Can. J. Math., Vol. XLII, No. 2, 1990, pp. 365–382

ATOMICITY AND NILPOTENCE

KEITH A. KEARNES

1. Introduction. There is a body of results for lattices known as "Decomposition Theory" which is aimed at proving certain existence and uniqueness theorems concerning irredundant representations of elements of a compactly generated lattice. The motivation for these results is certainly the quest for sufficient conditions on congruence lattices to insure irredundant subdirect representations of algebras. These theorems usually include some kind of modularity or distributivity hypothesis (for uniqueness) and some atomicity hypothesis (for existence); the precise details can be found in [**3**]. The atomicity condition is usually the hypothesis that the lattice in question is strongly atomic or at least atomic. Now, it is well-known that every algebra has a *weakly atomic* congruence lattice. That is, if $\alpha, \beta \in \text{Con } \mathbf{A}$ and $\alpha < \beta$, then we can always find $\alpha', \beta' \in \text{Con } \mathbf{A}$ such that $\alpha \leqq \alpha' \prec \beta' \leqq \beta$. But, in general, congruence lattices of algebras need not be atomic. We will show that the assumption that the congruence lattices of all algebras in a variety are atomic is a very strong one. The additional assumption that all congruence lattices are modular seems natural, considering our motivation, and with it we can completely characterize which varieties consist of algebras with atomic congruence lattices.

Our notation and language for algebras and varieties follows [**1**] and for commutator theory follows [**4**].

2. Atomicity.

Definition 2.1. A lattice $\mathbf{L}$ is *atomic* if whenever $\beta \in L$ and $0 < \beta$ there exists $\beta' \in L$ such that $0 \prec \beta' \leqq \beta$. $\mathbf{L}$ is *strongly atomic* if whenever $\alpha, \beta \in L$ and $\alpha < \beta$ there exists $\beta' \in L$ such that $\alpha \prec \beta' \leqq \beta$.

LEMMA 2.2. *Let $\mathcal{V}$ be a variety. The following are equivalent:*

(a) Con $\mathbf{A}$ *is strongly atomic for all* $\mathbf{A} \in \mathcal{V}$.

(b) Con $\mathbf{A}$ *is atomic for all* $\mathbf{A} \in \mathcal{V}$.

If $\mathcal{V}$ is congruence modular, then (*a*) *and* (*b*) *are also equivalent to:*

(c) *For all* $\mathbf{A} \in \mathcal{V}$, *each* $\alpha \in \text{Con } \mathbf{A}$ *has a cover.*

(d) *For all* $\mathbf{A} \in \mathcal{V}$, Con $\mathbf{A}$ *has an atom.*

Proof. The equivalence of (a) and (b) and of (c) and (d) follows from the fact that $\mathcal{V}$ is closed under homomorphisms. Certainly (b) is stronger than (d), so we will be done if we show that (c) implies (b) when $\mathcal{V}$ is congruence modular. Given $\mathbf{A} \in \mathcal{V}$ and $\beta \in \text{Con } \mathbf{A}$ choose an atom $\alpha \in \text{Con } \mathbf{A}$. If $\alpha < \beta$ we are done, so assume that $\alpha \nless \beta$. Then $\alpha \cdot \beta = 0$, and we may extend α to a

Received April 31, 1989.

congruence γ maximal with respect to $\gamma \cdot \beta = 0$. γ has a cover γ' and we have $0 \prec \beta \cdot \gamma' \leqq \beta$. Since $\mathbf{A}$ and β were arbitrary, (b) holds.

We will say that a variety is *congruence atomic* if all algebras in the variety have atomic congruence lattices. Theorem 6.4 of [**3**] implies that every algebra in a congruence atomic variety has an irredundant representation as a subdirect product of subdirectly irreducible algebras. Theorems 6.3 and 7.6 of [**3**] imply that a congruence modular variety is congruence atomic if and only if every algebra has *replaceable* irredundant subdirect representations.

THEOREM 2.3. *Assume that* $\mathcal{V}$ *is congruence atomic and that* $\mathbf{A}$ *is in* $\mathcal{V}$. *If* $\alpha \in \operatorname{Con} \mathbf{A}$ *is an atom, then* α *is a central congruence.*

Proof. Let T be a boolean space with no isolated points. (A *boolean space* is a compact, Hausdorff, totally disconnected topological space.) Giving $\mathbf{A}$ the discrete topology, let $\mathbf{B} = \mathbf{A}^*[T]$ be the algebra of continuous functions from T to $\mathbf{A}$ with operations defined pointwise. Let $\hat{\alpha} \in \operatorname{Con} \mathbf{B}$ be the congruence defined by the rule $(f,g) \in \hat{\alpha} \Leftrightarrow (f(i), g(i)) \in \alpha$ for all $i \in T$. Assume that $(a,b) \in \hat{\alpha} \setminus 0$ and that $\theta = \mathrm{Cg}_{\mathbf{B}}(a,b)$ is a minimal congruence. Since a continuous function from a compact, Hausdorff space to a discrete space assumes only finitely many distinct values, we can partition T into finitely many disjoint clopen sets $X_0, \ldots, X_n$ such that a and b are constant on each X_i and $a(i) \neq b(i)$ when $i \in X_0$. Let $c = a(i) \neq b(i) = d$ for $i \in X_0$. X_0 is infinite since T contains no isolated points. Therefore, we may partition X_0 into two nonempty disjoint clopen sets Y and Z.

Suppose that $\mathrm{C}(\alpha, 1; 0)$ fails. This means that there is an $(n+1)$-ary term p and n-tuples $\bar{u}$, $\bar{v} \in A^n$ such that

$$p^{\mathbf{A}}(c, \bar{u}) = p^{\mathbf{A}}(c, \bar{v}) \quad \text{but} \quad p^{\mathbf{A}}(d, \bar{u}) \neq p^{\mathbf{A}}(d, \bar{v})$$

or else that the same condition holds with c and d interchanged. Here we are using the fact that $\alpha = \mathrm{Cg}_{\mathbf{A}}(c,d)$, which is true since α is a minimal congruence and c and d are distinct α-related elements of A. Now, let $\bar{y}$, $\bar{z} \in \mathbf{B}$ be the (continuous) functions

$$\bar{y}(i) = \bar{u} \quad \text{and} \quad \bar{z}(i) = \begin{cases} \bar{u} & \text{if } i \notin Y \\ \bar{v} & \text{if } i \in Y. \end{cases}$$

Evaluating functions at each $i \in T$, we find that

$$e = p^{\mathbf{B}}(b, \bar{y}) \theta p^{\mathbf{B}}(a, \bar{y}) = p^{\mathbf{B}}(a, \bar{z}) \theta p^{\mathbf{B}}(b, \bar{z}) = f,$$

so $(e,f) \in \theta$. Now, $e(i) = f(i)$ if and only if $i \notin Y$. One consequence of this is that $\mathrm{Cg}_{\mathbf{B}}(e,f) > 0$. Further, every pair $(r,s) \in \mathrm{Cg}_{\mathbf{B}}(e,f)$ satisfies $r(i) = s(i)$ for $i \in Z$, so $(a,b) \notin \mathrm{Cg}_{\mathbf{B}}(e,f)$. This contradicts our assumption that θ is a minimal congruence on $\mathbf{B}$. We conclude that $\mathrm{C}(\alpha, 1; 0)$ holds.

We will call a variety $\mathcal{V}$ *centerfull* if every nontrivial member of $\mathcal{V}$ has a nonzero center. For an algebra $\mathbf{A}$ we will use the notation $\zeta^{\mathbf{A}}$ to denote the center of $\mathbf{A}$. We prove two lemmas to show that the center is a well-behaved congruence. We will follow [**4**] in our notation for congruences on (sub)direct products. In particular, if π_i is a coordinate projection and θ is a congruence on the i^{th} factor algebra, $\mathbf{A}_i$, then we will write θ_i for the congruence $\pi_i^{-1}(\theta)$. The only exception to this is when $\theta = 0$; we will write η_i for $\pi_i^{-1}(0)$.

