamma)$.

(5) *If* $\gamma \ge \beta(\alpha + \gamma\beta)$ *then* $C(\alpha, \beta; \gamma)$.

In particular, $C(\alpha, \beta; \alpha\beta)$ *holds.*

(6) *If* $\gamma \ge \beta(\alpha_i + \gamma\beta)$ *for every* $i \in I$, *then* $C(\bigvee_{i\in I}\alpha_i, \beta; \gamma)$.

In particular, if $\alpha_i\beta = \gamma$, *for every* $i \in I$, *then* $C(\bigvee_{i\in I}\alpha_i, \beta; \gamma)$.

(7) *If* $\mathrm{Con}\,\mathbf{A}$ *is modular and* $\gamma \ge \alpha\beta$, *then* $C(\alpha, \beta; \gamma)$.

(8) *If* $\mathrm{Con}\,\mathbf{A}$ *is modular and* $\gamma \ge \bigvee_{i\in I}\beta\alpha_i$, *then* $C(\bigvee_{i\in I}\alpha_i, \beta; \gamma)$.

The proofs follow trivially from the definitions, except (7) and (8) which are immediate from (5) and (6), respectively. □

1.3. Corollary. *For every algebra* $\mathbf{A}$ *and* $\alpha, \alpha_i, \beta, \gamma, \delta \in \mathrm{Con}\,\mathbf{A}$:

(a) $[\alpha, \beta]$ *is monotone in both arguments.*

(b) $[\alpha, \beta] \le \alpha\beta$.

(c) *If* $[\alpha_i, \beta] = \delta$, *for every* $i \in I$, *then* $[\bigvee_{i\in I}\alpha_i, \beta] = \delta$.

(d) *If* $\alpha_i\beta = \delta$ *for every* $i \in I$, *then* $[\bigvee_{i\in I}\alpha_i, \beta] \le \delta$.

(e) *If* $\mathrm{Con}\,\mathbf{A}$ *is modular, then* $[\bigvee_{i\in I}\alpha_i, \gamma] \le \bigvee_{i\in I}\gamma\alpha_i$. □

Proposition 1.2(5) is an important improvement of [HMK, Proposition 3.4(4)]; it is the main tool for showing that the shape of $\mathrm{Con}\,\mathbf{A}$ influences the behaviour of the operations of $\mathbf{A}$. Also 1.2(4) and 1.3(c) are very important: they give us as much distributivity (over joins) as we can get. 1.2(8) and 1.3(e) are just an example of the power of 1.2(4)(5). In general, a useful bound for $[\alpha + \beta, \gamma]$ is given in [Lp].

Notice that 1.3(e) is just what is needed in the proof of [Gu, Lemma 7.3]. Hence 1.3(e) allows a proof of [Gu, Theorem 7.4] which makes no use of join distributivity of the commutator: the only necessary prerequisite is the existence of a difference term! This remark applies also to the shorter proof given in [FMK, Theorem 6.4].

Within modular varieties, $C(\alpha, \beta; \gamma)$ and $[\alpha, \beta]$ have many pleasant properties. The proofs of the following theorem, which shall not be used in this paper (except in Theorem 4.4), can be found in [FMK] or [Gu].

1.4. Theorem. *If* $\mathbf{A} \in \underline{V}$ *and* $\underline{V}$ *is a congruence modular variety, then for every* $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$:

(I) *(commutativity)* $[\alpha, \beta] = [\beta, \alpha]$.

(II) *(left distributivity)* $[\bigvee_{i\in I}\alpha_i, \beta] = \bigvee_{i\in I}[\alpha_i, \beta]$.

(III) *(right distributivity)* $[\alpha, \bigvee_{i\in I}\beta_i] = \bigvee_{i\in I}[\alpha, \beta_i]$.

(IV) *If* $C(\alpha, \beta; \gamma)$ *and* $\gamma' \ge \gamma$, *then* $C(\alpha, \beta; \gamma')$. □

The rest of this section is devoted to the proofs of some weak but very useful versions of Theorem 1.4 holding for every algebra.

First, some comments: for our purposes, 1.4(I) is not very important, since we will mainly use $[\alpha, \alpha]$. However (I) could be used to derive (III) from (II). 1.2(4) is a weak version of 1.4(II); but a similar version of 1.4(III) does not hold in general, that is, we cannot prove $C(\alpha, \beta + \beta'; \gamma)$ from $C(\alpha, \beta, \gamma)$ and $C(\alpha, \beta'; \gamma)$. We have only some results for the very particular situation

when $\beta + \beta' = \beta \circ \beta' \circ \beta$. Luckily, it is exactly the situation in which we will need it (cf. the proof of Theorem 4.3).

1.5. Lemma. *If* **A** *is an algebra,* $\alpha, \beta, \beta', \gamma, \delta \in \mathrm{Con}\,\mathbf{A}$, $\beta + \beta' = \beta \circ \beta' \circ \beta$, $\delta \geq \beta'(\beta + \gamma(\beta + \beta'))$, $\gamma \geq (\alpha + \gamma(\beta + \beta'))(\beta + \delta\beta')$, *and* $C(\alpha, \beta'; \delta)$, *then also* $C(\alpha, \beta + \beta'; \gamma)$.

Proof. The proof is a variation of [Wi, Lemma 1.3]. Suppose that $\overline{a}\alpha\overline{b}$ and $\overline{c}\beta + \beta'\overline{d}$. We have to prove that if $t(\overline{a}, \overline{c})\gamma t(\overline{a}, \overline{d})$ then also $t(\overline{b}, \overline{c})\gamma t(\overline{b}, \overline{d})$.

Since $\beta + \beta' = \beta \circ \beta' \circ \beta$, there are $\overline{c}'$ and $\overline{d}'$ such that $\overline{c}\beta\overline{c}'\beta'\overline{d}'\beta\overline{d}$, so that $t(\overline{a}, \overline{c})\beta t(\overline{a}, \overline{c}')\beta' t(\overline{a}, \overline{d}')\beta t(\overline{a}, \overline{d})$, whence $t(\overline{a}, \overline{c}')\beta'(\beta + \gamma(\beta + \beta'))t(\overline{a}, \overline{d}')$, since $t(\overline{a}, \overline{c})\gamma(\beta + \beta')t(\overline{a}, \overline{d})$.

Since $\delta \geq \beta'(\beta + \gamma(\beta + \beta'))$ and $C(\alpha, \beta'; \delta)$, then $t(\overline{b}, \overline{c}')\delta t(\overline{b}, \overline{d}')$, which implies that $t(\overline{b}, \overline{c})\beta t(\overline{b}, \overline{c}')\delta\beta' t(\overline{b}, \overline{d}')\beta t(\overline{b}, \overline{d})$, so that $t(\overline{b}, \overline{c})\gamma t(\overline{b}, \overline{d})$, since $t(\overline{b}, \overline{c})\alpha t(\overline{a}, \overline{c})\gamma(\beta + \beta')t(\overline{a}, \overline{d})\alpha t(\overline{b}, \overline{d})$, and $\gamma \geq (\alpha + \gamma(\beta + \beta'))(\beta + \delta\beta')$. $\square$

Though seemingly a rather weak (and desirable) condition, 1.4(IV) has very strong consequences which almost imply congruence modularity (see the next proposition, and Theorem 3.2). In Proposition 4.2 we shall prove 1.4(IV) in the particular case when $\alpha = \beta$ (using a weak difference term).

1.6. Proposition. *If* **A** *is an algebra and* $C(\alpha, \beta, \gamma)$ *implies* $C(\alpha, \beta, \gamma')$, *for every* $\alpha, \beta, \gamma \leq \gamma' \in \mathrm{Con}\,\mathbf{A}$, *then*

$$[\alpha + \beta, \gamma] = [\alpha, \gamma] + [\beta, \gamma],$$

for every $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$.

Proof. The proof is implicit in the proof of [FMK, Proposition 4.3]. We have to show that $\alpha + \beta$ centralizes γ modulo $[\alpha, \gamma] + [\beta, \gamma]$. By Proposition 1.2(4), it is enough to show that both α and β centralize γ modulo $[\alpha, \gamma] + [\beta, \gamma]$. This follows, however, by the hypothesis and by the fact that, by definition, α centralizes γ modulo $[\alpha, \gamma]$. $\square$

1.7. Problems. (a) Find conditions implying (if possible, equivalent to) left join distributivity, right join distributivity or commutativity of the commutator (we always mean the commutator of Definition 1.1).

See Example 4.7 for a partial negative result. [Ke] has some results on commutativity and nilpotency in finite algebras. He also observed that, for every algebra, the existence of a difference term implies that the commutator is commutative. More generally, we will show in [Lp1] that the existence of a difference term implies that the commutator coincides with the 2-terms commutator [Ki], which is trivially commutative.

(b) In particular, is there a (weak) Mal'cev condition strictly weaker than modularity and implying left join distributivity of the commutator? (Cf. Theorem 4.4 for a partial negative answer.)

(c) Does right join distributivity always imply left join distributivity?

(d) Characterize, if possible, the commutator as the largest binary operation on congruences satisfying a certain property (cf. [FMK, Definition 3.1]).

(e) Answer the above questions at least in the particular cases of varieties with a (weak) difference term (Definition 2.1), n-permutable varieties, locally finite varieties (omitting type 1, or some other type).

Some remarks are in order: if an algebra has only unary operations, then $[\alpha, \beta] = 0$ constantly, so that the commutator is both distributive and commutative. This suggests that (e) is a question more approachable than (a)–(d).

Moreover, as is well known, every algebra has the same congruences of an algebra with just unary operations: this will show that, in most of our results, we actually need the hypothesis of the existence of a weak difference term.

2. ALGEBRAS WITH DIFFERENCE TERMS

In this section we introduce the notions of a difference term and of a weak difference term; and give examples of algebras and varieties having such terms. Apart from the classical characterization by Mal'cev of permutable varieties, the first example of varieties with a difference term were modular varieties (see [FMK] for credits and history). Almost at the same time [Ta] implicitly proved that n-permutable varieties have a weak difference term, but did not use the full power of his discovery. Weak difference terms have been used also in [HMK] for studying locally finite varieties omitting type 1. However, the concept has never been studied for its own sake before.