LEMMA 2.4. *Given a set of algebras $\mathbf{A}_i \in \mathcal{V}$, $i \in I$, we have:*

$$\zeta^{\Pi \mathbf{A}_i} = \Pi \zeta_i^{\mathbf{A}_i}.$$

That is, the center of the product is a product congruence equal to the product of the centers.

Proof. Assume that $(a, b) \in \Pi\zeta_i^{\mathbf{A}_i}$, i.e., $(a_i, b_i) \in \zeta^{\mathbf{A}_i}$ for all $i \in I$. Now, for any $(n+1)$-ary term p and any n-tuples $\bar{u}$, $\bar{v} \in (\prod_{i \in I} A_i)^n$ such that

$$p^{\Pi \mathbf{A}_i}(a, \bar{u}) = p^{\Pi \mathbf{A}_i}(a, \bar{v})$$

we must show that

$$p^{\Pi \mathbf{A}_i}(b, \bar{u}) = p^{\Pi \mathbf{A}_i}(b, \bar{v}).$$

However, $p^{\Pi \mathbf{A}_i}(a, \bar{u}) = p^{\Pi \mathbf{A}_i}(a, \bar{v})$ means that in each coordinate $p^{\mathbf{A}_i}(a_i, \bar{u}_i) = p^{\mathbf{A}_i}(a_i, \bar{v}_i)$, so $p^{\mathbf{A}_i}(b_i, \bar{u}_i) = p^{\mathbf{A}_i}(b_i, \bar{v}_i)$ in each coordinate. Thus, $p^{\Pi \mathbf{A}_i}(b, \bar{u}) = p^{\Pi \mathbf{A}_i}(b, \bar{v})$ as desired.

Now suppose that $(a, b) \notin \Pi\zeta_i^{\mathbf{A}_i}$. Then in some coordinate $j \in I$ we must have $(a_j, b_j) \notin \zeta^{\mathbf{A}_j}$. We can find an $(m+1)$-ary term q and m-tuples $\bar{r}_j$, $\bar{s}_j \in (A_j)^m$ such that

$$q^{\mathbf{A}_j}(a_j, \bar{r}_j) = q^{\mathbf{A}_j}(a_j, \bar{s}_j)$$

but

$$q^{\mathbf{A}_j}(b_j, \bar{r}_j) \neq q^{\mathbf{A}_j}(b_j, \bar{s}_j).$$

Let $\bar{x}$, $\bar{y} \in (\prod_{i \in I} A_i)^m$ be any pair of m-tuples such that $\bar{x}_j = \bar{r}_j$, $\bar{y}_j = \bar{s}_j$ and $\bar{x}_i = \bar{y}_i$ whenever $i \neq j$. Now,

$$q^{\Pi \mathbf{A}_i}(a, \bar{x}) = q^{\Pi \mathbf{A}_i}(a, \bar{y})$$

but

$$q^{\Pi \mathbf{A}_i}(b, \bar{x}) \neq q^{\Pi \mathbf{A}_i}(b, \bar{y})$$

so $(a, b) \notin \zeta^{\Pi \mathbf{A}_i}$.

LEMMA 2.5. *If* $\mathbf{A}$ *is a subalgebra of* $\mathbf{B} \in \mathcal{V}$, *then*

$$\zeta^{\mathbf{B}}|_{\mathbf{A}} \leqq \zeta^{\mathbf{A}}.$$

Proof. Saying that $(a, b) \in \zeta^{\mathbf{B}}|_{\mathbf{A}}$ is equivalent to saying that for every choice of n, an $(n+1)$-ary term p, and n-tuples $\bar{u}$, $\bar{v} \in B^n$ we have

$$p^{\mathbf{B}}(a, \bar{u}) = p^{\mathbf{B}}(a, \bar{v}) \Leftrightarrow p^{\mathbf{B}}(b, \bar{u}) = p^{\mathbf{B}}(b, \bar{v}).$$

If this is so, then the same implication holds when $\bar{u}$ and $\bar{v}$ are restricted to lie in A^n. This is precisely what it means for (a, b) to be a member of $\zeta^{\mathbf{A}}$.

The next result generalizes the well-known exercise in group theory which asks the student to prove that every nontrivial normal subgroup of a (finite) nilpotent group has a nontrivial intersection with the center.

THEOREM 2.6. *A variety* $\mathcal{V}$ *is centerfull if and only if whenever* $\mathbf{A} \in \mathcal{V}$ *and* α *is a nonzero congruence on* $\mathbf{A}$ *we have* $\alpha \cdot \zeta^{\mathbf{A}} > 0$.

Proof. If whenever α is a nonzero congruence on $\mathbf{A} \in \mathcal{V}$ we always have $\alpha \cdot \zeta^{\mathbf{A}} > 0$, then certainly we have $\zeta^{\mathbf{A}} > 0$. Therefore this condition is sufficient to imply that $\mathcal{V}$ is centerfull. To show that this condition is also necessary, suppose that α is a nonzero congruence on $\mathbf{A} \in \mathcal{V}$ and that $\alpha \cdot \zeta^{\mathbf{A}} = 0$. We will show that this assumption leads to the conclusion that $\mathcal{V}$ is not centerfull. Let ζ' be an extension of $\zeta^{\mathbf{A}}$ that is maximal with respect to the condition that $\alpha \cdot \zeta' = 0$. We claim that $\mathbf{A}/\zeta'$ has zero center. To show this, it will be useful to introduce the notation for residuation. If δ and θ are congruences on the algebra $\mathbf{X}$, then $(\delta : \theta)$ denotes the largest congruence γ on $\mathbf{X}$ such that $\mathrm{C}(\gamma, \theta; \delta)$ holds. Notice that in a centerfull variety, if $\delta \neq 1$ then $\delta < (\delta : 1)$ since $(\delta : 1)/\delta$ is the center of $\mathbf{X}/\delta$.

Since $\alpha \cdot \zeta' = 0$, the natural map from $\mathbf{A}$ to $\mathbf{B} = \mathbf{A}/\alpha \times \mathbf{A}/\zeta'$ is an embedding. By Lemma 2.4, $\zeta^{\mathbf{B}}$ is a product congruence equal to $((\alpha : 1)/\alpha)_0 \cdot ((\zeta' : 1)/\zeta')_1$. Using this and Lemma 2.5 we obtain

$$(\alpha : 1) \cdot (\zeta' : 1) = \zeta^{\mathbf{B}}|_{\mathbf{A}} \leqq \zeta^{\mathbf{A}} \leqq \zeta'.$$

Now $\alpha \leqq (\alpha : 1)$, so with $\alpha \cdot (\zeta^{\mathbf{B}}|_{\mathbf{A}}) \leqq \alpha \cdot \zeta' = 0$ we get $0 = \alpha \cdot (\zeta' : 1)$. By the maximality of ζ' we have $(\zeta' : 1) = \zeta'$. In other words, $\mathbf{A}/\zeta'$ has zero center.

COROLLARY 2.7. *A variety* $\mathcal{V}$ *is congruence atomic if and only if for all nontrivial* $\mathbf{A} \in \mathcal{V}$ *the interval* $I[0, \zeta^{\mathbf{A}}]$ *is nontrivial and atomic.*

Proof. One direction is clear. We have seen that any congruence atomic variety is centerfull and, since $I[0, \zeta]$ is an interval in an atomic lattice, $I[0, \zeta]$ is atomic. Our goal is to prove the other direction: if $I[0, \zeta^{\mathbf{A}}]$ is nontrivial and atomic for any $\mathbf{A} \in \mathcal{V}$, then the variety is congruence atomic.

Suppose that $\mathcal{V}$ is a variety with this property. The nontriviality of $I[0, \zeta^{\mathbf{A}}]$ for any $\mathbf{A} \in \mathcal{V}$ proves that $\mathcal{V}$ is centerfull. Now suppose that $\mathbf{A}$ is in $\mathcal{V}$ and that $\beta \in \operatorname{Con} \mathbf{A}$. By Theorem 2.6, $\beta \cdot \zeta^{\mathbf{A}} > 0$. But we can find an atom below $\beta \cdot \zeta^{\mathbf{A}}$ since $I[0, \zeta^{\mathbf{A}}]$ is atomic. Hence, we can produce an atomic congruence below β. Since β and $\mathbf{A}$ were arbitrary we are done.

The last corollary reduces the problem of determining which varieties are congruence atomic to a study of the center. Unfortunately, we do not understand the center very well in arbitrary varieties. However, one of the successes of modular commutator theory is an essentially complete understanding of the center in congruence modular varieties. Therefore, let us impose the hypothesis of congruence modularity and give a more explicit characterization of congruence atomicity.

3. Congruence modular varieties. In this section we will make use of commutator theory to characterize the congruence modular varieties that are congruence atomic. We adopt the custom that the ring of an abelian variety acts on the left.

THEOREM 3.1. *Let $\mathcal{V}$ be a congruence modular variety. $\mathcal{V}$ is congruence atomic if and only if:*
(a) *$\mathcal{V}$ is centerfull and*
(b) *The abelian subvariety $\mathcal{A} \subseteq \mathcal{V}$ is congruence atomic.*

Proof. The forward direction follows from Theorem 2.3. Now suppose that (a) and (b) hold and that $\mathbf{A} \in \mathcal{V}$. Since (a) holds, the interval $I[0, \zeta^{\mathbf{A}}]$ is nontrivial. We now proceed to argue that this interval is atomic.

Let $\mathbf{A}(\zeta^{\mathbf{A}})$ denote the subalgebra of $\mathbf{A}^2$ consisting of $\{(a,b) \in A^2 \mid a \zeta^{\mathbf{A}} b\}$. Let $\Delta = \Delta_{\zeta,1}$ be the congruence on $\mathbf{A}(\zeta^{\mathbf{A}})$ that is generated by the set of pairs $\{\langle (x,x),(y,y)\rangle \mid x,y \in A\}$.

The fact that $[1, \zeta^{\mathbf{A}}] = 0$ implies that $\eta_0 \cdot \Delta = 0$. Hence,

$$1/\Delta \searrow \eta_0/0 \nearrow (\eta_0 + \eta_1)/\eta_1.$$

But $\eta_0 + \eta_1 = \zeta_1$. Hence the interval $I[\Delta, 1]$ is isomorphic to the interval $I[\eta_1, \zeta_1]$. Of course, the latter interval is isomorphic to $I[0, \zeta^{\mathbf{A}}]$ in $\operatorname{Con} \mathbf{A}$. The former interval is just $\operatorname{Con} \mathbf{A}(\zeta^{\mathbf{A}})/\Delta$. Condition (b) guarantees that $\operatorname{Con} \mathbf{A}(\zeta^{\mathbf{A}})/\Delta$ is atomic. By Corollary 2.7, $\mathcal{V}$ is congruence atomic.

Definition 3.2. An associative, unital ring $\mathbf{R}$ is a *left Loewy ring* if and only if every left $\mathbf{R}$-module has a minimal submodule.

LEMMA 3.2. *The following conditions are equivalent:*
(a) *$\mathbf{R}$ is a left Loewy ring.*
(b) *The variety of left $\mathbf{R}$-modules is congruence atomic.*
(c) *The lattice of left ideals of $\mathbf{R}$ is strongly atomic.*

Proof. The equivalence of (a) and (b) follows from the definitions and the fact that the congruence lattice of a module is isomorphic to its lattice of submodules. Now, assuming (b), it follows from Lemma 2.2 that any left **R**-module has a strongly atomic lattice of submodules. Hence, ${}_{\mathbf{R}}\mathbf{R}$ has a strongly atomic lattice of submodules. But this lattice is just the left ideal lattice of **R**. Thus, (c) holds. We will be done if we show that (c) implies (a). Notice that to prove (a) it suffices to show that every nonzero cyclic module in the variety ${}_{\mathbf{R}}\mathbf{M}$ of left **R**-modules has a minimal nonzero submodule. This is because if $\mathbf{M} \in {}_{\mathbf{R}}\mathbf{M}$ is nontrivial, then **M** contains a nontrivial cyclic submodule **N**. If we can show that **N** has a minimal nonzero submodule, this submodule will be minimal in **M**, too. Since **N** is cyclic there is a left ideal **I** in **R** such that **N** is isomorphic to **R/I**. By (*c*), there is an ideal **J** covering **I** in the lattice of left ideals of **R**. Clearly, **JN** is a minimal nonzero submodule of **N**.

Any left Artinian ring is left Loewy, but there are left Loewy rings which are not left Artinian. The term "left semi-Artinian" has been used synonymously with the term "left Loewy". Although not all left Loewy rings are left Artinian it is known that left Loewy rings satisfy DCC on primitive ideals (see [**2**] for a proof of this).

Because of the relationship between abelian varieties and varieties of modules spelled out by Theorem 9.16 of [**4**], we can rewrite Theorem 3.1 as:

THEOREM 3.4. *Let $\mathcal{V}$ be a congruence modular variety and let $\mathcal{A} \subseteq \mathcal{V}$ be the abelian subvariety. $\mathcal{V}$ is congruence atomic if and only if:*
(*a*) *$\mathcal{V}$ is centerfull and*
(*b*) $\mathbf{R}(\mathcal{A})$ *is left Loewy.*

COROLLARY 3.5. *If* **A** *is a finite algebra which generates a modular variety, then $\mathcal{V} = \mathcal{V}(\mathbf{A})$ is congruence atomic if and only if* **A** *is nilpotent.*

Proof. Any finite algebra in centerfull variety is nilpotent so the forward direction is easy. Since $\mathcal{V}$ is congruence modular, if **A** is k-step nilpotent then it satisfies equations defining k-step nilpotency. Hence $\mathcal{V}$ consists of k-step nilpotent algebras. This shows that $\mathcal{V}$ is centerfull. $\mathcal{V}$, and therefore $\mathcal{A}$, is locally finite so the ring $\mathbf{R}(\mathcal{A})$ is finite. Any finite ring is left Loewy so we are done.

THEOREM 3.6. *If $\mathcal{V}$ is a centerfull, congruence modular variety, then $\mathcal{V}$ is congruence permutable, congruence uniform and congruence regular.*

Proof. First we prove that $\mathcal{V}$ is congruence permutable. Suppose that $\mathbf{A} \in \mathcal{V}$ and $\alpha \in \operatorname{Con} \mathbf{A}$. Let $\{\beta_i \in \operatorname{Con}\mathbf{A} \mid i \in I\}$ be any collection of congruences that form a chain in Con **A**. Assume that α permutes with any congruence in the set $\{\psi \in \operatorname{Con}\mathbf{A} \mid \psi \leqq \beta_i \text{ for some } i\}$. Now, $\bigcup_{i\in I}\beta_i$ is a congruence; assume that $\theta \leqq \bigcup_{i\in I}\beta_i$. We claim that α permutes with θ. Since

$$\theta = \theta \cap \left(\bigcup_{i\in I}\beta_i\right) = \bigcup_{i\in I}(\theta \cap \beta_i),$$

we may replace β_i by $\theta \cap \beta_i$ without violating any of our hypotheses. In this way we may assume that $\theta = \bigcup_{i\in I} \beta_i$. Now,

$$\alpha \circ \theta = \alpha \circ \left(\bigcup_{i\in I} \beta_i \right) = \bigcup_{i\in I} (\alpha \circ \beta_i) = \bigcup_{i\in I} (\beta_i \circ \alpha)$$
$$= \left(\bigcup_{i\in I} \beta_i \right) \circ \alpha = \theta \circ \alpha,$$

so α permutes with θ.

Suppose that $\beta \in \operatorname{Con} \mathbf{A}$ is an arbitrary congruence. By the result of the previous paragraph, we may apply Zorn's Lemma to find a congruence γ which is maximal among congruences in the following set:

$$S = \{\theta \in \operatorname{Con} \mathbf{A} \mid \theta \leqq \beta \text{ and every congruence } \leqq \theta \text{ permutes with } \alpha\ \}.$$

(S is non-empty since the zero congruence belongs to S.) Our goal is to prove that $\gamma = \beta$.