2.1. **Definition.** We say that a ternary term d of an algebra $\mathbf{A}$ is a *difference term* if and only if

$$a = d(a, b, b) \quad \text{and} \quad d(a, a, b)[\alpha, \alpha]b$$

hold, for every $\alpha \in \mathrm{Con}\,\mathbf{A}$ and $a\alpha b \in \mathbf{A}$.

A ternary term d is a *weak difference term* if and only if

$$a[\alpha, \alpha]d(a, b, b) \quad \text{and} \quad d(a, a, b)[\alpha, \alpha]b$$

hold, for every $\alpha \in \mathrm{Con}\,\mathbf{A}$ and $a\alpha b \in \mathbf{A}$.

A variety $\underline{V}$ has a (weak) difference term if and only if there is a ternary term of $\underline{V}$ which is a (weak) difference term for every $\mathbf{A} \in \underline{V}$.

2.2. **Examples.**

(1) According to [FMK, Theorem 5.5], every modular variety has a difference term. This applies, in particular, to groups, rings, quasigroups, lattices … .

(2) Let us say that an algebra $\mathbf{A}$ is *neutral* if and only if $[\alpha, \alpha] = \alpha$, for every $\alpha \in \mathrm{Con}\,\mathbf{A}$ (equivalently, $[\alpha, \beta] = \alpha\beta$, for every $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$).

Every neutral algebra has a difference term: take $d(x, y, z) = x$.

By Remark 2.4 below, semilattices are neutral, so that every semilattice has a difference term.

(3) By [HMK, Theorem 9.6(6) and Proposition 3.4(5)], a locally finite variety $\underline{V}$ has a weak difference term if and only if $\underline{V}$ omits type 1 (if and only if $\underline{V}$ satisfies a certain congruence identity, if and only if a certain lattice is not a sublattice of $\mathrm{Con}\,\mathbf{A}$, for $\mathbf{A} \in \underline{V}$).

(4) By the proof of [Ta, Theorem 2] (see [Lp]), every n-permutable variety has a weak difference term. This includes Polin's variety [DF] and some generalizations.

(5) If we add operations to $\mathbf{A}$, then the commutator grows larger, so that if $\mathbf{A}$ has a (weak) difference term, then any expansion of $\mathbf{A}$ has a (weak) difference term.

(6) More generally, it is possible to show [Lp] that the class of varieties with a (weak) difference term is a Mal'cev class, and this implies some other closure properties (see [Jo] or [Ta1]).

(7) Any semigroup satisfying $x^{n+1} = x$ and $x^n y^n = y^n x^n$, for some fixed $n > 0$, has a weak difference term. This is immediate from (8) below (the inverse of x is x^{n-1}).

This includes, at once, groups, semilattices and, more generally, commutative semigroups satisfying $x^{n+1} = x$.

Indeed, K. Kearnes has proved, with methods similar to those used in [HMK, §7], that a variety of semigroups has a weak difference term iff it omits type 1, iff there is some $n > 0$ such that the above identities hold (that is, iff it is a variety of inverse semigroups).

(8) Any inverse semigroup has a weak difference term. If S is a semigroup, and $a, b \in S$, then b is said to be an *inverse* of a iff $aba = a$ and $bab = b$. S is said to be an *inverse semigroup* iff every element of S has a unique inverse (equivalently, iff every element of S has an inverse, and all idempotents commute). The inverse of a is denoted by a^{-1} [Pe].

In the next theorem we are considering inverse semigroups as algebras of type $(2, 1)$, that is, inverse is considered as a unary operation.

2.3. Theorem. *If* $\mathbf{S} = (S, \cdot, ^{-1})$ *is an inverse semigroup, then* $d(a, b, c) = ab^{-1}c$ *is a weak difference term for* $\mathbf{S}$.

Proof. Let $a\alpha b$. Then $aa^{-1}ab^{-1}a = ab^{-1}a = ab^{-1}bb^{-1}a$, since in an inverse semigroup $(b^{-1})^{-1} = b$. Hence the matrix

$$\begin{vmatrix} aa^{-1}ab^{-1}a & ab^{-1}bb^{-1}a \\ aa^{-1}aa^{-1}a & ab^{-1}ba^{-1}a \end{vmatrix}$$

gives $a = aa^{-1}aa^{-1}a[\alpha, \alpha]ab^{-1}ba^{-1}a = aa^{-1}ab^{-1}b = ab^{-1}b = d(a, b, b)$, since in an inverse semigroup idempotents commute, and aa^{-1}, bb^{-1} are idempotents.

In a symmetrical way we prove that $d(a, a, b)[\alpha, \alpha]b$. □

2.4. Remark. In the particular case of semilattices, $x = x^{-1}$, and the proof shows that, if $a\alpha b$, then $ab[\alpha, \alpha]a$, and hence $a[\alpha, \alpha]b$ so that every semilattice is neutral.

2.5. Problems. (a) Characterize locally finite varieties with a difference term. (*Added in proof*: Meanwhile K. Kearnes has solved this problem.)

(b) Are there congruence identities σ_n (allowed to contain composition) such that for every variety $\underline{V}$, $\underline{V}$ has a weak difference term iff for some n σ_n holds in $\underline{V}$? (This problem has affirmative answer for locally finite varieties [HMK, Theorem 9.6].)

(c) In particular, can we take σ_n to be the identities in [HMK, Theorem 9.6(3)]?

As a partial solution, we will show in [Lp1] that (b) and (c) have an affirmative answer provided that every abelian congruence in $\underline{V}$ is abelian in the sense of the 2-terms condition [Ki].

3. COMMUTATOR IDENTITIES: JOINS AND PERMUTABILITY OF CONGRUENCES.

We are going to consider congruence identities involving the commutator (and composition). Our first identity gives a way to compute the join of two congruences in terms of their iterated commutators. As a consequence, we

obtain conditions for permutability of congruences (in terms of permutability of their commutators) and find some connections between commutator identities and congruence identities.

For algebras with a difference term, this follows essentially the lines of [Gu, Chapter 8], since there he generally used only the existence of a difference term, and not the full power of modularity. However, there are important exceptions: in Theorem 3.6 we succeed in giving a simpler proof of [Gu, Theorem 8.1(iii)⇒(i)] which works in our context and does not use the "Shifting lemma"; and in Theorem 3.2 we give simplified proofs, holding even for single algebras rather than varieties, of results which follow from the proof of [Gu, Theorem 7.4].

Rather surprisingly, we almost get the same results assuming only the existence of a weak difference term; however proofs become much more involved, and need the use of compatible relations, instead of congruences.

This section and the next one are very similar: the only difference is that throughout this section we will not use the actual definition of $[\alpha, \beta]$: we only need $[\alpha, \alpha]$ to be a congruence $\leq \alpha$, of course together with the existence of a weak difference term. Actually, considering the unary function $F(\alpha) = [\alpha, \alpha]$ generally will be enough.

This is exemplified in the next result, Lemma 3.1, which is given in a fairly general form. We will use it in the particular cases when $G(\alpha) = [\alpha, \alpha]$ and $F(\alpha)$ is either $[\alpha, \alpha]$ or constantly 0. We have chosen to give this general form mainly because it gives a unified treatment of the two cases. However, another interesting aspect of the lemma is that it can be applied also when F and G assume other values: for example, in Theorem 5.10 we shall use $F(\alpha) = G(\alpha) = [1, \alpha]$. Though seemingly less interesting, there is also the possibility of taking $F(\alpha) = G(\alpha) = [\alpha, 1]$. Moreover, an analysis of the proof of Lemma 3.1 shows that some results hold even without the hypotheses $F(\alpha) \leq \alpha$ and $G(\alpha) \leq \alpha$; so that we can take, e.g., $F(\alpha) = G(\alpha) = [1, 1]$.

Furthermore, sometimes it is enough to suppose that $F(\alpha)$ and $G(\alpha)$ are compatible and reflexive relations, rather than congruences.

More generally still, we could apply Lemma 3.1 when working with other commutators; for example, [Lp, Lemma 3(i)] is the particular case of 3.1(i) when $F(\alpha) = G(\alpha) = [\alpha, \alpha|n]$ is taken to be the smaller commutator used there. Other possibilities are given by the linear commutator [Qu], the 2-terms commutator [Ki], the weak commutator [Ke], the cyclic commutator [Lp1], and by all the commutators defined in [FMK, Chapter III]. We could also take $F(\alpha)$ to be the least congruence β such that α is strongly abelian over β [HMK, Definition 3.10]. More details and further applications shall be given in subsequent papers.

Here is the notation we use: if $\mathbf{A}$ is an algebra, and $\theta, \psi \subset A \times A$, then $\theta \circ \psi = \{(a, b) \in A \times A|$ there is $c \in A$ such that $a\theta c\psi b\}$; $\theta^{-1} = \{(a, b) \in A \times A|b\theta a\}$; and $\overline{\theta}$ denotes the least compatible (or admissible) relation on A containing θ, or, equivalently, the subalgebra of $A \times A$ generated by θ; $\leq$ denotes inclusion. By convention, (set-theoretical) intersection (denoted by juxtaposition) ties more than $+$, which ties more than $\circ$. If F is a function, F^n denotes the iteration of F n times, that is, $F^1 = F$ and $F^{n+1} = F \circ F^n$.

3.1. **Lemma.** *Suppose that* $\mathbf{A}$ *is an algebra, and* $F, G: \mathrm{Con}\,\mathbf{A} \to \mathrm{Con}\,\mathbf{A}$ *are functions such that* $F(\alpha) \leq \alpha$ *and* $G(\alpha) \leq \alpha$, *for every* $\alpha \in \mathrm{Con}\,\mathbf{A}$.

Suppose that $\mathbf{A}$ *has a ternary term* d *such that* $aF(\alpha)d(a, b, b)$ *and* $d(a, a, b)G(\alpha)b$, *whenever* $\alpha \in \mathrm{Con}\,\mathbf{A}$ *and* $a\alpha b$.

Then, for all positive integers m *and* n, $\mathbf{A}$ *has a ternary term* d^* *such that*:

$$(*)_{m,n} \qquad aF^m(\alpha)d^*(a, b, b) \quad and \quad d^*(a, a, b)G^n(\alpha)b,$$

whenever $\alpha \in \mathrm{Con}\,\mathbf{A}$ *and* $a\alpha b$.