Assume that $\beta > \gamma$. Applying Theorem 2.6 in $\mathbf{A}/\gamma$, we obtain that $\delta = \beta \cdot (\gamma : 1) > \gamma$ in $\operatorname{Con} \mathbf{A}$. Now $[\theta, \theta] \leqq [1, \delta] \leqq \gamma$ for any $\theta \leqq \delta$, so $[\theta, \theta]$ permutes with α for all $\theta \leqq \delta$. By Theorem 6.3 of [**4**], α permutes with any such θ. But this means that $\delta \in S$ which contradicts the maximality of γ. We conclude that $\gamma = \beta$. Since β was arbitrary, α permutes with any congruence of $\mathbf{A}$. Both $\mathbf{A}$ and α were chosen arbitrarily as well, so $\mathcal{V}$ is congruence permutable. For the rest of the proof we will let $p(x, y, z)$ be a Mal'cev term for $\mathcal{V}$.

Now let $\{\beta_i \in \operatorname{Con}\mathbf{A} \mid i \in I\}$ be any collection of uniform congruences that form a chain in $\operatorname{Con} \mathbf{A}$. Let $\beta = \bigcup_{i\in I} \beta_i$. If $a, b \in A$, then $|a/\beta| = \sup_{i\in I} |a/\beta_i|$ $= \sup_{i\in I} |b/\beta_i| = |b/\beta|$, so β is uniform. This shows that if α is an arbitrary congruence on $\mathbf{A}$ then we may apply Zorn's Lemma to find a congruence γ which is maximal among the uniform congruences $\leqq \alpha$. If α is not uniform, then $\gamma < \alpha$; in fact, $\gamma < (\gamma : 1) \cdot \alpha = \delta$. By the maximality condition on γ, δ is not uniform on $\mathbf{A}$; further, the central congruence $\psi = \delta/\gamma$ is not uniform on $\mathbf{B} = \mathbf{A}/\gamma$. Hence there are elements $u, v \in B$ such that $|u/\psi| > |v/\psi|$. The unary polynomial $p^{\mathbf{B}}(x, u, v)$ maps u/ψ to v/ψ; suppose that $a, b \in u/\psi$ and that $p^{\mathbf{B}}(a, u, v) = p^{\mathbf{B}}(b, u, v)$. Since $(a, b) \in \psi$ and the $1,\psi$-term condition holds,

$$a = p^{\mathbf{B}}(a, u, u) = p^{\mathbf{B}}(b, u, u) = b.$$

Thus, $p(x, u, v)$ is one to one. This contradicts the possibility that $|u/\psi| > |v/\psi|$, or equivalently, the possibility that δ is not uniform. The assumption that led to this contradiction was that α was not uniform. Since α and $\mathbf{A} \in \mathcal{V}$ were arbitrary, $\mathcal{V}$ is congruence uniform.

To finish, we observe that every congruence uniform variety is congruence regular. For if $\mathcal{V}$ fails to be congruence regular, then we can find distinct congruences α and β on an algebra $\mathbf{A}$ that agree on at least one congruence class. By replacing one of them by their meet and relabeling if necessary we may assume that $\alpha < \beta$. In $\mathbf{A}/\alpha$ the congruence β/α is not uniform, since it has some nontrivial congruence classes and at least one trivial congruence class; thus $\mathcal{V}$ is not congruence uniform.

Definition 3.7. We say that a variety $\mathcal{V}$ has *(first-order) definable centers* if there is a first-order formula $Z(x, y)$ in the language of $\mathcal{V}$ such that, for all $\mathbf{A} \in \mathcal{V}$ and all $a, b \in A$,

$$(a, b) \in \zeta^{\mathbf{A}} \text{ if and only if } \mathbf{A} \models Z(a, b).$$

In [**6**], R. McKenzie studies the first-order definability of a certain 4-ary "centralizer" relation $\mathrm{C}(x, y, z, u)$ for modular varieties. This relation is defined so that $\mathbf{A} \models \mathrm{C}(a, b, c, d)$ if and only if $[\mathrm{Cg}_{\mathbf{A}}(a, b), \mathrm{Cg}_{\mathbf{A}}(c, d)] = 0$. Certainly if the centralizer relation is definable for a variety then the variety must have definable centers. We simply choose $Z(x, y)$ to be the formula $\forall z, u\ \mathrm{C}(x, y, z, u)$.

THEOREM 3.8. *If $\mathcal{V}$ is congruence modular and has definable centers then there is an m, an n and n pairs of $m+2$-ary terms $(p_i(x, y, \bar{z}), q_i(x, y, \bar{z}))$ such that:*

$$Z(x, y) = \forall z_1, \ldots, z_m \left(\bigwedge_{i<n} p_i(x, y, z_1, \ldots, z_m) \approx q_i(x, y, z_1, \ldots, z_m) \right)$$

defines the center.

Proof. Assume that $Z'(x, y)$ is any first-order sentence that defines the center for $\mathcal{V}$ and that Σ is a set of equations that define $\mathcal{V}$. Expand the language of $\mathcal{V}$ to include two new constant symbols a and b and let $\mathcal{V}^*$ be the variety of this expanded type that is axiomatized by Σ. Let $\mathcal{W}$ be the subclass of $\mathcal{V}^*$ that is axiomatized by $\Sigma \cup \{Z'(a, b)\}$. The algebras in $\mathcal{W}$ are precisely the algebras of $\mathcal{V}$ with a and b interpreted as centrally related elements. Lemmas 2.4 and 2.5 imply that $\mathcal{W}$ is closed under the formation of direct products and subalgebras. The homomorphism property of the commutator implies that $\mathcal{W}$ is even a subvariety of $\mathcal{V}^*$. $\mathcal{W}$ is defined by the equations of $\mathcal{V}^*$ and a single first-order formula, so there exist finitely many equations in the language of $\mathcal{V}^*$ that define $\mathcal{W}$ as a subvariety of $\mathcal{V}^*$. But an equation of $\mathcal{V}^*$ is of the form

$$p(a, b, \bar{z}) \approx q(a, b, \bar{z})$$

where p and q are terms of $\mathcal{V}$. Hence, Σ and a sentence of the form

$$\forall \bar{z} \left(\bigwedge_{i<n} p_i(a, b, \bar{z}) \approx q_i(a, b, \bar{z}) \right)$$

defines $\mathcal{W}$. Therefore, if $\mathbf{A} \models \Sigma$, i.e., $\mathbf{A} \in \mathcal{V}$, then $c, d \in A$ are centrally related if and only if $\mathbf{A} \models \forall \bar{z}(\bigwedge_{i<n} p_i(c, d, \bar{z}) \approx q_i(c, d, \bar{z}))$. Thus,

$$Z(x, y) = \forall \bar{z}\left(\bigwedge_{i<n} p_i(x, y, \bar{z}) \approx q_i(x, y, \bar{z})\right)$$

defines the center for algebras in $\mathcal{V}$.

Theorem 3.8 gives a sufficiently nice form for $Z(x, y)$ for our needs. However, more can be said about sentences that define the center for a modular variety. The next results show explicitly how to construct a sentence that defines the center for any 2-finite, modular variety of finite type.

THEOREM 3.9. ([**4**], Theorem 14.1) *If $\mathcal{V}$ is congruence modular and $\mathbf{A} \in \mathcal{V}$, then $(a, b) \in \zeta^{\mathbf{A}}$ if and only if for all basic operations f, all $\bar{c} = (c_1, \ldots, c_n) \in A^n$, and all binary terms r and r_i we have*

(1) $$f(d(r_1(a, b), r_1(b, b), c_1), \ldots, d(r_n(a, b), r_n(b, b), c_n)) \\ = d(f(r_1(a, b), \ldots, r_n(a, b)), f(r_1(b, b), \ldots, r_n(b, b)), f(\bar{c}))$$

and

(2) $$d(r(a, b), r(b, b), r(b, b)) = r(a, b).$$

where d is a modular difference term for $\mathcal{V}$.

COROLLARY 3.10. *Suppose that $\mathcal{V}$ is a congruence modular variety of finite type and that $\mathbf{F}_{\mathcal{V}}(2)$ is finite. Then $\mathcal{V}$ has definable centers.*

Proof. We will call two binary terms $r(x, y)$ and $s(x, y)$ *$\mathcal{V}$-equivalent* if $\mathcal{V}$ satisfies the equation $r(x, y) \approx s(x, y)$. Since $\mathbf{F}_{\mathcal{V}}(2)$ is finite, we can find a finite set B of binary terms which represent all the $\mathcal{V}$-equivalence classes of binary terms. For each choice of a single n-ary basic operation f and n binary terms chosen from B, $r_1, \ldots, r_n$, we define a pair of terms (p_i, q_i) by

$$p_i(x, y, \bar{z}) = f(d(r_1(x, y), r_1(y, y), z_1), \ldots, d(r_n(x, y), r_n(y, y), z_n))$$
$$q_i(x, y, \bar{z}) = d(f(r_1(x, y), \ldots, r_n(x, y)), f(r_1(y, y), \ldots, r_n(y, y)), f(\bar{z})).$$

From our hypotheses there are only finitely many such pairs. Assume that they are indexed by the members of the finite set I. Now, for each binary term $r \in B$ define

$$p_j(x, y, \bar{z}) = d(r(x, y), r(y, y), r(y, y))$$
$$q_j(x, y, \bar{z}) = r(x, y).$$

These pairs may be indexed by the finite set B and we may assume that B is disjoint from I. It is clear from Theorem 3.9 that the formula

$$Z(x, y) = \forall \bar{z}\left(\bigwedge_{i \in I \cup B} p_i(x, y, \bar{z}) \approx q_i(x, y, \bar{z})\right)$$

defines the center in $\mathcal{V}$.

We remark that in a permutable variety one may choose a Mal'cev term for d and then 3.9 (2) holds trivially.

THEOREM 3.11. *If $\mathcal{V}$ is a centerfull, congruence modular variety with definable centers, then $\mathcal{V}$ is nilpotent.*

Proof. In this proof we will use the notation

$$\zeta_\lambda = \begin{cases} 0 & \text{if } \lambda = 0 \\ (\zeta_{\lambda-1} : 1) & \text{if } \lambda \text{ is a successor ordinal} \\ \bigvee_{\delta<\lambda} \zeta_\delta & \text{otherwise.} \end{cases}$$

Note that ζ_1 is just the center. For an algebra $\mathbf{C}$ the sequence $\zeta_0^{\mathbf{C}} \leqq \zeta_1^{\mathbf{C}} \leqq \cdots$ is the *ascending central series* of $\mathbf{C}$.

To prove this theorem we will argue by contradiction. Assume that $\mathcal{V}$ satisfies the hypotheses of the theorem but is not nilpotent. The assumption that $\mathcal{V}$ is not nilpotent means precisely that $\mathcal{V}$ satisfies no congruence equation of the form $\zeta_n \approx 1, n < \omega$. That is, there is no finite bound on the lengths of the ascending central series of algebras in $\mathcal{V}$. If $\mathbf{A}$ is a generic algebra, then $\mathbf{A} \not\models_{con} \zeta_n \approx 1$ for any finite n. Let $\mathbf{B} = \prod_{i<\omega} \mathbf{A}$. It is an immediate consequence of Lemma 2.4 and induction that $\zeta_n^{\mathbf{B}} = \Pi_{i<\omega}\zeta_n^{\mathbf{A}}$ for finite values of n. However, $\theta = \zeta_\omega^{\mathbf{B}} < \Pi_{i<\omega}\zeta_\omega^{\mathbf{A}} = \psi$. For example, any element $(a, b) \in B^2$ for which $(a_i, b_i) \in \zeta_{i+1}^{\mathbf{A}} \setminus \zeta_i^{\mathbf{A}}$ is a member of $\psi \setminus \theta$.

By applying Theorem 2.6 in $\mathbf{B}/\theta$ we find that $\psi \cdot (\theta : 1) > \theta$. Choose $(c, d) \in \psi \cdot (\theta : 1) \setminus \theta$. There is a function $f : \omega \longrightarrow \omega$ such that $f(i)$ equals the positive natural number r if $(c_i, d_i) \in \zeta_r \setminus \zeta_{r-1}$ and equals 0 if $c_i = d_i$. f is defined for each i since $(c, d) \in \psi$. That $(c, d) \notin \theta$ is equivalent to the fact f is not a bounded function.

Assume that the formula

$$Z(x, y) = \forall \bar{z} \left(\bigwedge_{j<n} p_j(x, y, \bar{z}) \approx q_j(x, y, \bar{z}) \right)$$

defines the center for algebras in $\mathcal{V}$. For any i for which $f(i) = r > 1$ we have

$$\mathbf{A} \models \forall \bar{e} \left(\bigwedge_{j<n} p_j^{\mathbf{A}}(c_i, d_i, \bar{e}) \zeta_{r-1}^{\mathbf{A}} q_j^{\mathbf{A}}(c_i, d_i, \bar{e}) \right)$$

but

$$\mathbf{A} \not\models \forall \bar{e} \left(\bigwedge_{j<n} p_j^{\mathbf{A}}(c_i, d_i, \bar{e}) \zeta_{r-2}^{\mathbf{A}} q_j^{\mathbf{A}}(c_i, d_i, \bar{e}) \right).$$

Thus, for each i for which $f(i) > 1$ there is a $j = j(i)$ and a tuple $\bar{e} = (\bar{e})_i \in A^m$ such that

$$(p_j^{\mathbf{A}}(c_i, d_i, (\bar{e})_i), q_j^{\mathbf{A}}(c_i, d_i, (\bar{e})_i)) \in \zeta_{r-1}^{\mathbf{A}} \setminus \zeta_{r-2}^{\mathbf{A}}.$$

Note that $(\bar{e})_i$ has been defined for those values of i for which $f(i) > 1$. Let $\bar{g} \in B^m$ be an m-tuple whose tuple of i^{th} components equals $(\bar{e})_i$ when $f(i) > 1$ and is an arbitrary element of A^m when $f(i) \leqq 1$. Since $(c, d) \in (\theta : 1)$ and $Z(x, y)$ defines the center in $\mathbf{B}/\theta$, we must have

$$\mathbf{B} \models \forall \bar{z}\left(\bigwedge_{j<n} p_j^{\mathbf{B}}(c, d, \bar{z})\theta q_j^{\mathbf{B}}(c, d, \bar{z})\right).$$

This means that for all $j < n$,

$$(p_j^{\mathbf{B}}(c, d, \bar{g}), q_j^{\mathbf{B}}(c, d, \bar{g})) \in \theta = \bigvee_{i<\omega} \zeta_i^{\mathbf{B}}.$$

This is a statement about only finitely many pairs in θ, so there is a $k < \omega$ such that for all $j < n$ we have

$$(p_j^{\mathbf{B}}(c, d, \bar{g}), q_j^{\mathbf{B}}(c, d, \bar{g})) \in \zeta_k^{\mathbf{B}} = \Pi \zeta_k^{\mathbf{A}}.$$

But f is an unbounded function. There is some value of i for which $f(i) \geqq k+2$. For this i and for $j = j(i)$ we have

$$(p_j^{\mathbf{A}}(c_i, d_i, (\bar{g})_i), q_j^{\mathbf{A}}(c_i, d_i, (\bar{g})_i)) \notin \zeta_k^{\mathbf{A}}$$

which contradicts the previous displayed equation.

COROLLARY 3.12. *Assume that $\mathcal{V}$ is congruence modular and has definable centers. $\mathcal{V}$ is congruence atomic if and only if $\mathcal{V}$ is nilpotent and the ring of the abelian subvariety is left Loewy. In particular, if $\mathcal{V}$ is congruence modular of finite type and $\mathbf{F}_{\mathcal{V}}(2)$ is finite, then $\mathcal{V}$ is congruence atomic if and only if $\mathcal{V}$ is nilpotent.*

Proof. The first statement follows from Theorem 3.4 and Theorem 3.11. For the second statement, notice that when $\mathbf{F}_{\mathcal{V}}(2)$ is finite, then so is the ring of the abelian subvariety. The second statement follows from this fact, the first statement and Corollary 3.10.