Moreover, if $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$ *and* $\theta \subset A \times A$, *then for every* $n > 0$:

(i) $\alpha \circ \theta \circ \beta \leq F^n(\alpha) \circ \overline{(\alpha \circ \theta) \cup (\theta \circ \beta)} \circ G^n(\beta)$.

(ii) $\gamma(\alpha \circ \theta) \leq \gamma(F^n(\alpha) \circ \overline{\theta \cup \alpha}) \circ G^n(\gamma)$.

(iii) $\alpha + \beta = (F^n(\alpha) + F^n(\beta)) \circ \alpha \circ \beta \circ (G^n(\alpha) + G^n(\beta))$.

(iv) $\gamma(\alpha + \beta) \leq (F^n(\alpha) + F^n(\beta)) \circ (\gamma + F^n(\alpha) + F^n(\beta))(\alpha \circ \beta)$
$\qquad \circ G^n(\gamma(\alpha + \beta) + F^n(\alpha) + F^n(\beta))$.

(v) *Suppose that* $F^n(\alpha) = 0$, *for every* $\alpha \in \mathrm{Con}\,\mathbf{A}$. *Then* $\mathrm{Con}\,\mathbf{A}$ *is modular if and only if* $G^m(\gamma(\alpha + \beta)) \leq \alpha(\beta + \gamma) + \beta(\alpha + \gamma)$, *for some (equivalently, every)* m.

Proof. First, observe that $F(0) \leq 0$ implies that $d(a, a, a) = a$, for every $a \in A$.

Suppose now that we have obtained a term d^* satisfying $(*)_{m,n}$ and define

$$d'(x, y, z) = d^*(x, d^*(x, y, y), d^*(x, y, z)).$$

We will show that d' satisfies $(*)_{m+1,n}$.
Indeed, if $a\alpha b$, then

$$d'(a, b, b) = d^*(a, d^*(a, b, b), d^*(a, b, b)F^m(F^m(\alpha))a,$$

since $aF^m(\alpha)d^*(a, b, b)$; so $d'(a, b, b)F^{m+1}(\alpha)$ follows, since $F^{2m}(\alpha) \leq F^{m+1}(\alpha)$. Moreover,

$$d'(a, a, b) = d^*(a, d^*(a, a, a), d^*(a, a, b))$$
$$= d^*(a, a, d^*(a, a, b))G^n(\alpha)d^*(a, a, b)G^n(\alpha)b.$$

Now, $(*)_{m,n}$ holds for every m, n (for some d^* depending on m, n) by a symmetrical argument and a double induction (the basis of the induction is given by the term d).

(i) Suppose that $a\alpha b\theta c\beta e$. If d^* is a term satisfying $(*)_{n,n}$, then:

$$aF^n(\alpha)d^*(a, b, b)\overline{(\alpha \circ \theta) \cup (\theta \circ \beta)}d^*(c, c, e)G^n(\beta)e.$$

Notice that if θ is compatible and reflexive then in (i) we can change $\leq$ to $=$.

(ii) If $a\alpha b\theta c$ and $a\gamma c$, then

$$aF^n(\alpha)d^*(a, b, b)\overline{\alpha \cup \theta}d^*(a, a, c)G^n(\gamma)c,$$

and $a\gamma c\gamma d^*(a, a, c)$, since $G^n(\gamma) \leq \gamma$.

(iii) It is enough to show that, for every $m \geq 2$, and every $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$:

(1) $\qquad \underbrace{\alpha \circ \beta \circ \alpha \ldots}_{m \text{ factors}} \leq (F^n(\alpha) + F^n(\beta)) \circ \overline{\alpha \cup \beta} \circ (G^n(\alpha) + G^n(\beta)),$

since $\alpha \circ \beta$ is a compatible relation containing $\alpha \cup \beta$.

We will prove by induction on m that (1) holds for every α, $\beta \in \operatorname{Con} \mathbf{A}$.

The case $m = 2$ follows from (i) when θ is the zero congruence (for locally finite varieties omitting type 1, $\alpha \circ \beta \leq [\alpha, \alpha] \circ \beta \circ \alpha \circ [\beta, \beta]$ has been noticed by R. McKenzie [KP, Theorem 5.14]).

So, suppose that (1) holds for m (say, m odd). Then

$$\underbrace{\alpha \circ \beta \circ \cdots \circ \beta}_{m+1 \text{ factors}} = \alpha \circ \theta \circ \beta,$$

where $\theta = \beta \circ \alpha \circ \cdots \circ \alpha$ ($m - 1$ factors).

Now, both $\alpha \circ \theta$ and $\theta \circ \beta$ have m factors, and (1), together with its formulation in which α and β are swapped, implies that both $\alpha \circ \theta$ and $\theta \circ \beta$ are contained in $(F^n(\alpha) + F^n(\beta)) \circ \overline{\alpha \cup \beta} \circ (G^n(\alpha) + G^n(\beta))$.

Since the latter is a compatible subset of $A \times A$, we can apply (i) in order to obtain:

$$\alpha \circ \theta \circ \beta \leq F^n(\alpha) \circ (F^n(\alpha) + F^n(\beta)) \circ \overline{\alpha \cup \beta} \circ (G^n(\alpha) + G^n(\beta)) \circ G^n(\beta)$$
$$= (F^n(\alpha) + F^n(\beta)) \circ \overline{\alpha \cup \beta} \circ (G^n(\alpha) + G^n(\beta)),$$

thus completing the induction step. The case m even is entirely similar.

(iv) is similar and much easier, using (ii). (Compare the remark at the end of the proof of Theorem 3.2(i).)

(v) If $\operatorname{Con} \mathbf{A}$ is modular, then for every m:

$$G^m(\gamma(\alpha + \beta)) \leq G(\gamma(\alpha + \beta)) \leq \gamma(\alpha + \beta) \leq \alpha(\gamma + \beta) + \beta(\alpha + \gamma).$$

For the converse, if $n' \geq \sup\{n, m\}$, the hypotheses give by (iv):

$$\gamma(\alpha + \beta) \leq \gamma(\alpha \circ \beta) \circ G^{n'}(\gamma(\alpha + \beta)) \leq \gamma(\alpha \circ \beta) \circ G^m(\gamma(\alpha + \beta))$$
$$\leq (\alpha(\gamma + \beta) + \beta(\alpha + \gamma)) \circ (\alpha(\gamma + \beta) + \beta(\alpha + \gamma));$$

and

$$\gamma(\alpha + \beta) \leq \alpha(\gamma + \beta) + \beta(\alpha + \gamma)$$

is an identity equivalent to modularity.   □

3.2.   **Theorem.** *Suppose that* $\mathbf{A}$ *is an algebra, and that* $[\alpha, \beta]^*$ *is a monotone binary operation on* $\operatorname{Con} \mathbf{A}$ *such that*

$$[\alpha, \beta]^* \leq \alpha\beta, \quad and \quad [\alpha + \beta, \gamma]^* = [\alpha, \gamma]^* + [\beta, \gamma]^*,$$

for every α, β, $\gamma \in \operatorname{Con} \mathbf{A}$. *Then*:

(i) *If there is a ternary term* d *of* $\mathbf{A}$ *such that* $d(a, b, b) = a[\alpha, \alpha]^* d(b, b, a)$, *for every* $\alpha \in \operatorname{Con} \mathbf{A}$ *and* $a\alpha b$, *then* $\operatorname{Con} \mathbf{A}$ *is modular.*

(ii) *If there is a ternary term* d *of* $\mathbf{A}$ *such that*

$$d(a, b, b)[\alpha, \alpha]^* a[\alpha, \alpha]^* d(b, b, a),$$

for every $\alpha \in \operatorname{Con} \mathbf{A}$ *and* $a\alpha b$, *then* $\operatorname{Con} \mathbf{A}$ *satisfies the following identities and implication*:

(a) $\delta(\gamma(\alpha + \beta) + \gamma'(\alpha' + \beta')) \leq \gamma(\alpha + \beta)(\gamma'(\alpha' + \beta') + \delta + \gamma\alpha + \gamma\beta) + \gamma'(\alpha' + \beta')$
$\cdot (\gamma(\alpha + \beta) + \delta + \gamma'\alpha' + \gamma'\beta')$.

(b) $\delta(\gamma(\alpha + \beta) + \varepsilon) \leq \varepsilon + \gamma(\alpha + \beta)(\varepsilon + \delta + \gamma\alpha + \gamma\beta)$.

(c) *if* $\alpha \leq \gamma\delta$ *and* $\varepsilon \leq \delta$ *then* $\delta(\gamma(\alpha + \beta) + \varepsilon) \leq \varepsilon + \gamma(\delta + \gamma\beta)$.

Proof. (i) For a whole variety the result is implicitly proved in [Gu, Theorem 7.4], since only the above formal properties of the commutator are used in the

proof of Lemma 7.3 therein. Cf. also the proof given in [FMK, Theorem 6.4]. The proof we give is simpler and holds in a more general context.

The hypotheses on $[\alpha, \beta]^*$ imply that

(1) $[\gamma(\alpha + \beta), \gamma(\alpha + \beta)]^* \le [\alpha + \beta, \gamma]^* = [\alpha, \gamma]^* + [\beta, \gamma]^* \le \alpha\gamma + \beta\gamma.$

(i) follows now from 3.1(v), by taking $n = 1$, $F(\alpha) = 0$ and $G(\alpha) = [\alpha, \alpha]^*$.

Notice that only a small part of Lemma 3.1 is used: as in 3.1(ii), one can show that:

$$\gamma(\underbrace{\alpha \circ \beta \circ \alpha \circ \cdots}_{n+1 \text{ factors}}) \le \gamma(\underbrace{\beta \circ \alpha \circ \cdots}_{n \text{ factors}}) \circ [\gamma, \gamma]^* \le \cdots \le \gamma(\alpha \circ \beta) \circ [\gamma, \gamma]^*;$$

and the proof can be finished using (1) above since, without loss of generality, we can take $\gamma = \gamma(\alpha + \beta)$.

Notice also that we have used only (1) rather than the full power of join distributivity.