In a variety which has an equationally definable constant we can say a bit more than is proven by the combination of 3.10 and 3.11. If we take 0 for the constant symbol, then one can prove an analogue of Corollary 3.10 giving a formula which defines the congruence class $0/\zeta$ using only the hypothesis that $\mathcal{V}$ is of finite type and that $\mathbf{F}_{\mathcal{V}}(1)$ is finite. This result and the congruence uniformity of $\mathcal{V}$ can be used in place of 3.10 to prove an analogue of Theorem 3.11. Hence, if $\mathcal{V}$ is a 1-finite modular variety of finite type and $\mathcal{V}$ has an equationally definable constant, then $\mathcal{V}$ is congruence atomic if and only if $\mathcal{V}$ is nilpotent.

It turns out that the congruence atomic varieties of groups (or rings) can be neatly characterized as precisely those varieties generated by a finite nilpotent group (or ring). To prove this, we require Lemmas 3.13 and 3.16 which are of interest themselves. In our arguments for groups we will require the notion of a *simple commutator* which is a group element of the form $[x_0, \ldots, x_{n-1}, x_n] = [[x_0, \ldots, x_{n-1}], x_n]$ where $[x, y] = x^{-1}y^{-1}xy$ is the usual commutator operation of group theory. Also, for a group $\mathbf{G}$ we will write

$\Gamma_1(\mathbf{G}) = \mathbf{G}$ and $\Gamma_{k+1}(\mathbf{G}) = [\Gamma_k(\mathbf{G}), \mathbf{G}]$ to denote the members of the lower central series for $\mathbf{G}$. $\mathbf{G}$ is k-step nilpotent if and only if $\Gamma_{k+1}(\mathbf{G}) = \{1\}$.

LEMMA 3.13. *If $\mathcal{G}$ is a variety of k-step nilpotent groups, then* $\mathcal{G} = \mathbf{HSP}\,(\mathbf{F}_{\mathcal{G}}(k))$.

Proof. The varieties of abelian groups are determined by their exponent, hence this lemma is true when k equals 1. Assume that the lemma is false and that k is the least positive integer (greater than 1) for which it fails. We will argue to a contradiction.

The claim that $\mathcal{G} = \mathbf{HSP}(\mathbf{F}_{\mathcal{G}}(k))$ is equivalent to the assertion that, for all positive integers m, the elements of $\mathbf{F}_{\mathcal{G}}(m)$ can be separated by homomorphisms into k-generated members of $\mathcal{G}$. As we are assuming the negation of this assertion, there is an m and a $p \in \mathbf{F} = \mathbf{F}_{\mathcal{G}}(x_0, \ldots, x_{m-1})$ such that $p \neq 1_{\mathbf{F}}$ but whenever $h : \mathbf{F} \longrightarrow \mathbf{L}$ is a homomorphism into a k-generated group $\mathbf{L} \in \mathcal{G}$, we have $h(p) = 1_{\mathbf{L}}$. (Necessarily, m is greater than k.) We will focus on contradicting the existence of such an m and such a p.

Let $\mathcal{H}$ be the subvariety of $\mathcal{G}$ consisting of $(k-1)$-step nilpotent groups. Our minimality hypothesis on k guarantees that, for all n, the elements of $\mathbf{F}_{\mathcal{H}}(n)$ can be separated by homomorphisms into $(k-1)$-generated groups in $\mathcal{H}$. But $\mathbf{F}_{\mathcal{H}}(m) \cong \mathbf{F}/\Gamma_k(\mathbf{F})$. Since the elements of $\mathbf{F}/\Gamma_k(\mathbf{F})$ can be separated by homomorphisms into $(k-1)$-generated groups in $\mathcal{H} \subseteq \mathcal{G}$, and p cannot be separated from $1_{\mathbf{F}}$ by homomorphisms into k-generated groups in $\mathcal{G}$, it follows that $p \in \Gamma_k(\mathbf{F})$.

Now we apply Theorem 10.2.3 of [**5**]:

THEOREM 3.14. *If a group* $\mathbf{F}$ *is generated by elements* $x_0, \ldots, x_{m-1}$, *then the group* $\Gamma_k(\mathbf{F})/\Gamma_{k+1}(\mathbf{F})$ *is generated by the simple commutators* $[y_0, \ldots, y_{k-1}]$ mod Γ_{k+1}, *where the y's are chosen from* $x_0, \ldots, x_m$ *and are not necessarily distinct.*

In our case, $\Gamma_{k+1} = \{1\}$. This theorem tells us that p may be expressed as a product of integer powers of simple commutators that each depend on k variables. We fix an expression $p = c_0c_1 \cdots c_n$ where each c_i is a simple commutator of length k or the inverse of a simple commutator of length k. We may assume that we have chosen the c_i's such that this expression has the smallest number of factors. Now, for $i = 0, \ldots, n$, let S_i denote the subset of $\{x_0, \ldots, x_{m-1}\}$ of those x_j's that occur in our fixed expression for c_i. Since Γ_k is central, these simple commutators commute with each other, therefore we may arrange them in any convenient order. We choose an order which groups together the simple commutators that depend on the same set of variables. That is, we assume that the simple commutators are ordered so that if $i \leqq j \leqq l$ and

https://doi.org/10.4153/CJM-1990-020-1 Published online by Cambridge University Press

$S_i = S_l$, then $S_j = S_l$. Further, we assume that S_0 is minimal under inclusion among the S_i's.

For some $u \leqq n$ we have that $S_0 = S_1 = \cdots = S_u$, but $S_i \nsubseteq S_0$ for any $i > u$. Let $e : \mathbf{F} \longrightarrow \mathbf{F}$ be the endomorphism of $\mathbf{F}$ determined by:

$$e(x_i) = \begin{cases} x_i & \text{if } i \in S_0 \\ 1_{\mathbf{F}} & \text{if } i \notin S_0. \end{cases}$$

Of course, S_0 contains no more than k elements. Thus, the image of e is contained in the k-generated subgroup of $\mathbf{F}$ that is generated by S_0. Hence, $1 = e(p) = c_0c_1 \cdots c_u$ by our assumption on p. If $u = n$, then $1 = e(p) = p$, a contradiction. Otherwise, $p = c_{u+1} \cdots c_n$ which contradicts the fact that we chose the c_i's so that their product was the shortest way to represent p as a product of simple commutators. Either way, we have contradicted the existence of p for any value of m and this finishes the proof.

Proposition 3.15. *The congruence atomic varieties of groups are precisely the varieties of groups generated by a finite nilpotent group.*

Proof. Certainly a finite nilpotent group generates a congruence atomic variety as Corollary 3.5 shows. We need to prove the other direction.

Any variety of groups has definable centers; a suitable formula is:

$$Z(x, y) = \forall z(z(xy^{-1}) \approx (xy^{-1})z).$$

If $\mathcal{G}$ is congruence atomic, then $\mathcal{G}$ is k-step nilpotent for some finite k. Lemma 3.13 shows that $\mathcal{G} = \mathbf{HSP}(\mathbf{F}_{\mathcal{G}}(k))$. We can finish this argument by showing that $\mathbf{F} = \mathbf{F}_{\mathcal{G}}(k)$ is finite.

The group $\mathbf{F}_{\mathcal{G}}(1)$ is a cyclic group with an atomic congruence lattice. The congruence lattice of the group of integers has no atoms, so $\mathbf{F}_{\mathcal{G}}(1)$ is not isomorphic to this group. Hence $\mathbf{F}_{\mathcal{G}}(1)$, and therefore $\mathcal{G}$, satisfies an equation of the form $x^n \approx 1$. This means that $\mathbf{F}$ is of exponent n, of nilpotency degree k and generated by k elements. This is enough to imply that $\mathbf{F}$ is finite. For $\Gamma_i(\mathbf{F})/\Gamma_{i+1}(\mathbf{F})$ is an abelian group of exponent n generated by the simple commutators of length i and there are only finitely many simple commutators of length i. (This is by Theorem 3.14: $\mathbf{F}$ is generated by k elements so there are no more than k^i distinct simple commutators of length i.) Hence, the cardinality of $\Gamma_i(\mathbf{F})/\Gamma_{i+1}(\mathbf{F})$ is no more than n^{k^i}. This yields:

$$|F| = \prod_{i=1}^{k} |\Gamma_i(\mathbf{F})/\Gamma_{i+1}(\mathbf{F})| \leqq \prod_{i=1}^{k} n^{k^i},$$

so $\mathbf{F}$ is finite. This proves the proposition.

In contrast to this result, Ralph Freese has pointed out to me that Example 1 of [**7**] contains a locally finite, congruence atomic variety of loops which is not generated by a finite loop. In this example, M. R. Vaughan-Lee constructs a variety of 3-step nilpotent loops in which every finitely generated member has order 2^k for some finite k. This variety is locally finite, so the ring of the abelian subvariety is finite and therefore left Loewy. Theorem 3.4 shows that this variety is congruence atomic. Next, Vaughan-Lee shows that this variety has no finite basis for its equations. However, Theorem 7.5 of the same paper shows that if a congruence modular variety $\mathcal{V}$ has an equationally-definable constant and is generated by a finite nilpotent algebra of prime-power cardinality, then the variety *must* have a finite basis for its equations. It follows that Vaughan-Lee's variety of loops is not finitely generated. This means that Lemma 3.13 and Proposition 3.15 do not have analogues for varieties of loops.

Our next two results concern varieties of rings. For these results **rings** will mean associative but not necessarily unital rings. No variety of unital rings is congruence atomic or even centerfull since simple unital rings have a trivial center.

We mention that a ring is k-step nilpotent in the sense of modular commutator theory if and only if it is k-step nilpotent in the usual sense: all $k+1$-fold products are equal to zero. In analogy with Lemma 3.13 we will use the notation $\Gamma_1(\mathbf{R}) = \mathbf{R}$ and $\Gamma_{k+1}(\mathbf{R}) = [\Gamma_k(\mathbf{R}), \mathbf{R}] = \Gamma_k(\mathbf{R}) \cdot \mathbf{R} + \mathbf{R} \cdot \Gamma_k(\mathbf{R})$. Clearly, $\Gamma_k(\mathbf{R})$ is the ideal of $\mathbf{R}$ generated by all of the k-fold products. $\mathbf{R}$ is k-step nilpotent if and only if $\Gamma_{k+1}(\mathbf{R}) = \{0\}$.

LEMMA 3.16. *If $\mathcal{R}$ is a variety of k-step nilpotent rings, then* $\mathcal{R} = \mathbf{HSP}(\mathbf{F}_{\mathcal{R}}(k))$.

Proof. This lemma will proceed along the same lines as Lemma 3.13. First, if $k = 1$ then $\mathcal{R}$ is a variety of zero-rings. This means that $\mathcal{R}$ is term-equivalent to a variety of abelian groups. (By ignoring the multiplication of a zero-ring we obtain an abelian group. The ring can be recovered from this group by defining the multiplication by $x \cdot y = 0$.) We have observed that varieties of abelian groups are generated by their 1-generated free member, so the same is true for varieties of zero-rings.

Now assume that this lemma is false and that k is the least positive integer greater than 1 for which it fails. Since the lemma fails, there is an $m > k$ and a $p \in \mathbf{F} = \mathbf{F}_{\mathcal{R}}(x_0, \ldots, x_{m-1})$ such that whenever $h : \mathbf{F} \longrightarrow \mathbf{L}$ is a homomorphism into a k-generated ring $\mathbf{L} \in \mathcal{R}$ we have $h(p) = 0_{\mathbf{L}}$.

Arguing as we did in Lemma 3.13 we see that the minimality assumption on k guarantees that $p \in \Gamma_k(\mathbf{F})$. That is, p is in the ideal generated by the k-fold products of the generators of $\mathbf{F}$. Since all $(k+1)$-fold products are zero in $\mathbf{F}$, we may find (and fix) an expression:

$$p = \sum_{i=0}^{n} m_i$$

where each m_i is a k-fold product of generators of $\mathbf{F}$. We may assume that n is the least positive integer for which such an expression exists. As before, we define S_i to be the subset of $\{x_0, \ldots, x_{m-1}\}$ of those x_j's that occur in our fixed expression for m_i, $i = 0, \ldots, n$. We may group together the m_i that depend on the same set of variables. and assume that S_0 is minimal under inclusion among the S_i's. Since m_0 is a k-fold product of not necessarily distinct generators, the set S_0 has no more than k elements.

For some $u \leqq n$ we have that $S_0 = S_1 = \cdots = S_u$, but $S_i \nsubseteq S_0$ for any $i > u$. Let $e : \mathbf{F} \longrightarrow \mathbf{F}$ be the endomorphism of $\mathbf{F}$ determined by:

$$e(x_i) = \begin{cases} x_i & \text{if } i \in S_0 \\ 0_{\mathbf{F}} & \text{if } i \notin S_0. \end{cases}$$

The image of e is contained in the k-generated subring of $\mathbf{F}$ that is generated by S_0. Hence, $0 = e(p) = \sum_{i=0}^{u} m_i$. If $u = n$, then $0 = e(p) = p$, a contradiction. Otherwise, $p = \sum_{i=u+1}^{n} m_i$ which contradicts the fact that we chose n so that it was minimal. This contradiction finishes the proof.

PROPOSITION 3.17. *The congruence atomic varieties of rings are precisely the varieties of rings generated by a finite nilpotent ring.*

Proof. Corollary 3.5 shows that every finite nilpotent ring generates a congruence atomic variety. We must show that if $\mathcal{R}$ is a congruence atomic variety of rings then $\mathcal{R}$ is generated by a finite nilpotent member.

Any variety of rings has definable centers; a formula is:

$$Z(x, y) = \forall z((z(x - y) \approx 0) \wedge ((x - y)z \approx 0)).$$

If $\mathcal{R}$ is congruence atomic, then by Theorem 3.11 $\mathcal{R}$ is k-step nilpotent for some finite k. Lemma 3.16 shows that $\mathcal{R} = \mathbf{HSP}(\mathbf{F}_{\mathcal{R}}(k))$. We will prove that $\mathbf{F} = \mathbf{F}_{\mathcal{R}}(k)$ is finite.

Let $\mathcal{A}$ denote the abelian subvariety of $\mathcal{R}$. $\mathcal{A}$ is term equivalent to a congruence atomic variety of abelian groups. This means that $\mathcal{A} \models n \cdot x \approx 0$ for some positive integer n.

Products of finitely generated ideals are again finitely generated, so it is clear that the ideals $\Gamma_i(\mathbf{F})$ are finitely generated for all i. This means that $\mathbf{I}_i = \Gamma_i(\mathbf{F})/\Gamma_{i+1}(\mathbf{F})$ is a finitely generated ideal of the ring $\mathbf{F}_i = \mathbf{F}/\Gamma_{i+1}(\mathbf{F})$. But $\mathbf{I}_i$ annihilates $\mathbf{F}_i$. It follows that $\mathbf{I}_i$ is even finitely generated as an abelian group. The ring $\mathbf{I}_i \in \mathcal{A}$ so, as an abelian group, $\mathbf{I}_i$ is finitely generated and of finite exponent. Hence, $\mathbf{I}_i = \Gamma_i(\mathbf{F})/\Gamma_{i+1}(\mathbf{F})$ is finite. It follows that $|F| = \prod_{i=1}^{k} |\Gamma_i(\mathbf{F})/\Gamma_{i+1}(\mathbf{F})|$ is finite.

The condition that $\mathbf{R}(\mathcal{A})$ is left Loewy in Theorem 3.4 may be considered to be a finiteness condition on $\mathbf{R}(\mathcal{A})$, hence on $\mathbf{F}_{\mathcal{V}}(2)$ from which $\mathbf{R}(\mathcal{A})$ is computed (see Definition 9.3 and Theorem 9.12 of [**4**]). In light of Theorem 3.10 and Corollary 3.12 we are led to pose the following problem:

Problem 1. Is there a congruence modular variety of finite type which is congruence atomic but fails to be nilpotent?