(ii) (a) Let $\theta = \gamma(\alpha + \beta)$ and $\theta' = \gamma'(\alpha' + \beta')$. Then, by taking $F(\alpha) = G(\alpha) = [\alpha, \alpha]^*$, Lemma 3.1(iii) implies: $\delta(\theta + \theta') = \delta(([\theta, \theta]^* + [\theta', \theta']^*) \circ \theta \circ \theta' \circ ([\theta, \theta]^* + [\theta', \theta']^*)) \le ([\theta, \theta]^* + [\theta', \theta']^*) \circ \theta(\theta' + \delta + [\theta, \theta]^*) \circ \theta'(\theta + \delta + [\theta', \theta']^*) \circ ([\theta, \theta]^* + [\theta', \theta']^*) \le \theta(\theta' + \delta + [\theta, \theta]^*) + \theta'(\theta + \delta + [\theta', \theta']^*).$

But $[\theta, \theta]^* = [\gamma(\alpha+\beta), \gamma(\alpha+\beta)]^* \le [\alpha+\beta, \gamma]^* = [\alpha, \gamma]^* + [\beta, \gamma]^* \le \alpha\gamma + \beta\gamma$; and similarly $[\theta', \theta']^* \le \alpha'\gamma' + \beta'\gamma'$; so that (a) follows by substituting those values in the above inequality.

(b) is the particular case of (a) when $\alpha' = \beta' = \gamma' = \varepsilon$.

(c) follows from (b) since, under the hypotheses of (c):

$$\delta(\gamma(\alpha + \beta) + \varepsilon) \le \varepsilon + \gamma(\alpha + \beta)(\delta + \gamma\beta) \le \varepsilon + \gamma(\delta + \gamma\beta). \quad \square$$

Remarks. As a consequence of Theorem 3.2(i), if **A** has a difference term and Con **A** is not modular, then the commutator is neither left distributive (nor right distributive, by symmetry) over joins. In particular, distributivity of the commutator does not hold in nonmodular neutral varieties; e.g. in Polin's algebra [DF]. Indeed, it is trivial to show that if **A** is a neutral algebra and the commutator is left (or right) distributive, then Con **A** is even distributive:

$$\alpha(\beta + \gamma) = [\alpha(\beta + \gamma), \alpha(\beta + \gamma)] \le [\beta + \gamma, \alpha] = [\beta, \alpha] + [\gamma, \alpha] = \beta\alpha + \gamma\alpha.$$

We shall prove in a forthcoming paper that the condition "V has a difference term" is a Mal'cev condition (strictly weaker than modularity, since, e.g., semilattices have a difference term). Hence, Theorem 3.2(i) implies that if Problem 1.7(b) has an affirmative answer, then there are two Mal'cev conditions both strictly weaker than modularity, which together imply modularity: this would solve a long-standing problem.

Standard computations show that the identity in Theorem 3.2(ii)(a) is satisfied in the smallest nonmodular lattice N_5; so that (ii)(a) is an identity strictly weaker than modularity. It it a nontrivial identity, since already (ii)(c) fails in the lattice:
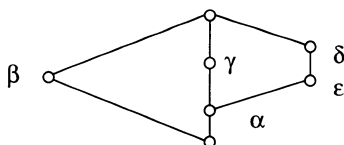
Let us remark, however, that we shall prove in Corollary 5.8(3) that the above lattice cannot be a sublattice of $\mathrm{Con}\,\mathbf{A}$, if $\mathbf{A}$ has a weak difference term.

3.3. Theorem. *If* α, α', β, $\beta' \in \mathrm{Con}\,\mathbf{A}$, $\alpha^{(n)} \le \alpha' \le \alpha$ *and* $\beta^{(n)} \le \beta' \le \beta$ *and* $\mathbf{A}$ *has a weak difference term, then*

(i) $\alpha + \beta = (\alpha' + \beta') \circ \alpha \circ \beta \circ (\alpha' + \beta')$.

(ii) *If* α *permutes with* β', *then*

$$\alpha + \beta = \alpha \circ \beta \circ \alpha = \alpha' \circ \beta \circ \alpha = \alpha \circ \beta \circ \alpha'.$$

(iii) *If* α' *and* β' *permute, then*

$$\alpha + \beta = \alpha' \circ \beta \circ \alpha \circ \beta' = \beta' \circ \alpha \circ \beta \circ \alpha';$$

in particular, α *and* β *4-permute.*

(iv) *If* α *permutes with* β' *and* β *permutes with* α' *then* α *and* β *permute.*

(v) *If* $\gamma \ge \beta$ *and* $\gamma \ge \alpha'$ *then* $\gamma(\alpha + \beta) = \gamma\alpha + \beta$.

(vi) $\gamma(\alpha + \beta) = \gamma(\alpha(\gamma + \beta + \alpha') + \beta(\gamma + \alpha + \beta'))$.

Proof. (i) is immediate from Lemma 3.1(iii), with $F(\alpha) = G(\alpha) = [\alpha, \alpha]$, since $\alpha + \beta = (\alpha^{(n)} + \beta^{(n)}) \circ \alpha \circ \beta \circ (\alpha^{(n)} + \beta^{(n)}) \le (\alpha' + \beta') \circ \alpha \circ \beta \circ (\alpha' + \beta') \le \alpha + \beta$.

(ii) By (i), $\alpha + \beta = (\alpha' + \beta') \circ \alpha \circ \beta \circ (\alpha' + \beta') \le (\alpha + \beta') \circ \alpha \circ \beta \circ (\alpha + \beta') = \alpha \circ \beta' \circ \alpha \circ \beta \circ \beta' \circ \alpha = \alpha \circ \alpha \circ \beta' \circ \beta \circ \alpha = \alpha \circ \beta \circ \alpha \le \alpha + \beta$.

Moreover, by 3.1(i) with $\theta = 0$: $\alpha \circ \beta \le \alpha' \circ \beta \circ \alpha \circ \beta' = \alpha' \circ \beta \circ \alpha$, and hence $\alpha \circ \beta \circ \alpha \le \alpha' \circ \beta \circ \alpha \le \alpha + \beta$. The other identity follows by symmetry.

(iii) and (iv) are proved in a similar fashion.

(v) By (i), $\gamma(\alpha + \beta) = \gamma((\alpha' + \beta') \circ \alpha \circ \beta \circ (\alpha' + \beta')) = (\alpha' + \beta') \circ \gamma\alpha \circ \beta \circ (\alpha' + \beta') \le \gamma\alpha + \beta \le \gamma(\alpha + \beta)$.

(vi) is proved similarly. □

3.4. Corollary. *If* $\mathbf{A}$ *is solvable and has a weak difference term, then* $\mathrm{Con}\,\mathbf{A}$ *is modular.*

Proof. Immediate from 3.3(v). □

As one could expect, Theorem 3.3 can be strengthened, if the existence of a difference term is assumed.

3.5. Theorem. *If* α, β, $\gamma \in \mathrm{Con}\,\mathbf{A}$ *and* $\mathbf{A}$ *has a difference term, then for every* n:

(i) $\alpha + \beta = (\alpha^{(n)} + \beta^{(n)}) \circ \alpha \circ \beta = \alpha \circ (\alpha^{(n)} + \beta^{(n)}) \circ \beta = \alpha \circ \beta \circ (\alpha^{(n)} + \beta^{(n)})$.

(ii) $\gamma(\alpha + \beta) = \gamma(\alpha \circ \beta) \circ (\gamma(\alpha + \beta))^{(n)} = \gamma(\alpha(\beta + \gamma) + \beta(\alpha + \gamma)) \circ (\gamma(\alpha + \beta))^{(n)}$.

Proof. (i) Similar to the proof of Theorem 3.3 (cf. also [Gu, Lemma 8.4]).

(ii) uses Lemma 3.1(iv). □

3.6. Theorem. *If* α, α', β, $\beta' \in \mathrm{Con}\,\mathbf{A}$, $\alpha^{(n)} \le \alpha' \le \alpha$, $\beta^{(n)} \le \beta' \le \beta$, *and* $\mathbf{A}$ *has a difference term, then* α *and* β *permute if and only if* α' *and* β' *permute.*

Proof. If α' and β' permute than α and β permute by Theorem 3.5(i).

For the converse, suppose that α and β permute, and $\beta^{(n)} \le \beta' \le \beta$.

If $a\alpha b\beta'c$ then $a\alpha + \beta c$, and hence there is an e such that $a\beta e\alpha c$; so that $e\alpha c\beta'b\alpha a$, and $a\beta(\alpha + \beta')e$.

By the symmetric version of Theorem 3.5(ii), $\beta(\alpha + \beta') \le \beta^{(n)} \circ \beta(\beta' \circ \alpha) \le \beta' \circ \alpha$. Hence $a\beta' \circ \alpha e\alpha c$, so that $a\beta' \circ \alpha c$.

We have proved that $\alpha \circ \beta' \leq \beta' \circ \alpha$; a symmetric argument gives the other inclusion, and hence α and β' permute. Now, starting with $\beta = \beta'$, the above argument shows that α' and β' permute. $\square$

We mention also the following interesting corollary of (the proof of) Lemma 3.1, though it will not be needed. If $\psi \subset A \times A$, then $Cg\psi$ denotes the least congruence of **A** containing ψ.

3.7. Proposition. *Suppose that* **A** *has a weak difference term, and* ψ *is a compatible relation on* $A \times A$ *containing the zero congruence. Then, for every* n:

$$Cg\psi = (Cg\psi)^{(n)} \circ \psi \circ (Cg\psi)^{(n)}.$$

If **A** *has a difference term, then*

$$Cg\psi = (Cg\psi)^{(n)} \circ \psi = \psi \circ (Cg\psi)^{(n)}.$$

Proof. Let $\gamma = (Cg\psi)^{(n)}$.

$\psi \circ \psi \circ \cdots \circ \psi \leq \gamma \circ \psi \circ \gamma$ is proved as Lemma 3.1(iii), by noting that in 3.1(i) we do not need α and β to be congruences, provided we use $F(Cg\alpha)$ and $G(Cg\alpha)$ in place of $F(\alpha)$ and $G(\alpha)$, and provided at least one of α or β is reflexive.

It remains to show that $(\gamma \circ \psi \circ \gamma)^{-1} \leq \gamma \circ \psi \circ \gamma$.

But if $a\gamma b\psi c\gamma e$, then $e\gamma c\gamma d^*(c, b, b)\psi d^*(c, c, b)\gamma b\gamma a$.

Similarly, if we have a difference term, and $a\psi b\gamma c$ then

$$c = d^*(c, a, a)\psi d^*(c, b, a)\gamma d^*(b, b, a)\gamma a;$$

so that $(\psi \circ \gamma)^{-1} \leq \psi \circ \gamma$ (where, in both cases, d^* is given by Lemma 3.1). $\square$

Notice that (the proof of) Proposition 3.7 generalizes a well-known theorem asserting that, in a permutable variety, every compatible relation on $A \times A$ containing the zero congruence is a congruence (observe that, in the case of permutable varieties, we can take $F = 0$ and $G = 0$ constantly).

3.8. *Remark.* All results of this section can be generalized for joins of three or more congruences. For example, Theorem 3.1(iii) becomes

$$\alpha + \beta + \gamma = (\alpha^{(n)} + \beta^{(n)} + \gamma^{(n)}) \circ \alpha \circ \beta \circ \gamma \circ (\alpha^{(n)} + \beta^{(n)} + \gamma^{(n)}).$$

We leave the proof and the other generalizations to the reader.

The following identity ("three subgroups lemma"):

$$[\alpha, [\beta, \gamma]] \leq [\beta, [\alpha, \gamma]] + [\gamma, [\alpha, \beta]]$$

does not necessarily hold even in permutable varieties: nonassociative rings do not satisfy it, though associative rings do (in rings, the general commutator corresponds to the ideal $IJ + JI$).

3.9. Problem. Find useful consequences of the above identity. Characterize varieties (modular varieties, locally finite varieties,...) satisfying it. Notice that, if the commutator is not commutative, we can write many similar identities which are not necessarily equivalent.

4. COMMUTATOR IDENTITIES: COMMUTATORS OF JOINS

For the "real" commutator Theorem 3.2(i) and Lemma 3.1(v) can be strengthened:

4.1. Proposition. *Suppose that* **A** *has a difference term. Then the following are equivalent*:

(i) Con **A** *is modular.*

(ii) $[\alpha + \beta, \gamma] \le \gamma\alpha + \gamma\beta$, *for every* $\alpha, \beta, \gamma \in$ Con **A**.

(iii) $[\gamma(\alpha + \beta), \gamma(\alpha + \beta)] \le \gamma\alpha + \gamma\beta$, *for every* $\alpha, \beta, \gamma \in$ Con **A**.

(iv) $[\alpha + \beta, \gamma] \le \alpha + \gamma\beta$, *for every* $\alpha, \beta, \gamma \in$ Con **A** *with* $\alpha \le \gamma$.

(v) $[\gamma(\alpha + \beta), \gamma(\alpha + \beta)] \le \alpha + \gamma\beta$, *for every* $\alpha, \beta, \gamma \in$ Con **A** *with* $\alpha \le \gamma$.

(vi) $[\gamma(\alpha + \beta), \gamma(\alpha + \beta)] \le \alpha(\beta + \gamma) + \beta(\alpha + \gamma)$, *for every* $\alpha, \beta, \gamma \in$ Con **A**.

Proof. (ii) $\Rightarrow$ (iv) and (iii) $\Rightarrow$ (vi) are trivial.

(i) $\Rightarrow$ (ii) is Corollary 1.3(e).

(ii) $\Rightarrow$ (iii) $[\gamma(\alpha + \beta), \gamma(\alpha + \beta)] \le [\alpha + \beta, \gamma] \le \gamma\alpha + \gamma\beta$.

(iv) $\Rightarrow$ (v) is similar.

(v) $\Rightarrow$ (i) follows from the left-hand identity in Theorem 3.5(ii).

(vi) $\Rightarrow$ (i) follows from Lemma 3.1(v). $\square$

4.2. Proposition. *Suppose that* **A** *has a weak difference term, and* $\alpha, \gamma \in$ Con **A**. *Then* $\gamma \ge [\alpha, \alpha]$ *if and only if* α *centralizes* α *modulo* γ.

Proof. The if part is the definition of the commutator.

For the other part, suppose that $a\gamma b$ and $\left|\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right| \in M(\alpha, \alpha)$. Then also $\left|\begin{smallmatrix} a & a \\ a & a \end{smallmatrix}\right|$ and $\left|\begin{smallmatrix} b & a \\ b & a \end{smallmatrix}\right| \in M(\alpha, \alpha)$, and hence $\left|\begin{smallmatrix} d(a,a,b) & d(b,a,a) \\ d(c,a,b) & d(e,a,a) \end{smallmatrix}\right| \in M(\alpha, \alpha)$.

But $d(a, a, b)[\alpha, \alpha] d(b, a, a)$, since d is a weak difference term; hence $d(c, a, b)[\alpha, \alpha] d(e, a, a)$, since α centralizes α modulo $[\alpha, \alpha]$.

But $c[\alpha, \alpha] d(c, a, a)\gamma d(c, a, b)[\alpha, \alpha] d(e, a, a)[\alpha, \alpha]e$, and hence $c\gamma e$, as $\gamma \ge [\alpha, \alpha]$. $\square$

Remark. More generally, the above proof shows that if $\gamma \ge \beta^{(n)}$, $\gamma \ge \delta \ge (\gamma\alpha)^{(n)}$ and $C(\beta, \alpha; \delta)$, then $C(\beta, \alpha; \gamma)$. Use the term d^* of Lemma 3.1, and observe that $d^*(e, a, a)\gamma d^*(e, b, b)\beta^{(n)}e$.

Moreover, if there is a difference term, then the hypothesis $\gamma \ge \beta^{(n)}$ is unnecessary.

4.3. Theorem. *If* **A** *has a weak difference term, then for every* $\alpha, \gamma \in$ Con **A**:

(i) $[\gamma + \alpha, \gamma + \alpha] \le \gamma + [\alpha, \alpha]$.

(ii) *If* $p + q = m$, *then* $(\gamma + \alpha)^{(m)} \le \gamma^{(p)} + \alpha^{(q)}$.

(iii) $[(\alpha + \gamma)/\gamma, (\alpha + \gamma)/\gamma] = ([\alpha + \gamma, \alpha + \gamma] + \gamma)/\gamma = (\gamma + [\alpha, \alpha])/\gamma$ *(where the left-hand commutator is computed in* **A**/γ).

Proof. (i) Without loss of generality, we may assume $\gamma = \gamma + [\alpha, \alpha]$; hence, by Theorem 3.3(ii), $\gamma + \alpha = \gamma \circ \alpha \circ \gamma$. We will show that $\gamma + \alpha$ centralizes $\gamma + \alpha$ modulo γ.

By Proposition 1.2(4), it is enough to show $C(\gamma, \gamma + \alpha; \gamma)$ and $C(\alpha, \gamma + \alpha; \gamma)$. The first relation is trivial (by Proposition 1.2(5)).

For the second relation, first observe that $C(\alpha, \alpha; \gamma)$, by Proposition 4.2. Now apply Lemma 1.5 with $\beta' = \alpha$ and $\beta = \gamma = \delta$, in order to obtain $C(\alpha, \gamma + \alpha; \gamma)$.

(ii) follows from $\beta^{(p+q)} = (\beta^{(q)})^{(p)}$ and from $(\gamma + \alpha)^{(q)} \le \gamma + \alpha^{(q)}$, which are proved by induction, using (i).

(iii) $[(\alpha + \gamma)/\gamma, (\alpha + \gamma)/\gamma] \ge (\gamma + [\alpha, \alpha])/\gamma$ is trivial. $(\gamma + [\alpha, \alpha])/\gamma \ge ([\alpha + \gamma, \alpha + \gamma] + \gamma)/\delta$ follows from (i).

By Proposition 4.2, $C(\alpha + \gamma, \alpha + \gamma, [\alpha + \gamma, \alpha + \gamma] + \gamma)$, and hence $[(\alpha+\gamma)/\gamma, (\alpha+\gamma)/\gamma] \le ([\alpha+\gamma, \alpha+\gamma]+\gamma)/\gamma$, by [HMK, Proposition 3.4(5)]. $\square$

The next theorem uses a result by A. Day and R. Freese on Polin's variety (see [DF]) in order to show that a solution of Problem 1.7(b) cannot be given by any (weak) Mal'cev condition arising from some lattice identity.

Recall that, if P and Q are two properties which can be satisfied by congruence lattices, then $P \models_c Q$ means that, for every variety $\underline{V}$, if $\mathrm{Con}\,\mathbf{A}$ satisfies P, for every $\mathbf{A} \in \underline{V}$, then $\mathrm{Con}\,\mathbf{A}$ satisfies Q, for every $\mathbf{A} \in \underline{V}$.

Mod is the modular identity.

4.4.   Theorem. *If σ is any lattice identity, then the following are equivalent:*

(a) $\sigma \models_c$ *"the commutator is distributive".*
(b) $\sigma \models_c$ *"the commutator is left distributive".*
(c) $\sigma \models_c [\beta + \gamma, \alpha] \le \alpha\beta + \alpha\gamma$.
(d) $\sigma \models_c [\beta + \gamma, \alpha] \le \beta(\alpha + \gamma) + \gamma(\alpha + \beta)$.
(e) σ *fails in every nonmodular neutral variety.*
(f) σ *fails in Polin's variety.*
(g) $\sigma \models_c \mathrm{Mod}$.

Proof. (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) are trivial.

(d) $\Rightarrow$ (e) $\alpha(\beta + \gamma) = [\beta + \gamma, \alpha] \le \beta(\alpha + \gamma) + \gamma(\alpha + \beta)$.

(e) $\Rightarrow$ (f) Polin's variety is neutral, since it has a semilattice operation [DF] (cf. Remark 2.4).

(f) $\Rightarrow$ (g) follows from [DF, Theorem 6.1].

(g) $\Rightarrow$ (a) is Theorem 1.4. $\square$

Conjecture. The identity in Theorem 3.2(ii)(a) is satisfied in Polin's variety.

4.5.   Example. We now show that our results about algebras with a difference term do not necessarily hold if only the existence of a weak difference term is assumed.

Let $\mathbf{A} = S_2 \times \mathbf{Z}_2$, where S_2 and $\mathbf{Z}_2$ are the 2-element semilattice, respectively, cyclic group (thought of as a semigroup).

$\mathrm{Con}\,\mathbf{A}$ has five elements: $0, 1, \alpha$ (γ, respectively) the kernel of the projection onto $\mathbf{Z}_2$ (S_2, respectively), and β, the congruence which identifies $(0, 1)$ and $(0, 0)$:
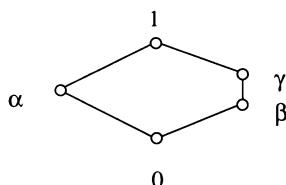
A belongs to a locally finite variety having a weak difference term, by Example 2.2(7), and hence omitting type 1, by 2.2(3).