4. Related results. When I first wondered, "Which varieties consist of algebras with atomic congruence lattices?" only two kinds of examples came to mind at first: varieties of vector spaces and of sets. Any congruence majorizes a principal congruence and principal congruences are atomic congruences for vector spaces or sets. Hence, these varieties are congruence atomic. At this point, it was reasonable to ask which other varieties have this property that principal congruences on algebras are atomic congruences. It turns out that a locally finite or congruence modular variety with this property must be polynomially equivalent to a variety of sets or vector spaces, so the property is too restrictive to be very interesting. In this section we investigate weaker forms of this property.

Definition 4.1. If α is an element of a (*lower*) bounded lattice, then we will call α an *Artin element* if the interval $I[0, \alpha]$ satisfies the descending chain condition (DCC). We will call α a *Noether element* if $I[0, \alpha]$ satisfies ACC.

If every element in the lattice **L** is the (possibly infinite) join of Artin elements, then the lattice is atomic.

Definition 4.2. $\mathcal{V}$ is *Artinian (Noetherian)* if, for every $\mathbf{A} \in \mathcal{V}$, the compact elements of Con **A** are Artin (Noether) elements.

Varieties of sets or vector spaces are both Artinian and Noetherian. Any locally finite variety that is essentially unary is both Artinian and Noetherian. The line before Definition 4.2 shows that every Artinian variety is congruence atomic; however, the converse of this is not true as we will soon see. Noetherian varieties need not be congruence atomic, e.g., the variety of all abelian groups is Noetherian but not congruence atomic.

THEOREM 4.3. *An Artinian or Noetherian variety consists of abelian algebras.*

Proof. Assume that the term condition fails in some algebra **A**. That is, suppose that $a, b \in A$ and that there is an $(n+1)$-ary term p and n-tuples $\bar{u}, \bar{v} \in A^n$ such that

$$p^{\mathbf{A}}(a, \bar{u}) = p^{\mathbf{A}}(a, \bar{v}) \quad \text{but} \quad p^{\mathbf{A}}(b, \bar{u}) \neq p^{\mathbf{A}}(b, \bar{v}).$$

We will prove that **A** belongs to no Artinian or Noetherian variety.

Let X be an infinite set and let $c, d \in A^X$ be the constant tuples defined by $c_i = a$ and $d_i = b$. Let $\gamma = \mathrm{Cg}_{\mathbf{B}}(c, d)$ where $\mathbf{B} = \mathbf{A}^X$. For any subset $Y \subseteq X$ we will write η_Y to denote

$$\{\, (x, y) \in B^2 \mid x_i = y_i \text{ for all } i \in Y \,\};$$

η_Y is a congruence on **B**.

CLAIM. *If* $Y \nsubseteq Z$, *then* $\eta_Z \cdot \gamma \nleq \eta_Y \cdot \gamma$.

Poof of Claim. Suppose that $j \in Y \setminus Z$. Define $\bar{e}, \bar{f} \in B^n$ as follows:

$$\bar{e}_i = \bar{u} \quad \text{and} \quad \bar{f}_i = \begin{cases} \bar{u} & \text{if } i \neq j \\ \bar{v} & \text{if } i = j. \end{cases}$$

Now, $g = p^{\mathbf{B}}(d, \bar{e}) \ \gamma \ p^{\mathbf{B}}(c, \bar{e}) = p^{\mathbf{B}}(c, \bar{f}) \ \gamma \ p^{\mathbf{B}}(d, \bar{f}) = h$ and $(g, h) \in \eta_Z$, so $(g, h) \in \eta_Z \cdot \gamma$. However, $(g, h) \notin \eta_Y$ since $g_j \neq h_j$.

Suppose that $X_0 \subset X_1 \subset \cdots$ is any infinite, properly ascending chain of subsets of X. The claim proves that $\eta_{X_0} \cdot \gamma > \eta_{X_1} \cdot \gamma > \cdots$ is an infinite properly descending chain of congruences in $I[0, \gamma]$. Similarly, if $X_0 \supset X_1 \supset \cdots$ is an infinite, properly descending chain of subsets of X, then $\eta_{X_0} \cdot \gamma < \eta_{X_1} \cdot \gamma < \cdots$ is an infinite properly ascending chain of congruences in $I[0, \gamma]$. Hence γ is neither an Artin element nor a Noether element of Con **B**. γ is a compact congruence, so **A** and $\mathbf{B} = \mathbf{A}^X$ belong to no Artinian or Noetherian variety.

THEOREM 4.4. *Assume that $\mathcal{V}$ is congruence modular. $\mathcal{V}$ is Artinian if and only if $\mathcal{V}$ is affine and $\mathbf{R}(\mathcal{V})$ is left Artinian. $\mathcal{V}$ is Noetherian ifand only if $\mathcal{V}$ is affine and $\mathbf{R}(\mathcal{V})$ is left Noetherian.*

Proof. Theorem 4.3 is enough to prove that Artinian or Noetherian modular varieties are affine. We will prove that an affine variety is Artinian if and only if $\mathbf{R}(\mathcal{V})$ is left Artinian. The proof for Noetherian varieties is similar.

Assume that $\mathcal{V}$ is affine and that $\mathbf{R} = \mathbf{R}(\mathcal{V})$. The class of congruence lattices of algebras in $\mathcal{V}$ is the same as class of congruence lattices of left **R**-modules, so $\mathcal{V}$ is Artinian if and only if the variety of left **R**-modules is. We may assume that $\mathcal{V}$ *is* the variety of left **R**-modules.

Suppose that $\mathcal{V}$ is Artinian and let $\mathbf{A} = {}_{\mathbf{R}}\mathbf{R}$. Since **R** is unital, $1_{\mathbf{A}}$ is a compact congruence. This shows that Con **A** has DCC; equivalently, that **R** is left Artinian.

Now suppose that **R** is left Artinian. If $\mathbf{A} \in \mathcal{V}$ and α is a compact congruence on **A** then $B = 0/\alpha$ is the universe of a finitely generated submodule of **A** which has the property that Con $\mathbf{B} \cong I[0, \alpha]$. If we can show that finitely generated (left) modules over a left Artinian ring have DCC on congruences, then we will be done. For this it suffices to consider finitely generated free modules. However, a finitely generated free module is isomorphic to a finite direct power of ${}_{\mathbf{R}}\mathbf{R}$ and this module has DCC. Now, it is very easy to prove that, in a modular variety, a finite direct product of algebras has DCC (or ACC) on congruences if and only if each factor does.

COROLLARY 4.5. *A locally finite, congruence modular variety is affine if and only if it is Artinian if and only if it is Noetherian.*

There are a number of papers investigating properties of locally finite varieties consisting of abelian algebras. The most significant open problem in this area is whether or not these varieties are Hamiltonian. As the Hamiltonian property for affine algebras plays a role in the proofs of Theorem 4.4 and its Corollary, we feel that the following problem ought to be investigated as well:

Problem 2. Is every locally finite abelian variety Artinian and Noetherian?

References

1. S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics *78* (Springer-Verlag, New York, 1981).
2. V. Camillo and K. Fuller, *A note on Loewy rings and chain conditions on primitive ideals*, in *Module theory*, Lecture Notes in Mathematics *700* (Springer-Verlag, New York, 1979), 75–86.
3. P. Crawley and R. P. Dilworth, *Algebraic theory of lattices* (Prentice-Hall, Engelwood Cliffs, N.J., 1973).
4. R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*, LMS Lecture Note Series *125*, Cambridge (1987).
5. M. Hall, Jr., *Theory of groups*, 2nd ed. (Chelsea Publishing Co., New York, 1976).
6. R. McKenzie, *Finite equational bases for congruence modular varieties*, Algebra Universalis *24*, (1987), 224–250.
7. M.R. Vaughan-Lee, *Nilpotence in permutable varieties*, in *Universal algebra and lattice theory*, Lecture Notes in Mathematics, *1004* (Springer-Verlag, New York, 1983), 293–308.

University of Hawaii at Manoa,
Honolulu, Hawaii