By [HMK, Proposition 3.4(5)], $C(1, 1; \alpha)$, and not $C(1, 1; \gamma)$; hence, by §5 of the present paper, $[1, 1] = \alpha$, $[\gamma, \gamma] = 0$, and hence $[\alpha, \alpha] = [1, \alpha] = [\alpha, 1] = \alpha$.

Moreover, $[\gamma, 1] = [1, \gamma] = 0$, since both $[\gamma, 1] \le [1, 1] \le \alpha$, and $[\gamma, 1] \le \gamma$, and symmetrically.

It follows that the commutator is distributive (also commutative) in $\mathrm{Con}\,\mathbf{A}$, but $\mathrm{Con}\,\mathbf{A}$ is not modular, thus showing that Theorem 3.2 and Proposition 4.1 do not generalize.

Moreover, $[\beta, \beta] = 0$ and α permute, but α and β do not permute. Also, 1 and β permute, but $[1, 1] = \alpha$ and β do not permute; hence no direction of Theorem 3.6 holds, for algebras with a weak difference term (that is, Theorem 3.3(ii) is the best possible).

The computations

$$([\beta, \beta] + [\alpha, \alpha]) \circ \alpha \circ \beta = \alpha \circ ([\beta, \beta] + [\alpha, \alpha]) \circ \beta = \alpha \circ \beta \neq \alpha + \beta$$

and $\gamma(\alpha \circ \beta) + [\gamma, \gamma] = \gamma(\alpha(\beta + \gamma) \circ \beta) = \beta \neq \gamma = \gamma(\alpha + \beta)$ show that Theorem 3.5 does not hold, either.

We have

$$([\alpha, \alpha] + [\beta, \beta]) \circ (\gamma + [\alpha, \alpha] + [\beta, \beta])(\alpha \circ \beta) \circ [\gamma + [\beta, \beta], \gamma + [\beta, \beta]]$$
$$= \alpha \circ \beta \not\geq \gamma = \gamma(\alpha + \beta),$$

and hence we cannot expect to improve Lemma 3.1(iv) to

$$\gamma(\alpha + \beta) \leq (F^n(\alpha) + F^n(\beta))$$
$$\circ (\gamma + F^n(\alpha) + F^n(\beta))(\alpha \circ \beta) \circ G^n(\gamma(\alpha + \beta) + F^n(\beta)).$$

Let us remark that, by the results we are going to prove in §5, all the above follows just from the assumptions that **A** has a weak difference term, that $\mathrm{Con}\, \mathbf{A} = N_5$ and that $[1, 1] < 1$.

4.6. Example. With some more efforts, we can get counterexamples to everything above even in the case of an algebra in a locally finite 4-permutable variety.

Let $\mathbf{S}_2 = (S_2, \cdot, ')$, where $(S_2, \cdot)$ is the 2-element semilattice, and $0' = 1$, $1' = 0$. Let $\mathbf{Z}_2 = (Z_2, \cdot, ')$, where $(Z_2, \cdot)$ is the 2-element group, and $0' = 1' = 0$.

Let $\mathbf{A} = \mathbf{S}_2 \times \mathbf{Z}_2$. Clearly, all the arguments of Example 4.5 carry over.

We now show that **A** belongs to a 4-permutable variety. Define $a \oplus b = (ab)'(a'b')'$. Then $\oplus$ acts as symmetric difference on the first coordinate, and is constantly 0 on the second coordinate. Hence

$$t_1(x, y, z) = x(x \oplus y \oplus z),$$
$$t_2(x, y, z) = xyz, \quad \text{and}$$
$$t_3(x, y, z) = (x \oplus y \oplus z)z,$$

satisfy the Hagemann-Mitschke identities for 4-permutability (see e.g. [HMK, Lemma 9.13]).

In order to show that $\underline{V}(\mathbf{A})$ is locally finite, define $a + b = (a'b')'$. Then $(S_2, \cdot, +, ')$ is the 2-element Boolean algebra, while $+$ is constantly 0 on Z_2. Whence, in $\underline{V}(\mathbf{A})$, $+$ and $\cdot$ are commutative and associative, the two distributive laws hold, and moreover $(a + b)' = a'b'$, $(ab)' = a' + b'$, $a'' = aa$, $a^3 = a$, and $a + a + a = a + a$. The above identities imply that $\underline{V}(\mathbf{A})$ is locally finite (argue as in the case of Boolean algebras).

The above construction is a version of Polin's algebra [DF], when the 2-element group replaces the 2-element Boolean algebra as "internal" algebra.

It would be interesting to study the congruence identities (with or without the commutator) satisfied in this and similar generalizations of Polin's variety.

4.7. Example. We show that the commutator is not necessarily commutative even in 4-permutable locally finite varieties. This improves on (and is very similar to) [KP, Example 5.17].

Let **A** be as in 4.6, with α, β and γ as in 4.5.

The matrix

$$\begin{vmatrix} (0,1)(1,1) & (0,1)(1,0) \\ (1,1)(1,1) & (1,1)(1,0) \end{vmatrix}$$

shows that $C(\alpha,\gamma;\beta)$ fails, and hence $C(1,\gamma;\beta)$ fails, too.

The next proposition implies that $C(\gamma,1;\beta)$ holds, whence in $\mathbf{A}/\beta$ $[\gamma/\beta, 1/\beta] = \beta/\beta \neq \gamma/\beta = [1/\beta, \gamma/\beta]$, by the above and [HMK, Proposition 3.4(5)].

4.8. Proposition. *Suppose that* **A** *is any algebra, and* $\alpha, \varepsilon, \gamma, \delta \in \mathrm{Con}\,\mathbf{A}$. *If* $C(\alpha, \varepsilon; \delta)$, $\gamma \geq \delta$, *and every* γ-*block is either a* δ-*block or an* α-*block, then* $C(\alpha, \varepsilon; \gamma)$ *holds, too.*

Proof. Let $\left|\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right| \in M(\alpha,\varepsilon)$, and $a\gamma b$.

If $a\delta b$ then $C(\alpha,\varepsilon;\delta)$ implies that $c\delta d$, hence $c\gamma d$.

Otherwise, the γ-block containing a coincides with the α-block containing a. Whence $a\alpha b$, and $c\alpha a$, $d\alpha b$, implying $c\gamma a$, $d\gamma b$ and hence $c\gamma d$.

In any case, $C(\alpha,\varepsilon;\gamma)$ holds. □

4.9. Remark. If $[\alpha,\beta] \neq [\beta,\alpha]$ then the commutator is necessarily distinct from any other commutative binary operation defined on congruences! This implies at once that the commutator is distinct from the linear commutator [Qu], from the 2-terms commutator [Ki], from the weak commutator [Ke], and from the commutators defined in [FMK, Definitions 3.1 and 3.2(4)]. Thus, in 4-permutable locally finite varieties, the weak commutator is strictly smaller than the two terms commutator.

5. SUBLATTICES OF CONGRUENCE LATTICES

A quotient interval $I(\alpha,\beta)$ is *abelian* (*solvable*) if and only if $[\beta,\beta] \leq \alpha$ ($\beta^{(n)} \leq \alpha$, for some n).

5.1. Theorem. (*Abelian and solvable quotients are preserved under transposition.*) *Suppose that* **A** *has a weak difference term,* $\alpha, \beta, \gamma, \delta \in \mathrm{Con}\,\mathbf{A}$, $\alpha+\beta = \gamma$ *and* $\alpha\beta = \delta$.

That is, the following is a sublattice of $\mathrm{Con}\,\mathbf{A}$:
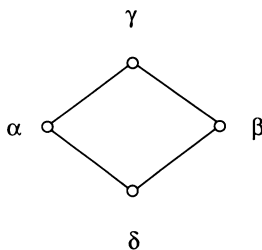
Then $[\gamma,\gamma] \leq \alpha$ *if and only if* $[\beta,\beta] \leq \delta$; *and, for every* $n \geq 1$,

$$\gamma^{(n)} \leq \alpha \quad \text{if and only if} \quad \beta^{(n)} \leq \delta.$$

Proof. If $[\gamma,\gamma] \leq \alpha$, then $[\beta,\beta] \leq \beta$, and $[\beta,\beta] \leq [\gamma,\gamma] \leq \alpha$, implying $[\beta,\beta] \leq \alpha\beta = \delta$.

If $[\beta,\beta] \leq \delta$, then, by Theorem 4.3(i), $[\gamma,\gamma] = [\alpha+\beta, \alpha+\beta] \leq \alpha+[\beta,\beta] = \alpha$.
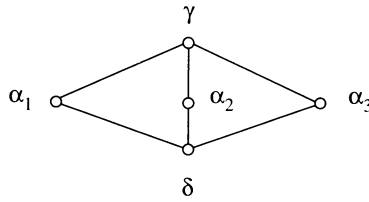
The last statement is proved in a similar way, using 4.3(ii). □

For modular varieties Theorem 5.1 follows from Remarks 4.6 in [FMK]. For locally finite varieties similar results are obtained in [HMK, Lemmata 6.2 and 7.4].

5.2. Theorem. *Suppose that* **A** *has a weak difference term,* $\alpha_1, \alpha_2, \alpha_3, \gamma, \delta \in$ Con **A**, *and*

$$\alpha_i \alpha_j = \delta; \quad \alpha_i + \alpha_j = \gamma \quad (1 \le i < j \le 3).$$

That is, the following is a sublattice of Con **A** :

Then $[\gamma, \gamma] \le \delta$.

Proof. By Proposition 1.2(6), $C(\gamma, \alpha_1; \delta)$. In particular, $[\alpha_1, \alpha_1] \le \delta$. By Theorem 5.1, both $[\gamma, \gamma] \le \alpha_2$ and $[\gamma, \gamma] \le \alpha_3$, whence $[\gamma, \gamma] \le \delta$. □

Theorem 5.2 has a trivial proof for modular varieties (using distributivity of the commutator); and for locally finite varieties omitting type 1 it has been proved in [Wi, Theorem 1.5], where it is also shown that it does not hold in general for locally finite varieties. So, the existence of a weak difference term (or some other hypothesis) is necessary in proving both Theorem 5.2 and Theorem 5.1 (Theorem 5.1 must fail in Willard's algebras, since, under the hypotheses of 5.2, $[\alpha_1, \alpha_1] \le \delta$ holds in every algebra).

For locally finite varieties omitting type 1 the next theorem follows from [HMK, Lemma 6.5].

5.3. Theorem. *Suppose that* $n \ge 1$ *and that* **A** *has a weak difference term,* $\alpha, \beta, \gamma, \delta, \varepsilon \in$ Con **A**, $\beta < \gamma$, $\gamma + \alpha = \alpha + \beta = \varepsilon$, *and* $\gamma \alpha = \beta \alpha = \delta$. *That is, the following is a sublattice of* Con **A** :
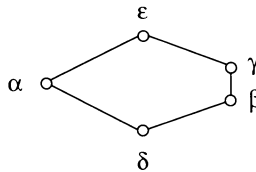
N_5

Then neither $\alpha^{(n)} \le \delta$ *nor* $\varepsilon^{(n)} \le \gamma$.

Moreover, if either $\beta^{(n)} \le \delta$, *or* $\varepsilon^{(n)} \le \alpha$, *then also* $\gamma^{(n)} \le \delta$.

If **A** *has a difference term, then* $\gamma^{(n)} + \beta = \gamma$, *and hence neither* $\gamma^{(n)} \le \beta$, *nor* $\beta^{(n)} \le \delta$, *nor* $\varepsilon^{(n)} \le \alpha$ *(that is, no interval in the picture is solvable).*

Proof. Suppose by contradiction $\alpha^{(n)} \le \delta$. Then Theorem 3.3(ii) implies $\gamma = \gamma(\alpha + \beta) = \gamma(\beta \circ \alpha \circ \beta) = \beta \circ \gamma \alpha \circ \beta = \beta$, which is absurd.

Suppose that **A** has a difference term. Then, by Theorem 3.5(ii), $\gamma = \gamma(\alpha + \beta) = \gamma(\alpha \circ \beta) \circ \gamma^{(n)} = \gamma\alpha \circ \beta \circ \gamma^{(n)} = \beta \circ \gamma^{(n)} \leq \beta + \gamma^{(n)} \leq \gamma$.

All the rest follows from Theorem 5.1.   □

5.4. Corollary. *If* **A** *has a weak difference term and, for some* n, $\gamma^{(n)} \leq \alpha \leq \gamma$, *then the interval lattice* $I(\alpha, \gamma)$ *is modular.*

Proof. A lattice is modular if and only if it does not contain any pentagon as a sublattice. If $\beta \in I(\alpha, \gamma)$, then $\beta^{(n)} \leq \gamma^{(n)} \leq \alpha$, and the conclusion is immediate from Theorem 5.3.   □

There are two interesting alternative proofs of Corollary 5.4. The first: by Theorem 3.3(iv), $I(\alpha, \gamma)$ is a lattice of permuting equivalence relations and hence is modular (indeed, Arguesian: see [Jo, Theorem 1.9]).

As for the second proof, each block of γ/α, under restriction [HMK, Definition 2.2], is an algebra in a permutable variety, by Lemma 3.1 and the classical Mal'cev classification of permutable varieties (if $[\gamma, \gamma] \leq \alpha \leq \gamma$ then, by Theorem 4.3(iii) and Herrmann's Theorem [He], every one of such blocks is polynomially equivalent to a module), hence has a modular congruence lattice. It is not difficult to show that the lattice $I(\alpha, \gamma)$ is a subdirect product of the congruence lattices of those blocks, hence, modular.

Indeed, the latter proof gives more:

5.5. Corollary. *If* **A** *has a weak difference term and* $[\gamma, \gamma] \leq \alpha \leq \gamma$, *then the interval lattice* $I(\alpha, \gamma)$ *satisfies all the quasi identities* (*in the language of lattices*) *holding in the congruence lattices of abelian groups.*

*Proof.* By the above remark and [Jo, Theorem 2.16(i)].   □

5.6. Corollary. *If* **A** *has a weak difference term and, for every* $\alpha, \beta, \gamma \in$ Con **A**, $[\alpha + \beta, \gamma] = [\alpha, \gamma] + [\beta, \gamma]$, *then, for every* $\alpha, \beta, \gamma \in$ Con **A**, $I(\gamma\alpha + \gamma\beta, \gamma(\alpha + \beta))$ *is a modular lattice.*

Proof. $[\gamma(\alpha + \beta), \gamma(\alpha + \beta)] \leq [\alpha + \beta, \gamma] = [\alpha, \gamma] + [\beta, \gamma] \leq \gamma\alpha + \gamma\beta$. The conclusion follows from Corollary 5.4.   □

5.7. Theorem. *If* **A** *has a weak difference term and one of the lattices pictured below is a sublattice of* Con **A**, *then the thick lines are abelian intervals, and the double lines are nonabelian* (*even, nonsolvable*) *intervals.*

If **A** *has a difference term, then* (1) *and* (2) *cannot be sublattices of* Con **A**.

(1)   (2)

(3)   (4)   (5)
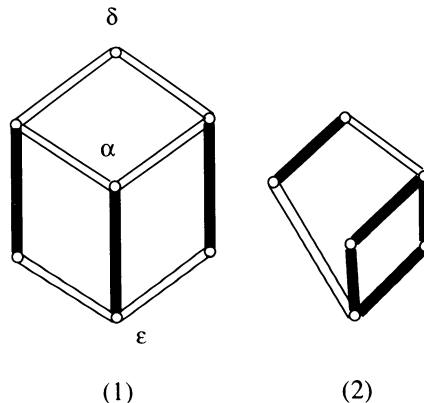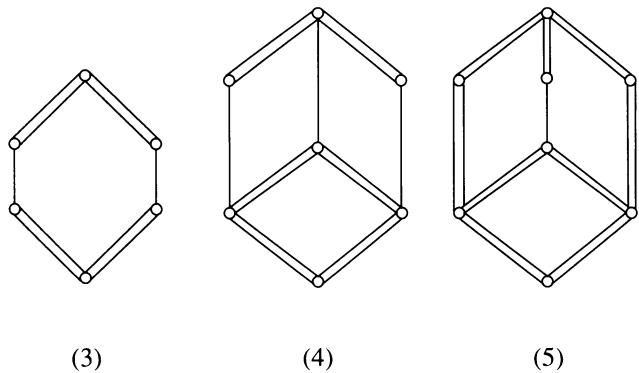
Proof. Consider the lattice pictured in (1). By Proposition 1.2(6), $C(\delta, \alpha; \varepsilon)$; in particular, $[\alpha, \alpha] \leq \varepsilon$. Everything now follows applying Theorems 5.1 and 5.3 many times.

The other lattices are treated in a similar way. □

Problems. Is Theorem 5.7 the best possible?

In particular, can the lattice pictured in (1) be a sublattice of Con A, for some A with a weak difference term?

Can some of the intervals pictured in (4) be abelian?

Both problems have negative answer in the particular case of finite algebras in locally finite varieties omitting type 1, by [HMK, Theorem 7.9 and Lemma 6.3].

5.8. Corollary. *None of the following lattices can be a sublattice of* Con A, *if* A *has a weak difference term*:

(1)   (2)   (3)   (4)

(5)   (6)   (7)
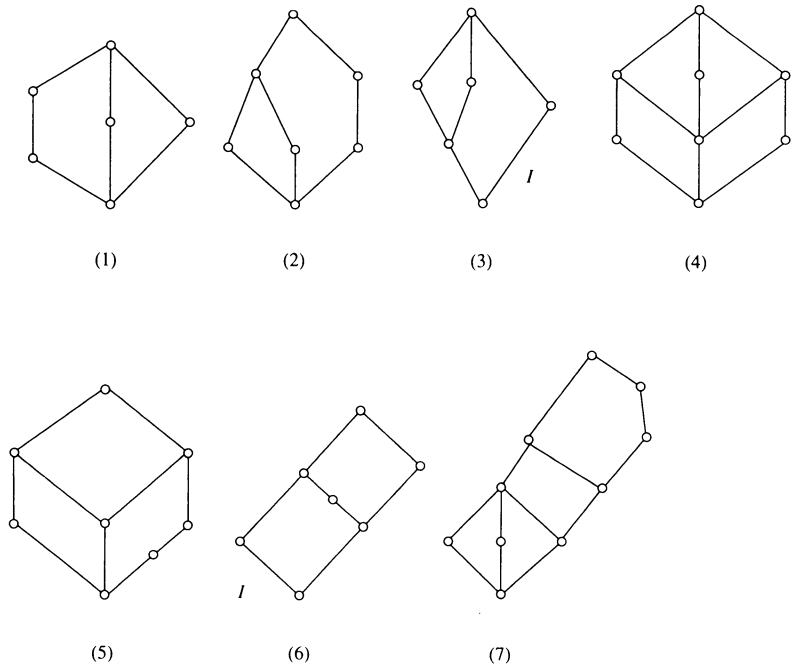
Proof. Everything follows from Corollary 5.7 and Theorems 5.1 and 5.3. The less trivial cases are (3) and (6); use Proposition 1.2(6) to show that I is abelian, thus contradicting Theorem 5.3. □

Theorem 5.2 can be used to show that many definitions of "abelian" coincide, for varieties having a weak difference term.

An algebra is said to be *affine* iff it has the same polynomial operations as a module over some ring. A sublattice L' of some lattice L is a 0, 1-*sublattice* iff L and L' have the same largest element, and the same smallest element.

5.9. Corollary. *If V has a weak difference term, then, for every $\mathbf{A} \in V$, the following are equivalent*:

(i) $\mathbf{A}$ *is abelian.*

(ii) $\mathbf{A}$ *is affine.*

(iii) $0_\mathbf{A}$ *is a block of some congruence of $\mathbf{A} \times \mathbf{A}$.*

(iv) *In* $\mathrm{Con}(\mathbf{A} \times \mathbf{A})$ *the kernels of the two canonical projections have a common complement.*

(v) M_3 *is a* 0, 1-*sublattice of* $\mathrm{Con}(\mathbf{A} \times \mathbf{A})$.

(vi) $\mathbf{A} \times \mathbf{A}$ *is abelian.*

Proof. (i) $\Rightarrow$ (ii) Since $\mathbf{A}$ is abelian, the weak difference term d satisfies $d(a, a, b) = b = d(b, a, a)$, for every $a, b \in A$; and hence $\mathbf{A}$ generates a permutable variety, by Mal'cev's Theorem. The result is now immediate from Herrmann's Theorem (indeed, just from the particular case for permutable varieties).

(i) $\Leftrightarrow$ (iii), (ii) $\Rightarrow$ (iv) $\Rightarrow$ (v) and (vi) $\Rightarrow$ (i) are trivial.

(v) $\Rightarrow$ (vi) follows from Theorem 5.2. □

Some of the results of the present paper can be generalized to a broader class of algebras.

If F, G: $\mathrm{Con}\,\mathbf{A} \to \mathrm{Con}\,\mathbf{A}$, and d is a ternary term, let us say that d is an *F-G-difference term* of $\mathbf{A}$ if and only if:

$$aF(\alpha)\,d(a, b, b) \quad \text{and} \quad d(a, a, b)G(\alpha)b$$

hold, for every $\alpha \in \mathrm{Con}\,\mathbf{A}$ and $a\alpha b \in A$.

An *F-difference term* is an F-F-difference term.

A variety $\underline{V}$ has an F-G-difference term if and only if every algebra in $\underline{V}$ does.

Thus, a weak difference term is the same as a $[-, -]$-difference term; and a difference term is the same as a 0-$[-, -]$-difference term.

Since in §3 we have not used the actual definition of the commutator (cf. Lemma 3.1), Theorem 3.3 generalizes to algebras with a $[1, -]$-difference term, provided we replace $\alpha^{(n)}$ and $\beta^{(n)}$ with $F^n(\alpha)$ and $F^n(\beta)$, where $F(\alpha) = [1, \alpha]$.

Moreover, the proofs of Proposition 4.2, Theorems 4.3, 5.1, 5.2 and 5.3 give, without any essential change (just replacing $[\alpha, \alpha]$ by $[1, \alpha]$):

5.10. Theorem. *Suppose that $\mathbf{A}$ has a $[1, -]$-difference term. Then, for every $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$:*

(1) $\gamma \geq [1, \alpha]$ *implies* $C(\alpha, \alpha; \gamma)$.

(2) $[\gamma + \alpha, \gamma + \alpha] \leq \gamma + [1, \alpha]$.

(3) *If* $\alpha + \beta = 1$ *then* $[1, 1] \le \alpha$ *if and only if* $[1, \beta] \le \alpha\beta$.

(4) *If* $\alpha_i\alpha_j = \delta$ *and* $\alpha_i + \alpha_j = 1$, *for* $1 \le i \ne j \le 3$, *then* $[1, 1] \le \delta$.

(5) *If the lattice pictured in Theorem 5.3 is a sublattice of* Con A *then not* $[1, \alpha] \le \delta$.

Suppose that, in addition, $\varepsilon = 1$. *Then not* $[1, 1] \le \gamma$. *Moreover,* $[1, 1] \le \alpha$ *iff* $[1, \beta] \le \delta$ *iff* $[1, \gamma] \le \delta$.

(6) *None of the lattices in 5.8(1)–(4) can be a sublattice of* A, *provided the top element is* 1.

(7) *The conclusion of Corollary 5.9 still holds.* □

(b) *Suppose that* A *has a* 0-$[1, -]$-*difference term. Then, for every* $\alpha, \beta, \gamma \in$ Con A:

(1) $\gamma \ge [1, \alpha]$ *if and only if* $C(1, \alpha; \gamma)$.

(2) $[1, \gamma + \alpha] \le \gamma + [1, \alpha]$.

(3) $[1, \alpha + \beta] \le \alpha$ *if and only if* $[1, \beta] \le \alpha\beta$.

(4) *If the lattice pictured in Theorem 5.3 is a sublattice of* Con A *then* $\gamma = \beta + [1, \gamma]$, *and neither* $[1, \alpha] \le \delta$, *nor* $[1, \varepsilon] \le \gamma$, *nor* $[1, \varepsilon] \le \alpha$, *nor* $[1, \beta] \le \delta$, *nor* $[1, \gamma] \le \beta$.

(5) *None of the lattices in 5.8(1)–(6) can be a sublattice of* A, *provided the top element is* 1. □

Notice that the proof of 5.10 does not seem to generalize for algebras with a $[-, 1]$-difference term!

Notice also that the results in [Gu, Chapter 11] show that Corollary 5.8 does not generalize to varieties with a 0-$[1, 1]$-difference term. Indeed, [Gu, Proposition 11.4 and Theorem 11.8] imply that the *F P-varieties* defined there have a 0-$[1, 1]$-difference term, but the example on p. 66 there shows that every *finite* lattice is a sublattice of Con A, for some A belonging to an *F P*-variety (but this is not the case for the infinite lattice implying the term condition of [Ta]!)

We end with some problems.

5.11. **Conjectures.** (a) If A has a weak difference term and Con A is modular, then Con A is Arguesian (it is true that if $\underline{V}$ is modular then $\underline{V}$ is Arguesian [Jo]).

(b) If $\underline{V}$ satisfies some nontrivial lattice identity, then $\underline{V}$ has a weak difference term.

The latter conjecture is true for locally finite varieties [HMK, Theorem 9.18]. The main result of [Lp] shows that the conclusion cannot be strengthened to the existence of a difference term, since there are 4-permutable varieties without a difference term (Example 4.6). By a classical result of R. Freese and J. B. Nation [FN], the converse of this conjecture is false. The variety of semilattices has a difference term but satisfies no nontrivial lattice identities.

5.12. **Problem.** Define

$$[\alpha, \beta]^* = [\alpha, \beta] + Cg\left\{(c, d)\middle| \begin{vmatrix} a & b \\ c & d \end{vmatrix} \in M(\alpha, \beta)\quad \text{and}\right.$$

$$\left.(c, d) \notin [\alpha, \beta] + Cg(a, b)\right\}.$$

By [FMK, Proposition 4.2], $[\alpha, \beta] = [\alpha, \beta]^*$, within modular varieties.

In general, $[\alpha, \beta]^*$ is such that $C(\alpha, \beta; \gamma)$ holds, whenever $[\alpha, \beta]^* \leq \gamma$.
Of course, $[\alpha, \beta]^* \leq \beta$; but $[\alpha, \beta]^* \leq \alpha$ does not necessarily hold.

The problem is to study $[\alpha, \beta]^*$ in general, and to evaluate it in known varieties (e.g. n-permutable ones).

5.13. Problem. Commutator theory shows that seemingly different concepts used in group and ring theory have a common generalization.

Do other methods admit a similar unification, in a nontrivial way?

In particular, is there a common generalization of the Frattini subgroup of a group and of the Jacobson radical of ring?

BIBLIOGRAPHY

[BS]   S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Math., 78, Springer, New York, 1981.

[DF]   A. Day and R. Freese, *A characterization of identities implying congruence modularity. I*, Canad. J. Math. **32** (1980), 1149–1167.

[DG]   A. Day and H. P. Gumm, *Some characterizations of the commutator*, Algebra Universalis **29** (1992), 61–78.

[FLT]   R. Freese, W. A. Lampe, and W. Taylor, *Congruence lattices of algebras of fixed similarity type. I*, Pacific J. Math. **82** (1979), 59–68.

[FMK]   R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*, London Math. Soc. Lecture Notes No. 125, London Math. Soc., 1987.

[FN]   R. Freese and J. B. Nation, *Congruence lattices of semilattices*, Pacific J. Math. **49** (1973), 51–58.

[Gu]   H. P. Gumm, *Geometrical methods in congruence modular algebras*, Mem. Amer. Math. Soc. No. 286 (1983).

[He]   C. Herrmann, *Affine algebras in congruence modular varieties*, Acta Sci. Math. (Szeged) **41** (1979), 119–125.

[HH]   J. Hagemann and C. Herrmann, *A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity*, Arch. Math. (Basel) **32** (1979), 234–245.

[HMK]   D. Hobby and R. McKenzie, *The structure of finite algebras*, Contemp. Math., vol. 76, Amer. Math. Soc., Providence, R.I., 1988.

[Jo]   B. Jonsson, *Congruence varieties*, Algebra Universalis **10** (1980), 355–394.

[Ke]   K. A. Kearnes, *An order-theoretic property of the commutator*, preprint.

[KMK]   K. A. Kearnes and R. McKenzie, *Commutator theory for relatively modular quasivarieties*, Trans. Amer. Math. Soc. **331** (1992), 465–502.

[Ki]   E. W. Kiss, *Three remarks on the modular commutator*, Algebra Universalis **29** (1992), 455–476.

[KP]   E. W. Kiss and P. Pröhle, *Problems and results in tame congruence theory. A survey of the '88 Budapest Workshop*, Algebra Universalis **29** (1992), 151–171.

[Lp]   P. Lipparini, *n-permutable varieties satisfy nontrivial congruence identities*, Algebra Universalis (to appear).

[Lp1]   ——, *Varieties satisfying some form of the Herrmann Theorem* (in preparation).

[MK]   R. McKenzie, *Some interactions between group theory and the general theory of algebras*, Groups, Canberra 1989 (L. G. Kovacs, ed.), Lecture Notes in Math., vol. 1456, Springer, New York, 1990.

[MKNT] R. McKenzie, G. McNulty, and W. Taylor, *Algebras, lattices, varieties*, vol. I, Wadsworth & Brooks/Cole, Monterey, Calif., 1987.

[Pe]   M. Petrich, *Inverse semigroups*, Wiley, 1984.

[Qu]   R. Quackenbush, *Quasi-affine algebras*, Algebra Universalis **20** (1985), 318–327.

[Sm]   J. D. H. Smith, *Mal'cev varieties*, Lecture Notes in Math., vol. 554, Springer, 1976.

[Ta]   W. Taylor, *Some applications of the term condition*, Algebra Universalis **14** (1982), 11–24.

[Ta1] W. Taylor, *Characterizing Mal'cev conditions*, Algebra Universalis **3** (1973), 351–397.

[Wi]   R. Willard, M_n *as* 0, 1-*sublattice of* Con(**A**) *does not force the term condition*, Proc. Amer. Math. Soc. **104** (1988), 349–356.

VIA ZUCCHINI 8, I-40126 BOLOGNA, ITALY